

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference document: Secure Controls Framework (SCF) version 2026.1
STRM Guidance: <https://securecontrolsframework.com/vstarr/relationships-mapping-strm/>

Focal Document: Focal Document URL:
Published STRM URL:

Notion Picture Association (MPA) Content Security Best Practices Common Guidelines v5.1.1
Focal Document URL: https://www.tppn.org/wp-content/uploads/2025/08/MPA-Content-Security-Best-Practices-v5.1.1-August-7-2025_English.xlsx
Published STRM URL: <https://content.securecontrolsframework.com/vstarr/scfm-general-mpa-cstp-5-3-1.pdf>

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Relationship	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
OR-1.0	Information Security Management	Establish and regularly review an Information Security Management System (ISMS), Information Security Manual (ISM), or Information Security Policy (ISP), approved by leadership, to include the following: <ul style="list-style-type: none"> Control framework Governance, Risk, and Compliance (GRC) Update upon significant changes 	Functional	Subset Of	Security, Compliance & Resilience Program (SCRFP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	<ul style="list-style-type: none"> Reference established Information and Content Security Frameworks (e.g., ISO 27001, NIST 800-53, SANS, CEBIT, CSA, CIS, etc.) Establish a designated team for Information Security, including a Governance Committee, to develop policies addressing threats, incidents, risks, etc. Prepare organizational charts and job descriptions to facilitate role designation and responsibilities pertaining to security
OR-1.0	Information Security Management	Establish and regularly review an Information Security Management System (ISMS), Information Security Manual (ISM), or Information Security Policy (ISP), approved by leadership, to include the following: <ul style="list-style-type: none"> Control framework Governance, Risk, and Compliance (GRC) Update upon significant changes 	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	<ul style="list-style-type: none"> Reference established Information and Content Security Frameworks (e.g., ISO 27001, NIST 800-53, SANS, CEBIT, CSA, CIS, etc.) Establish a designated team for Information Security, including a Governance Committee, to develop policies addressing threats, incidents, risks, etc. Prepare organizational charts and job descriptions to facilitate role designation and responsibilities pertaining to security
OR-1.0	Information Security Management	Establish and regularly review an Information Security Management System (ISMS), Information Security Manual (ISM), or Information Security Policy (ISP), approved by leadership, to include the following: <ul style="list-style-type: none"> Control framework Governance, Risk, and Compliance (GRC) Update upon significant changes 	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRFP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	<ul style="list-style-type: none"> Reference established Information and Content Security Frameworks (e.g., ISO 27001, NIST 800-53, SANS, CEBIT, CSA, CIS, etc.) Establish a designated team for Information Security, including a Governance Committee, to develop policies addressing threats, incidents, risks, etc. Prepare organizational charts and job descriptions to facilitate role designation and responsibilities pertaining to security
OR-1.0	Information Security Management	Establish and regularly review an Information Security Management System (ISMS), Information Security Manual (ISM), or Information Security Policy (ISP), approved by leadership, to include the following: <ul style="list-style-type: none"> Control framework Governance, Risk, and Compliance (GRC) Update upon significant changes 	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	5	<ul style="list-style-type: none"> Reference established Information and Content Security Frameworks (e.g., ISO 27001, NIST 800-53, SANS, CEBIT, CSA, CIS, etc.) Establish a designated team for Information Security, including a Governance Committee, to develop policies addressing threats, incidents, risks, etc. Prepare organizational charts and job descriptions to facilitate role designation and responsibilities pertaining to security
OR-1.0	Information Security Management	Establish and regularly review an Information Security Management System (ISMS), Information Security Manual (ISM), or Information Security Policy (ISP), approved by leadership, to include the following: <ul style="list-style-type: none"> Control framework Governance, Risk, and Compliance (GRC) Update upon significant changes 	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	5	<ul style="list-style-type: none"> Reference established Information and Content Security Frameworks (e.g., ISO 27001, NIST 800-53, SANS, CEBIT, CSA, CIS, etc.) Establish a designated team for Information Security, including a Governance Committee, to develop policies addressing threats, incidents, risks, etc. Prepare organizational charts and job descriptions to facilitate role designation and responsibilities pertaining to security
OR-1.0	Information Security Management	Establish and regularly review an Information Security Management System (ISMS), Information Security Manual (ISM), or Information Security Policy (ISP), approved by leadership, to include the following: <ul style="list-style-type: none"> Control framework Governance, Risk, and Compliance (GRC) Update upon significant changes 	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5	<ul style="list-style-type: none"> Reference established Information and Content Security Frameworks (e.g., ISO 27001, NIST 800-53, SANS, CEBIT, CSA, CIS, etc.) Establish a designated team for Information Security, including a Governance Committee, to develop policies addressing threats, incidents, risks, etc. Prepare organizational charts and job descriptions to facilitate role designation and responsibilities pertaining to security
OR-1.0	Information Security Management	Establish and regularly review an Information Security Management System (ISMS), Information Security Manual (ISM), or Information Security Policy (ISP), approved by leadership, to include the following: <ul style="list-style-type: none"> Control framework Governance, Risk, and Compliance (GRC) Update upon significant changes 	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP) or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	<ul style="list-style-type: none"> Reference established Information and Content Security Frameworks (e.g., ISO 27001, NIST 800-53, SANS, CEBIT, CSA, CIS, etc.) Establish a designated team for Information Security, including a Governance Committee, to develop policies addressing threats, incidents, risks, etc. Prepare organizational charts and job descriptions to facilitate role designation and responsibilities pertaining to security
OR-1.1	Acceptable Use Policy	Establish and regularly review an Acceptable Use Policy (AUP) governing Internet use (e.g., social media, communication activities, etc.) to include the following: <ul style="list-style-type: none"> Do not share on any social media platform, forum, blog post, or website any information related to pre-release content and related project activities, unless express written consent from the client is obtained 	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	8	<ul style="list-style-type: none"> List of products approved by the organization Define acceptable uses of technologies Use dedicated, company-administered accounts for marketing and communication purposes
OR-1.1	Acceptable Use Policy	Establish and regularly review an Acceptable Use Policy (AUP) governing Internet use (e.g., social media, communication activities, etc.) to include the following: <ul style="list-style-type: none"> Do not share on any social media platform, forum, blog post, or website any information related to pre-release content and related project activities, unless express written consent from the client is obtained 	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	8	<ul style="list-style-type: none"> List of products approved by the organization Define acceptable uses of technologies Use dedicated, company-administered accounts for marketing and communication purposes
OR-1.1	Acceptable Use Policy	Establish and regularly review an Acceptable Use Policy (AUP) governing Internet use (e.g., social media, communication activities, etc.) to include the following: <ul style="list-style-type: none"> Do not share on any social media platform, forum, blog post, or website any information related to pre-release content and related project activities, unless express written consent from the client is obtained 	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential for cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	<ul style="list-style-type: none"> List of products approved by the organization Define acceptable uses of technologies Use dedicated, company-administered accounts for marketing and communication purposes
OR-1.1	Acceptable Use Policy	Establish and regularly review an Acceptable Use Policy (AUP) governing Internet use (e.g., social media, communication activities, etc.) to include the following: <ul style="list-style-type: none"> Do not share on any social media platform, forum, blog post, or website any information related to pre-release content and related project activities, unless express written consent from the client is obtained 	Functional	Intersects With	Use of Critical Technologies	HRS-05.4	Mechanisms exist to govern usage policies for critical technologies.	8	<ul style="list-style-type: none"> List of products approved by the organization Define acceptable uses of technologies Use dedicated, company-administered accounts for marketing and communication purposes
OR-1.1	Acceptable Use Policy	Establish and regularly review an Acceptable Use Policy (AUP) governing Internet use (e.g., social media, communication activities, etc.) to include the following: <ul style="list-style-type: none"> Do not share on any social media platform, forum, blog post, or website any information related to pre-release content and related project activities, unless express written consent from the client is obtained 	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	8	<ul style="list-style-type: none"> List of products approved by the organization Define acceptable uses of technologies Use dedicated, company-administered accounts for marketing and communication purposes
OR-1.2	Business Continuity Plan	Establish and regularly review a formal Business Continuity Plan (BCP) and policy, to include the following: <ul style="list-style-type: none"> Team responsible for developing, maintaining, and communicating the BCP Define threats to critical assets, locations, infrastructure, and business operations (e.g., loss of power or communications, systems failure, natural disasters, pandemics, breaches, etc.) Include Incident Response as part of the BCP For applications, outline Application Security Testing in the BCP 	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BCDR) playbooks).	5	<ul style="list-style-type: none"> Validate BCP via tabletop exercises Incorporate a systematic approach that uses likelihood of risk occurrence, impact to business objectives/content protection, and asset classification for assigning priority (e.g., Business Impact Analysis (BIA)) Define and document Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for critical services and operations as defined in the Business Impact Analysis (BIA) Assign a designated team member to oversee continuity planning efforts Define workarounds, alternate solutions, etc. Protect security systems from disruption in power (e.g., alarms, electronic access, etc.) For template examples, refer to FEMA: https://www.ready.gov/business/emergency-plans/continuity-planning, or TPN Partner Resource Center in TPN+ https://plus.tppn.org/partner-resources
OR-1.2	Business Continuity Plan	Establish and regularly review a formal Business Continuity Plan (BCP) and policy, to include the following: <ul style="list-style-type: none"> Team responsible for developing, maintaining, and communicating the BCP Define threats to critical assets, locations, infrastructure, and business operations (e.g., loss of power or communications, systems failure, natural disasters, pandemics, breaches, etc.) Include Incident Response as part of the BCP For applications, outline Application Security Testing in the BCP 	Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5	<ul style="list-style-type: none"> Validate BCP via tabletop exercises Incorporate a systematic approach that uses likelihood of risk occurrence, impact to business objectives/content protection, and asset classification for assigning priority (e.g., Business Impact Analysis (BIA)) Define and document Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for critical services and operations as defined in the Business Impact Analysis (BIA) Assign a designated team member to oversee continuity planning efforts Define workarounds, alternate solutions, etc. Protect security systems from disruption in power (e.g., alarms, electronic access, etc.) For template examples, refer to FEMA: https://www.ready.gov/business/emergency-plans/continuity-planning, or TPN Partner Resource Center in TPN+ https://plus.tppn.org/partner-resources
OR-1.2	Business Continuity Plan	Establish and regularly review a formal Business Continuity Plan (BCP) and policy, to include the following: <ul style="list-style-type: none"> Team responsible for developing, maintaining, and communicating the BCP Define threats to critical assets, locations, infrastructure, and business operations (e.g., loss of power or communications, systems failure, natural disasters, pandemics, breaches, etc.) Include Incident Response as part of the BCP For applications, outline Application Security Testing in the BCP 	Functional	Intersects With	Resume All Missions & Business Functions	BCD-02.1	Mechanisms exist to resume all missions and business functions within Recovery Time Objectives (RTO) of the contingency plan's activation.	5	<ul style="list-style-type: none"> Validate BCP via tabletop exercises Incorporate a systematic approach that uses likelihood of risk occurrence, impact to business objectives/content protection, and asset classification for assigning priority (e.g., Business Impact Analysis (BIA)) Define and document Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for critical services and operations as defined in the Business Impact Analysis (BIA) Assign a designated team member to oversee continuity planning efforts Define workarounds, alternate solutions, etc. Protect security systems from disruption in power (e.g., alarms, electronic access, etc.) For template examples, refer to FEMA: https://www.ready.gov/business/emergency-plans/continuity-planning, or TPN Partner Resource Center in TPN+ https://plus.tppn.org/partner-resources
OR-1.2	Business Continuity Plan	Establish and regularly review a formal Business Continuity Plan (BCP) and policy, to include the following: <ul style="list-style-type: none"> Team responsible for developing, maintaining, and communicating the BCP Define threats to critical assets, locations, infrastructure, and business operations (e.g., loss of power or communications, systems failure, natural disasters, pandemics, breaches, etc.) Include Incident Response as part of the BCP For applications, outline Application Security Testing in the BCP 	Functional	Intersects With	Continue Essential Missions & Business Functions	BCD-02.2	Mechanisms exist to continue essential missions and business functions with little or no loss of operational continuity and sustain that continuity until full system restoration at primary processing and/or storage sites.	5	<ul style="list-style-type: none"> Validate BCP via tabletop exercises Incorporate a systematic approach that uses likelihood of risk occurrence, impact to business objectives/content protection, and asset classification for assigning priority (e.g., Business Impact Analysis (BIA)) Define and document Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for critical services and operations as defined in the Business Impact Analysis (BIA) Assign a designated team member to oversee continuity planning efforts Define workarounds, alternate solutions, etc. Protect security systems from disruption in power (e.g., alarms, electronic access, etc.) For template examples, refer to FEMA: https://www.ready.gov/business/emergency-plans/continuity-planning, or TPN Partner Resource Center in TPN+ https://plus.tppn.org/partner-resources
OR-1.2	Business Continuity Plan	Establish and regularly review a formal Business Continuity Plan (BCP) and policy, to include the following: <ul style="list-style-type: none"> Team responsible for developing, maintaining, and communicating the BCP Define threats to critical assets, locations, infrastructure, and business operations (e.g., loss of power or communications, systems failure, natural disasters, pandemics, breaches, etc.) Include Incident Response as part of the BCP For applications, outline Application Security Testing in the BCP 	Functional	Intersects With	Resume Essential Missions & Business Functions	BCD-02.3	Mechanisms exist to resume essential missions and business functions within an organization-defined time period of contingency plan activation.	5	<ul style="list-style-type: none"> Validate BCP via tabletop exercises Incorporate a systematic approach that uses likelihood of risk occurrence, impact to business objectives/content protection, and asset classification for assigning priority (e.g., Business Impact Analysis (BIA)) Define and document Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for critical services and operations as defined in the Business Impact Analysis (BIA) Assign a designated team member to oversee continuity planning efforts Define workarounds, alternate solutions, etc. Protect security systems from disruption in power (e.g., alarms, electronic access, etc.) For template examples, refer to FEMA: https://www.ready.gov/business/emergency-plans/continuity-planning, or TPN Partner Resource Center in TPN+ https://plus.tppn.org/partner-resources
OR-1.2	Business Continuity Plan	Establish and regularly review a formal Business Continuity Plan (BCP) and policy, to include the following: <ul style="list-style-type: none"> Team responsible for developing, maintaining, and communicating the BCP Define threats to critical assets, locations, infrastructure, and business operations (e.g., loss of power or communications, systems failure, natural disasters, pandemics, breaches, etc.) Include Incident Response as part of the BCP For applications, outline Application Security Testing in the BCP 	Functional	Intersects With	Risk Catalog	RSK-03.1	Mechanisms exist to develop and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use.	3	<ul style="list-style-type: none"> Validate BCP via tabletop exercises Incorporate a systematic approach that uses likelihood of risk occurrence, impact to business objectives/content protection, and asset classification for assigning priority (e.g., Business Impact Analysis (BIA)) Define and document Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for critical services and operations as defined in the Business Impact Analysis (BIA) Assign a designated team member to oversee continuity planning efforts Define workarounds, alternate solutions, etc. Protect security systems from disruption in power (e.g., alarms, electronic access, etc.) For template examples, refer to FEMA: https://www.ready.gov/business/emergency-plans/continuity-planning, or TPN Partner Resource Center in TPN+ https://plus.tppn.org/partner-resources

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Relationship	STRM Relationship	SCF Control	SCF #	Security Controls Framework (SCF) Control Description	Strength of Relationship	Notes
OR-1.2	Business Continuity Plan	Establish and regularly review a formal Business Continuity Plan (BCP) and policy, to include the following: <ul style="list-style-type: none"> Team responsible for developing, maintaining, and communicating the BCP Define threats to critical assets, locations, infrastructure, and business operations (e.g., loss of power or communications, systems failure, natural disasters, pandemics, breaches, etc.) Include Incident Response as part of the BCP For applications, outline Application Security Testing in the BCP 	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	3	<ul style="list-style-type: none"> Validate BCP via tabletop exercises Incorporate a systematic approach that uses likelihood of risk occurrence, impact to business objectives/content protection, and asset classification for assigning priority (e.g., Business Impact Analysis (BIA)) Define and document Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for critical services and operations as defined in the Business Impact Analysis (BIA) Assign a designated team member to oversee continuity planning efforts Define workarounds, alternate solutions, etc. Protect security systems from disruption in power (e.g., alarms, electronic access, etc.) For template examples, refer to FEMA: https://www.ready.gov/business/emergency-plans/continuity-planning, or TPN Partner Resource Center in TPN+ https://plus.tpn.org/partner-resources
OR-1.2	Business Continuity Plan	Establish and regularly review a formal Business Continuity Plan (BCP) and policy, to include the following: <ul style="list-style-type: none"> Team responsible for developing, maintaining, and communicating the BCP Define threats to critical assets, locations, infrastructure, and business operations (e.g., loss of power or communications, systems failure, natural disasters, pandemics, breaches, etc.) Include Incident Response as part of the BCP For applications, outline Application Security Testing in the BCP 	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: <ol style="list-style-type: none"> Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and Document the results. 	3	<ul style="list-style-type: none"> Validate BCP via tabletop exercises Incorporate a systematic approach that uses likelihood of risk occurrence, impact to business objectives/content protection, and asset classification for assigning priority (e.g., Business Impact Analysis (BIA)) Define and document Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for critical services and operations as defined in the Business Impact Analysis (BIA) Assign a designated team member to oversee continuity planning efforts Define workarounds, alternate solutions, etc. Protect security systems from disruption in power (e.g., alarms, electronic access, etc.) For template examples, refer to FEMA: https://www.ready.gov/business/emergency-plans/continuity-planning, or TPN Partner Resource Center in TPN+ https://plus.tpn.org/partner-resources
OR-1.2	Business Continuity Plan	Establish and regularly review a formal Business Continuity Plan (BCP) and policy, to include the following: <ul style="list-style-type: none"> Team responsible for developing, maintaining, and communicating the BCP Define threats to critical assets, locations, infrastructure, and business operations (e.g., loss of power or communications, systems failure, natural disasters, pandemics, breaches, etc.) Include Incident Response as part of the BCP For applications, outline Application Security Testing in the BCP 	Functional	Intersects With	Threat Catalog	THR-09	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	8	<ul style="list-style-type: none"> Validate BCP via tabletop exercises Incorporate a systematic approach that uses likelihood of risk occurrence, impact to business objectives/content protection, and asset classification for assigning priority (e.g., Business Impact Analysis (BIA)) Define and document Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for critical services and operations as defined in the Business Impact Analysis (BIA) Assign a designated team member to oversee continuity planning efforts Define workarounds, alternate solutions, etc. Protect security systems from disruption in power (e.g., alarms, electronic access, etc.) For template examples, refer to FEMA: https://www.ready.gov/business/emergency-plans/continuity-planning, or TPN Partner Resource Center in TPN+ https://plus.tpn.org/partner-resources
OR-1.2	Business Continuity Plan	Establish and regularly review a formal Business Continuity Plan (BCP) and policy, to include the following: <ul style="list-style-type: none"> Team responsible for developing, maintaining, and communicating the BCP Define threats to critical assets, locations, infrastructure, and business operations (e.g., loss of power or communications, systems failure, natural disasters, pandemics, breaches, etc.) Include Incident Response as part of the BCP For applications, outline Application Security Testing in the BCP 	Functional	Intersects With	Threat Analysis	THR-10	Mechanisms exist to identify, assess, prioritize and document the potential impacts and likelihoods of applicable internal and external threats.	8	<ul style="list-style-type: none"> Validate BCP via tabletop exercises Incorporate a systematic approach that uses likelihood of risk occurrence, impact to business objectives/content protection, and asset classification for assigning priority (e.g., Business Impact Analysis (BIA)) Define and document Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for critical services and operations as defined in the Business Impact Analysis (BIA) Assign a designated team member to oversee continuity planning efforts Define workarounds, alternate solutions, etc. Protect security systems from disruption in power (e.g., alarms, electronic access, etc.) For template examples, refer to FEMA: https://www.ready.gov/business/emergency-plans/continuity-planning, or TPN Partner Resource Center in TPN+ https://plus.tpn.org/partner-resources
OR-1.3	Disaster Recovery Plan	Establish and regularly review a formal Disaster Recovery Plan (DR) and policy, to include the following: <ul style="list-style-type: none"> Team responsible for developing, maintaining, and communicating the DR Plan Include Incident Response as part of the DR Plan Restrict access to modify or delete backups to only authorized users Perform regular backups of business-critical data per client requirements Encrypt regular backups of business-critical data per client requirements 	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	<ul style="list-style-type: none"> Validate DR Plan via testing (e.g., tabletop exercises, partial disaster, full scale disaster, etc.) to defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) Assign a designated team member to oversee recovery efforts Priorities for recovery procedures, including steps to restore systems Backups that are marked for full recovery are tested on a regular basis Store regular backups of business-critical data in multiple locations per client requirements For template examples, refer to FEMA: https://www.ready.gov/business/emergency-plans/recovery-plan, or TPN Partner Resource Center in TPN+ https://plus.tpn.org/partner-resources
OR-1.3	Disaster Recovery Plan	Establish and regularly review a formal Disaster Recovery Plan (DR) and policy, to include the following: <ul style="list-style-type: none"> Team responsible for developing, maintaining, and communicating the DR Plan Include Incident Response as part of the DR Plan Restrict access to modify or delete backups to only authorized users Perform regular backups of business-critical data per client requirements Encrypt regular backups of business-critical data per client requirements 	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	<ul style="list-style-type: none"> Validate DR Plan via testing (e.g., tabletop exercises, partial disaster, full scale disaster, etc.) to defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) Assign a designated team member to oversee recovery efforts Priorities for recovery procedures, including steps to restore systems Backups that are marked for full recovery are tested on a regular basis Store regular backups of business-critical data in multiple locations per client requirements For template examples, refer to FEMA: https://www.ready.gov/business/emergency-plans/recovery-plan, or TPN Partner Resource Center in TPN+ https://plus.tpn.org/partner-resources
OR-1.3	Disaster Recovery Plan	Establish and regularly review a formal Disaster Recovery Plan (DR) and policy, to include the following: <ul style="list-style-type: none"> Team responsible for developing, maintaining, and communicating the DR Plan Include Incident Response as part of the DR Plan Restrict access to modify or delete backups to only authorized users Perform regular backups of business-critical data per client requirements Encrypt regular backups of business-critical data per client requirements 	Functional	Intersects With	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	5	<ul style="list-style-type: none"> Validate DR Plan via testing (e.g., tabletop exercises, partial disaster, full scale disaster, etc.) to defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) Assign a designated team member to oversee recovery efforts Priorities for recovery procedures, including steps to restore systems Backups that are marked for full recovery are tested on a regular basis Store regular backups of business-critical data in multiple locations per client requirements For template examples, refer to FEMA: https://www.ready.gov/business/emergency-plans/recovery-plan, or TPN Partner Resource Center in TPN+ https://plus.tpn.org/partner-resources
OR-1.3	Disaster Recovery Plan	Establish and regularly review a formal Disaster Recovery Plan (DR) and policy, to include the following: <ul style="list-style-type: none"> Team responsible for developing, maintaining, and communicating the DR Plan Include Incident Response as part of the DR Plan Restrict access to modify or delete backups to only authorized users Perform regular backups of business-critical data per client requirements Encrypt regular backups of business-critical data per client requirements 	Functional	Intersects With	Backup Access	BCD-11.9	Mechanisms exist to restrict access to backups to privileged users with assigned roles for data backup and recovery operations.	5	<ul style="list-style-type: none"> Validate DR Plan via testing (e.g., tabletop exercises, partial disaster, full scale disaster, etc.) to defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) Assign a designated team member to oversee recovery efforts Priorities for recovery procedures, including steps to restore systems Backups that are marked for full recovery are tested on a regular basis Store regular backups of business-critical data in multiple locations per client requirements For template examples, refer to FEMA: https://www.ready.gov/business/emergency-plans/recovery-plan, or TPN Partner Resource Center in TPN+ https://plus.tpn.org/partner-resources
OR-1.3	Disaster Recovery Plan	Establish and regularly review a formal Disaster Recovery Plan (DR) and policy, to include the following: <ul style="list-style-type: none"> Team responsible for developing, maintaining, and communicating the DR Plan Include Incident Response as part of the DR Plan Restrict access to modify or delete backups to only authorized users Perform regular backups of business-critical data per client requirements Encrypt regular backups of business-critical data per client requirements 	Functional	Intersects With	Incident Response Plan (IRP)	IRK-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	<ul style="list-style-type: none"> Validate DR Plan via testing (e.g., tabletop exercises, partial disaster, full scale disaster, etc.) to defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) Assign a designated team member to oversee recovery efforts Priorities for recovery procedures, including steps to restore systems Backups that are marked for full recovery are tested on a regular basis Store regular backups of business-critical data in multiple locations per client requirements For template examples, refer to FEMA: https://www.ready.gov/business/emergency-plans/recovery-plan, or TPN Partner Resource Center in TPN+ https://plus.tpn.org/partner-resources
OR-1.4	Data & Assets	Establish and regularly review a policy and process for Data & Assets, to include the following: <ul style="list-style-type: none"> Classification Protection Database security guidelines Defined segregation of duties Handling throughout data life cycle In accordance with local laws, regulations, and agreements 	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	<ul style="list-style-type: none"> Data retention periods Classification according to data sensitivity Third-party Service Provider data sharing responsibilities (e.g., via contract clauses, etc.) Version control of the policy and process
OR-1.4	Data & Assets	Establish and regularly review a policy and process for Data & Assets, to include the following: <ul style="list-style-type: none"> Classification Protection Database security guidelines Defined segregation of duties Handling throughout data life cycle In accordance with local laws, regulations, and agreements 	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	8	<ul style="list-style-type: none"> Data retention periods Classification according to data sensitivity Third-party Service Provider data sharing responsibilities (e.g., via contract clauses, etc.) Version control of the policy and process
OR-1.4	Data & Assets	Establish and regularly review a policy and process for Data & Assets, to include the following: <ul style="list-style-type: none"> Classification Protection Database security guidelines Defined segregation of duties Handling throughout data life cycle In accordance with local laws, regulations, and agreements 	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	8	<ul style="list-style-type: none"> Data retention periods Classification according to data sensitivity Third-party Service Provider data sharing responsibilities (e.g., via contract clauses, etc.) Version control of the policy and process
OR-1.4	Data & Assets	Establish and regularly review a policy and process for Data & Assets, to include the following: <ul style="list-style-type: none"> Classification Protection Database security guidelines Defined segregation of duties Handling throughout data life cycle In accordance with local laws, regulations, and agreements 	Functional	Intersects With	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Segregation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5	<ul style="list-style-type: none"> Data retention periods Classification according to data sensitivity Third-party Service Provider data sharing responsibilities (e.g., via contract clauses, etc.) Version control of the policy and process
OR-2.0	Risk Management	Establish and regularly review a formal security Risk Management program, to include the following: <ul style="list-style-type: none"> Address workflows, assets, operations, applications, and personnel Apply principles of confidentiality, integrity, and availability (CIA) Review and update upon significant changes Conduct a risk assessment annually Classify and prioritize risks by severity (e.g., Critical, High, Medium, etc.) Document decisions on Risk Management to include monitoring and reporting remediation status with relevant stakeholders 	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: <ol style="list-style-type: none"> Deficiency tracking number; Applicable security, compliance and/or resilience control; Description of the deficiency(ies); Risk associated with the deficiency(ies); Source deficiency identification/detection; Temporary compensating controls, if applicable; Point of Contact (POC) (e.g., asset/process owner); Resources required to conduct remediation actions; Planned remedial actions to the deficiency(ies); Proposed remediation timeline; and Disposition statement (e.g., closure summary). 	5	<ul style="list-style-type: none"> Define a clear scope for the security risk assessment Use an accredited third party to conduct risk assessments Track and maintain a Threat Modeling and Analysis process Regularly meet with management and key stakeholders to identify and document risks Risks identified are addressed in Business Continuity (BCP) and Disaster Recovery (DR) Plans Include risks to all environments and infrastructure, along with a Risk Security Plan A formal exception policy Utilize a Risk Team or cybersecurity professionals to identify vulnerabilities Cybersecurity insurance to help manage financial impact from a cyberattack Leverage established information Security Risk Management framework (e.g., NIST 8286, FAIR framework, ISO 31000:2018/31010:2019, ISO 27005, and/or NIST 800-30)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
OR-2.0	Risk Management	Establish and regularly review a formal security Risk Management program, to include the following: <ul style="list-style-type: none"> Address work/life, assets, operations, applications, and personnel Apply principles of Confidentiality, Integrity, and Availability (CIA) Review and update upon significant changes Conduct a risk assessment annually Classify and prioritize risks by severity (e.g., Critical, High, Medium, etc.) Document decisions on Risk Management to include monitoring and reporting remediation status with relevant stakeholders 	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	<ul style="list-style-type: none"> Define a clear scope for the security risk assessment Use an accredited third party to conduct risk assessments Document and maintain a Threat Modeling and Analysis process Regularly meet with management and key stakeholders to identify and document risks Risks identified are addressed in Business Continuity (BCP) and Disaster Recovery (DR) Plans Include risks to all environments and infrastructure, along with a Site Security Plan for each location A formal exception policy Utilize a Red Team or cybersecurity professionals to identify vulnerabilities Cybersecurity insurance to help manage financial impact from a cyberattack Leverage established Information Security Risk Management framework (e.g., NIST 8236, FAIR frameworks, ISO 31000:2018/ISO 31010:2019, ISO 27005, and/or NIST 800-30)
OR-2.0	Risk Management	Establish and regularly review a formal security Risk Management program, to include the following: <ul style="list-style-type: none"> Address work/life, assets, operations, applications, and personnel Apply principles of Confidentiality, Integrity, and Availability (CIA) Review and update upon significant changes Conduct a risk assessment annually Classify and prioritize risks by severity (e.g., Critical, High, Medium, etc.) Document decisions on Risk Management to include monitoring and reporting remediation status with relevant stakeholders 	Functional	Intersects With	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	<ul style="list-style-type: none"> Define a clear scope for the security risk assessment Use an accredited third party to conduct risk assessments Document and maintain a Threat Modeling and Analysis process Regularly meet with management and key stakeholders to identify and document risks Risks identified are addressed in Business Continuity (BCP) and Disaster Recovery (DR) Plans Include risks to all environments and infrastructure, along with a Site Security Plan for each location A formal exception policy Utilize a Red Team or cybersecurity professionals to identify vulnerabilities Cybersecurity insurance to help manage financial impact from a cyberattack Leverage established Information Security Risk Management framework (e.g., NIST 8236, FAIR frameworks, ISO 31000:2018/ISO 31010:2019, ISO 27005, and/or NIST 800-30)
OR-2.0	Risk Management	Establish and regularly review a formal security Risk Management program, to include the following: <ul style="list-style-type: none"> Address work/life, assets, operations, applications, and personnel Apply principles of Confidentiality, Integrity, and Availability (CIA) Review and update upon significant changes Conduct a risk assessment annually Classify and prioritize risks by severity (e.g., Critical, High, Medium, etc.) Document decisions on Risk Management to include monitoring and reporting remediation status with relevant stakeholders 	Functional	Intersects With	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that: (1) Document the security categorization results (including supporting rationale) in the security plan for systems; and (2) Ensure the security categorization decision is reviewed and approved by the asset owner.	5	<ul style="list-style-type: none"> Define a clear scope for the security risk assessment Use an accredited third party to conduct risk assessments Document and maintain a Threat Modeling and Analysis process Regularly meet with management and key stakeholders to identify and document risks Risks identified are addressed in Business Continuity (BCP) and Disaster Recovery (DR) Plans Include risks to all environments and infrastructure, along with a Site Security Plan for each location A formal exception policy Utilize a Red Team or cybersecurity professionals to identify vulnerabilities Cybersecurity insurance to help manage financial impact from a cyberattack Leverage established Information Security Risk Management framework (e.g., NIST 8236, FAIR frameworks, ISO 31000:2018/ISO 31010:2019, ISO 27005, and/or NIST 800-30)
OR-2.0	Risk Management	Establish and regularly review a formal security Risk Management program, to include the following: <ul style="list-style-type: none"> Address work/life, assets, operations, applications, and personnel Apply principles of Confidentiality, Integrity, and Availability (CIA) Review and update upon significant changes Conduct a risk assessment annually Classify and prioritize risks by severity (e.g., Critical, High, Medium, etc.) Document decisions on Risk Management to include monitoring and reporting remediation status with relevant stakeholders 	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	<ul style="list-style-type: none"> Define a clear scope for the security risk assessment Use an accredited third party to conduct risk assessments Document and maintain a Threat Modeling and Analysis process Regularly meet with management and key stakeholders to identify and document risks Risks identified are addressed in Business Continuity (BCP) and Disaster Recovery (DR) Plans Include risks to all environments and infrastructure, along with a Site Security Plan for each location A formal exception policy Utilize a Red Team or cybersecurity professionals to identify vulnerabilities Cybersecurity insurance to help manage financial impact from a cyberattack Leverage established Information Security Risk Management framework (e.g., NIST 8236, FAIR frameworks, ISO 31000:2018/ISO 31010:2019, ISO 27005, and/or NIST 800-30)
OR-2.0	Risk Management	Establish and regularly review a formal security Risk Management program, to include the following: <ul style="list-style-type: none"> Address work/life, assets, operations, applications, and personnel Apply principles of Confidentiality, Integrity, and Availability (CIA) Review and update upon significant changes Conduct a risk assessment annually Classify and prioritize risks by severity (e.g., Critical, High, Medium, etc.) Document decisions on Risk Management to include monitoring and reporting remediation status with relevant stakeholders 	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	<ul style="list-style-type: none"> Define a clear scope for the security risk assessment Use an accredited third party to conduct risk assessments Document and maintain a Threat Modeling and Analysis process Regularly meet with management and key stakeholders to identify and document risks Risks identified are addressed in Business Continuity (BCP) and Disaster Recovery (DR) Plans Include risks to all environments and infrastructure, along with a Site Security Plan for each location A formal exception policy Utilize a Red Team or cybersecurity professionals to identify vulnerabilities Cybersecurity insurance to help manage financial impact from a cyberattack Leverage established Information Security Risk Management framework (e.g., NIST 8236, FAIR frameworks, ISO 31000:2018/ISO 31010:2019, ISO 27005, and/or NIST 800-30)
OR-2.0	Risk Management	Establish and regularly review a formal security Risk Management program, to include the following: <ul style="list-style-type: none"> Address work/life, assets, operations, applications, and personnel Apply principles of Confidentiality, Integrity, and Availability (CIA) Review and update upon significant changes Conduct a risk assessment annually Classify and prioritize risks by severity (e.g., Critical, High, Medium, etc.) Document decisions on Risk Management to include monitoring and reporting remediation status with relevant stakeholders 	Functional	Intersects With	Instances Requiring A Risk Assessment	RSK-04.3	Mechanisms exist to define instances that require a risk assessment to be performed.	5	<ul style="list-style-type: none"> Define a clear scope for the security risk assessment Use an accredited third party to conduct risk assessments Document and maintain a Threat Modeling and Analysis process Regularly meet with management and key stakeholders to identify and document risks Risks identified are addressed in Business Continuity (BCP) and Disaster Recovery (DR) Plans Include risks to all environments and infrastructure, along with a Site Security Plan for each location A formal exception policy Utilize a Red Team or cybersecurity professionals to identify vulnerabilities Cybersecurity insurance to help manage financial impact from a cyberattack Leverage established Information Security Risk Management framework (e.g., NIST 8236, FAIR frameworks, ISO 31000:2018/ISO 31010:2019, ISO 27005, and/or NIST 800-30)
OR-2.0	Risk Management	Establish and regularly review a formal security Risk Management program, to include the following: <ul style="list-style-type: none"> Address work/life, assets, operations, applications, and personnel Apply principles of Confidentiality, Integrity, and Availability (CIA) Review and update upon significant changes Conduct a risk assessment annually Classify and prioritize risks by severity (e.g., Critical, High, Medium, etc.) Document decisions on Risk Management to include monitoring and reporting remediation status with relevant stakeholders 	Functional	Intersects With	Risk Ranking	RSK-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities that is based on industry-recognized practices.	5	<ul style="list-style-type: none"> Define a clear scope for the security risk assessment Use an accredited third party to conduct risk assessments Document and maintain a Threat Modeling and Analysis process Regularly meet with management and key stakeholders to identify and document risks Risks identified are addressed in Business Continuity (BCP) and Disaster Recovery (DR) Plans Include risks to all environments and infrastructure, along with a Site Security Plan for each location A formal exception policy Utilize a Red Team or cybersecurity professionals to identify vulnerabilities Cybersecurity insurance to help manage financial impact from a cyberattack Leverage established Information Security Risk Management framework (e.g., NIST 8236, FAIR frameworks, ISO 31000:2018/ISO 31010:2019, ISO 27005, and/or NIST 800-30)
OR-2.0	Risk Management	Establish and regularly review a formal security Risk Management program, to include the following: <ul style="list-style-type: none"> Address work/life, assets, operations, applications, and personnel Apply principles of Confidentiality, Integrity, and Availability (CIA) Review and update upon significant changes Conduct a risk assessment annually Classify and prioritize risks by severity (e.g., Critical, High, Medium, etc.) Document decisions on Risk Management to include monitoring and reporting remediation status with relevant stakeholders 	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	<ul style="list-style-type: none"> Define a clear scope for the security risk assessment Use an accredited third party to conduct risk assessments Document and maintain a Threat Modeling and Analysis process Regularly meet with management and key stakeholders to identify and document risks Risks identified are addressed in Business Continuity (BCP) and Disaster Recovery (DR) Plans Include risks to all environments and infrastructure, along with a Site Security Plan for each location A formal exception policy Utilize a Red Team or cybersecurity professionals to identify vulnerabilities Cybersecurity insurance to help manage financial impact from a cyberattack Leverage established Information Security Risk Management framework (e.g., NIST 8236, FAIR frameworks, ISO 31000:2018/ISO 31010:2019, ISO 27005, and/or NIST 800-30)
OR-2.0	Risk Management	Establish and regularly review a formal security Risk Management program, to include the following: <ul style="list-style-type: none"> Address work/life, assets, operations, applications, and personnel Apply principles of Confidentiality, Integrity, and Availability (CIA) Review and update upon significant changes Conduct a risk assessment annually Classify and prioritize risks by severity (e.g., Critical, High, Medium, etc.) Document decisions on Risk Management to include monitoring and reporting remediation status with relevant stakeholders 	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-06.4	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	5	<ul style="list-style-type: none"> Define a clear scope for the security risk assessment Use an accredited third party to conduct risk assessments Document and maintain a Threat Modeling and Analysis process Regularly meet with management and key stakeholders to identify and document risks Risks identified are addressed in Business Continuity (BCP) and Disaster Recovery (DR) Plans Include risks to all environments and infrastructure, along with a Site Security Plan for each location A formal exception policy Utilize a Red Team or cybersecurity professionals to identify vulnerabilities Cybersecurity insurance to help manage financial impact from a cyberattack Leverage established Information Security Risk Management framework (e.g., NIST 8236, FAIR frameworks, ISO 31000:2018/ISO 31010:2019, ISO 27005, and/or NIST 800-30)
OR-3.0	Background Screening	Establish and regularly review a policy and process for Background Screening on all relevant full- and part-time employees, consultants, contractors, and interns, to include the following: <ul style="list-style-type: none"> In accordance with local laws, regulations, agreements, and cultural considerations Retain all signed agreements and results 	Functional	Subset Of	Human Resources Security Management	HR5-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	<ul style="list-style-type: none"> Apply to freelancers and temporary workers Use a third-party background screening company
OR-3.0	Background Screening	Establish and regularly review a policy and process for Background Screening on all relevant full- and part-time employees, consultants, contractors, and interns, to include the following: <ul style="list-style-type: none"> In accordance with local laws, regulations, agreements, and cultural considerations Retain all signed agreements and results 	Functional	Intersects With	Personnel Screening	HR5-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	8	<ul style="list-style-type: none"> Apply to freelancers and temporary workers Use a third-party background screening company
OR-3.0	Background Screening	Establish and regularly review a policy and process for Background Screening on all relevant full- and part-time employees, consultants, contractors, and interns, to include the following: <ul style="list-style-type: none"> In accordance with local laws, regulations, agreements, and cultural considerations Retain all signed agreements and results 	Functional	Intersects With	Roles With Special Protection Measures	HR5-04.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	8	<ul style="list-style-type: none"> Apply to freelancers and temporary workers Use a third-party background screening company
OR-3.0	Background Screening	Establish and regularly review a policy and process for Background Screening on all relevant full- and part-time employees, consultants, contractors, and interns, to include the following: <ul style="list-style-type: none"> In accordance with local laws, regulations, agreements, and cultural considerations Retain all signed agreements and results 	Functional	Intersects With	Terms of Employment	HR5-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	5	<ul style="list-style-type: none"> Apply to freelancers and temporary workers Use a third-party background screening company

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Relationship	STRM Relationship	SCF Control	SCF #	Security Controls Framework (SCF) Control Description	Strength of Relationship	Notes
OR-3.3	Training & Awareness Program	Establish and regularly review a Training & Awareness Program about security policies and procedures and train all relevant full- and part-time employees, consultants, contractors, interns, freelancers, and temporary workers, upon hire and annually, to include the following: • For executive management and owners, tailor specific training • For developers, support, and maintenance personnel of the application, tailor specific training (e.g., secure coding, etc.) • Develop tailored training based on job responsibilities (e.g., interaction with content) • Review, update, and conduct training after introduction of new processes and technologies • Maintain a log of all training and attendees	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5	• Training for business email compromise, social engineering, ransomware, malware, and phishing • Develop a program to test effectiveness of training (e.g., phishing campaigns, tabletop exercises, etc.) • Training covers the restriction of personal devices • Training covers Authentication Best Practices (TS-1.6) (e.g., complexity, multiple account usage, etc.) • Perform project-specific training, including access approval process and incident escalation, before commencement of project
OR-3.3	Training & Awareness Program	Establish and regularly review a Training & Awareness Program about security policies and procedures and train all relevant full- and part-time employees, consultants, contractors, interns, freelancers, and temporary workers, upon hire and annually, to include the following: • For executive management and owners, tailor specific training • For developers, support, and maintenance personnel of the application, tailor specific training (e.g., secure coding, etc.) • Develop tailored training based on job responsibilities (e.g., interaction with content) • Review, update, and conduct training after introduction of new processes and technologies • Maintain a log of all training and attendees	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	8	• Training for business email compromise, social engineering, ransomware, malware, and phishing • Develop a program to test effectiveness of training (e.g., phishing campaigns, tabletop exercises, etc.) • Training covers Authentication Best Practices (TS-1.6) (e.g., complexity, multiple account usage, etc.) • Perform project-specific training, including access approval process and incident escalation, before commencement of project
OR-3.3	Training & Awareness Program	Establish and regularly review a Training & Awareness Program about security policies and procedures and train all relevant full- and part-time employees, consultants, contractors, interns, freelancers, and temporary workers, upon hire and annually, to include the following: • For executive management and owners, tailor specific training • For developers, support, and maintenance personnel of the application, tailor specific training (e.g., secure coding, etc.) • Develop tailored training based on job responsibilities (e.g., interaction with content) • Review, update, and conduct training after introduction of new processes and technologies • Maintain a log of all training and attendees	Functional	Intersects With	Social Engineering & Mining	SAT-02.2	Mechanisms exist to include awareness training on recognizing and reporting potential and actual instances of social engineering and social mining.	5	• Training for business email compromise, social engineering, ransomware, malware, and phishing • Develop a program to test effectiveness of training (e.g., phishing campaigns, tabletop exercises, etc.) • Training covers Authentication Best Practices (TS-1.6) (e.g., complexity, multiple account usage, etc.) • Perform project-specific training, including access approval process and incident escalation, before commencement of project
OR-3.3	Training & Awareness Program	Establish and regularly review a Training & Awareness Program about security policies and procedures and train all relevant full- and part-time employees, consultants, contractors, interns, freelancers, and temporary workers, upon hire and annually, to include the following: • For executive management and owners, tailor specific training • For developers, support, and maintenance personnel of the application, tailor specific training (e.g., secure coding, etc.) • Develop tailored training based on job responsibilities (e.g., interaction with content) • Review, update, and conduct training after introduction of new processes and technologies • Maintain a log of all training and attendees	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: 1) Before authorizing access to the system or performing assigned duties; 2) When required by system changes; and 3) Annually thereafter.	8	• Training for business email compromise, social engineering, ransomware, malware, and phishing • Develop a program to test effectiveness of training (e.g., phishing campaigns, tabletop exercises, etc.) • Training covers Authentication Best Practices (TS-1.6) (e.g., complexity, multiple account usage, etc.) • Perform project-specific training, including access approval process and incident escalation, before commencement of project
OR-3.3	Training & Awareness Program	Establish and regularly review a Training & Awareness Program about security policies and procedures and train all relevant full- and part-time employees, consultants, contractors, interns, freelancers, and temporary workers, upon hire and annually, to include the following: • For executive management and owners, tailor specific training • For developers, support, and maintenance personnel of the application, tailor specific training (e.g., secure coding, etc.) • Develop tailored training based on job responsibilities (e.g., interaction with content) • Review, update, and conduct training after introduction of new processes and technologies • Maintain a log of all training and attendees	Functional	Intersects With	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5	• Training for business email compromise, social engineering, ransomware, malware, and phishing • Develop a program to test effectiveness of training (e.g., phishing campaigns, tabletop exercises, etc.) • Training covers Authentication Best Practices (TS-1.6) (e.g., complexity, multiple account usage, etc.) • Perform project-specific training, including access approval process and incident escalation, before commencement of project
OR-3.3	Training & Awareness Program	Establish and regularly review a Training & Awareness Program about security policies and procedures and train all relevant full- and part-time employees, consultants, contractors, interns, freelancers, and temporary workers, upon hire and annually, to include the following: • For executive management and owners, tailor specific training • For developers, support, and maintenance personnel of the application, tailor specific training (e.g., secure coding, etc.) • Develop tailored training based on job responsibilities (e.g., interaction with content) • Review, update, and conduct training after introduction of new processes and technologies • Maintain a log of all training and attendees	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	5	• Training for business email compromise, social engineering, ransomware, malware, and phishing • Develop a program to test effectiveness of training (e.g., phishing campaigns, tabletop exercises, etc.) • Training covers Authentication Best Practices (TS-1.6) (e.g., complexity, multiple account usage, etc.) • Perform project-specific training, including access approval process and incident escalation, before commencement of project
OR-3.3	Training & Awareness Program	Establish and regularly review a Training & Awareness Program about security policies and procedures and train all relevant full- and part-time employees, consultants, contractors, interns, freelancers, and temporary workers, upon hire and annually, to include the following: • For executive management and owners, tailor specific training • For developers, support, and maintenance personnel of the application, tailor specific training (e.g., secure coding, etc.) • Develop tailored training based on job responsibilities (e.g., interaction with content) • Review, update, and conduct training after introduction of new processes and technologies • Maintain a log of all training and attendees	Functional	Intersects With	Privileged Users	SAT-03.5	Mechanisms exist to provide specific training for privileged users to ensure privileged users understand their unique roles and responsibilities	5	• Training for business email compromise, social engineering, ransomware, malware, and phishing • Develop a program to test effectiveness of training (e.g., phishing campaigns, tabletop exercises, etc.) • Training covers the restriction of personal devices • Training covers Authentication Best Practices (TS-1.6) (e.g., complexity, multiple account usage, etc.) • Perform project-specific training, including access approval process and incident escalation, before commencement of project
OR-3.3	Training & Awareness Program	Establish and regularly review a Training & Awareness Program about security policies and procedures and train all relevant full- and part-time employees, consultants, contractors, interns, freelancers, and temporary workers, upon hire and annually, to include the following: • For executive management and owners, tailor specific training • For developers, support, and maintenance personnel of the application, tailor specific training (e.g., secure coding, etc.) • Develop tailored training based on job responsibilities (e.g., interaction with content) • Review, update, and conduct training after introduction of new processes and technologies • Maintain a log of all training and attendees	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	• Training for business email compromise, social engineering, ransomware, malware, and phishing • Develop a program to test effectiveness of training (e.g., phishing campaigns, tabletop exercises, etc.) • Training covers Authentication Best Practices (TS-1.6) (e.g., complexity, multiple account usage, etc.) • Perform project-specific training, including access approval process and incident escalation, before commencement of project
OR-3.3	Training & Awareness Program	Establish and regularly review a Training & Awareness Program about security policies and procedures and train all relevant full- and part-time employees, consultants, contractors, interns, freelancers, and temporary workers, upon hire and annually, to include the following: • For executive management and owners, tailor specific training • For developers, support, and maintenance personnel of the application, tailor specific training (e.g., secure coding, etc.) • Develop tailored training based on job responsibilities (e.g., interaction with content) • Review, update, and conduct training after introduction of new processes and technologies • Maintain a log of all training and attendees	Functional	Intersects With	Security, Compliance & Resilience Training Records	SAT-04	Mechanisms exist to document, retain and monitor individual training activities, including: 1) Initial security, compliance and resilience awareness training; 2) Recurring awareness training; and 3) Technology Assets, Applications and/or Services (TAAS)-specific training.	5	• Training for business email compromise, social engineering, ransomware, malware, and phishing • Develop a program to test effectiveness of training (e.g., phishing campaigns, tabletop exercises, etc.) • Training covers Authentication Best Practices (TS-1.6) (e.g., complexity, multiple account usage, etc.) • Perform project-specific training, including access approval process and incident escalation, before commencement of project
OR-3.4	Contracts & Service Level Agreements	Confirm that Contracts & Service Level Agreements (SLAs) with third-party Service Providers (i.e., external companies that are paid for services provided, including support, development, and maintenance of applications), include the following: • Business Continuity (BCP) and Disaster Recovery (DR) Plans • Incident Response process • Data handover and destruction upon service termination • Risk Management process • Ability to obtain requested Information Security compliance certificates and/or attestations • Background screening of all third-party full- and part-time employees, consultants, contractors, interns, freelancers, and temporary workers • Confidentiality Agreements/NDAs for all third-party full- and part-time employees, consultants, contractors, interns, freelancers, and temporary workers • Client notification if services are outsourced or subcontracted • In accordance with local laws, regulations, and agreements, including third-party consent for Background Screening and Confidentiality Agreements/NDAs	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	• An independent, third-party review/audit of the effectiveness of the third-party Service Provider's security and privacy controls (e.g., MPA Content Security Best Practices, CSA Star, ISO, SOC 2 Type 2, etc.)
OR-3.4	Contracts & Service Level Agreements	Confirm that Contracts & Service Level Agreements (SLAs) with third-party Service Providers (i.e., external companies that are paid for services provided, including support, development, and maintenance of applications), include the following: • Business Continuity (BCP) and Disaster Recovery (DR) Plans • Incident Response process • Data handover and destruction upon service termination • Risk Management process • Ability to obtain requested Information Security compliance certificates and/or attestations • Background screening of all third-party full- and part-time employees, consultants, contractors, interns, freelancers, and temporary workers • Confidentiality Agreements/NDAs for all third-party full- and part-time employees, consultants, contractors, interns, freelancers, and temporary workers • Client notification if services are outsourced or subcontracted • In accordance with local laws, regulations, and agreements, including third-party consent for Background Screening and Confidentiality Agreements/NDAs	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8	• An independent, third-party review/audit of the effectiveness of the third-party Service Provider's security and privacy controls (e.g., MPA Content Security Best Practices, CSA Star, ISO, SOC 2 Type 2, etc.)
OR-3.4	Contracts & Service Level Agreements	Confirm that Contracts & Service Level Agreements (SLAs) with third-party Service Providers (i.e., external companies that are paid for services provided, including support, development, and maintenance of applications), include the following: • Business Continuity (BCP) and Disaster Recovery (DR) Plans • Incident Response process • Data handover and destruction upon service termination • Risk Management process • Ability to obtain requested Information Security compliance certificates and/or attestations • Background screening of all third-party full- and part-time employees, consultants, contractors, interns, freelancers, and temporary workers • Confidentiality Agreements/NDAs for all third-party full- and part-time employees, consultants, contractors, interns, freelancers, and temporary workers • Client notification if services are outsourced or subcontracted • In accordance with local laws, regulations, and agreements, including third-party consent for Background Screening and Confidentiality Agreements/NDAs	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RACSI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RACSI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	5	• An independent, third-party review/audit of the effectiveness of the third-party Service Provider's security and privacy controls (e.g., MPA Content Security Best Practices, CSA Star, ISO, SOC 2 Type 2, etc.)
OR-3.4	Contracts & Service Level Agreements	Confirm that Contracts & Service Level Agreements (SLAs) with third-party Service Providers (i.e., external companies that are paid for services provided, including support, development, and maintenance of applications), include the following: • Business Continuity (BCP) and Disaster Recovery (DR) Plans • Incident Response process • Data handover and destruction upon service termination • Risk Management process • Ability to obtain requested Information Security compliance certificates and/or attestations • Background screening of all third-party full- and part-time employees, consultants, contractors, interns, freelancers, and temporary workers • Confidentiality Agreements/NDAs for all third-party full- and part-time employees, consultants, contractors, interns, freelancers, and temporary workers • Client notification if services are outsourced or subcontracted • In accordance with local laws, regulations, and agreements, including third-party consent for Background Screening and Confidentiality Agreements/NDAs	Functional	Intersects With	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to subcontractors.	5	• An independent, third-party review/audit of the effectiveness of the third-party Service Provider's security and privacy controls (e.g., MPA Content Security Best Practices, CSA Star, ISO, SOC 2 Type 2, etc.)
OR-3.4	Contracts & Service Level Agreements	Confirm that Contracts & Service Level Agreements (SLAs) with third-party Service Providers (i.e., external companies that are paid for services provided, including support, development, and maintenance of applications), include the following: • Business Continuity (BCP) and Disaster Recovery (DR) Plans • Incident Response process • Data handover and destruction upon service termination • Risk Management process • Ability to obtain requested Information Security compliance certificates and/or attestations • Background screening of all third-party full- and part-time employees, consultants, contractors, interns, freelancers, and temporary workers • Confidentiality Agreements/NDAs for all third-party full- and part-time employees, consultants, contractors, interns, freelancers, and temporary workers • Client notification if services are outsourced or subcontracted • In accordance with local laws, regulations, and agreements, including third-party consent for Background Screening and Confidentiality Agreements/NDAs	Functional	Intersects With	Third-Party Attestation (3PA)	TPM-05.8	Mechanisms exist to obtain an attestation from an independent Third-Party Assessor/Inspector (TPA) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.	5	• An independent, third-party review/audit of the effectiveness of the third-party Service Provider's security and privacy controls (e.g., MPA Content Security Best Practices, CSA Star, ISO, SOC 2 Type 2, etc.)
OR-3.4	Contracts & Service Level Agreements	Confirm that Contracts & Service Level Agreements (SLAs) with third-party Service Providers (i.e., external companies that are paid for services provided, including support, development, and maintenance of applications), include the following: • Business Continuity (BCP) and Disaster Recovery (DR) Plans • Incident Response process • Data handover and destruction upon service termination • Risk Management process • Ability to obtain requested Information Security compliance certificates and/or attestations • Background screening of all third-party full- and part-time employees, consultants, contractors, interns, freelancers, and temporary workers • Confidentiality Agreements/NDAs for all third-party full- and part-time employees, consultants, contractors, interns, freelancers, and temporary workers • Client notification if services are outsourced or subcontracted • In accordance with local laws, regulations, and agreements, including third-party consent for Background Screening and Confidentiality Agreements/NDAs	Functional	Intersects With	Third-Party Personnel Security	TPM-06	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	5	• An independent, third-party review/audit of the effectiveness of the third-party Service Provider's security and privacy controls (e.g., MPA Content Security Best Practices, CSA Star, ISO, SOC 2 Type 2, etc.)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Relationship	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
OR-3.4	Contracts & Service Level Agreements	<ul style="list-style-type: none"> Confirm that Contracts & Service Level Agreements (SLAs) with third-party Service Providers (i.e., external companies that are not for services provided, including support, development, and maintenance of applications), include the following: <ul style="list-style-type: none"> Business Continuity (BCP) and Disaster Recovery (DR) Plans Incident Response process Data handover and destruction upon service termination Risk Management process Ability to obtain requested Information Security compliance certificates and/or attestations Background screening of all third-party full- and part-time employees, consultants, contractors, interns, freelancers, and temporary workers Confidentiality Agreements/NDAs for all third-party full- and part-time employees, consultants, contractors, interns, freelancers, and temporary workers Client notification if services are outsourced or subcontracted In accordance with local laws, regulations, and agreements, including third-party consent for Background Screening and Confidentiality Agreements/NDAs 	Functional	Intersects With	Review of Third-Party Services	TRM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5	<ul style="list-style-type: none"> Establish an Incident Response team, including a designated lead Incidents are addressed within 48 hours Notify impacted clients as soon as possible and provide high-level incident details Regularly update, through an established cadence with clients, with new information throughout the investigation Apply to all relevant full- and part-time employees, consultants, contractors, interns, freelancers, temporary workers, and visitors Maintain key contact information, including business partners and clients Notification of law enforcement Anonymous reporting Hire third-party cybersecurity partner for incidents, as needed
OR-4.0	Incident Response	<ul style="list-style-type: none"> Establish and regularly review a formal Incident Response policy and process, which covers both IT and content incidents/events, to include the following: <ul style="list-style-type: none"> Detection Analysis Escalation Response Evidence/forensics Remediation Reporting and metrics A corrective action process to include Root Cause Analysis (RCA), lessons learned, preventative measures taken, etc. Notification of affected business partners and clients in a timely manner Utilize this URL to report privacy incidents: https://www.alliancecreativity.com/report-privacy/ 	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	<ul style="list-style-type: none"> Establish an Incident Response team, including a designated lead Incidents are addressed within 48 hours Notify impacted clients as soon as possible and provide high-level incident details Regularly update, through an established cadence with clients, with new information throughout the investigation Apply to all relevant full- and part-time employees, consultants, contractors, interns, freelancers, temporary workers, and visitors Maintain key contact information, including business partners and clients Notification of law enforcement Anonymous reporting Hire third-party cybersecurity partner for incidents, as needed
OR-4.0	Incident Response	<ul style="list-style-type: none"> Establish and regularly review a formal Incident Response policy and process, which covers both IT and content incidents/events, to include the following: <ul style="list-style-type: none"> Detection Analysis Escalation Response Evidence/forensics Remediation Reporting and metrics A corrective action process to include Root Cause Analysis (RCA), lessons learned, preventative measures taken, etc. Notification of affected business partners and clients in a timely manner Utilize this URL to report privacy incidents: https://www.alliancecreativity.com/report-privacy/ 	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: <ol style="list-style-type: none"> Preparation; Automated early detection or manual incident report intake; Analysis; Containment; Eradication; and Recovery. 	5	<ul style="list-style-type: none"> Establish an Incident Response team, including a designated lead Incidents are addressed within 48 hours Notify impacted clients as soon as possible and provide high-level incident details Regularly update, through an established cadence with clients, with new information throughout the investigation Apply to all relevant full- and part-time employees, consultants, contractors, interns, freelancers, temporary workers, and visitors Maintain key contact information, including business partners and clients Notification of law enforcement Anonymous reporting Hire third-party cybersecurity partner for incidents, as needed
OR-4.0	Incident Response	<ul style="list-style-type: none"> Establish and regularly review a formal Incident Response policy and process, which covers both IT and content incidents/events, to include the following: <ul style="list-style-type: none"> Detection Analysis Escalation Response Evidence/forensics Remediation Reporting and metrics A corrective action process to include Root Cause Analysis (RCA), lessons learned, preventative measures taken, etc. Notification of affected business partners and clients in a timely manner Utilize this URL to report privacy incidents: https://www.alliancecreativity.com/report-privacy/ 	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	<ul style="list-style-type: none"> Establish an Incident Response team, including a designated lead Incidents are addressed within 48 hours Notify impacted clients as soon as possible and provide high-level incident details Regularly update, through an established cadence with clients, with new information throughout the investigation Apply to all relevant full- and part-time employees, consultants, contractors, interns, freelancers, temporary workers, and visitors Maintain key contact information, including business partners and clients Notification of law enforcement Anonymous reporting Hire third-party cybersecurity partner for incidents, as needed
OR-4.0	Incident Response	<ul style="list-style-type: none"> Establish and regularly review a formal Incident Response policy and process, which covers both IT and content incidents/events, to include the following: <ul style="list-style-type: none"> Detection Analysis Escalation Response Evidence/forensics Remediation Reporting and metrics A corrective action process to include Root Cause Analysis (RCA), lessons learned, preventative measures taken, etc. Notification of affected business partners and clients in a timely manner Utilize this URL to report privacy incidents: https://www.alliancecreativity.com/report-privacy/ 	Functional	Intersects With	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	5	<ul style="list-style-type: none"> Establish an Incident Response team, including a designated lead Incidents are addressed within 48 hours Notify impacted clients as soon as possible and provide high-level incident details Regularly update, through an established cadence with clients, with new information throughout the investigation Apply to all relevant full- and part-time employees, consultants, contractors, interns, freelancers, temporary workers, and visitors Maintain key contact information, including business partners and clients Notification of law enforcement Anonymous reporting Hire third-party cybersecurity partner for incidents, as needed
OR-4.0	Incident Response	<ul style="list-style-type: none"> Establish and regularly review a formal Incident Response policy and process, which covers both IT and content incidents/events, to include the following: <ul style="list-style-type: none"> Detection Analysis Escalation Response Evidence/forensics Remediation Reporting and metrics A corrective action process to include Root Cause Analysis (RCA), lessons learned, preventative measures taken, etc. Notification of affected business partners and clients in a timely manner Utilize this URL to report privacy incidents: https://www.alliancecreativity.com/report-privacy/ 	Functional	Intersects With	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	5	<ul style="list-style-type: none"> Establish an Incident Response team, including a designated lead Incidents are addressed within 48 hours Notify impacted clients as soon as possible and provide high-level incident details Regularly update, through an established cadence with clients, with new information throughout the investigation Apply to all relevant full- and part-time employees, consultants, contractors, interns, freelancers, temporary workers, and visitors Maintain key contact information, including business partners and clients Notification of law enforcement Anonymous reporting Hire third-party cybersecurity partner for incidents, as needed
OR-4.0	Incident Response	<ul style="list-style-type: none"> Establish and regularly review a formal Incident Response policy and process, which covers both IT and content incidents/events, to include the following: <ul style="list-style-type: none"> Detection Analysis Escalation Response Evidence/forensics Remediation Reporting and metrics A corrective action process to include Root Cause Analysis (RCA), lessons learned, preventative measures taken, etc. Notification of affected business partners and clients in a timely manner Utilize this URL to report privacy incidents: https://www.alliancecreativity.com/report-privacy/ 	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely report incidents to applicable: <ol style="list-style-type: none"> Internal stakeholders; Affected clients & third parties; and Regulatory authorities. 	5	<ul style="list-style-type: none"> Establish an Incident Response team, including a designated lead Incidents are addressed within 48 hours Notify impacted clients as soon as possible and provide high-level incident details Regularly update, through an established cadence with clients, with new information throughout the investigation Apply to all relevant full- and part-time employees, consultants, contractors, interns, freelancers, temporary workers, and visitors Maintain key contact information, including business partners and clients Notification of law enforcement Anonymous reporting Hire third-party cybersecurity partner for incidents, as needed
OR-5.0	AI/ML - Security Management	<ul style="list-style-type: none"> Establish and regularly review a formal Artificial Intelligence (AI) & Machine Learning (ML) Security Management policy for in-house developed or third-party licensed AI/ML, to include the following: <ul style="list-style-type: none"> Tailor policy to include applicable AI/ML content and applications Identify and manage risks to include security controls associated with changes to datasets, applications, network infrastructure, and systems Obtain client approval for AI/ML application use Review data sources and data integrity before use In accordance with local laws, regulations, agreements, and client policy when using AI/ML data Outline appropriate usage for AI/ML datasets Include AI/ML in Acceptable Use Policy Best Practices (OR-1.1) 	Functional	Subset Of	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-01	Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively.	10	<ul style="list-style-type: none"> Develop tailored training program for use of AI/ML applications based on job responsibilities Only use internally managed and sandboxed LLMs
OR-5.0	AI/ML - Security Management	<ul style="list-style-type: none"> Establish and regularly review a formal Artificial Intelligence (AI) & Machine Learning (ML) Security Management policy for in-house developed or third-party licensed AI/ML, to include the following: <ul style="list-style-type: none"> Tailor policy to include applicable AI/ML content and applications Identify and manage risks to include security controls associated with changes to datasets, applications, network infrastructure, and systems Obtain client approval for AI/ML application use Review data sources and data integrity before use In accordance with local laws, regulations, agreements, and client policy when using AI/ML data Outline appropriate usage for AI/ML datasets Include AI/ML in Acceptable Use Policy Best Practices (OR-1.1) 	Functional	Intersects With	Situational Awareness of AI & Autonomous Technologies	AAT-02	Mechanisms exist to develop and maintain an inventory of Artificial Intelligence (AI) and Autonomous Technologies (AAT) (internal and third-party).	5	<ul style="list-style-type: none"> Develop tailored training program for use of AI/ML applications based on job responsibilities Only use internally managed and sandboxed LLMs
OR-5.0	AI/ML - Security Management	<ul style="list-style-type: none"> Establish and regularly review a formal Artificial Intelligence (AI) & Machine Learning (ML) Security Management policy for in-house developed or third-party licensed AI/ML, to include the following: <ul style="list-style-type: none"> Tailor policy to include applicable AI/ML content and applications Identify and manage risks to include security controls associated with changes to datasets, applications, network infrastructure, and systems Obtain client approval for AI/ML application use Review data sources and data integrity before use In accordance with local laws, regulations, agreements, and client policy when using AI/ML data Outline appropriate usage for AI/ML datasets Include AI/ML in Acceptable Use Policy Best Practices (OR-1.1) 	Functional	Intersects With	AI & Autonomous Technologies Risk Mapping	AAT-02.1	Mechanisms exist to identify Artificial Intelligence (AI) and Autonomous Technologies (AAT)-specific threat modeling and risk assessments to address the following criteria across the lifecycle of the AAT: <ol style="list-style-type: none"> Adversarial threats; and Abuse / misuse scenarios. 	5	<ul style="list-style-type: none"> Develop tailored training program for use of AI/ML applications based on job responsibilities Only use internally managed and sandboxed LLMs
OR-5.0	AI/ML - Security Management	<ul style="list-style-type: none"> Establish and regularly review a formal Artificial Intelligence (AI) & Machine Learning (ML) Security Management policy for in-house developed or third-party licensed AI/ML, to include the following: <ul style="list-style-type: none"> Tailor policy to include applicable AI/ML content and applications Identify and manage risks to include security controls associated with changes to datasets, applications, network infrastructure, and systems Obtain client approval for AI/ML application use Review data sources and data integrity before use In accordance with local laws, regulations, agreements, and client policy when using AI/ML data Outline appropriate usage for AI/ML datasets Include AI/ML in Acceptable Use Policy Best Practices (OR-1.1) 	Functional	Intersects With	AI Threat Modeling & Risk Assessment	AAT-02.4	Mechanisms exist to conduct Artificial Intelligence (AI) and Autonomous Technologies (AAT)-specific threat modeling and risk assessments to address the following criteria across the lifecycle of the AAT: <ol style="list-style-type: none"> Adversarial threats; and Abuse / misuse scenarios. 	5	<ul style="list-style-type: none"> Develop tailored training program for use of AI/ML applications based on job responsibilities Only use internally managed and sandboxed LLMs
OR-5.0	AI/ML - Security Management	<ul style="list-style-type: none"> Establish and regularly review a formal Artificial Intelligence (AI) & Machine Learning (ML) Security Management policy for in-house developed or third-party licensed AI/ML, to include the following: <ul style="list-style-type: none"> Tailor policy to include applicable AI/ML content and applications Identify and manage risks to include security controls associated with changes to datasets, applications, network infrastructure, and systems Obtain client approval for AI/ML application use Review data sources and data integrity before use In accordance with local laws, regulations, agreements, and client policy when using AI/ML data Outline appropriate usage for AI/ML datasets Include AI/ML in Acceptable Use Policy Best Practices (OR-1.1) 	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CP-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	<ul style="list-style-type: none"> Develop tailored training program for use of AI/ML applications based on job responsibilities Only use internally managed and sandboxed LLMs
OP-1.0	Receiving	Establish and regularly review a Receiving process for physical client assets, to include maintaining a receiving log to be filled out by designated personnel upon receipt of deliveries.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated employee points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	8	<ul style="list-style-type: none"> For receiving log, include the following information: name and signature of courier/delivering entity, name and signature of recipient, and time and date of receipt For assets that can't be delivered immediately, store in a secure area (e.g., vault, safe, high-security cage, etc.), including after-hours deliveries If physical assets are not normally handled, notify clients when physical assets are received
OP-1.0	Receiving	Establish and regularly review a Receiving process for physical client assets, to include maintaining a receiving log to be filled out by designated personnel upon receipt of deliveries.	Functional	Intersects With	Controlled Ingress & Egress Points	PES-03.1	Physical access control mechanisms exist to limit and monitor physical access through controlled ingress and egress points.	8	<ul style="list-style-type: none"> For receiving log, include the following information: name and signature of courier/delivering entity, name and signature of recipient, and time and date of receipt For assets that can't be delivered immediately, store in a secure area (e.g., vault, safe, high-security cage, etc.), including after-hours deliveries If physical assets are not normally handled, notify clients when physical assets are received
OP-1.0	Receiving	Establish and regularly review a Receiving process for physical client assets, to include maintaining a receiving log to be filled out by designated personnel upon receipt of deliveries.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	<ul style="list-style-type: none"> For receiving log, include the following information: name and signature of courier/delivering entity, name and signature of recipient, and time and date of receipt For assets that can't be delivered immediately, store in a secure area (e.g., vault, safe, high-security cage, etc.), including after-hours deliveries If physical assets are not normally handled, notify clients when physical assets are received

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Relationship	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
OP-10	Receiving	Establish and regularly review a Receiving process for physical client assets, to include maintaining a receiving log to be filed out by designated personnel upon receipt of deliveries.	Functional	Intersects With	Delivery & Removal	PES-10	Physical security mechanisms exist to isolate information processing facilities from points such as delivery and loading areas and other points to avoid unauthorized access.	8	<ul style="list-style-type: none"> For receiving log, include the following information: name and signature of recipient, time and date of receipt For assets that can't be delivered immediately, store in a secure area (e.g., vault, safe, high-security cage, etc.), including after-hours deliveries If physical assets are not normally handled, notify clients when physical assets are received
OP-11	Packaging	Establish and regularly review a Packaging process to package assets in accordance with local laws, regulations, and agreements.	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	<ul style="list-style-type: none"> Monitor the on-site packaging and loading of content Secure containers depending on asset value (e.g., case with a combination lock) Utilize tamper-evident tape, packaging, and/or seals Labels only include address, barcode, aliases (i.e., non-descript)
OP-11	Packaging	Establish and regularly review a Packaging process to package assets in accordance with local laws, regulations, and agreements.	Functional	Intersects With	Data Stewardship	DCH-01.1	Mechanisms exist to ensure data stewardship is assigned, documented and communicated.	5	<ul style="list-style-type: none"> Monitor the on-site packaging and loading of content Secure containers depending on asset value (e.g., case with a combination lock) Utilize tamper-evident tape, packaging, and/or seals Labels only include address, barcode, aliases (i.e., non-descript)
OP-11	Packaging	Establish and regularly review a Packaging process to package assets in accordance with local laws, regulations, and agreements.	Functional	Intersects With	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	5	<ul style="list-style-type: none"> Monitor the on-site packaging and loading of content Secure containers depending on asset value (e.g., case with a combination lock) Utilize tamper-evident tape, packaging, and/or seals Labels only include address, barcode, aliases (i.e., non-descript)
OP-11	Packaging	Establish and regularly review a Packaging process to package assets in accordance with local laws, regulations, and agreements.	Functional	Intersects With	Custodians	DCH-07.1	Mechanisms exist to identify custodians throughout the transport of digital or non-digital media.	5	<ul style="list-style-type: none"> Monitor the on-site packaging and loading of content Secure containers depending on asset value (e.g., case with a combination lock) Utilize tamper-evident tape, packaging, and/or seals Labels only include address, barcode, aliases (i.e., non-descript)
OP-12	Shipping	Establish and regularly review a Shipping process for client assets, to include the following: <ul style="list-style-type: none"> Maintain a log that includes: Time of shipment, recipient name, contact number, address of destination, and tracking number from shipper Retain logs for one year at a minimum, or the maximum time allowed, in accordance with local laws, regulations, and agreements Use client-approved shipping vendor 	Functional	Intersects With	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	5	<ul style="list-style-type: none"> Generate a work/shipping order to authorize client asset shipments Content awaiting shipment is in a secure area under camera surveillance If physical assets are not normally handled, notify clients when physical assets are received Delivery confirmation Utilize GPS tracking
OP-12	Shipping	Establish and regularly review a Shipping process for client assets, to include the following: <ul style="list-style-type: none"> Maintain a log that includes: Time of shipment, recipient name, contact number, address of destination, and tracking number from shipper Retain logs for one year at a minimum, or the maximum time allowed, in accordance with local laws, regulations, and agreements Use client-approved shipping vendor 	Functional	Intersects With	Custodians	DCH-07.1	Mechanisms exist to identify custodians throughout the transport of digital or non-digital media.	5	<ul style="list-style-type: none"> Generate a work/shipping order to authorize client asset shipments Content awaiting shipment is in a secure area under camera surveillance If physical assets are not normally handled, notify clients when physical assets are received Delivery confirmation Utilize GPS tracking
OP-13	Transport Vehicles	Establish and regularly review a process for Transport Vehicles handling assets, to include the following: <ul style="list-style-type: none"> Always lock the vehicle Handling during loading and unloading Verify packages are out of view Direct delivery without unnecessary stops Third-party couriers 	Functional	Intersects With	Media Storage	DCH-06	Mechanisms exist to: <ol style="list-style-type: none"> Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures. 	5	<ul style="list-style-type: none"> Threat insurance when transporting sensitive assets or per client requirements Restrict courier access into high-security areas
OP-13	Transport Vehicles	Establish and regularly review a process for Transport Vehicles handling assets, to include the following: <ul style="list-style-type: none"> Always lock the vehicle Handling during loading and unloading Verify packages are out of view Direct delivery without unnecessary stops Third-party couriers 	Functional	Intersects With	Physically Secure All Media	DCH-06.1	Mechanisms exist to physically secure all media that contains sensitive information.	5	<ul style="list-style-type: none"> Threat insurance when transporting sensitive assets or per client requirements Restrict courier access into high-security areas
OP-13	Transport Vehicles	Establish and regularly review a process for Transport Vehicles handling assets, to include the following: <ul style="list-style-type: none"> Always lock the vehicle Handling during loading and unloading Verify packages are out of view Direct delivery without unnecessary stops Third-party couriers 	Functional	Intersects With	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	5	<ul style="list-style-type: none"> Threat insurance when transporting sensitive assets or per client requirements Restrict courier access into high-security areas
OP-13	Transport Vehicles	Establish and regularly review a process for Transport Vehicles handling assets, to include the following: <ul style="list-style-type: none"> Always lock the vehicle Handling during loading and unloading Verify packages are out of view Direct delivery without unnecessary stops Third-party couriers 	Functional	Intersects With	Custodians	DCH-07.1	Mechanisms exist to identify custodians throughout the transport of digital or non-digital media.	5	<ul style="list-style-type: none"> Threat insurance when transporting sensitive assets or per client requirements Restrict courier access into high-security areas
OP-20	Work From Home/Remote Workers	Establish and regularly review a policy and process for Work From Home (WFH)/Remote Workers, in accordance with local laws, regulations, and agreements, and apply the following MPA Content Security Best Practices, tailored to WFH/Remote Workers: <ul style="list-style-type: none"> Authentication (TS-1.6) Authorization (TS-1.7) Background Screening (OR-3.0) Business Continuity Plan (OR-1.2) Endpoint Protection (TS-1.3) Identity Access Management (TS-1.8) On-boarding (OR-3.1) Off-boarding (OR-3.2) Remote Sites & Locations (OR-2.1) Risk Management (OR-2.0) Training & Awareness Program (OR-3.3) Wireless Networks (TS-2.11) 	Functional	Intersects With	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	<ul style="list-style-type: none"> Apply Incident Response Best Practices (OR-4.0) For on-boarding, confidentiality agreements for other members at the remote location (e.g., roommate, spouse, etc.) per client requirements Maintain a list of authorized remote access users Regularly review user list for discrepancies and unusual or suspicious activity Disconnect wireless networks while accessing content locally Training includes permissible working locations (e.g., non-public spaces, areas where content is visible to unauthorized parties, etc.) Change default credentials on home networking equipment for sensitive content and data, per client requirements Apply Alarm System Best Practices (PS-1.4) Apply Camera System Best Practices (PS-3.0) Apply Entry/Exit Points Best Practices (PS-3.0)
OP-20	Work From Home/Remote Workers	Establish and regularly review a policy and process for Work From Home (WFH)/Remote Workers, in accordance with local laws, regulations, and agreements, and apply the following MPA Content Security Best Practices, tailored to WFH/Remote Workers: <ul style="list-style-type: none"> Authentication (TS-1.6) Authorization (TS-1.7) Background Screening (OR-3.0) Business Continuity Plan (OR-1.2) Endpoint Protection (TS-1.3) Identity Access Management (TS-1.8) On-boarding (OR-3.1) Off-boarding (OR-3.2) Remote Sites & Locations (OR-2.1) Risk Management (OR-2.0) Training & Awareness Program (OR-3.3) Wireless Networks (TS-2.11) 	Functional	Intersects With	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	5	<ul style="list-style-type: none"> Apply Incident Response Best Practices (OR-4.0) For on-boarding, confidentiality agreements for other members at the remote location (e.g., roommate, spouse, etc.) per client requirements Maintain a list of authorized remote access users Regularly review user list for discrepancies and unusual or suspicious activity Disconnect wireless networks while accessing content locally Training includes permissible working locations (e.g., non-public spaces, areas where content is visible to unauthorized parties, etc.) Change default credentials on home networking equipment for sensitive content and data, per client requirements Apply Alarm System Best Practices (PS-1.4) Apply Camera System Best Practices (PS-3.0) Apply Entry/Exit Points Best Practices (PS-3.0)
OP-20	Work From Home/Remote Workers	Establish and regularly review a policy and process for Work From Home (WFH)/Remote Workers, in accordance with local laws, regulations, and agreements, and apply the following MPA Content Security Best Practices, tailored to WFH/Remote Workers: <ul style="list-style-type: none"> Authentication (TS-1.6) Authorization (TS-1.7) Background Screening (OR-3.0) Business Continuity Plan (OR-1.2) Endpoint Protection (TS-1.3) Identity Access Management (TS-1.8) On-boarding (OR-3.1) Off-boarding (OR-3.2) Remote Sites & Locations (OR-2.1) Risk Management (OR-2.0) Training & Awareness Program (OR-3.3) Wireless Networks (TS-2.11) 	Functional	Intersects With	Work From Anywhere (WFA) - Telecommuting Security	NET-14.5	Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers.	8	<ul style="list-style-type: none"> Apply Incident Response Best Practices (OR-4.0) For on-boarding, confidentiality agreements for other members at the remote location (e.g., roommate, spouse, etc.) per client requirements Maintain a list of authorized remote access users Regularly review user list for discrepancies and unusual or suspicious activity Disconnect wireless networks while accessing content locally Training includes permissible working locations (e.g., non-public spaces, areas where content is visible to unauthorized parties, etc.) Change default credentials on home networking equipment for sensitive content and data, per client requirements Apply Alarm System Best Practices (PS-1.4) Apply Camera System Best Practices (PS-3.0) Apply Entry/Exit Points Best Practices (PS-3.0)
OP-21	Remote Sites & Locations	Establish and regularly review a policy and process to secure Remote Sites & Locations, and apply the following MPA Content Security Best Practices: <ul style="list-style-type: none"> Disaster Recovery Plan (OR-1.3) Entry/Exit Points (PS-1.0) Remote Access (TS-2.9) 	Functional	Intersects With	Alternate Storage & Processing Sites	BCD-04.2	Mechanisms exist to test contingency plans at alternate storage & processing sites to both familiarize contingency personnel with the facility and evaluate the capabilities of the alternate processing site to support contingency operations.	5	<ul style="list-style-type: none"> For sensitive content and data: Restrict unauthorized access to content from others at the remote working location Attach privacy screens to monitors where content or sensitive information is visible to unauthorized parties Apply Tracking Best Practices (OR-3.0) Apply Alarm System Best Practices (PS-1.4) Apply Camera System Best Practices (PS-3.0)
OP-21	Remote Sites & Locations	Establish and regularly review a policy and process to secure Remote Sites & Locations, and apply the following MPA Content Security Best Practices: <ul style="list-style-type: none"> Disaster Recovery Plan (OR-1.3) Entry/Exit Points (PS-1.0) Remote Access (TS-2.9) 	Functional	Intersects With	Alternate Storage Site	BCD-08	Mechanisms exist to establish an alternate storage site that includes both the assets and necessary agreements to permit the storage and recovery of system backup information.	5	<ul style="list-style-type: none"> For sensitive content and data: Restrict unauthorized access to content from others at the remote working location Attach privacy screens to monitors where content or sensitive information is visible to unauthorized parties Apply Tracking Best Practices (OR-3.0) Apply Alarm System Best Practices (PS-1.4) Apply Camera System Best Practices (PS-3.0)
OP-21	Remote Sites & Locations	Establish and regularly review a policy and process to secure Remote Sites & Locations, and apply the following MPA Content Security Best Practices: <ul style="list-style-type: none"> Disaster Recovery Plan (OR-1.3) Entry/Exit Points (PS-1.0) Remote Access (TS-2.9) 	Functional	Intersects With	Alternate Processing Site	BCD-09	Mechanisms exist to establish an alternate processing site that provides security measures equivalent to that of the primary site.	5	<ul style="list-style-type: none"> For sensitive content and data: Restrict unauthorized access to content from others at the remote working location Attach privacy screens to monitors where content or sensitive information is visible to unauthorized parties Apply Tracking Best Practices (OR-3.0) Apply Alarm System Best Practices (PS-1.4) Apply Camera System Best Practices (PS-3.0)
OP-21	Remote Sites & Locations	Establish and regularly review a policy and process to secure Remote Sites & Locations, and apply the following MPA Content Security Best Practices: <ul style="list-style-type: none"> Disaster Recovery Plan (OR-1.3) Entry/Exit Points (PS-1.0) Remote Access (TS-2.9) 	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	<ul style="list-style-type: none"> For sensitive content and data: Restrict unauthorized access to content from others at the remote working location Attach privacy screens to monitors where content or sensitive information is visible to unauthorized parties Apply Tracking Best Practices (OR-3.0) Apply Alarm System Best Practices (PS-1.4) Apply Camera System Best Practices (PS-3.0)
OP-21	Remote Sites & Locations	Establish and regularly review a policy and process to secure Remote Sites & Locations, and apply the following MPA Content Security Best Practices: <ul style="list-style-type: none"> Disaster Recovery Plan (OR-1.3) Entry/Exit Points (PS-1.0) Remote Access (TS-2.9) 	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5	<ul style="list-style-type: none"> For sensitive content and data: Restrict unauthorized access to content from others at the remote working location Attach privacy screens to monitors where content or sensitive information is visible to unauthorized parties Apply Tracking Best Practices (OR-3.0) Apply Alarm System Best Practices (PS-1.4) Apply Camera System Best Practices (PS-3.0)
OP-21	Remote Sites & Locations	Establish and regularly review a policy and process to secure Remote Sites & Locations, and apply the following MPA Content Security Best Practices: <ul style="list-style-type: none"> Disaster Recovery Plan (OR-1.3) Entry/Exit Points (PS-1.0) Remote Access (TS-2.9) 	Functional	Intersects With	Alternate Work Site	PES-11	Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.	5	<ul style="list-style-type: none"> For sensitive content and data: Restrict unauthorized access to content from others at the remote working location Attach privacy screens to monitors where content or sensitive information is visible to unauthorized parties Apply Tracking Best Practices (OR-3.0) Apply Alarm System Best Practices (PS-1.4) Apply Camera System Best Practices (PS-3.0)
OP-30	Tracking	Establish and regularly review a Tracking process for physical and/or digital client assets, to include the following: <ul style="list-style-type: none"> Leverage a content asset management system Utilize a unique asset identifier (e.g., barcode, unique ID, etc.) to include the location, time, and date of each asset transaction Retain transaction logs for at least one year, or the maximum time allowed, in accordance with local laws, regulations, and agreements 	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	<ul style="list-style-type: none"> Regularly review transaction logs for anomalies Watermark assets per client requirements (e.g., spoiling, visible, forensic, etc.)
OP-30	Tracking	Establish and regularly review a Tracking process for physical and/or digital client assets, to include the following: <ul style="list-style-type: none"> Leverage a content asset management system Utilize a unique asset identifier (e.g., barcode, unique ID, etc.) to include the location, time, and date of each asset transaction Retain transaction logs for at least one year, or the maximum time allowed, in accordance with local laws, regulations, and agreements 	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: <ol style="list-style-type: none"> Accurately reflects the current TAASD in use; Identifies authorized software products, including business justification details; Is at the level of granularity deemed necessary for tracking and reporting; Includes organizational information deemed necessary to achieve effective property accountability; and Is available for review and audit by designated organizational personnel. 	3	<ul style="list-style-type: none"> Regularly review transaction logs for anomalies Watermark assets per client requirements (e.g., spoiling, visible, forensic, etc.)
OP-30	Tracking	Establish and regularly review a Tracking process for physical and/or digital client assets, to include the following: <ul style="list-style-type: none"> Leverage a content asset management system Utilize a unique asset identifier (e.g., barcode, unique ID, etc.) to include the location, time, and date of each asset transaction Retain transaction logs for at least one year, or the maximum time allowed, in accordance with local laws, regulations, and agreements 	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	<ul style="list-style-type: none"> Regularly review transaction logs for anomalies Watermark assets per client requirements (e.g., spoiling, visible, forensic, etc.)
OP-30	Tracking	Establish and regularly review a Tracking process for physical and/or digital client assets, to include the following: <ul style="list-style-type: none"> Leverage a content asset management system Utilize a unique asset identifier (e.g., barcode, unique ID, etc.) to include the location, time, and date of each asset transaction Retain transaction logs for at least one year, or the maximum time allowed, in accordance with local laws, regulations, and agreements 	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	5	<ul style="list-style-type: none"> Regularly review transaction logs for anomalies Watermark assets per client requirements (e.g., spoiling, visible, forensic, etc.)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Relationship	STRM Relationship	SCF Control	SCF #	Security Controls Framework (SCF) Control Description	Strength of Relationship	Notes
OP-3.0	Tracking	Establish and regularly review a Tracking process for physical and/or digital client assets, to include the following: • Leverage a content asset management system • Filter a unique asset identifier (e.g., barcode, unique ID, etc.) to include the location, time, and date of each asset transaction • Retain transaction logs for at least one year, or the maximum time allowed, in accordance with local laws, regulations, and agreements	Functional	Intersects With	Sensitive / Regulated Media Records	DCH-01.3	Mechanisms exist to ensure media records for sensitive/regulated data contain sufficient information to determine the potential impact in the event of a data loss incident.	5	• Regularly review transaction logs for anomalies • Watermark assets per client requirements (e.g., spooling, visible, forensic, etc.)
OP-3.0	Tracking	Establish and regularly review a Tracking process for physical and/or digital client assets, to include the following: • Leverage a content asset management system • Filter a unique asset identifier (e.g., barcode, unique ID, etc.) to include the location, time, and date of each asset transaction • Retain transaction logs for at least one year, or the maximum time allowed, in accordance with local laws, regulations, and agreements	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	• Regularly review transaction logs for anomalies • Watermark assets per client requirements (e.g., spooling, visible, forensic, etc.)
OP-3.1	High-Security Titles	Establish and regularly review a process to support the handling of content for client-classified High-Security Titles, to include the following: • Assets (e.g., AKA, working title, code name, etc.) • Access limited to only authorized personnel • Individual NDA/Confidentiality Agreements • Use of mobile devices is only used for business purposes, unless client approved	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	• Use client-assigned security title aliases on assets and in asset tracking systems including life cycle management (e.g., handling of alias pre- vs. post-release) • Communications do not include both project alias and client title together (e.g., emails, memos, etc.) • Use of separate network (i.e., physical or logical segmentation) • A dedicated partition on shared storage • Store physical assets for High-Security Titles (e.g., scripts, art, external hard drives, etc.) in a secured area while not in use • For aliases, use a generic alias that does not reference anything that might hint at the actual project or production name (e.g., characters, locations, genre, etc.) • If aliases are used on any production signage, use generic signage that does not contain any artwork that might hint at the actual project or production name
OP-3.1	High-Security Titles	Establish and regularly review a process to support the handling of content for client-classified High-Security Titles, to include the following: • Assets (e.g., AKA, working title, code name, etc.) • Access limited to only authorized personnel • Individual NDA/Confidentiality Agreements • Use of mobile devices is only used for business purposes, unless client approved	Functional	Intersects With	Defining Access Authorizations for Sensitive / Regulated Data	DCH-01.4	Mechanisms exist to explicitly define authorizations for specific individuals and/or titles for logical and/or physical access to sensitive/regulated data.	8	• Use client-assigned security title aliases on assets and in asset tracking systems including life cycle management (e.g., handling of alias pre- vs. post-release) • Communications do not include both project alias and client title together (e.g., emails, memos, etc.) • Use of separate network (i.e., physical or logical segmentation) • A dedicated partition on shared storage • Store physical assets for High-Security Titles (e.g., scripts, art, external hard drives, etc.) in a secured area while not in use • For aliases, use a generic alias that does not reference anything that might hint at the actual project or production name (e.g., characters, locations, genre, etc.) • If aliases are used on any production signage, use generic signage that does not contain any artwork that might hint at the actual project or production name
OP-3.1	High-Security Titles	Establish and regularly review a process to support the handling of content for client-classified High-Security Titles, to include the following: • Assets (e.g., AKA, working title, code name, etc.) • Access limited to only authorized personnel • Individual NDA/Confidentiality Agreements • Use of mobile devices is only used for business purposes, unless client approved	Functional	Intersects With	Code Names	DCH-23.9	Mechanisms exist to use aliases to name assets, which are mission-critical and/or contain highly sensitive/regulated data, are unique and not readily associated with a product, project or type of data.	8	• Use client-assigned security title aliases on assets and in asset tracking systems including life cycle management (e.g., handling of alias pre- vs. post-release) • Communications do not include both project alias and client title together (e.g., emails, memos, etc.) • Use of separate network (i.e., physical or logical segmentation) • A dedicated partition on shared storage • Store physical assets for High-Security Titles (e.g., scripts, art, external hard drives, etc.) in a secured area while not in use • For aliases, use a generic alias that does not reference anything that might hint at the actual project or production name (e.g., characters, locations, genre, etc.) • If aliases are used on any production signage, use generic signage that does not contain any artwork that might hint at the actual project or production name
OP-3.2	Destruction	Establish and regularly review a process for the Destruction of stock/client assets (e.g., discs, storyboards, scripts, hard drives, data files, etc.) to include the following: • Segregation of duties between asset handler/creator and personnel performing the destruction of assets • Store assets in a secure location/container prior to destruction • Erase, degauss, shred, or destroy prior to physical disposal	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	• Destruction is performed on-site • Destruction is supervised by company personnel, including a sign-off • When using a third-party company for Destruction, obtain a Certificate of Destruction (CoD) • Maintain destruction logs for at least one year • Shred bins are locked with openings small enough that a hand cannot fit inside • Restrict keys to shred bins to authorized personnel only • Maintain destruction logs for at least one year • For hardware (e.g., laptops, servers, etc.), utilize corporate IT Asset Disposition standards • Reference U.S. Department of Defense 5220.22-M & NIST SP 800-88 for data wiping standards
OP-3.2	Destruction	Establish and regularly review a process for the Destruction of stock/client assets (e.g., discs, storyboards, scripts, hard drives, data files, etc.) to include the following: • Segregation of duties between asset handler/creator and personnel performing the destruction of assets • Store assets in a secure location/container prior to destruction • Erase, degauss, shred, or destroy prior to physical disposal	Functional	Intersects With	Media Storage	DCH-06	Mechanisms exist to: 1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures, and 2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	5	• Destruction is performed on-site • Destruction is supervised by company personnel, including a sign-off • When using a third-party company for Destruction, obtain a Certificate of Destruction (CoD) • Complete Destruction within 30 days • Shred bins are locked with openings small enough that a hand cannot fit inside • Restrict keys to shred bins to authorized personnel only • Maintain destruction logs for at least one year • For hardware (e.g., laptops, servers, etc.), utilize corporate IT Asset Disposition standards • Reference U.S. Department of Defense 5220.22-M & NIST SP 800-88 for data wiping standards
OP-3.2	Destruction	Establish and regularly review a process for the Destruction of stock/client assets (e.g., discs, storyboards, scripts, hard drives, data files, etc.) to include the following: • Segregation of duties between asset handler/creator and personnel performing the destruction of assets • Store assets in a secure location/container prior to destruction • Erase, degauss, shred, or destroy prior to physical disposal	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	• Destruction is performed on-site • Destruction is supervised by company personnel, including a sign-off • When using a third-party company for Destruction, obtain a Certificate of Destruction (CoD) • Complete Destruction within 30 days • Shred bins are locked with openings small enough that a hand cannot fit inside • Restrict keys to shred bins to authorized personnel only • Maintain destruction logs for at least one year • For hardware (e.g., laptops, servers, etc.), utilize corporate IT Asset Disposition standards • Reference U.S. Department of Defense 5220.22-M & NIST SP 800-88 for data wiping standards
OP-3.2	Destruction	Establish and regularly review a process for the Destruction of stock/client assets (e.g., discs, storyboards, scripts, hard drives, data files, etc.) to include the following: • Segregation of duties between asset handler/creator and personnel performing the destruction of assets • Store assets in a secure location/container prior to destruction • Erase, degauss, shred, or destroy prior to physical disposal	Functional	Intersects With	Separation of Duties (SoD)	HR5-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5	• Destruction is performed on-site • Destruction is supervised by company personnel, including a sign-off • When using a third-party company for Destruction, obtain a Certificate of Destruction (CoD) • Complete Destruction within 30 days • Shred bins are locked with openings small enough that a hand cannot fit inside • Restrict keys to shred bins to authorized personnel only • Maintain destruction logs for at least one year • For hardware (e.g., laptops, servers, etc.), utilize corporate IT Asset Disposition standards • Reference U.S. Department of Defense 5220.22-M & NIST SP 800-88 for data wiping standards
PS-1.0	Entry/Exit Points	Establish and regularly review a process to physically secure all Entry/Exit Points, to include the following: • Apply to server room, screening room, loading docks, etc. • Access control segmentation between other businesses and tenants • Secure and cover ground floor windows where content could be visible from the outside	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility designated as publicly accessible).	8	• Access control segmentation between content areas and other parts of the facility (e.g., administrative offices, waiting rooms, loading docks, courier pickup and drop-off areas, replication, mastering, etc.) • Attach privacy screens to monitors where content or sensitive information is visible to unauthorized parties • For signage utilized at the facility or remote site/location, use generic signage that does not contain any artwork that might hint at the actual project or production name
PS-1.0	Entry/Exit Points	Establish and regularly review a process to physically secure all Entry/Exit Points, to include the following: • Apply to server room, screening room, loading docks, etc. • Access control segmentation between other businesses and tenants • Secure and cover ground floor windows where content could be visible from the outside	Functional	Intersects With	Controlled Ingress & Egress Points	PES-03.1	Physical access control mechanisms exist to limit and monitor physical access through controlled ingress and egress points.	8	• Access control segmentation between content areas and other parts of the facility (e.g., administrative offices, waiting rooms, loading docks, courier pickup and drop-off areas, replication, mastering, etc.) • Attach privacy screens to monitors where content or sensitive information is visible to unauthorized parties • For signage utilized at the facility or remote site/location, use generic signage that does not contain any artwork that might hint at the actual project or production name
PS-1.0	Entry/Exit Points	Establish and regularly review a process to physically secure all Entry/Exit Points, to include the following: • Apply to server room, screening room, loading docks, etc. • Access control segmentation between other businesses and tenants • Secure and cover ground floor windows where content could be visible from the outside	Functional	Intersects With	Access To Critical Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical systems or sensitive/regulated data, in addition to the physical access controls for the facility.	8	• Access control segmentation between content areas and other parts of the facility (e.g., administrative offices, waiting rooms, loading docks, courier pickup and drop-off areas, replication, mastering, etc.) • Attach privacy screens to monitors where content or sensitive information is visible to unauthorized parties • For signage utilized at the facility or remote site/location, use generic signage that does not contain any artwork that might hint at the actual project or production name
PS-1.0	Entry/Exit Points	Establish and regularly review a process to physically secure all Entry/Exit Points, to include the following: • Apply to server room, screening room, loading docks, etc. • Access control segmentation between other businesses and tenants • Secure and cover ground floor windows where content could be visible from the outside	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	8	• Access control segmentation between content areas and other parts of the facility (e.g., administrative offices, waiting rooms, loading docks, courier pickup and drop-off areas, replication, mastering, etc.) • Attach privacy screens to monitors where content or sensitive information is visible to unauthorized parties • For signage utilized at the facility or remote site/location, use generic signage that does not contain any artwork that might hint at the actual project or production name
PS-1.0	Entry/Exit Points	Establish and regularly review a process to physically secure all Entry/Exit Points, to include the following: • Apply to server room, screening room, loading docks, etc. • Access control segmentation between other businesses and tenants • Secure and cover ground floor windows where content could be visible from the outside	Functional	Intersects With	Working In Secure Areas	PES-04.1	Physical security mechanisms exist to allow only authorized personnel access to secure areas.	5	• Access control segmentation between content areas and other parts of the facility (e.g., administrative offices, waiting rooms, loading docks, courier pickup and drop-off areas, replication, mastering, etc.) • Attach privacy screens to monitors where content or sensitive information is visible to unauthorized parties • For signage utilized at the facility or remote site/location, use generic signage that does not contain any artwork that might hint at the actual project or production name
PS-1.0	Entry/Exit Points	Establish and regularly review a process to physically secure all Entry/Exit Points, to include the following: • Apply to server room, screening room, loading docks, etc. • Access control segmentation between other businesses and tenants • Secure and cover ground floor windows where content could be visible from the outside	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	8	• Access control segmentation between content areas and other parts of the facility (e.g., administrative offices, waiting rooms, loading docks, courier pickup and drop-off areas, replication, mastering, etc.) • Attach privacy screens to monitors where content or sensitive information is visible to unauthorized parties • For signage utilized at the facility or remote site/location, use generic signage that does not contain any artwork that might hint at the actual project or production name
PS-1.1	Visitors	Establish a process for Visitors who have access to high-security areas, to include the following: • Visitor logs • Retain visitor logs for one year at a minimum, or the maximum time allowed, in accordance with local laws, regulations, and agreements • Verification of identity via valid government-issued photo (e.g., driver's license, passport, etc.) • NDA/Confidentiality Agreement for Visitors per client requirements	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	8	• Visitor logs to capture name, company, entry/exit time, reason for visit, person(s) visiting, and signature of Visitor • Visitors are issued a badge/identifier • Conceal the names of previous Visitors in logs • Make Visitor badge/identifiers easily distinguishable from company personnel badges • Visitor badge/identifiers are surrendered before leaving the facility • Communicate restrictions of recording/photographing content on premises • Visitors are accompanied by an authorized employee according to security considerations
PS-1.1	Visitors	Establish a process for Visitors who have access to high-security areas, to include the following: • Visitor logs • Retain visitor logs for one year at a minimum, or the maximum time allowed, in accordance with local laws, regulations, and agreements • Verification of identity via valid government-issued photo (e.g., driver's license, passport, etc.) • NDA/Confidentiality Agreement for Visitors per client requirements	Functional	Intersects With	Physical Access Logs	PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	8	• Visitor logs to capture name, company, entry/exit time, reason for visit, person(s) visiting, and signature of Visitor • Visitors are issued a badge/identifier • Conceal the names of previous Visitors in logs • Make Visitor badge/identifiers easily distinguishable from company personnel badges • Visitor badge/identifiers are surrendered before leaving the facility • Communicate restrictions of recording/photographing content on premises • Visitors are accompanied by an authorized employee according to security considerations

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Relationship	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
PS-1.1	Visitors	Establish a process for Visitors who have access to high-security areas, to include the following: <ul style="list-style-type: none"> Visitor log Return visitor log(s) for one year at a minimum, or the maximum time allowed, in accordance with local laws, regulations, and agreements Verification of identity via valid government-issued photo ID (e.g., driver's license, passport, etc.) NDA/Confidentiality Agreement for visitors per client requirements 	Functional	Intersects With	Visitor Control	PE5-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	<ul style="list-style-type: none"> Visitor log(s) to capture: name, company, entry/exit time, reason for visit, personal visiting, and signature of visitor Visitors are issued a badge/visitor Control the names of previous visitors in logs Make Visitor badge/visitors easily distinguishable from company personnel badges Visitor badge/visitors are surrendered before leaving the facility Communicate restrictions of recording/photographing content on premises Visitors are accompanied by an authorized employee according to security considerations
PS-1.1	Visitors	Establish a process for Visitors who have access to high-security areas, to include the following: <ul style="list-style-type: none"> Visitor log Return visitor log(s) for one year at a minimum, or the maximum time allowed, in accordance with local laws, regulations, and agreements Verification of identity via valid government-issued photo ID (e.g., driver's license, passport, etc.) NDA/Confidentiality Agreement for visitors per client requirements 	Functional	Intersects With	Identification Requirement	PE5-02	Physical access control mechanisms exist to require at least one(1) form of government issued or organization-issued photo identification to authenticate individuals before they can gain access to the facility.	5	<ul style="list-style-type: none"> Visitor log(s) to capture: name, company, entry/exit time, reason for visit, personal visiting, and signature of visitor Visitors are issued a badge/visitor Control the names of previous visitors in logs Make Visitor badge/visitors easily distinguishable from company personnel badges Visitor badge/visitors are surrendered before leaving the facility Communicate restrictions of recording/photographing content on premises Visitors are accompanied by an authorized employee according to security considerations
PS-1.1	Visitors	Establish a process for Visitors who have access to high-security areas, to include the following: <ul style="list-style-type: none"> Visitor log Return visitor log(s) for one year at a minimum, or the maximum time allowed, in accordance with local laws, regulations, and agreements Verification of identity via valid government-issued photo ID (e.g., driver's license, passport, etc.) NDA/Confidentiality Agreement for visitors per client requirements 	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PE5-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	5	<ul style="list-style-type: none"> Visitor log(s) to capture: name, company, entry/exit time, reason for visit, personal visiting, and signature of visitor Visitors are issued a badge/visitor Control the names of previous visitors in logs Make Visitor badge/visitors easily distinguishable from company personnel badges Visitor badge/visitors are surrendered before leaving the facility Communicate restrictions of recording/photographing content on premises Visitors are accompanied by an authorized employee according to security considerations
PS-1.1	Visitors	Establish a process for Visitors who have access to high-security areas, to include the following: <ul style="list-style-type: none"> Visitor log Return visitor log(s) for one year at a minimum, or the maximum time allowed, in accordance with local laws, regulations, and agreements Verification of identity via valid government-issued photo ID (e.g., driver's license, passport, etc.) NDA/Confidentiality Agreement for visitors per client requirements 	Functional	Intersects With	Working in Secure Areas	PE5-04.1	Physical security mechanisms exist to allow only authorized personnel access to secure areas.	5	<ul style="list-style-type: none"> Visitor log(s) to capture: name, company, entry/exit time, reason for visit, personal visiting, and signature of visitor Visitors are issued a badge/visitor Control the names of previous visitors in logs Make Visitor badge/visitors easily distinguishable from company personnel badges Visitor badge/visitors are surrendered before leaving the facility Communicate restrictions of recording/photographing content on premises Visitors are accompanied by an authorized employee according to security considerations
PS-1.2	Electronic Access Control	Establish and regularly review a process to apply Electronic Access Control (EAC) to cover all high-security areas, to include the following: <ul style="list-style-type: none"> Designate personnel to authorize access Assign electronic access to specific areas based on job function and responsibilities (e.g., vault, server/machine room, etc.) Restrict Electronic Access system administration to appropriate personnel Keep a log that ties the device (e.g., badge, keycard/ID, etc.) to personnel Store and manage badge and keycard/ID stock securely Deploy Electronic Access Control system on a dedicated network 	Functional	Intersects With	Physical Access Authorizations	PE5-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5	<ul style="list-style-type: none"> Set third-party (e.g., consultant, contractor, etc.) to approved timeframe with expiration date (e.g., 90 days) Log access rights changes
PS-1.2	Electronic Access Control	Establish and regularly review a process to apply Electronic Access Control (EAC) to cover all high-security areas, to include the following: <ul style="list-style-type: none"> Designate personnel to authorize access Assign electronic access to specific areas based on job function and responsibilities (e.g., vault, server/machine room, etc.) Restrict Electronic Access system administration to appropriate personnel Keep a log that ties the device (e.g., badge, keycard/ID, etc.) to personnel Store and manage badge and keycard/ID stock securely Deploy Electronic Access Control system on a dedicated network 	Functional	Intersects With	Physical Access Control	PE5-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	<ul style="list-style-type: none"> Set third-party (e.g., consultant, contractor, etc.) to approved timeframe with expiration date (e.g., 90 days) Log access rights changes
PS-1.2	Electronic Access Control	Establish and regularly review a process to apply Electronic Access Control (EAC) to cover all high-security areas, to include the following: <ul style="list-style-type: none"> Designate personnel to authorize access Assign electronic access to specific areas based on job function and responsibilities (e.g., vault, server/machine room, etc.) Restrict Electronic Access system administration to appropriate personnel Keep a log that ties the device (e.g., badge, keycard/ID, etc.) to personnel Store and manage badge and keycard/ID stock securely Deploy Electronic Access Control system on a dedicated network 	Functional	Intersects With	Controlled Ingress & Egress Points	PE5-03.1	Physical access control mechanisms exist to limit and monitor physical access through controlled ingress and egress points.	5	<ul style="list-style-type: none"> Set third-party (e.g., consultant, contractor, etc.) to approved timeframe with expiration date (e.g., 90 days) Log access rights changes
PS-1.2	Electronic Access Control	Establish and regularly review a process to apply Electronic Access Control (EAC) to cover all high-security areas, to include the following: <ul style="list-style-type: none"> Designate personnel to authorize access Assign electronic access to specific areas based on job function and responsibilities (e.g., vault, server/machine room, etc.) Restrict Electronic Access system administration to appropriate personnel Keep a log that ties the device (e.g., badge, keycard/ID, etc.) to personnel Store and manage badge and keycard/ID stock securely Deploy Electronic Access Control system on a dedicated network 	Functional	Intersects With	Physical Access Logs	PE5-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	5	<ul style="list-style-type: none"> Set third-party (e.g., consultant, contractor, etc.) to approved timeframe with expiration date (e.g., 90 days) Log access rights changes
PS-1.3	Electronic Access Control Logging & Monitoring	Establish and regularly review a process for Electronic Access Control Logging & Monitoring, to include the following: <ul style="list-style-type: none"> System enabled logging Return logs for one year at a minimum, or the maximum time allowed, in accordance with local laws, regulations, and agreements 	Functional	Intersects With	Media & Data Retention	DC1-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	<ul style="list-style-type: none"> Automated alerts for suspicious or unusual events for restricted areas Escalation procedures to appropriate personnel Regularly review logs for discrepancies
PS-1.3	Electronic Access Control Logging & Monitoring	Establish and regularly review a process for Electronic Access Control Logging & Monitoring, to include the following: <ul style="list-style-type: none"> System enabled logging Return logs for one year at a minimum, or the maximum time allowed, in accordance with local laws, regulations, and agreements 	Functional	Intersects With	Physical Access Logs	PE5-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	5	<ul style="list-style-type: none"> Automated alerts for suspicious or unusual events for restricted areas Escalation procedures to appropriate personnel Regularly review logs for discrepancies
PS-1.4	Alarm System	Install and maintain an Alarm System that covers all entry/exit points to high-security areas (including emergency exits), windows, loading docks, fire escapes, and restricted areas (e.g., vault, server/machine room, etc.) to include the following: <ul style="list-style-type: none"> Enable the alarm when facility is unattended Automated alerts of each unauthorized/failed attempt including when physical keys are used to override electronic access controls Escalation configurations and/or procedures to appropriate personnel Issue unique alarm codes and administrator rights to authorized individuals Regularly review users Regularly test Alarm System 	Functional	Intersects With	Monitoring Physical Access	PE5-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	5	<ul style="list-style-type: none"> Log every alarm state change (e.g., Set change to Unset), the time, and the individual that triggered the change Install Alarm System in all areas of the facility, including non-high-security areas High security and all areas processing or handling content: Motion sensors Door pro-alerts
PS-1.4	Alarm System	Install and maintain an Alarm System that covers all entry/exit points to high-security areas (including emergency exits), windows, loading docks, fire escapes, and restricted areas (e.g., vault, server/machine room, etc.) to include the following: <ul style="list-style-type: none"> Enable the alarm when facility is unattended Automated alerts of each unauthorized/failed attempt including when physical keys are used to override electronic access controls Escalation configurations and/or procedures to appropriate personnel Issue unique alarm codes and administrator rights to authorized individuals Regularly review users Regularly test Alarm System 	Functional	Intersects With	Intrusion Alarms / Surveillance Equipment	PE5-05.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	5	<ul style="list-style-type: none"> Log every alarm state change (e.g., Set change to Unset), the time, and the individual that triggered the change Install Alarm System in all areas of the facility, including non-high-security areas High security and all areas processing or handling content: Motion sensors Door pro-alerts
PS-1.4	Alarm System	Install and maintain an Alarm System that covers all entry/exit points to high-security areas (including emergency exits), windows, loading docks, fire escapes, and restricted areas (e.g., vault, server/machine room, etc.) to include the following: <ul style="list-style-type: none"> Enable the alarm when facility is unattended Automated alerts of each unauthorized/failed attempt including when physical keys are used to override electronic access controls Escalation configurations and/or procedures to appropriate personnel Issue unique alarm codes and administrator rights to authorized individuals Regularly review users Regularly test Alarm System 	Functional	Intersects With	Monitoring Physical Access To Critical Systems	PE5-05.2	Facility security mechanisms exist to monitor physical access to critical systems or sensitive/regarded data, in addition to the physical access monitoring of the facility.	5	<ul style="list-style-type: none"> Log every alarm state change (e.g., Set change to Unset), the time, and the individual that triggered the change Install Alarm System in all areas of the facility, including non-high-security areas High security and all areas processing or handling content: Motion sensors Door pro-alerts
PS-1.5	Keys	Establish and regularly review a process to manage the distribution of physical keys to restricted areas to authorized personnel only (e.g., owner, facilities management, etc.) to include the following: <ul style="list-style-type: none"> A check-in/check-out process for master keys to track and monitor distribution Maintain and regularly review a list of company personnel who are allowed to check out master keys Regular inventory checks of physical keys and master keys Store all keys in a safe location (e.g., lockbox or safe) Change the locks when keys to restricted areas cannot be accounted for 	Functional	Subst Of	Physical & Environmental Protections	PE5-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	<ul style="list-style-type: none"> A check-in/check-out process for non-master keys to track and monitor distribution
PS-2.0	Replication Facilities	Establish and regularly review a policy and process for Replication Facilities, to include the following: <ul style="list-style-type: none"> Perform searches of persons, bags, packages, and personal belongings for content/assets Perform searches at key entry/exit points Regular audit to test validity of processes In accordance with local laws, regulations, and agreements 	Functional	Intersects With	Searches	PE5-04.2	Physical access control mechanisms exist to inspect personnel and their personal effects (e.g., personal property ordinarily worn or carried by the individual, including vehicles) to prevent the unauthorized exfiltration of data and technology assets.	8	<ul style="list-style-type: none"> Restrict recording/storage devices (e.g., USB thumb drives, cameras, mobile phones, etc.) in high-security areas Use transparent bags and containers Document any incidents that occur
PS-3.0	Camera System	Install and maintain a Camera System that covers all entry/exit points to high-security areas (including emergency exits), windows, loading docks, fire escapes, and restricted areas (e.g., vault, server/machine room, etc.) to include the following: <ul style="list-style-type: none"> Restrict access to the surveillance camera console and camera equipment (e.g., DVRs, NVRs, etc.) to authorized personnel only Configure cameras to capture adequate coverage of recorded areas, image quality, lighting, date and time stamps, frame rate, etc. Return footage in a secure location for at least 90 days, or the maximum time allowed, in accordance with local laws, regulations, and agreements 	Functional	Intersects With	Media & Data Retention	DC1-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	<ul style="list-style-type: none"> Discretely hide all camera cables and wiring from view and keep out of reach Avoid capturing content on displays Monitor footage during operating hours and immediately investigate detected security incidents Test surveillance equipment regularly Verify surveillance equipment functions properly, including an uninterruptible power supply All cameras provided by the building or landlord are adequate and footage is accessible Install cameras in all areas of the facility, including non-high-security areas
PS-3.0	Camera System	Install and maintain a Camera System that covers all entry/exit points to high-security areas (including emergency exits), windows, loading docks, fire escapes, and restricted areas (e.g., vault, server/machine room, etc.) to include the following: <ul style="list-style-type: none"> Restrict access to the surveillance camera console and camera equipment (e.g., DVRs, NVRs, etc.) to authorized personnel only Configure cameras to capture adequate coverage of recorded areas, image quality, lighting, date and time stamps, frame rate, etc. Return footage in a secure location for at least 90 days, or the maximum time allowed, in accordance with local laws, regulations, and agreements 	Functional	Intersects With	Intrusion Alarms / Surveillance Equipment	PE5-05.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	5	<ul style="list-style-type: none"> Discretely hide all camera cables and wiring from view and keep out of reach Avoid capturing content on displays Monitor footage during operating hours and immediately investigate detected security incidents Test surveillance equipment regularly Verify surveillance equipment functions properly, including an uninterruptible power supply All cameras provided by the building or landlord are adequate and footage is accessible Install cameras in all areas of the facility, including non-high-security areas
PS-3.1	Environmental Controls	Install and regularly review Environmental Controls for facilities that contain servers, storage devices, LAN equipment, network communications devices, and storage media, to include the following: <ul style="list-style-type: none"> Maintain ideal temperature and humidity settings Alerting system for temperatures and humidity levels beyond the set parameters 	Functional	Intersects With	Supporting Utilities	PE5-07	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.	5	<p>Environmental Control settings (range):</p> <ul style="list-style-type: none"> Temperature (Low End): 64.4 degrees F (18 degrees C) or above Temperature (High End): 80.6 degrees F (27 degrees C) or below Moisture (Low End): 40% relative humidity and 41.9 degrees F (5.3 degrees C) dew point or above Moisture (High End): 60% relative humidity and 59 degrees F (15 degrees C) dew point or below
PS-3.1	Environmental Controls	Install and regularly review Environmental Controls for facilities that contain servers, storage devices, LAN equipment, network communications devices, and storage media, to include the following: <ul style="list-style-type: none"> Maintain ideal temperature and humidity settings Alerting system for temperatures and humidity levels beyond the set parameters 	Functional	Intersects With	Automatic Voltage Controls	PE5-07.1	Facility security mechanisms exist to utilize automatic voltage controls for critical system components.	5	<p>Environmental Control settings (range):</p> <ul style="list-style-type: none"> Temperature (Low End): 64.4 degrees F (18 degrees C) or above Temperature (High End): 80.6 degrees F (27 degrees C) or below Moisture (Low End): 40% relative humidity and 41.9 degrees F (5.3 degrees C) dew point or above Moisture (High End): 60% relative humidity and 59 degrees F (15 degrees C) dew point or below
PS-3.1	Environmental Controls	Install and regularly review Environmental Controls for facilities that contain servers, storage devices, LAN equipment, network communications devices, and storage media, to include the following: <ul style="list-style-type: none"> Maintain ideal temperature and humidity settings Alerting system for temperatures and humidity levels beyond the set parameters 	Functional	Intersects With	Emergency Shutoff	PE5-07.2	Facility security mechanisms exist to shut off power in emergency situations by: <ol style="list-style-type: none"> Placing emergency shutoff switches or devices in close proximity to systems or system components to facilitate safe and easy access for personnel, and Protecting emergency power shutoff capability from unauthorized activation. 	5	<p>Environmental Control settings (range):</p> <ul style="list-style-type: none"> Temperature (Low End): 64.4 degrees F (18 degrees C) or above Temperature (High End): 80.6 degrees F (27 degrees C) or below Moisture (Low End): 40% relative humidity and 41.9 degrees F (5.3 degrees C) dew point or above Moisture (High End): 60% relative humidity and 59 degrees F (15 degrees C) dew point or below
PS-3.1	Environmental Controls	Install and regularly review Environmental Controls for facilities that contain servers, storage devices, LAN equipment, network communications devices, and storage media, to include the following: <ul style="list-style-type: none"> Maintain ideal temperature and humidity settings Alerting system for temperatures and humidity levels beyond the set parameters 	Functional	Intersects With	Emergency Power	PE5-07.3	Facility security mechanisms exist to supply alternate power, capable of maintaining minimally required operational capability, in the event of an extended loss of the primary power source.	5	<p>Environmental Control settings (range):</p> <ul style="list-style-type: none"> Temperature (Low End): 64.4 degrees F (18 degrees C) or above Temperature (High End): 80.6 degrees F (27 degrees C) or below Moisture (Low End): 40% relative humidity and 41.9 degrees F (5.3 degrees C) dew point or above Moisture (High End): 60% relative humidity and 59 degrees F (15 degrees C) dew point or below

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Relationship	STRM Relationship	SCF Control	SCF #	Security Controls Framework (SCF) Control Description	Strength of Relationship	Notes
PS-3.1	Environmental Controls	Install and regularly review Environmental Controls for facilities that contain servers, storage devices, LAN equipment, network communications devices, and storage media, to include the following: • Maintain ideal temperature and humidity settings. • Alerting system for temperatures and humidity levels beyond the set parameters	Functional	Intersects With	Emergency Lighting	PES-07.4	Facility security mechanisms exist to utilize and maintain automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	5	Environmental Control settings (range): • Temperature (Low End): 64.4 degrees F (18 degrees C) or above • Temperature (High End): 80.6 degrees F (27 degrees C) or below • Moisture (Low End): 40% relative humidity and 41.9 degrees F (5.5 degrees C) dew point or above • Moisture (High End): 60% relative humidity and 59 degrees F (15 degrees C) dew point or below
PS-3.1	Environmental Controls	Install and regularly review Environmental Controls for facilities that contain servers, storage devices, LAN equipment, network communications devices, and storage media, to include the following: • Maintain ideal temperature and humidity settings. • Alerting system for temperatures and humidity levels beyond the set parameters	Functional	Intersects With	Water Damage Protection	PES-07.5	Facility security mechanisms exist to protect systems from damage resulting from water leakage by providing master shut-off valves that are accessible, working properly and known to key personnel.	5	Environmental Control settings (range): • Temperature (Low End): 64.4 degrees F (18 degrees C) or above • Temperature (High End): 80.6 degrees F (27 degrees C) or below • Moisture (Low End): 40% relative humidity and 41.9 degrees F (5.5 degrees C) dew point or above • Moisture (High End): 60% relative humidity and 59 degrees F (15 degrees C) dew point or below
PS-3.1	Environmental Controls	Install and regularly review Environmental Controls for facilities that contain servers, storage devices, LAN equipment, network communications devices, and storage media, to include the following: • Maintain ideal temperature and humidity settings. • Alerting system for temperatures and humidity levels beyond the set parameters	Functional	Intersects With	Fire Protection	PES-08	Facility security mechanisms exist to utilize and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy source.	5	Environmental Control settings (range): • Temperature (Low End): 64.4 degrees F (18 degrees C) or above • Temperature (High End): 80.6 degrees F (27 degrees C) or below • Moisture (Low End): 40% relative humidity and 41.9 degrees F (5.5 degrees C) dew point or above • Moisture (High End): 60% relative humidity and 59 degrees F (15 degrees C) dew point or below
PS-3.1	Environmental Controls	Install and regularly review Environmental Controls for facilities that contain servers, storage devices, LAN equipment, network communications devices, and storage media, to include the following: • Maintain ideal temperature and humidity settings. • Alerting system for temperatures and humidity levels beyond the set parameters	Functional	Intersects With	Fire Detection Devices	PES-08.1	Facility security mechanisms exist to utilize and maintain fire detection devices/systems that activate automatically and notify organizational personnel and emergency responders in the event of a fire.	5	Environmental Control settings (range): • Temperature (Low End): 64.4 degrees F (18 degrees C) or above • Temperature (High End): 80.6 degrees F (27 degrees C) or below • Moisture (Low End): 40% relative humidity and 41.9 degrees F (5.5 degrees C) dew point or above • Moisture (High End): 60% relative humidity and 59 degrees F (15 degrees C) dew point or below
PS-3.1	Environmental Controls	Install and regularly review Environmental Controls for facilities that contain servers, storage devices, LAN equipment, network communications devices, and storage media, to include the following: • Maintain ideal temperature and humidity settings. • Alerting system for temperatures and humidity levels beyond the set parameters	Functional	Intersects With	Temperature & Humidity Controls	PES-09	Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.	5	Environmental Control settings (range): • Temperature (Low End): 64.4 degrees F (18 degrees C) or above • Temperature (High End): 80.6 degrees F (27 degrees C) or below • Moisture (Low End): 40% relative humidity and 41.9 degrees F (5.5 degrees C) dew point or above • Moisture (High End): 60% relative humidity and 59 degrees F (15 degrees C) dew point or below
PS-3.1	Environmental Controls	Install and regularly review Environmental Controls for facilities that contain servers, storage devices, LAN equipment, network communications devices, and storage media, to include the following: • Maintain ideal temperature and humidity settings. • Alerting system for temperatures and humidity levels beyond the set parameters	Functional	Intersects With	Monitoring with Alarms / Notifications	PES-09.1	Facility security mechanisms exist to trigger an alarm or notification of temperature and humidity changes that are potentially harmful to personnel or equipment.	5	Environmental Control settings (range): • Temperature (Low End): 64.4 degrees F (18 degrees C) or above • Temperature (High End): 80.6 degrees F (27 degrees C) or below • Moisture (Low End): 40% relative humidity and 41.9 degrees F (5.5 degrees C) dew point or above • Moisture (High End): 60% relative humidity and 59 degrees F (15 degrees C) dew point or below
PS-3.2	Data Centers, Co-location	When utilizing a Data Center and/or Co-location, provide proof via policy, procedure, or audit report documents, that the following MPA Content Security Best Practices are implemented: • Alarm System (PS-1.4) • Camera System (PS-1.0) • Contracts & Service Level Agreements (DR-3.4) • Entry/Exit Points (PS-1.0) • Environmental Controls (PS-3.1) • Incident Response (DR-2.0) • Network Topology Diagram (TS-2.2) • Risk Management (DR-2.0) • Shared Security Responsibility Model (TS-1.11) • Systems Configuration (TS-1.1) • Visitors (PS-1.1) • Vulnerability Management (TS-4.0)	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	When utilizing a Data Center and/or Co-location, provide proof via policy, procedure, or audit report documents that includes the following: • CCTV captures vendor cabinets • Cabinets are physically segregated from other tenants and Data Center employees
PS-3.2	Data Centers, Co-location	When utilizing a Data Center and/or Co-location, provide proof via policy, procedure, or audit report documents, that the following MPA Content Security Best Practices are implemented: • Alarm System (PS-1.4) • Camera System (PS-1.0) • Contracts & Service Level Agreements (DR-3.4) • Entry/Exit Points (PS-1.0) • Environmental Controls (PS-3.1) • Incident Response (DR-2.0) • Network Topology Diagram (TS-2.2) • Risk Management (DR-2.0) • Shared Security Responsibility Model (TS-1.11) • Systems Configuration (TS-1.1) • Visitors (PS-1.1) • Vulnerability Management (TS-4.0)	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8	When utilizing a Data Center and/or Co-location, provide proof via policy, procedure, or audit report documents that includes the following: • CCTV captures vendor cabinets • Cabinets are physically segregated from other tenants and Data Center employees
PS-3.2	Data Centers, Co-location	When utilizing a Data Center and/or Co-location, provide proof via policy, procedure, or audit report documents, that the following MPA Content Security Best Practices are implemented: • Alarm System (PS-1.4) • Camera System (PS-1.0) • Contracts & Service Level Agreements (DR-3.4) • Entry/Exit Points (PS-1.0) • Environmental Controls (PS-3.1) • Incident Response (DR-2.0) • Network Topology Diagram (TS-2.2) • Risk Management (DR-2.0) • Shared Security Responsibility Model (TS-1.11) • Systems Configuration (TS-1.1) • Visitors (PS-1.1) • Vulnerability Management (TS-4.0)	Functional	Intersects With	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to subcontractors.	3	When utilizing a Data Center and/or Co-location, provide proof via policy, procedure, or audit report documents that includes the following: • CCTV captures vendor cabinets • Cabinets are physically segregated from other tenants and Data Center employees
PS-3.2	Data Centers, Co-location	When utilizing a Data Center and/or Co-location, provide proof via policy, procedure, or audit report documents, that the following MPA Content Security Best Practices are implemented: • Alarm System (PS-1.4) • Camera System (PS-1.0) • Contracts & Service Level Agreements (DR-3.4) • Entry/Exit Points (PS-1.0) • Environmental Controls (PS-3.1) • Incident Response (DR-2.0) • Network Topology Diagram (TS-2.2) • Risk Management (DR-2.0) • Shared Security Responsibility Model (TS-1.11) • Systems Configuration (TS-1.1) • Visitors (PS-1.1) • Vulnerability Management (TS-4.0)	Functional	Intersects With	Third-Party Attestation (3PA)	TPM-05.8	Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractor and subcontractor.	3	When utilizing a Data Center and/or Co-location, provide proof via policy, procedure, or audit report documents that includes the following: • CCTV captures vendor cabinets • Cabinets are physically segregated from other tenants and Data Center employees
PS-3.3	Cloud Providers	When utilizing a third-party Cloud Provider, provide proof via policy, procedure, or audit report documents, that the following MPA Content Security Best Practices are implemented: • Application Configuration Guidelines (Licensed) (TS-1.17) • Application Configuration Guidelines (In-House Developed) (TS-1.18) • Authentication (TS-1.6) • Authorization (TS-1.7) • Change Control (TS-1.0) • Contracts & Service Level Agreements (DR-3.4) • Encryption (TS-3.0) • Endpoint Protection (TS-3.3) • Identity Access Management (TS-1.8) • Incident Response (DR-2.0) • Network Topology Diagram (TS-2.2) • Patching (TS-4.2) • Penetration Testing (TS-4.1) • Risk Management (DR-2.0) • Shared Security Responsibility Model (TS-1.11) • Systems Configuration (TS-1.1) • Vulnerability Management (TS-4.0) • Web Portals (TS-1.10)	Functional	Subset Of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10	When utilizing a Cloud Provider, provide proof via policy, procedure, or audit report documents that includes the following: • Regularly review user access list to the client cloud portal • Use of a Cloud Access Security Broker (CASB) to monitor and restrict cloud software usage and access • Cloud Service Providers (CSPs) provide Cloud Service Consumer (CSC) with the ability to manage their own encryption keys • Intra-tenant segregation between Cloud Service Provider (CSP) and Cloud Service Consumer (CSC) • Use of cloud hosted directory services (e.g., JumpCloud, Okta, Azure Active Directory, AWS Directory Service, etc.) • Use of exclusive, unique, or dedicated primary encryption keys to encrypt content data
PS-3.3	Cloud Providers	When utilizing a third-party Cloud Provider, provide proof via policy, procedure, or audit report documents, that the following MPA Content Security Best Practices are implemented: • Application Configuration Guidelines (Licensed) (TS-1.17) • Application Configuration Guidelines (In-House Developed) (TS-1.18) • Authentication (TS-1.6) • Authorization (TS-1.7) • Change Control (TS-1.0) • Contracts & Service Level Agreements (DR-3.4) • Encryption (TS-3.0) • Endpoint Protection (TS-3.3) • Identity Access Management (TS-1.8) • Incident Response (DR-2.0) • Network Topology Diagram (TS-2.2) • Patching (TS-4.2) • Penetration Testing (TS-4.1) • Risk Management (DR-2.0) • Shared Security Responsibility Model (TS-1.11) • Systems Configuration (TS-1.1) • Vulnerability Management (TS-4.0) • Web Portals (TS-1.10)	Functional	Intersects With	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud environments.	8	When utilizing a Cloud Provider, provide proof via policy, procedure, or audit report documents that includes the following: • Regularly review user access list to the client cloud portal • Use of a Cloud Access Security Broker (CASB) to monitor and restrict cloud software usage and access • Cloud Service Providers (CSPs) provide Cloud Service Consumer (CSC) with the ability to manage their own encryption keys • Intra-tenant segregation between Cloud Service Provider (CSP) and Cloud Service Consumer (CSC) • Use of cloud hosted directory services (e.g., JumpCloud, Okta, Azure Active Directory, AWS Directory Service, etc.) • Use of exclusive, unique, or dedicated primary encryption keys to encrypt content data
TS-1.0	Data IO Workflows & Systems	Establish and regularly review a process and workflow for Data IO Workflows & Systems to include the following: • Use dedicated (i.e., isolated) systems to move content between external networks (i.e., Internet) and internal networks (e.g., Data IO network, production, etc.) • Scan all content for viruses and malware prior to ingest onto the network • Segregation of duties between Data IO staff and other staff (e.g., production, development, etc.) • Content movement is initiated from the more secure layer (e.g., push/pull content at the Data IO zone bottom Internet; push/pull content at the production network from the Data IO zone) • Strict IP and port layer 3/3 Access Control Lists (ACLs) to allow outbound network requests from the more trusted inner layer and deny all inbound requests from the less trusted outer layers • Hardware-encrypted hard drives using at least AES-256 encryption can also be used to transfer data between production networks and Data IO systems (e.g., air gapped network) • Delete content after it has been on the system for more than 24 hours • When preparing or transferring content, utilize dedicated rooms with fully covered windows and closed door when work is in progress • For Applications: • Data caching • Use a secure vault to store user credentials	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	• Allowing to restrict content downloads and uploads to only authorized external sources and destinations • Enable alerts when transfer is complete and/or downloaded • Use valid DNS entry for allowing
TS-1.0	Data IO Workflows & Systems	Establish and regularly review a process and workflow for Data IO Workflows & Systems to include the following: • Use dedicated (i.e., isolated) systems to move content between external networks (i.e., Internet) and internal networks (e.g., Data IO network, production, etc.) • Scan all content for viruses and malware prior to ingest onto the network • Segregation of duties between Data IO staff and other staff (e.g., production, development, etc.) • Content movement is initiated from the more secure layer (e.g., push/pull content at the Data IO zone bottom Internet; push/pull content at the production network from the Data IO zone) • Strict IP and port layer 3/3 Access Control Lists (ACLs) to allow outbound network requests from the more trusted inner layer and deny all inbound requests from the less trusted outer layers • Hardware-encrypted hard drives using at least AES-256 encryption can also be used to transfer data between production networks and Data IO systems (e.g., air gapped network) • Delete content after it has been on the system for more than 24 hours • When preparing or transferring content, utilize dedicated rooms with fully covered windows and closed door when work is in progress • For Applications: • Data caching • Use a secure vault to store user credentials	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	• Allowing to restrict content downloads and uploads to only authorized external sources and destinations • Enable alerts when transfer is complete and/or downloaded • Use valid DNS entry for allowing

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Relationship	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
TS-1.0	Data I/O Workflows & Systems	<p>Establish and regularly review a process and workflow for Data I/O Workflows & Systems to include the following:</p> <ul style="list-style-type: none"> Use dedicated (i.e., isolated) systems to move content between external networks (i.e., Internet) and internal networks (e.g., Data I/O network, production, etc.) Scan all content for viruses and malware prior to ingest onto the network Segregation of duties between Data I/O staff and other staff (e.g., production, development, etc.) Content movement is initiated from the more secure layer (e.g., push/pull content at the Data I/O zone bottom Internet; push/pull content at the production network to/from the Data I/O zone) Strict IP and port/layer 2/3 Access Control Lists (ACLs) to allow outbound network requests from the more trusted inner layer and deny all inbound requests from the less trusted outer layers Hardware-encrypted hard drives using at least AES-256 encryption can also be used to transfer data between production networks and Data I/O systems (e.g., air-gapped network) Delete content after it has been on the system for more than 24 hours When preparing or transferring content, utilize dedicated rooms with fully covered windows and closed door when work is in progress <p>For Applications:</p> <ul style="list-style-type: none"> Data caching Use a secret vault to store user credentials 	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	<ul style="list-style-type: none"> Allowing to restrict content downloads and uploads to only authorized external sources and destinations Enable alerts when transfer is complete and/or downloaded Use valid DNS entry for allowing
TS-1.0	Data I/O Workflows & Systems	<p>Establish and regularly review a process and workflow for Data I/O Workflows & Systems to include the following:</p> <ul style="list-style-type: none"> Use dedicated (i.e., isolated) systems to move content between external networks (i.e., Internet) and internal networks (e.g., Data I/O network, production, etc.) Scan all content for viruses and malware prior to ingest onto the network Segregation of duties between Data I/O staff and other staff (e.g., production, development, etc.) Content movement is initiated from the more secure layer (e.g., push/pull content at the Data I/O zone bottom Internet; push/pull content at the production network to/from the Data I/O zone) Strict IP and port/layer 2/3 Access Control Lists (ACLs) to allow outbound network requests from the more trusted inner layer and deny all inbound requests from the less trusted outer layers Hardware-encrypted hard drives using at least AES-256 encryption can also be used to transfer data between production networks and Data I/O systems (e.g., air-gapped network) Delete content after it has been on the system for more than 24 hours When preparing or transferring content, utilize dedicated rooms with fully covered windows and closed door when work is in progress <p>For Applications:</p> <ul style="list-style-type: none"> Data caching Use a secret vault to store user credentials 	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	<ul style="list-style-type: none"> Allowing to restrict content downloads and uploads to only authorized external sources and destinations Enable alerts when transfer is complete and/or downloaded Use valid DNS entry for allowing
TS-1.0	Data I/O Workflows & Systems	<p>Establish and regularly review a process and workflow for Data I/O Workflows & Systems to include the following:</p> <ul style="list-style-type: none"> Use dedicated (i.e., isolated) systems to move content between external networks (i.e., Internet) and internal networks (e.g., Data I/O network, production, etc.) Scan all content for viruses and malware prior to ingest onto the network Segregation of duties between Data I/O staff and other staff (e.g., production, development, etc.) Content movement is initiated from the more secure layer (e.g., push/pull content at the Data I/O zone bottom Internet; push/pull content at the production network to/from the Data I/O zone) Strict IP and port/layer 2/3 Access Control Lists (ACLs) to allow outbound network requests from the more trusted inner layer and deny all inbound requests from the less trusted outer layers Hardware-encrypted hard drives using at least AES-256 encryption can also be used to transfer data between production networks and Data I/O systems (e.g., air-gapped network) Delete content after it has been on the system for more than 24 hours When preparing or transferring content, utilize dedicated rooms with fully covered windows and closed door when work is in progress <p>For Applications:</p> <ul style="list-style-type: none"> Data caching Use a secret vault to store user credentials 	Functional	Intersects With	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	5	<ul style="list-style-type: none"> Allowing to restrict content downloads and uploads to only authorized external sources and destinations Enable alerts when transfer is complete and/or downloaded Use valid DNS entry for allowing
TS-1.0	Data I/O Workflows & Systems	<p>Establish and regularly review a process and workflow for Data I/O Workflows & Systems to include the following:</p> <ul style="list-style-type: none"> Use dedicated (i.e., isolated) systems to move content between external networks (i.e., Internet) and internal networks (e.g., Data I/O network, production, etc.) Scan all content for viruses and malware prior to ingest onto the network Segregation of duties between Data I/O staff and other staff (e.g., production, development, etc.) Content movement is initiated from the more secure layer (e.g., push/pull content at the Data I/O zone bottom Internet; push/pull content at the production network to/from the Data I/O zone) Strict IP and port/layer 2/3 Access Control Lists (ACLs) to allow outbound network requests from the more trusted inner layer and deny all inbound requests from the less trusted outer layers Hardware-encrypted hard drives using at least AES-256 encryption can also be used to transfer data between production networks and Data I/O systems (e.g., air-gapped network) Delete content after it has been on the system for more than 24 hours When preparing or transferring content, utilize dedicated rooms with fully covered windows and closed door when work is in progress <p>For Applications:</p> <ul style="list-style-type: none"> Data caching Use a secret vault to store user credentials 	Functional	Intersects With	Unified Endpoint Device Management (UEDM)	END-01.1	Mechanisms exist to utilize a centralized Unified Endpoint Device Management (UEDM) solution that provides agent and/or agentless management of endpoint devices regardless of device location.	5	<ul style="list-style-type: none"> Allowing to restrict content downloads and uploads to only authorized external sources and destinations Enable alerts when transfer is complete and/or downloaded Use valid DNS entry for allowing
TS-1.0	Data I/O Workflows & Systems	<p>Establish and regularly review a process and workflow for Data I/O Workflows & Systems to include the following:</p> <ul style="list-style-type: none"> Use dedicated (i.e., isolated) systems to move content between external networks (i.e., Internet) and internal networks (e.g., Data I/O network, production, etc.) Scan all content for viruses and malware prior to ingest onto the network Segregation of duties between Data I/O staff and other staff (e.g., production, development, etc.) Content movement is initiated from the more secure layer (e.g., push/pull content at the Data I/O zone bottom Internet; push/pull content at the production network to/from the Data I/O zone) Strict IP and port/layer 2/3 Access Control Lists (ACLs) to allow outbound network requests from the more trusted inner layer and deny all inbound requests from the less trusted outer layers Hardware-encrypted hard drives using at least AES-256 encryption can also be used to transfer data between production networks and Data I/O systems (e.g., air-gapped network) Delete content after it has been on the system for more than 24 hours When preparing or transferring content, utilize dedicated rooms with fully covered windows and closed door when work is in progress <p>For Applications:</p> <ul style="list-style-type: none"> Data caching Use a secret vault to store user credentials 	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	<ul style="list-style-type: none"> Allowing to restrict content downloads and uploads to only authorized external sources and destinations Enable alerts when transfer is complete and/or downloaded Use valid DNS entry for allowing
TS-1.0	Data I/O Workflows & Systems	<p>Establish and regularly review a process and workflow for Data I/O Workflows & Systems to include the following:</p> <ul style="list-style-type: none"> Use dedicated (i.e., isolated) systems to move content between external networks (i.e., Internet) and internal networks (e.g., Data I/O network, production, etc.) Scan all content for viruses and malware prior to ingest onto the network Segregation of duties between Data I/O staff and other staff (e.g., production, development, etc.) Content movement is initiated from the more secure layer (e.g., push/pull content at the Data I/O zone bottom Internet; push/pull content at the production network to/from the Data I/O zone) Strict IP and port/layer 2/3 Access Control Lists (ACLs) to allow outbound network requests from the more trusted inner layer and deny all inbound requests from the less trusted outer layers Hardware-encrypted hard drives using at least AES-256 encryption can also be used to transfer data between production networks and Data I/O systems (e.g., air-gapped network) Delete content after it has been on the system for more than 24 hours When preparing or transferring content, utilize dedicated rooms with fully covered windows and closed door when work is in progress <p>For Applications:</p> <ul style="list-style-type: none"> Data caching Use a secret vault to store user credentials 	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize anti-malware technologies to detect and eradicate malicious code.	5	<ul style="list-style-type: none"> Allowing to restrict content downloads and uploads to only authorized external sources and destinations Enable alerts when transfer is complete and/or downloaded Use valid DNS entry for allowing
TS-1.0	Data I/O Workflows & Systems	<p>Establish and regularly review a process and workflow for Data I/O Workflows & Systems to include the following:</p> <ul style="list-style-type: none"> Use dedicated (i.e., isolated) systems to move content between external networks (i.e., Internet) and internal networks (e.g., Data I/O network, production, etc.) Scan all content for viruses and malware prior to ingest onto the network Segregation of duties between Data I/O staff and other staff (e.g., production, development, etc.) Content movement is initiated from the more secure layer (e.g., push/pull content at the Data I/O zone bottom Internet; push/pull content at the production network to/from the Data I/O zone) Strict IP and port/layer 2/3 Access Control Lists (ACLs) to allow outbound network requests from the more trusted inner layer and deny all inbound requests from the less trusted outer layers Hardware-encrypted hard drives using at least AES-256 encryption can also be used to transfer data between production networks and Data I/O systems (e.g., air-gapped network) Delete content after it has been on the system for more than 24 hours When preparing or transferring content, utilize dedicated rooms with fully covered windows and closed door when work is in progress <p>For Applications:</p> <ul style="list-style-type: none"> Data caching Use a secret vault to store user credentials 	Functional	Intersects With	Always On Protection	END-04.7	Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period.	5	<ul style="list-style-type: none"> Allowing to restrict content downloads and uploads to only authorized external sources and destinations Enable alerts when transfer is complete and/or downloaded Use valid DNS entry for allowing
TS-1.0	Data I/O Workflows & Systems	<p>Establish and regularly review a process and workflow for Data I/O Workflows & Systems to include the following:</p> <ul style="list-style-type: none"> Use dedicated (i.e., isolated) systems to move content between external networks (i.e., Internet) and internal networks (e.g., Data I/O network, production, etc.) Scan all content for viruses and malware prior to ingest onto the network Segregation of duties between Data I/O staff and other staff (e.g., production, development, etc.) Content movement is initiated from the more secure layer (e.g., push/pull content at the Data I/O zone bottom Internet; push/pull content at the production network to/from the Data I/O zone) Strict IP and port/layer 2/3 Access Control Lists (ACLs) to allow outbound network requests from the more trusted inner layer and deny all inbound requests from the less trusted outer layers Hardware-encrypted hard drives using at least AES-256 encryption can also be used to transfer data between production networks and Data I/O systems (e.g., air-gapped network) Delete content after it has been on the system for more than 24 hours When preparing or transferring content, utilize dedicated rooms with fully covered windows and closed door when work is in progress <p>For Applications:</p> <ul style="list-style-type: none"> Data caching Use a secret vault to store user credentials 	Functional	Intersects With	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5	<ul style="list-style-type: none"> Allowing to restrict content downloads and uploads to only authorized external sources and destinations Enable alerts when transfer is complete and/or downloaded Use valid DNS entry for allowing
TS-1.0	Data I/O Workflows & Systems	<p>Establish and regularly review a process and workflow for Data I/O Workflows & Systems to include the following:</p> <ul style="list-style-type: none"> Use dedicated (i.e., isolated) systems to move content between external networks (i.e., Internet) and internal networks (e.g., Data I/O network, production, etc.) Scan all content for viruses and malware prior to ingest onto the network Segregation of duties between Data I/O staff and other staff (e.g., production, development, etc.) Content movement is initiated from the more secure layer (e.g., push/pull content at the Data I/O zone bottom Internet; push/pull content at the production network to/from the Data I/O zone) Strict IP and port/layer 2/3 Access Control Lists (ACLs) to allow outbound network requests from the more trusted inner layer and deny all inbound requests from the less trusted outer layers Hardware-encrypted hard drives using at least AES-256 encryption can also be used to transfer data between production networks and Data I/O systems (e.g., air-gapped network) Delete content after it has been on the system for more than 24 hours When preparing or transferring content, utilize dedicated rooms with fully covered windows and closed door when work is in progress <p>For Applications:</p> <ul style="list-style-type: none"> Data caching Use a secret vault to store user credentials 	Functional	Intersects With	Dedicated Administrative Machines	IAC-20.4	Mechanisms exist to restrict executing administrative tasks or tasks requiring elevated access to a dedicated machine.	5	<ul style="list-style-type: none"> Allowing to restrict content downloads and uploads to only authorized external sources and destinations Enable alerts when transfer is complete and/or downloaded Use valid DNS entry for allowing
TS-1.0	Data I/O Workflows & Systems	<p>Establish and regularly review a process and workflow for Data I/O Workflows & Systems to include the following:</p> <ul style="list-style-type: none"> Use dedicated (i.e., isolated) systems to move content between external networks (i.e., Internet) and internal networks (e.g., Data I/O network, production, etc.) Scan all content for viruses and malware prior to ingest onto the network Segregation of duties between Data I/O staff and other staff (e.g., production, development, etc.) Content movement is initiated from the more secure layer (e.g., push/pull content at the Data I/O zone bottom Internet; push/pull content at the production network to/from the Data I/O zone) Strict IP and port/layer 2/3 Access Control Lists (ACLs) to allow outbound network requests from the more trusted inner layer and deny all inbound requests from the less trusted outer layers Hardware-encrypted hard drives using at least AES-256 encryption can also be used to transfer data between production networks and Data I/O systems (e.g., air-gapped network) Delete content after it has been on the system for more than 24 hours When preparing or transferring content, utilize dedicated rooms with fully covered windows and closed door when work is in progress <p>For Applications:</p> <ul style="list-style-type: none"> Data caching Use a secret vault to store user credentials 	Functional	Intersects With	Data Flow Enforcement - Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	5	<ul style="list-style-type: none"> Allowing to restrict content downloads and uploads to only authorized external sources and destinations Enable alerts when transfer is complete and/or downloaded Use valid DNS entry for allowing

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Relationship	STRM Relationship	SCF Control	SCF #	Security Controls Framework (SCF) Control Description	Strength of Relationship	Notes
TS-1.0	Data I/O Workflows & Systems	<ul style="list-style-type: none"> Establish and regularly review a process and workflow for Data I/O Workflows & Systems to include the following: <ul style="list-style-type: none"> Use dedicated (i.e., isolated) systems to move content between external networks (i.e., Internet) and internal networks (e.g., Data I/O network, production, etc.) Scan all content for viruses and malware prior to ingest onto the network Segregation of duties between Data I/O staff and other staff (e.g., production, development, etc.) Content movement is initiated from the more secure layer (e.g., push/pull content at the Data I/O zone bottom Internet; push/pull content at the production network bottom the Data I/O zone) Strict (IP and port) layer 3/3 Access Control Lists (ACLs) to allow outbound network requests from the more trusted inner layer and deny all inbound requests from the less trusted outer layers Hardware-encrypted hard drives using at least AES-256 encryption can also be used to transfer data between production networks and Data I/O systems (e.g., all gapped networks) Delete content after it has been on the system for more than 24 hours When preparing or transferring content, utilize dedicated rooms with fully covered windows and closed door when work is in progress For Applications: <ul style="list-style-type: none"> Data caching Use a secure vault to store user credentials 	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5	<ul style="list-style-type: none"> Allowlisting to restrict content downloads and uploads to only authorized external sources and destinations Enable alerts when transfer is complete and/or downloaded Use valid DNS entry for allowlisting
TS-1.0	Data I/O Workflows & Systems	<ul style="list-style-type: none"> Establish and regularly review a process and workflow for Data I/O Workflows & Systems to include the following: <ul style="list-style-type: none"> Use dedicated (i.e., isolated) systems to move content between external networks (i.e., Internet) and internal networks (e.g., Data I/O network, production, etc.) Scan all content for viruses and malware prior to ingest onto the network Segregation of duties between Data I/O staff and other staff (e.g., production, development, etc.) Content movement is initiated from the more secure layer (e.g., push/pull content at the Data I/O zone bottom Internet; push/pull content at the production network bottom the Data I/O zone) Strict (IP and port) layer 3/3 Access Control Lists (ACLs) to allow outbound network requests from the more trusted inner layer and deny all inbound requests from the less trusted outer layers Hardware-encrypted hard drives using at least AES-256 encryption can also be used to transfer data between production networks and Data I/O systems (e.g., all gapped networks) Delete content after it has been on the system for more than 24 hours When preparing or transferring content, utilize dedicated rooms with fully covered windows and closed door when work is in progress For Applications: <ul style="list-style-type: none"> Data caching Use a secure vault to store user credentials 	Functional	Intersects With	Segregation From Enterprise Services	NET-06.4	Mechanisms exist to isolate sensitive/regulatory data enclaves (secure zones) from separate provided IT resources by providing enclave-specific IT services (e.g., directory services, DNS, NTP, ITAM, anti-malware, patch management, etc.) to those isolated network segments.	5	<ul style="list-style-type: none"> Allowlisting to restrict content downloads and uploads to only authorized external sources and destinations Enable alerts when transfer is complete and/or downloaded Use valid DNS entry for allowlisting
TS-1.0	Data I/O Workflows & Systems	<ul style="list-style-type: none"> Establish and regularly review a process and workflow for Data I/O Workflows & Systems to include the following: <ul style="list-style-type: none"> Use dedicated (i.e., isolated) systems to move content between external networks (i.e., Internet) and internal networks (e.g., Data I/O network, production, etc.) Scan all content for viruses and malware prior to ingest onto the network Segregation of duties between Data I/O staff and other staff (e.g., production, development, etc.) Content movement is initiated from the more secure layer (e.g., push/pull content at the Data I/O zone bottom Internet; push/pull content at the production network bottom the Data I/O zone) Strict (IP and port) layer 3/3 Access Control Lists (ACLs) to allow outbound network requests from the more trusted inner layer and deny all inbound requests from the less trusted outer layers Hardware-encrypted hard drives using at least AES-256 encryption can also be used to transfer data between production networks and Data I/O systems (e.g., all gapped networks) Delete content after it has been on the system for more than 24 hours When preparing or transferring content, utilize dedicated rooms with fully covered windows and closed door when work is in progress For Applications: <ul style="list-style-type: none"> Data caching Use a secure vault to store user credentials 	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	5	<ul style="list-style-type: none"> Allowlisting to restrict content downloads and uploads to only authorized external sources and destinations Enable alerts when transfer is complete and/or downloaded Use valid DNS entry for allowlisting
TS-1.0	Data I/O Workflows & Systems	<ul style="list-style-type: none"> Establish and regularly review a process and workflow for Data I/O Workflows & Systems to include the following: <ul style="list-style-type: none"> Use dedicated (i.e., isolated) systems to move content between external networks (i.e., Internet) and internal networks (e.g., Data I/O network, production, etc.) Scan all content for viruses and malware prior to ingest onto the network Segregation of duties between Data I/O staff and other staff (e.g., production, development, etc.) Content movement is initiated from the more secure layer (e.g., push/pull content at the Data I/O zone bottom Internet; push/pull content at the production network bottom the Data I/O zone) Strict (IP and port) layer 3/3 Access Control Lists (ACLs) to allow outbound network requests from the more trusted inner layer and deny all inbound requests from the less trusted outer layers Hardware-encrypted hard drives using at least AES-256 encryption can also be used to transfer data between production networks and Data I/O systems (e.g., all gapped networks) Delete content after it has been on the system for more than 24 hours When preparing or transferring content, utilize dedicated rooms with fully covered windows and closed door when work is in progress For Applications: <ul style="list-style-type: none"> Data caching Use a secure vault to store user credentials 	Functional	Intersects With	Working in Secure Areas	PES-04.1	Physical security mechanisms exist to allow only authorized personnel access to secure areas.	5	<ul style="list-style-type: none"> Allowlisting to restrict content downloads and uploads to only authorized external sources and destinations Enable alerts when transfer is complete and/or downloaded Use valid DNS entry for allowlisting
TS-1.1	Systems Configuration	<ul style="list-style-type: none"> Establish and regularly review security baselines, policies, and procedures to Configure Corporate Systems and Infrastructure (e.g., laptops, workstations, servers, SAN/NAS, virtual machine infrastructure, WAN, LAN, etc.) to include the following: <ul style="list-style-type: none"> Install anti-virus/anti-malware Disable or remove local accounts on systems or change default username and password Remove users from active network shares Remove, uninstall, or disable all unnecessary software, protocols, and services Monitor users from screen administrators on their own workstations unless required for software Block removable (SD), mass storage, external storage, and mobile storage devices on all systems that are not required for business operations Apply secure configuration standards before a system is connected to the environment Monitor the use of wireless transfer applications (e.g., Bluetooth, NFC, AirDrop, etc.) on production systems Enable password protected screensavers and/or screen-lock software that activates after a maximum of 15 minutes of inactivity 	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	<ul style="list-style-type: none"> Enable local firewalls Utilize centralized configuration (e.g., Group Policy, MDM, etc.) to standardize security baselines
TS-1.2	Default Accounts	<ul style="list-style-type: none"> Establish and regularly review a process for all Default Accounts (e.g., admin, infrastructure, applications, etc.) to include the following: <ul style="list-style-type: none"> Identify all Default Accounts Change passwords or passphrases Change usernames For applications, allow for deletion and removal of application Default Accounts 	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	<ul style="list-style-type: none"> Limit the use of Default Accounts to special situations as required (e.g., operating system updates, patch installations, software updates, etc.)
TS-1.2	Default Accounts	<ul style="list-style-type: none"> Establish and regularly review a process for all Default Accounts (e.g., admin, infrastructure, applications, etc.) to include the following: <ul style="list-style-type: none"> Identify all Default Accounts Change passwords or passphrases Change usernames For applications, allow for deletion and removal of application Default Accounts 	Functional	Intersects With	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	8	<ul style="list-style-type: none"> Limit the use of Default Accounts to special situations as required (e.g., operating system updates, patch installations, software updates, etc.)
TS-1.3	Endpoint Protection	<ul style="list-style-type: none"> Establish and regularly review a process for Endpoint Protection, to include the following: <ul style="list-style-type: none"> Manage anti-virus/anti-malware software with a centralized management console Update anti-virus/anti-malware definitions regularly Perform regular scans on systems Apply to the following: <ul style="list-style-type: none"> Workstations (e.g., desktop, laptop, etc.) Mobile devices Servers SAN/NAS Virtual Machines 	Functional	Subset Of	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	10	<ul style="list-style-type: none"> Logs sent to a centralized logging solution Initial Endpoint Detection and Response (EDR), XDR (Extended Detection and Response), or MXDR (Managed Extended Detection and Response)
TS-1.3	Endpoint Protection	<ul style="list-style-type: none"> Establish and regularly review a process for Endpoint Protection, to include the following: <ul style="list-style-type: none"> Manage anti-virus/anti-malware software with a centralized management console Update anti-virus/anti-malware definitions regularly Perform regular scans on systems Apply to the following: <ul style="list-style-type: none"> Workstations (e.g., desktop, laptop, etc.) Mobile devices Servers SAN/NAS Virtual Machines 	Functional	Intersects With	Unified Endpoint Device Management (UEDM)	END-01.1	Mechanisms exist to utilize a centralized Unified Endpoint Device Management (UEDM) solution that provides agent and/or agentless management of endpoint devices regardless of device location.	5	<ul style="list-style-type: none"> Logs sent to a centralized logging solution Initial Endpoint Detection and Response (EDR), XDR (Extended Detection and Response), or MXDR (Managed Extended Detection and Response)
TS-1.3	Endpoint Protection	<ul style="list-style-type: none"> Establish and regularly review a process for Endpoint Protection, to include the following: <ul style="list-style-type: none"> Manage anti-virus/anti-malware software with a centralized management console Update anti-virus/anti-malware definitions regularly Perform regular scans on systems Apply to the following: <ul style="list-style-type: none"> Workstations (e.g., desktop, laptop, etc.) Mobile devices Servers SAN/NAS Virtual Machines 	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	<ul style="list-style-type: none"> Logs sent to a centralized logging solution Initial Endpoint Detection and Response (EDR), XDR (Extended Detection and Response), or MXDR (Managed Extended Detection and Response)
TS-1.3	Endpoint Protection	<ul style="list-style-type: none"> Establish and regularly review a process for Endpoint Protection, to include the following: <ul style="list-style-type: none"> Manage anti-virus/anti-malware software with a centralized management console Update anti-virus/anti-malware definitions regularly Perform regular scans on systems Apply to the following: <ul style="list-style-type: none"> Workstations (e.g., desktop, laptop, etc.) Mobile devices Servers SAN/NAS Virtual Machines 	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize anti-malware technologies to detect and eradicate malicious code.	5	<ul style="list-style-type: none"> Logs sent to a centralized logging solution Initial Endpoint Detection and Response (EDR), XDR (Extended Detection and Response), or MXDR (Managed Extended Detection and Response)
TS-1.3	Endpoint Protection	<ul style="list-style-type: none"> Establish and regularly review a process for Endpoint Protection, to include the following: <ul style="list-style-type: none"> Manage anti-virus/anti-malware software with a centralized management console Update anti-virus/anti-malware definitions regularly Perform regular scans on systems Apply to the following: <ul style="list-style-type: none"> Workstations (e.g., desktop, laptop, etc.) Mobile devices Servers SAN/NAS Virtual Machines 	Functional	Intersects With	Automatic Antismalware Signature Updates	END-04.1	Automated mechanisms exist to update anti-malware technologies, including signature definitions.	5	<ul style="list-style-type: none"> Logs sent to a centralized logging solution Initial Endpoint Detection and Response (EDR), XDR (Extended Detection and Response), or MXDR (Managed Extended Detection and Response)
TS-1.3	Endpoint Protection	<ul style="list-style-type: none"> Establish and regularly review a process for Endpoint Protection, to include the following: <ul style="list-style-type: none"> Manage anti-virus/anti-malware software with a centralized management console Update anti-virus/anti-malware definitions regularly Perform regular scans on systems Apply to the following: <ul style="list-style-type: none"> Workstations (e.g., desktop, laptop, etc.) Mobile devices Servers SAN/NAS Virtual Machines 	Functional	Intersects With	Always On Protection	END-04.7	Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period.	5	<ul style="list-style-type: none"> Logs sent to a centralized logging solution Initial Endpoint Detection and Response (EDR), XDR (Extended Detection and Response), or MXDR (Managed Extended Detection and Response)
TS-1.4	Mobile Devices	<ul style="list-style-type: none"> Establish and regularly review a policy and process for company issued and managed Mobile Devices (e.g., tablets, cell phones, laptops, etc.). To include the following: <ul style="list-style-type: none"> Apply Acceptable Use Policy (AUP) Best Practices (OR-1.1) Report all lost or stolen devices immediately Anti-virus/anti-malware protection Automatic inactivity lock Mobile Device Management (MDM) Mobile Application Management (MAM) Ability to conduct a remote wipe should the device be lost, stolen, compromised, etc. Encryption of the entire device Where mobile devices are, or are not, permitted in a site to prevent unauthorized content recording 	Functional	Intersects With	Unified Endpoint Device Management (UEDM)	END-01.1	Mechanisms exist to utilize a centralized Unified Endpoint Device Management (UEDM) solution that provides agent and/or agentless management of endpoint devices regardless of device location.	5	<ul style="list-style-type: none"> Bring Your Own Devices (BYOD), in accordance with local laws, regulations, and agreements, apply the following MPA Content Security Best Practices: <ul style="list-style-type: none"> Corporate Email Filtering (TS-1.9) Endpoint Protection (TS-1.3) Content Security (TS-1.1) Systems Configuration (TS-1.1) Web Filtering (TS-2.10) Training & Awareness for key personnel who handle content (OR-3.3)
TS-1.4	Mobile Devices	<ul style="list-style-type: none"> Establish and regularly review a policy and process for company issued and managed Mobile Devices (e.g., tablets, cell phones, laptops, etc.). To include the following: <ul style="list-style-type: none"> Apply Acceptable Use Policy (AUP) Best Practices (OR-1.1) Report all lost or stolen devices immediately Anti-virus/anti-malware protection Automatic inactivity lock Mobile Device Management (MDM) Mobile Application Management (MAM) Ability to conduct a remote wipe should the device be lost, stolen, compromised, etc. Encryption of the entire device Where mobile devices are, or are not, permitted in a site to prevent unauthorized content recording 	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize anti-malware technologies to detect and eradicate malicious code.	5	<ul style="list-style-type: none"> Bring Your Own Devices (BYOD), in accordance with local laws, regulations, and agreements, apply the following MPA Content Security Best Practices: <ul style="list-style-type: none"> Corporate Email Filtering (TS-1.9) Endpoint Protection (TS-1.3) Content Security (TS-1.1) Systems Configuration (TS-1.1) Web Filtering (TS-2.10) Training & Awareness for key personnel who handle content (OR-3.3)
TS-1.4	Mobile Devices	<ul style="list-style-type: none"> Establish and regularly review a policy and process for company issued and managed Mobile Devices (e.g., tablets, cell phones, laptops, etc.). To include the following: <ul style="list-style-type: none"> Apply Acceptable Use Policy (AUP) Best Practices (OR-1.1) Report all lost or stolen devices immediately Anti-virus/anti-malware protection Automatic inactivity lock Mobile Device Management (MDM) Mobile Application Management (MAM) Ability to conduct a remote wipe should the device be lost, stolen, compromised, etc. Encryption of the entire device Where mobile devices are, or are not, permitted in a site to prevent unauthorized content recording 	Functional	Intersects With	Incident Handling	IRI-02	Mechanisms exist to cover: <ol style="list-style-type: none"> Preparation; Automated event detection or manual incident report intake; Analysis; Containment; Eradication; and Recovery. 	5	<ul style="list-style-type: none"> Bring Your Own Devices (BYOD), in accordance with local laws, regulations, and agreements, apply the following MPA Content Security Best Practices: <ul style="list-style-type: none"> Corporate Email Filtering (TS-1.9) Endpoint Protection (TS-1.3) Content Security (TS-1.1) Systems Configuration (TS-1.1) Web Filtering (TS-2.10) Training & Awareness for key personnel who handle content (OR-3.3)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Relationship	STRM Relationship	SCF Control	SCF #	Security Controls Framework (SCF) Control Description	Strength of Relationship	Notes
TS-1.4	Mobile Devices	Establish and regularly review a policy and process for company issued and managed Mobile Devices (e.g., tablets, cell phones, laptops, etc.). To include the following: • Apply Acceptable Use Policy (AUP) Best Practices (OR-1.1) • Report all lost or stolen devices immediately • Anti-virus/anti-malware protection • Automatic inactivity lock • Mobile Device Management (MDM) • Mobile Application Management (MAM) • Ability to conduct a remote wipe should the device be lost, stolen, compromised, etc. • Encryption of the entire device • Where mobile devices are, or are not, permitted in a site to prevent unauthorized content recording	Functional	Intersects With	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	5	For Bring Your Own Devices (BYOD), in accordance with local laws, regulations, and agreements, apply the following MPA Content Security Best Practices: • Corporate Email Filtering (TS-1.9) • Endpoint Protection (TS-1.3) • Patching (TS-4.2) • Systems Configuration (TS-1.1) • Web Filtering (TS-2.10) • Training & Awareness for key personnel who handle content (OR-3.1)
TS-1.4	Mobile Devices	Establish and regularly review a policy and process for company issued and managed Mobile Devices (e.g., tablets, cell phones, laptops, etc.). To include the following: • Apply Acceptable Use Policy (AUP) Best Practices (OR-1.1) • Report all lost or stolen devices immediately • Anti-virus/anti-malware protection • Automatic inactivity lock • Mobile Device Management (MDM) • Mobile Application Management (MAM) • Ability to conduct a remote wipe should the device be lost, stolen, compromised, etc. • Encryption of the entire device • Where mobile devices are, or are not, permitted in a site to prevent unauthorized content recording	Functional	Intersects With	Remote Purging	MDM-05	Mechanisms exist to remotely purge selected information from mobile devices.	5	For Bring Your Own Devices (BYOD), in accordance with local laws, regulations, and agreements, apply the following MPA Content Security Best Practices: • Corporate Email Filtering (TS-1.9) • Endpoint Protection (TS-1.3) • Patching (TS-4.2) • Systems Configuration (TS-1.1) • Web Filtering (TS-2.10) • Training & Awareness for key personnel who handle content (OR-3.1)
TS-1.5	Security Information & Event Management	Establish a policy and process for Security Information & Event Management (SIEM), to include the following: • Centralized real-time logging of firewalls, authentication servers, network operating systems, content transfer systems, virtual machines/servers, storage services, databases, container-based application services, API gateway connectors, key generation/management, etc. • Log the following attributes for network activity: source IP address, destination URL, or IP address, username, action attempted, action result, execution/file path, timestamp • Send automatic notifications when security events are detected • Assign personnel to review logs and respond to notifications • Log all remote access activities • Encrypt logs and associated logging data over external networks • Restrict access to, deletion, and modification of logs to authorized personnel only • Regularly review system logs • Retain logs for a period of one year, or the maximum time allowed in accordance with local laws, regulations, and agreements • Utilize a synchronized time service protocol (e.g., Network Time Protocol (NTP)) • Incorporate into Business Continuity Plan (OR-1.2) & Incident Response (OR-4.0) procedures	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	• Enable local logging on isolated systems • Include logging and monitoring of spikes in resource utilization and capacity management • Enable dual authorization for movement and deletion of audit log information • Security event notifications include the following: • Successful and unsuccessful attempts to connect to the content and production network • Unusual file size and/or time of day transport of content • Repeated attempts for unauthorized access • Attempts at privileged access (e.g., different locations, time of day, etc.) • Administrator account creation, modification, or deletion • File Integrity Monitoring (FIM) for sensitive data and applications • Failure of critical security systems (e.g., Firewall, IDS/IPS, endpoint protection, physical and logical access controls, etc.)
TS-1.5	Security Information & Event Management	Establish a policy and process for Security Information & Event Management (SIEM), to include the following: • Centralized real-time logging of firewalls, authentication servers, network operating systems, content transfer systems, virtual machines/servers, storage services, databases, container-based application services, API gateway connectors, key generation/management, etc. • Log the following attributes for network activity: source IP address, destination URL, or IP address, username, action attempted, action result, execution/file path, timestamp • Send automatic notifications when security events are detected • Assign personnel to review logs and respond to notifications • Log all remote access activities • Encrypt logs and associated logging data over external networks • Restrict access to, deletion, and modification of logs to authorized personnel only • Regularly review system logs • Retain logs for a period of one year, or the maximum time allowed in accordance with local laws, regulations, and agreements • Utilize a synchronized time service protocol (e.g., Network Time Protocol (NTP)) • Incorporate into Business Continuity Plan (OR-1.2) & Incident Response (OR-4.0) procedures	Functional	Intersects With	Automated Tools For Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	8	• Enable local logging on isolated systems • Include logging and monitoring of spikes in resource utilization and capacity management • Enable dual authorization for movement and deletion of audit log information • Security event notifications include the following: • Successful and unsuccessful attempts to connect to the content and production network • Unusual file size and/or time of day transport of content • Repeated attempts for unauthorized access • Attempts at privileged access (e.g., different locations, time of day, etc.) • Administrator account creation, modification, or deletion • File Integrity Monitoring (FIM) for sensitive data and applications • Failure of critical security systems (e.g., Firewall, IDS/IPS, endpoint protection, physical and logical access controls, etc.)
TS-1.5	Security Information & Event Management	Establish a policy and process for Security Information & Event Management (SIEM), to include the following: • Centralized real-time logging of firewalls, authentication servers, network operating systems, content transfer systems, virtual machines/servers, storage services, databases, container-based application services, API gateway connectors, key generation/management, etc. • Log the following attributes for network activity: source IP address, destination URL, or IP address, username, action attempted, action result, execution/file path, timestamp • Send automatic notifications when security events are detected • Assign personnel to review logs and respond to notifications • Log all remote access activities • Encrypt logs and associated logging data over external networks • Restrict access to, deletion, and modification of logs to authorized personnel only • Regularly review system logs • Retain logs for a period of one year, or the maximum time allowed in accordance with local laws, regulations, and agreements • Utilize a synchronized time service protocol (e.g., Network Time Protocol (NTP)) • Incorporate into Business Continuity Plan (OR-1.2) & Incident Response (OR-4.0) procedures	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	• Enable local logging on isolated systems • Include logging and monitoring of spikes in resource utilization and capacity management • Enable dual authorization for movement and deletion of audit log information • Security event notifications include the following: • Successful and unsuccessful attempts to connect to the content and production network • Unusual file size and/or time of day transport of content • Repeated attempts for unauthorized access • Attempts at privileged access (e.g., different locations, time of day, etc.) • Administrator account creation, modification, or deletion • File Integrity Monitoring (FIM) for sensitive data and applications • Failure of critical security systems (e.g., Firewall, IDS/IPS, endpoint protection, physical and logical access controls, etc.)
TS-1.5	Security Information & Event Management	Establish a policy and process for Security Information & Event Management (SIEM), to include the following: • Centralized real-time logging of firewalls, authentication servers, network operating systems, content transfer systems, virtual machines/servers, storage services, databases, container-based application services, API gateway connectors, key generation/management, etc. • Log the following attributes for network activity: source IP address, destination URL, or IP address, username, action attempted, action result, execution/file path, timestamp • Send automatic notifications when security events are detected • Assign personnel to review logs and respond to notifications • Log all remote access activities • Encrypt logs and associated logging data over external networks • Restrict access to, deletion, and modification of logs to authorized personnel only • Regularly review system logs • Retain logs for a period of one year, or the maximum time allowed in accordance with local laws, regulations, and agreements • Utilize a synchronized time service protocol (e.g., Network Time Protocol (NTP)) • Incorporate into Business Continuity Plan (OR-1.2) & Incident Response (OR-4.0) procedures	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5	• Enable local logging on isolated systems • Include logging and monitoring of spikes in resource utilization and capacity management • Enable dual authorization for movement and deletion of audit log information • Security event notifications include the following: • Successful and unsuccessful attempts to connect to the content and production network • Unusual file size and/or time of day transport of content • Repeated attempts for unauthorized access • Attempts at privileged access (e.g., different locations, time of day, etc.) • Administrator account creation, modification, or deletion • File Integrity Monitoring (FIM) for sensitive data and applications • Failure of critical security systems (e.g., Firewall, IDS/IPS, endpoint protection, physical and logical access controls, etc.)
TS-1.5	Security Information & Event Management	Establish a policy and process for Security Information & Event Management (SIEM), to include the following: • Centralized real-time logging of firewalls, authentication servers, network operating systems, content transfer systems, virtual machines/servers, storage services, databases, container-based application services, API gateway connectors, key generation/management, etc. • Log the following attributes for network activity: source IP address, destination URL, or IP address, username, action attempted, action result, execution/file path, timestamp • Send automatic notifications when security events are detected • Assign personnel to review logs and respond to notifications • Log all remote access activities • Encrypt logs and associated logging data over external networks • Restrict access to, deletion, and modification of logs to authorized personnel only • Regularly review system logs • Retain logs for a period of one year, or the maximum time allowed in accordance with local laws, regulations, and agreements • Utilize a synchronized time service protocol (e.g., Network Time Protocol (NTP)) • Incorporate into Business Continuity Plan (OR-1.2) & Incident Response (OR-4.0) procedures	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	• Enable local logging on isolated systems • Include logging and monitoring of spikes in resource utilization and capacity management • Enable dual authorization for movement and deletion of audit log information • Security event notifications include the following: • Successful and unsuccessful attempts to connect to the content and production network • Unusual file size and/or time of day transport of content • Repeated attempts for unauthorized access • Attempts at privileged access (e.g., different locations, time of day, etc.) • Administrator account creation, modification, or deletion • File Integrity Monitoring (FIM) for sensitive data and applications • Failure of critical security systems (e.g., Firewall, IDS/IPS, endpoint protection, physical and logical access controls, etc.)
TS-1.5	Security Information & Event Management	Establish a policy and process for Security Information & Event Management (SIEM), to include the following: • Centralized real-time logging of firewalls, authentication servers, network operating systems, content transfer systems, virtual machines/servers, storage services, databases, container-based application services, API gateway connectors, key generation/management, etc. • Log the following attributes for network activity: source IP address, destination URL, or IP address, username, action attempted, action result, execution/file path, timestamp • Send automatic notifications when security events are detected • Assign personnel to review logs and respond to notifications • Log all remote access activities • Encrypt logs and associated logging data over external networks • Restrict access to, deletion, and modification of logs to authorized personnel only • Regularly review system logs • Retain logs for a period of one year, or the maximum time allowed in accordance with local laws, regulations, and agreements • Utilize a synchronized time service protocol (e.g., Network Time Protocol (NTP)) • Incorporate into Business Continuity Plan (OR-1.2) & Incident Response (OR-4.0) procedures	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	5	• Enable local logging on isolated systems • Include logging and monitoring of spikes in resource utilization and capacity management • Enable dual authorization for movement and deletion of audit log information • Security event notifications include the following: • Successful and unsuccessful attempts to connect to the content and production network • Unusual file size and/or time of day transport of content • Repeated attempts for unauthorized access • Attempts at privileged access (e.g., different locations, time of day, etc.) • Administrator account creation, modification, or deletion • File Integrity Monitoring (FIM) for sensitive data and applications • Failure of critical security systems (e.g., Firewall, IDS/IPS, endpoint protection, physical and logical access controls, etc.)
TS-1.5	Security Information & Event Management	Establish a policy and process for Security Information & Event Management (SIEM), to include the following: • Centralized real-time logging of firewalls, authentication servers, network operating systems, content transfer systems, virtual machines/servers, storage services, databases, container-based application services, API gateway connectors, key generation/management, etc. • Log the following attributes for network activity: source IP address, destination URL, or IP address, username, action attempted, action result, execution/file path, timestamp • Send automatic notifications when security events are detected • Assign personnel to review logs and respond to notifications • Log all remote access activities • Encrypt logs and associated logging data over external networks • Restrict access to, deletion, and modification of logs to authorized personnel only • Regularly review system logs • Retain logs for a period of one year, or the maximum time allowed in accordance with local laws, regulations, and agreements • Utilize a synchronized time service protocol (e.g., Network Time Protocol (NTP)) • Incorporate into Business Continuity Plan (OR-1.2) & Incident Response (OR-4.0) procedures	Functional	Intersects With	Clock Synchronization	SEA-20	Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.	5	• Enable local logging on isolated systems • Include logging and monitoring of spikes in resource utilization and capacity management • Enable dual authorization for movement and deletion of audit log information • Security event notifications include the following: • Successful and unsuccessful attempts to connect to the content and production network • Unusual file size and/or time of day transport of content • Repeated attempts for unauthorized access • Attempts at privileged access (e.g., different locations, time of day, etc.) • Administrator account creation, modification, or deletion • File Integrity Monitoring (FIM) for sensitive data and applications • Failure of critical security systems (e.g., Firewall, IDS/IPS, endpoint protection, physical and logical access controls, etc.)
TS-1.6	Authentication	Establish and regularly review a policy to enforce Authentication of all relevant full- and part-time employees, consultants, contractors, interns, freelancers, temporary workers, authorized accounts, and service accounts, to include the following: • Enforce strong authentication (MFA), apply to the following: • For Multi-Factor Authentication (MFA), apply to the following: • Minimum assessment or passphrase age of 1 year (not applicable to service accounts) • Configure a maximum of 5 invalid login attempts, prohibit reuse of previous 5 passwords or passphrases (not applicable to service accounts) and restrict reuse up to 10 system administrators • Any internet-facing systems (e.g., webmail, web portals, etc.) • Authentication access to hosting infrastructure and managed systems (e.g., Firewall, IDS/IPS, endpoint protection, physical and logical access controls, etc.) • One factor is provided by a separate system (e.g., authenticator apps, biometrics, etc.) • For passwords or passphrases: • Minimum 16 character length • Minimum of 3 of the following parameters: upper case, lower case, numeric, or special characters • Maximum password or passphrase age of 1 year (not applicable to service accounts) • Minimum assessment or passphrase age of 1 year (not applicable to service accounts) • Change password or passphrase upon suspicious activity or incident • For all accounts: • Use secondary communication protocol to share passwords and passphrases • Do not include repeating characters, patterns (e.g., 123123), account name, service name, company name, individual's name, individual's date of birth, any personal details, weak, compromised, and/or commonly known passwords	Functional	Subset Of	Identify & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	• Apply MFA to all accounts • For MFA, avoid using SMS, RBA (Knowledge Based Authentication), or email • Change all account passwords every 90 days • Always use company email address when registering, logging in, or creating applications to transfer controls • Validate user against existing authentication platforms (e.g., Duo, Okta, etc.) through integrations to a Single Sign-On service • Utilize passkeys instead of passwords • For admin accounts, use hardware tokens or FIDO2 Standards/UF2 compliant solutions • Verify accounts are used for intended purposes only (e.g., administrative, application-to-application communications, etc.) • Monitor and centrally log of successful and failed logins • Establish periodic audits of authentication and access activities • Utilize Privileged Account Management (PAM) tool • For admin accounts, use hardware tokens or FIDO2 Standards/UF2 compliant solutions

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Relationship	STRM Relationship	SCF Control	SCF #	Security Controls Framework (SCF) Control Description	Strength of Relationship	Notes
TS-1.6	Authentication	<p>Establish and regularly review a policy to enforce Authentication of all relevant full- and part-time employees, consultants, contractors, interns, freelancers, temporary workers, administrative accounts, and service accounts, to include the following:</p> <ul style="list-style-type: none"> Unique username For Multi-Factor Authentication (MFA), apply to the following: <ul style="list-style-type: none"> Use an application-based TOTP solution or hardware-based keys (e.g., FIDO2, WebAuthn keys, etc.) Any internet-facing systems (e.g., external, web portals, etc.) Administrative access to hosting infrastructure and management consoles One factor is provided by a separate system (e.g., authenticator apps, biometrics, etc.) For passwords and passphrases: <ul style="list-style-type: none"> Minimum 16 character length Minimum 3 of the following parameters: upper case, lower case, numeric, or special characters Maximum password or passphrase age of 1 year (not applicable to service accounts) Minimum password or passphrase age of 1 day (not applicable to service accounts) Configure a maximum of 5 invalid login attempts, prohibit reuse of previous 5 passwords or passphrases (not applicable to service accounts), and restrict account unlocking to system administrators Change password or passphrase upon suspicious activity or incident For new accounts, use temporary passwords that are randomly generated, unique, and comply with complexity rules Use secondary communication protocol to share passwords and passphrases Do not include repeating characters, patterns (e.g., 123123), account name, service name, company name, individual's name, individual's date of birth, any personal details, weak, compromised, and/or commonly known passwords 	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAE-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP)	8	<ul style="list-style-type: none"> Apply MFA to all accounts For MFA, avoid using SMS, SBA (Knowledge Based Authentication), or email Change all account passwords every 90 days Always use company email address when registering, logging into, or accessing applications to transfer content Validate users against existing authentication platforms (e.g., Active Directory) through integration to a Single Sign-On service Utilize passkeys instead of passwords Standardize naming conventions for usernames Review user accounts regularly and decommission expired or inactive accounts For administrator, service accounts, and personnel who support, develop or maintain applications: <ul style="list-style-type: none"> Verify accounts are used for intended purposes only (e.g., database queries, application-to-application communication, etc.) Monitor and centrally log of successful and failed logins Establish procedures to define and lockout suspicious activity Utilize Privileged Account Management (PAM) tool For admin accounts, use hardware tokens or FIDO2 Standard/U2F compliant solutions
TS-1.6	Authentication	<p>Establish and regularly review a policy to enforce Authentication of all relevant full- and part-time employees, consultants, contractors, interns, freelancers, temporary workers, administrative accounts, and service accounts, to include the following:</p> <ul style="list-style-type: none"> Unique username For Multi-Factor Authentication (MFA), apply to the following: <ul style="list-style-type: none"> Use an application-based TOTP solution or hardware-based keys (e.g., FIDO2, WebAuthn keys, etc.) Any internet-facing systems (e.g., external, web portals, etc.) Administrative access to hosting infrastructure and management consoles One factor is provided by a separate system (e.g., authenticator apps, biometrics, etc.) For passwords and passphrases: <ul style="list-style-type: none"> Minimum 16 character length Minimum 3 of the following parameters: upper case, lower case, numeric, or special characters Maximum password or passphrase age of 1 year (not applicable to service accounts) Minimum password or passphrase age of 1 day (not applicable to service accounts) Configure a maximum of 5 invalid login attempts, prohibit reuse of previous 5 passwords or passphrases (not applicable to service accounts), and restrict account unlocking to system administrators Change password or passphrase upon suspicious activity or incident For new accounts, use temporary passwords that are randomly generated, unique, and comply with complexity rules Use secondary communication protocol to share passwords and passphrases Do not include repeating characters, patterns (e.g., 123123), account name, service name, company name, individual's name, individual's date of birth, any personal details, weak, compromised, and/or commonly known passwords 	Functional	Intersects With	Identification & Authentication for Organizational Users	IAE-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users	5	<ul style="list-style-type: none"> Apply MFA to all accounts For MFA, avoid using SMS, SBA (Knowledge Based Authentication), or email Change all account passwords every 90 days Always use company email address when registering, logging into, or accessing applications to transfer content Validate users against existing authentication platforms (e.g., Active Directory) through integration to a Single Sign-On service Utilize passkeys instead of passwords Review user accounts regularly and decommission expired or inactive accounts For administrator, service accounts, and personnel who support, develop or maintain applications: <ul style="list-style-type: none"> Verify accounts are used for intended purposes only (e.g., database queries, application-to-application communication, etc.) Monitor and centrally log of successful and failed logins Establish procedures to define and lockout suspicious activity Utilize Privileged Account Management (PAM) tool For admin accounts, use hardware tokens or FIDO2 Standard/U2F compliant solutions
TS-1.6	Authentication	<p>Establish and regularly review a policy to enforce Authentication of all relevant full- and part-time employees, consultants, contractors, interns, freelancers, temporary workers, administrative accounts, and service accounts, to include the following:</p> <ul style="list-style-type: none"> Unique username For Multi-Factor Authentication (MFA), apply to the following: <ul style="list-style-type: none"> Use an application-based TOTP solution or hardware-based keys (e.g., FIDO2, WebAuthn keys, etc.) Any internet-facing systems (e.g., external, web portals, etc.) Administrative access to hosting infrastructure and management consoles One factor is provided by a separate system (e.g., authenticator apps, biometrics, etc.) For passwords and passphrases: <ul style="list-style-type: none"> Minimum 16 character length Minimum 3 of the following parameters: upper case, lower case, numeric, or special characters Maximum password or passphrase age of 1 year (not applicable to service accounts) Minimum password or passphrase age of 1 day (not applicable to service accounts) Configure a maximum of 5 invalid login attempts, prohibit reuse of previous 5 passwords or passphrases (not applicable to service accounts), and restrict account unlocking to system administrators Change password or passphrase upon suspicious activity or incident For new accounts, use temporary passwords that are randomly generated, unique, and comply with complexity rules Use secondary communication protocol to share passwords and passphrases Do not include repeating characters, patterns (e.g., 123123), account name, service name, company name, individual's name, individual's date of birth, any personal details, weak, compromised, and/or commonly known passwords 	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAE-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: <ol style="list-style-type: none"> Remote network access; Third-party Technology Assets, Applications and/or Services (TAAS); and/or Non-combined access for critical TAAS that store, transmit and/or process sensitive/regulated data. 	5	<ul style="list-style-type: none"> Apply MFA to all accounts For MFA, avoid using SMS, SBA (Knowledge Based Authentication), or email Change all account passwords every 90 days Always use company email address when registering, logging into, or accessing applications to transfer content Validate users against existing authentication platforms (e.g., Active Directory) through integration to a Single Sign-On service Utilize passkeys instead of passwords Standardize naming conventions for usernames Review user accounts regularly and decommission expired or inactive accounts For administrator, service accounts, and personnel who support, develop or maintain applications: <ul style="list-style-type: none"> Verify accounts are used for intended purposes only (e.g., database queries, application-to-application communication, etc.) Monitor and centrally log of successful and failed logins Establish procedures to define and lockout suspicious activity Utilize Privileged Account Management (PAM) tool For admin accounts, use hardware tokens or FIDO2 Standard/U2F compliant solutions
TS-1.6	Authentication	<p>Establish and regularly review a policy to enforce Authentication of all relevant full- and part-time employees, consultants, contractors, interns, freelancers, temporary workers, administrative accounts, and service accounts, to include the following:</p> <ul style="list-style-type: none"> Unique username For Multi-Factor Authentication (MFA), apply to the following: <ul style="list-style-type: none"> Use an application-based TOTP solution or hardware-based keys (e.g., FIDO2, WebAuthn keys, etc.) Any internet-facing systems (e.g., external, web portals, etc.) Administrative access to hosting infrastructure and management consoles One factor is provided by a separate system (e.g., authenticator apps, biometrics, etc.) For passwords and passphrases: <ul style="list-style-type: none"> Minimum 16 character length Minimum 3 of the following parameters: upper case, lower case, numeric, or special characters Maximum password or passphrase age of 1 year (not applicable to service accounts) Minimum password or passphrase age of 1 day (not applicable to service accounts) Configure a maximum of 5 invalid login attempts, prohibit reuse of previous 5 passwords or passphrases (not applicable to service accounts), and restrict account unlocking to system administrators Change password or passphrase upon suspicious activity or incident For new accounts, use temporary passwords that are randomly generated, unique, and comply with complexity rules Use secondary communication protocol to share passwords and passphrases Do not include repeating characters, patterns (e.g., 123123), account name, service name, company name, individual's name, individual's date of birth, any personal details, weak, compromised, and/or commonly known passwords 	Functional	Intersects With	Identifier Management (User Names)	IAE-09	Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS)	5	<ul style="list-style-type: none"> Apply MFA to all accounts For MFA, avoid using SMS, SBA (Knowledge Based Authentication), or email Change all account passwords every 90 days Always use company email address when registering, logging into, or accessing applications to transfer content Validate users against existing authentication platforms (e.g., Active Directory) through integration to a Single Sign-On service Utilize passkeys instead of passwords Standardize naming conventions for usernames Review user accounts regularly and decommission expired or inactive accounts For administrator, service accounts, and personnel who support, develop or maintain applications: <ul style="list-style-type: none"> Verify accounts are used for intended purposes only (e.g., database queries, application-to-application communication, etc.) Monitor and centrally log of successful and failed logins Establish procedures to define and lockout suspicious activity Utilize Privileged Account Management (PAM) tool For admin accounts, use hardware tokens or FIDO2 Standard/U2F compliant solutions
TS-1.6	Authentication	<p>Establish and regularly review a policy to enforce Authentication of all relevant full- and part-time employees, consultants, contractors, interns, freelancers, temporary workers, administrative accounts, and service accounts, to include the following:</p> <ul style="list-style-type: none"> Unique username For Multi-Factor Authentication (MFA), apply to the following: <ul style="list-style-type: none"> Use an application-based TOTP solution or hardware-based keys (e.g., FIDO2, WebAuthn keys, etc.) Any internet-facing systems (e.g., external, web portals, etc.) Administrative access to hosting infrastructure and management consoles One factor is provided by a separate system (e.g., authenticator apps, biometrics, etc.) For passwords and passphrases: <ul style="list-style-type: none"> Minimum 16 character length Minimum 3 of the following parameters: upper case, lower case, numeric, or special characters Maximum password or passphrase age of 1 year (not applicable to service accounts) Minimum password or passphrase age of 1 day (not applicable to service accounts) Configure a maximum of 5 invalid login attempts, prohibit reuse of previous 5 passwords or passphrases (not applicable to service accounts), and restrict account unlocking to system administrators Change password or passphrase upon suspicious activity or incident For new accounts, use temporary passwords that are randomly generated, unique, and comply with complexity rules Use secondary communication protocol to share passwords and passphrases Do not include repeating characters, patterns (e.g., 123123), account name, service name, company name, individual's name, individual's date of birth, any personal details, weak, compromised, and/or commonly known passwords 	Functional	Intersects With	User Identity (ID) Management	IAE-09.1	Mechanisms exist to ensure proper user identification management for non-consumer users and administrators.	5	<ul style="list-style-type: none"> Apply MFA to all accounts For MFA, avoid using SMS, SBA (Knowledge Based Authentication), or email Change all account passwords every 90 days Always use company email address when registering, logging into, or accessing applications to transfer content Validate users against existing authentication platforms (e.g., Active Directory) through integration to a Single Sign-On service Utilize passkeys instead of passwords Standardize naming conventions for usernames Review user accounts regularly and decommission expired or inactive accounts For administrator, service accounts, and personnel who support, develop or maintain applications: <ul style="list-style-type: none"> Verify accounts are used for intended purposes only (e.g., database queries, application-to-application communication, etc.) Monitor and centrally log of successful and failed logins Establish procedures to define and lockout suspicious activity Utilize Privileged Account Management (PAM) tool For admin accounts, use hardware tokens or FIDO2 Standard/U2F compliant solutions
TS-1.6	Authentication	<p>Establish and regularly review a policy to enforce Authentication of all relevant full- and part-time employees, consultants, contractors, interns, freelancers, temporary workers, administrative accounts, and service accounts, to include the following:</p> <ul style="list-style-type: none"> Unique username For Multi-Factor Authentication (MFA), apply to the following: <ul style="list-style-type: none"> Use an application-based TOTP solution or hardware-based keys (e.g., FIDO2, WebAuthn keys, etc.) Any internet-facing systems (e.g., external, web portals, etc.) Administrative access to hosting infrastructure and management consoles One factor is provided by a separate system (e.g., authenticator apps, biometrics, etc.) For passwords and passphrases: <ul style="list-style-type: none"> Minimum 16 character length Minimum 3 of the following parameters: upper case, lower case, numeric, or special characters Maximum password or passphrase age of 1 year (not applicable to service accounts) Minimum password or passphrase age of 1 day (not applicable to service accounts) Configure a maximum of 5 invalid login attempts, prohibit reuse of previous 5 passwords or passphrases (not applicable to service accounts), and restrict account unlocking to system administrators Change password or passphrase upon suspicious activity or incident For new accounts, use temporary passwords that are randomly generated, unique, and comply with complexity rules Use secondary communication protocol to share passwords and passphrases Do not include repeating characters, patterns (e.g., 123123), account name, service name, company name, individual's name, individual's date of birth, any personal details, weak, compromised, and/or commonly known passwords 	Functional	Intersects With	Authenticator Management	IAE-10	Mechanisms exist to: <ol style="list-style-type: none"> Securely manage authenticators for users and devices; and Ensure the strength of authentication is appropriate to the classification of the data being accessed. 	5	<ul style="list-style-type: none"> Apply MFA to all accounts For MFA, avoid using SMS, SBA (Knowledge Based Authentication), or email Change all account passwords every 90 days Always use company email address when registering, logging into, or accessing applications to transfer content Validate users against existing authentication platforms (e.g., Active Directory) through integration to a Single Sign-On service Utilize passkeys instead of passwords Standardize naming conventions for usernames Review user accounts regularly and decommission expired or inactive accounts For administrator, service accounts, and personnel who support, develop or maintain applications: <ul style="list-style-type: none"> Verify accounts are used for intended purposes only (e.g., database queries, application-to-application communication, etc.) Monitor and centrally log of successful and failed logins Establish procedures to define and lockout suspicious activity Utilize Privileged Account Management (PAM) tool For admin accounts, use hardware tokens or FIDO2 Standard/U2F compliant solutions
TS-1.6	Authentication	<p>Establish and regularly review a policy to enforce Authentication of all relevant full- and part-time employees, consultants, contractors, interns, freelancers, temporary workers, administrative accounts, and service accounts, to include the following:</p> <ul style="list-style-type: none"> Unique username For Multi-Factor Authentication (MFA), apply to the following: <ul style="list-style-type: none"> Use an application-based TOTP solution or hardware-based keys (e.g., FIDO2, WebAuthn keys, etc.) Any internet-facing systems (e.g., external, web portals, etc.) Administrative access to hosting infrastructure and management consoles One factor is provided by a separate system (e.g., authenticator apps, biometrics, etc.) For passwords and passphrases: <ul style="list-style-type: none"> Minimum 16 character length Minimum 3 of the following parameters: upper case, lower case, numeric, or special characters Maximum password or passphrase age of 1 year (not applicable to service accounts) Minimum password or passphrase age of 1 day (not applicable to service accounts) Configure a maximum of 5 invalid login attempts, prohibit reuse of previous 5 passwords or passphrases (not applicable to service accounts), and restrict account unlocking to system administrators Change password or passphrase upon suspicious activity or incident For new accounts, use temporary passwords that are randomly generated, unique, and comply with complexity rules Use secondary communication protocol to share passwords and passphrases Do not include repeating characters, patterns (e.g., 123123), account name, service name, company name, individual's name, individual's date of birth, any personal details, weak, compromised, and/or commonly known passwords 	Functional	Intersects With	Password-Based Authentication	IAE-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication	5	<ul style="list-style-type: none"> Apply MFA to all accounts For MFA, avoid using SMS, SBA (Knowledge Based Authentication), or email Change all account passwords every 90 days Always use company email address when registering, logging into, or accessing applications to transfer content Validate users against existing authentication platforms (e.g., Active Directory) through integration to a Single Sign-On service Utilize passkeys instead of passwords Standardize naming conventions for usernames Review user accounts regularly and decommission expired or inactive accounts For administrator, service accounts, and personnel who support, develop or maintain applications: <ul style="list-style-type: none"> Verify accounts are used for intended purposes only (e.g., database queries, application-to-application communication, etc.) Monitor and centrally log of successful and failed logins Establish procedures to define and lockout suspicious activity Utilize Privileged Account Management (PAM) tool For admin accounts, use hardware tokens or FIDO2 Standard/U2F compliant solutions
TS-1.7	Authorization	<p>Establish and regularly review a process for Authorization based on a User Model. To include the following:</p> <ul style="list-style-type: none"> Based on the Principle of Least Privilege (POLP) For application development, separate user roles between development and deployment Define and manage interactive and non-interactive (e.g., programmatic access, NHI, API, etc.) roles, functions, and permissions Perform permissions and access reviews of all accounts, including expired and inactive accounts, on a quarterly basis at a minimum 	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAE-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP)	5	<ul style="list-style-type: none"> Regularly review application resources (e.g., servers, databases, applications, SaaS apps, etc.) for appropriate access and privileges
TS-1.7	Authorization	<p>Establish and regularly review a process for Authorization based on a User Model. To include the following:</p> <ul style="list-style-type: none"> Based on the Principle of Least Privilege (POLP) For application development, separate user roles between development and deployment Define and manage interactive and non-interactive (e.g., programmatic access, NHI, API, etc.) roles, functions, and permissions Perform permissions and access reviews of all accounts, including expired and inactive accounts, on a quarterly basis at a minimum 	Functional	Intersects With	Role-Based Access Control (RBAC)	IAE-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	<ul style="list-style-type: none"> Regularly review application resources (e.g., servers, databases, applications, SaaS apps, etc.) for appropriate access and privileges

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Relationship	STRM Relationship	SCF Control	SCF #	Security Controls Framework (SCF) Control Description	Strength of Relationship	Notes
TS-1.13	Secure Software Development Life Cycle	Establish and regularly review a policy and process for Secure Software Development Life Cycle (SSDLC) for application design, development, deployment, to include the following: • A software testing strategy • Perform a code review for each release • Restrict deployment of non-production testing functions into production (e.g., debug functions, flags, etc.) • Scan open source libraries • Identify Access Management (IAM) to manage access to Continuous Integration (CI)/Continuous Delivery/Deployment (CD) components • Scanning (e.g., TFSAC) coverage for CI/CD automated pipelines and deployments (e.g., WhiteHat) • Investigate and have a remediation plan for issues • Do not hard code passwords, credentials, secrets, or other authentication data into source code or scripts • Mask passwords and other authentication data when displayed on screen by default • Obtain client approval for use of client data in non-production environments (e.g., Dev, QA, etc.) • Files containing executable content are digitally signed • Leverage Open Web Application Security Project (OWASP) Top Ten Web Application Security Risks • Perform security testing when changes are made to application code (e.g., updates, enhancements, etc.) • Store application security reports in an accessible repository	Functional	Intersects With	Software Design Review	TDA-06.5	Mechanisms exist to have an independent review of the software design to validate: 1) Applicable security, compliance and resilience requirements are met and 2) Identified risks are remediated.	5	<ul style="list-style-type: none"> Conduct an independent review of the code annually or on other releases Document and restrict the results of the code review to authorized personnel only Employ inspection relay techniques to prevent Man-In-The-Middle (MITM) attacks on client and server software Test Open Source Software (OSS) and third-party software or source code for vulnerabilities Incorporate Root or jailbreak detection Utilize code protection techniques (e.g., obfuscation, debug detection, etc.) Reference NIST: Secure Software Development Framework (SSDF) NIST 800-218 (https://csrc.nist.gov/projects/ssf) as an example for Threat Modeling and on how to develop a Secure Software Development Life Cycle (SSDLC) process for coverage of training, requirements, design, development, testing, release, and response.
TS-1.13	Secure Software Development Life Cycle	Establish and regularly review a policy and process for Secure Software Development Life Cycle (SSDLC) for application design, development, deployment, to include the following: • A software testing strategy • Perform a code review for each release • Restrict deployment of non-production testing functions into production (e.g., debug functions, flags, etc.) • Scan open source libraries • Identify Access Management (IAM) to manage access to Continuous Integration (CI)/Continuous Delivery/Deployment (CD) components • Scanning (e.g., TFSAC) coverage for CI/CD automated pipelines and deployments (e.g., WhiteHat) • Investigate and have a remediation plan for issues • Do not hard code passwords, credentials, secrets, or other authentication data into source code or scripts • Mask passwords and other authentication data when displayed on screen by default • Obtain client approval for use of client data in non-production environments (e.g., Dev, QA, etc.) • Files containing executable content are digitally signed • Leverage Open Web Application Security Project (OWASP) Top Ten Web Application Security Risks • Perform security testing when changes are made to application code (e.g., updates, enhancements, etc.) • Store application security reports in an accessible repository	Functional	Intersects With	Software Design Root Cause Analysis	TDA-06.6	Mechanisms exist to assess software design processes that includes: 1) Conducting Root Cause Analysis (RCA) to identify the underlying causes of issues or failures 2) Developing actions to address the root cause of the issue or failure; and 3) Implementing the actions and monitoring the implementation for effectiveness.	5	<ul style="list-style-type: none"> Conduct an independent review of the code annually or on other releases Document and restrict the results of the code review to authorized personnel only Employ inspection relay techniques to prevent Man-In-The-Middle (MITM) attacks on client and server software Test Open Source Software (OSS) and third-party software or source code for vulnerabilities Incorporate Root or jailbreak detection Utilize code protection techniques (e.g., obfuscation, debug detection, etc.) Reference NIST: Secure Software Development Framework (SSDF) NIST 800-218 (https://csrc.nist.gov/projects/ssf) as an example for Threat Modeling and on how to develop a Secure Software Development Life Cycle (SSDLC) process for coverage of training, requirements, design, development, testing, release, and response.
TS-1.13	Secure Software Development Life Cycle	Establish and regularly review a policy and process for Secure Software Development Life Cycle (SSDLC) for application design, development, deployment, to include the following: • A software testing strategy • Perform a code review for each release • Restrict deployment of non-production testing functions into production (e.g., debug functions, flags, etc.) • Scan open source libraries • Identify Access Management (IAM) to manage access to Continuous Integration (CI)/Continuous Delivery/Deployment (CD) components • Scanning (e.g., TFSAC) coverage for CI/CD automated pipelines and deployments (e.g., WhiteHat) • Investigate and have a remediation plan for issues • Do not hard code passwords, credentials, secrets, or other authentication data into source code or scripts • Mask passwords and other authentication data when displayed on screen by default • Obtain client approval for use of client data in non-production environments (e.g., Dev, QA, etc.) • Files containing executable content are digitally signed • Leverage Open Web Application Security Project (OWASP) Top Ten Web Application Security Risks • Perform security testing when changes are made to application code (e.g., updates, enhancements, etc.) • Store application security reports in an accessible repository	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: 1) Create and implement a Security Testing and Evaluation (SSTE) plan, or similar capability 2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and 3) Document the results.	5	<ul style="list-style-type: none"> Conduct an independent review of the code annually or on other releases Document and restrict the results of the code review to authorized personnel only Employ inspection relay techniques to prevent Man-In-The-Middle (MITM) attacks on client and server software Test Open Source Software (OSS) and third-party software or source code for vulnerabilities Incorporate Root or jailbreak detection Utilize code protection techniques (e.g., obfuscation, debug detection, etc.) Reference NIST: Secure Software Development Framework (SSDF) NIST 800-218 (https://csrc.nist.gov/projects/ssf) as an example for Threat Modeling and on how to develop a Secure Software Development Life Cycle (SSDLC) process for coverage of training, requirements, design, development, testing, release, and response.
TS-1.14	Security by Design & Privacy by Design	Incorporate the principles of Security by Design (SbD) and Privacy by Design (PbD) into system and application development, to include the following: • Data protection and privacy requirements are included by default across development life cycle • In accordance with local laws, regulations, and agreements	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-designed security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	8	<ul style="list-style-type: none"> Design documentation to describe how data is protected Utilize Data Loss Prevention (DLP) tools
TS-1.14	Security by Design & Privacy by Design	Incorporate the principles of Security by Design (SbD) and Privacy by Design (PbD) into system and application development, to include the following: • Data protection and privacy requirements are included by default across development life cycle • In accordance with local laws, regulations, and agreements	Functional	Intersects With	Reasonable Data Privacy Practices	PRD-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	8	<ul style="list-style-type: none"> Design documentation to describe how data is protected Utilize Data Loss Prevention (DLP) tools
TS-1.15	Code Repositories	Establish and regularly review a process for all forms of Code, to include the following: • Apply Encryption Best Practices (TS-3.0) to Code Repositories • Apply Authentication Best Practices (TS-1.6) to Code Repositories • Apply Authorization Best Practices (TS-1.7) to Code Repositories • Code version control • If maintained in-house, perform regular security test and scanning of repositories, and regularly update	Functional	Intersects With	Access to Program Source Code	TDA-20	Mechanisms exist to limit privileges to change software resident within software libraries.	8	<ul style="list-style-type: none"> Leverage a secrets management service to rotate, manage, and retrieve credentials or secrets (e.g., Vault, AWS KMS, GCP KMS, etc.) Key Management System (KMS) encryption for credentials and sensitive data
TS-1.15	Code Repositories	Establish and regularly review a process for all forms of Code, to include the following: • Apply Encryption Best Practices (TS-3.0) to Code Repositories • Apply Authentication Best Practices (TS-1.6) to Code Repositories • Apply Authorization Best Practices (TS-1.7) to Code Repositories • Code version control • If maintained in-house, perform regular security test and scanning of repositories, and regularly update	Functional	Intersects With	Software Release Integrity Verification	TDA-20.1	Mechanisms exist to publish integrity verification information for software releases.	8	<ul style="list-style-type: none"> Leverage a secrets management service to rotate, manage, and retrieve credentials or secrets (e.g., Vault, AWS KMS, GCP KMS, etc.) Key Management System (KMS) encryption for credentials and sensitive data
TS-1.15	Code Repositories	Establish and regularly review a process for all forms of Code, to include the following: • Apply Encryption Best Practices (TS-3.0) to Code Repositories • Apply Authentication Best Practices (TS-1.6) to Code Repositories • Apply Authorization Best Practices (TS-1.7) to Code Repositories • Code version control • If maintained in-house, perform regular security test and scanning of repositories, and regularly update	Functional	Intersects With	Archiving Software Releases	TDA-20.2	Mechanisms exist to archive software releases and all of their components (e.g., code, package file, third-party libraries, documentation) to maintain integrity verification information.	8	<ul style="list-style-type: none"> Leverage a secrets management service to rotate, manage, and retrieve credentials or secrets (e.g., Vault, AWS KMS, GCP KMS, etc.) Key Management System (KMS) encryption for credentials and sensitive data
TS-1.15	Code Repositories	Establish and regularly review a process for all forms of Code, to include the following: • Apply Encryption Best Practices (TS-3.0) to Code Repositories • Apply Authentication Best Practices (TS-1.6) to Code Repositories • Apply Authorization Best Practices (TS-1.7) to Code Repositories • Code version control • If maintained in-house, perform regular security test and scanning of repositories, and regularly update	Functional	Intersects With	Approved Code	TDA-20.4	Mechanisms exist to govern the approval of binaries and code for production use.	8	<ul style="list-style-type: none"> Leverage a secrets management service to rotate, manage, and retrieve credentials or secrets (e.g., Vault, AWS KMS, GCP KMS, etc.) Key Management System (KMS) encryption for credentials and sensitive data
TS-1.16	Content Transfer Systems	Establish and regularly review a policy and process to deploy and use Content Transfer Systems, to include the following: • Transfer content via dedicated Content Transfer Systems • Approval process to authorize the transfer of content • Separate Content Transfer Systems from production, non-production, and external networks • Delete content after it has been on the system for more than 24 hours • Apply Encryption Best Practices (TS-3.0)	Functional	Intersects With	As-He-Transfers	DCH-17	Mechanisms exist to secure as-he-exchanges of large digital files with internal or external parties.	3	<ul style="list-style-type: none"> Use client-approved transfer systems Configure an exception process Send automatic notifications upon outbound content Create and maintain a list of users who are responsible for transferring content Configure allowing on content transfer servers to only allow transfers to and from authorized external transfer servers Do not embed usernames and passwords into content links or cache them in browsers Distribute user credentials and content links using separate forms of communication Avoid using SMS for distributing user credentials and content links Assign Static IPs and/or utilize MAC filtering
TS-1.17	Application Configuration (Guidelines) (Licensed)	Source, apply, and annually review formal Licensed Application Configuration Guidelines provided by the licensee, to include the following: • Confirm licensing agreement is from an authorized source and is not expired • Review and update the application configuration guidelines annually and/or when system components are installed or upgraded • Implement the following from the guidelines: • Minimize the number of identities with privileged or administrator level access • Disable unnecessary, unused, or insecure identities • Disable or restrict unnecessary functions and services • Sessions automatically expire after a maximum of 15 minutes of user inactivity	Functional	Intersects With	Software Licensing Restrictions	AST-02.7	Mechanisms exist to protect Intellectual Property (IP) rights with software licensing restrictions.	5	<ul style="list-style-type: none"> Package installed matches published version Verify checksums
TS-1.17	Application Configuration (Guidelines) (Licensed)	Source, apply, and annually review formal Licensed Application Configuration Guidelines provided by the licensee, to include the following: • Confirm licensing agreement is from an authorized source and is not expired • Review and update the application configuration guidelines annually and/or when system components are installed or upgraded • Implement the following from the guidelines: • Minimize the number of identities with privileged or administrator level access • Disable unnecessary, unused, or insecure identities • Disable or restrict unnecessary functions and services • Sessions automatically expire after a maximum of 15 minutes of user inactivity	Functional	Intersects With	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: 1) Secure configuration, installation and operation of the TAAS; 2) Effective use and maintenance of security features/functions; and 3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	5	<ul style="list-style-type: none"> Package installed matches published version Verify checksums
TS-1.18	Application Configuration (Guidelines) (In-House Developed)	Establish and annually review a process for formal In-House Developed Application Guidelines, to include the following: • Update when system components are installed, upgraded, or decommissioned • For application design documents, review and update annually and/or when system components are installed, upgraded, or decommissioned • Apply to in-house developed scripts • Implement the following from the guidelines: • Minimize the number of identities with privileged or administrator level access • Disable unnecessary, unused, or insecure identities • Disable or restrict unnecessary functions and services • Sessions automatically expire after a maximum of 15 minutes of user inactivity	Functional	Intersects With	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: 1) Secure configuration, installation and operation of the TAAS; 2) Effective use and maintenance of security features/functions; and 3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	5	<ul style="list-style-type: none"> Document components used as application building blocks Leverage Red Team or cybersecurity professionals to identify vulnerabilities (e.g., source code, source code repositories, API integrations, etc.) Adhere to Center for Internet Security (CIS) Critical Security Controls, implementation Group (IG1) hardening Make configuration guidelines available to licensees
TS-2.0	Network Configuration	Place externally accessible servers (e.g., web servers, remote access servers, VPN gateways, remote access brokers, application servers, etc.) within a DMZ, VLAN, or a public subnet DMZ within a Virtual Private Cloud (VPC), to include the following: • Isolate servers in the DMZ to provide only one type of service each • Restrict access to the internal network from the DMZ • Restrict access from public subnets to private subnets within a VPC (e.g., ACLs, security groups, etc.) • Maintain an inventory of external IP addresses and components exposed to the Internet	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	<ul style="list-style-type: none"> Regularly review managed network device (e.g., Firewalls, Routers, ISPs, etc.) configurations Regularly review restrictions (e.g., IP addresses, ACLs, security groups, etc.)
TS-2.0	Network Configuration	Place externally accessible servers (e.g., web servers, remote access servers, VPN gateways, remote access brokers, application servers, etc.) within a DMZ, VLAN, or a public subnet DMZ within a Virtual Private Cloud (VPC), to include the following: • Isolate servers in the DMZ to provide only one type of service each • Restrict access to the internal network from the DMZ • Restrict access from public subnets to private subnets within a VPC (e.g., ACLs, security groups, etc.) • Maintain an inventory of external IP addresses and components exposed to the Internet	Functional	Intersects With	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to security design, configure and maintain cloud environments.	5	<ul style="list-style-type: none"> Regularly review managed network device (e.g., Firewalls, Routers, ISPs, etc.) configurations Regularly review restrictions (e.g., IP addresses, ACLs, security groups, etc.)
TS-2.0	Network Configuration	Place externally accessible servers (e.g., web servers, remote access servers, VPN gateways, remote access brokers, application servers, etc.) within a DMZ, VLAN, or a public subnet DMZ within a Virtual Private Cloud (VPC), to include the following: • Isolate servers in the DMZ to provide only one type of service each • Restrict access to the internal network from the DMZ • Restrict access from public subnets to private subnets within a VPC (e.g., ACLs, security groups, etc.) • Maintain an inventory of external IP addresses and components exposed to the Internet	Functional	Intersects With	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	5	<ul style="list-style-type: none"> Regularly review managed network device (e.g., Firewalls, Routers, ISPs, etc.) configurations Regularly review restrictions (e.g., IP addresses, ACLs, security groups, etc.)
TS-2.0	Network Configuration	Place externally accessible servers (e.g., web servers, remote access servers, VPN gateways, remote access brokers, application servers, etc.) within a DMZ, VLAN, or a public subnet DMZ within a Virtual Private Cloud (VPC), to include the following: • Isolate servers in the DMZ to provide only one type of service each • Restrict access to the internal network from the DMZ • Restrict access from public subnets to private subnets within a VPC (e.g., ACLs, security groups, etc.) • Maintain an inventory of external IP addresses and components exposed to the Internet	Functional	Intersects With	Layered Network Defenses	NET-02	Mechanisms exist to implement security functions as a layered structure that minimizes interactions between layers of the design avoids any dependence by lower layers on the functionality or correctness of higher layers.	5	<ul style="list-style-type: none"> Regularly review managed network device (e.g., Firewalls, Routers, ISPs, etc.) configurations Regularly review restrictions (e.g., IP addresses, ACLs, security groups, etc.)
TS-2.0	Network Configuration	Place externally accessible servers (e.g., web servers, remote access servers, VPN gateways, remote access brokers, application servers, etc.) within a DMZ, VLAN, or a public subnet DMZ within a Virtual Private Cloud (VPC), to include the following: • Isolate servers in the DMZ to provide only one type of service each • Restrict access to the internal network from the DMZ • Restrict access from public subnets to private subnets within a VPC (e.g., ACLs, security groups, etc.) • Maintain an inventory of external IP addresses and components exposed to the Internet	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	<ul style="list-style-type: none"> Regularly review managed network device (e.g., Firewalls, Routers, ISPs, etc.) configurations Regularly review restrictions (e.g., IP addresses, ACLs, security groups, etc.)
TS-2.0	Network Configuration	Place externally accessible servers (e.g., web servers, remote access servers, VPN gateways, remote access brokers, application servers, etc.) within a DMZ, VLAN, or a public subnet DMZ within a Virtual Private Cloud (VPC), to include the following: • Isolate servers in the DMZ to provide only one type of service each • Restrict access to the internal network from the DMZ • Restrict access from public subnets to private subnets within a VPC (e.g., ACLs, security groups, etc.) • Maintain an inventory of external IP addresses and components exposed to the Internet	Functional	Intersects With	Data Flow Enforcement - Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	5	<ul style="list-style-type: none"> Regularly review managed network device (e.g., Firewalls, Routers, ISPs, etc.) configurations Regularly review restrictions (e.g., IP addresses, ACLs, security groups, etc.)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Relationship	STRM Relationship	SCF Control	SCF #	Security Controls Framework (SCF) Control Description	Strength of Relationship	Notes
TS-2.0	Network Configuration	Place externally accessible servers (e.g., web servers, remote access servers, VPN gateways, remote access brokers, application servers, etc.) within a DMZ, VLAN, or a public subnet DMZ within a Virtual Private Cloud (VPC). To include the following: • Isolate servers in the DMZ to provide only one type of service each. • Restrict access to the internal network from the DMZ. • Restrict access from public subnets to private subnets within a VPC (e.g., ACLs, security groups, etc.) • Maintain an inventory of external IP addresses and components exposed to the Internet.	Functional	Intersects With	Web Security	WEB-01	Mechanisms exist to facilitate the implementation of an enterprise-wide web management policy, as well as associated standards, controls, and procedures.	5	• Regularly review managed network device (e.g., Firewalls, Routers, IS/SPs, etc.) configurations. • Regularly review restrictions (e.g., IP addresses, ACLs, security groups, etc.)
TS-2.0	Network Configuration	Place externally accessible servers (e.g., web servers, remote access servers, VPN gateways, remote access brokers, application servers, etc.) within a DMZ, VLAN, or a public subnet DMZ within a Virtual Private Cloud (VPC). To include the following: • Isolate servers in the DMZ to provide only one type of service each. • Restrict access to the internal network from the DMZ. • Restrict access from public subnets to private subnets within a VPC (e.g., ACLs, security groups, etc.) • Maintain an inventory of external IP addresses and components exposed to the Internet.	Functional	Intersects With	Use of Demilitarized Zones (DMZ)	WEB-02	Mechanisms exist to utilize a Demilitarized Zone (DMZ) to restrict inbound traffic to authorized Technology Assets, Applications and/or Services (TAAS) on certain services, protocols and ports.	5	• Regularly review managed network device (e.g., Firewalls, Routers, IS/SPs, etc.) configurations. • Regularly review restrictions (e.g., IP addresses, ACLs, security groups, etc.)
TS-2.1	Point-to-Point Connections	Establish and regularly review a process to secure any Point-to-Point Connections, to include the following: • Use and encrypt communication over private connections (e.g., dark fiber, leased lines, MPLS, etc.) • Encrypt using AES-256 with TLS 1.3 at a minimum. • Document all Point-to-Point Connections (e.g., VPN, private fiber, etc.).	Functional	Subset Of	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	10	• If using a public network or a connection over the Internet, use a secure connection. • Regularly review Point-to-Point Connections
TS-2.2	Network Topology Diagram	Create a Network Infrastructure and Topology Diagram, to include the following: • Network segments (e.g., internal, DMZ, Data VO, etc.) • Access to the Internet and boundary controls. • Network path for client content data. • Remote-accessible network segments. • Update upon significant changes.	Functional	Subset Of	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: 1) Contain sufficient detail to assess the security of the network's architecture; 2) Reflect the current architecture of the network environment; and 3) Document all sensitive/regulatory data flows.	10	• Include WAN, DMZ, LAN, WLAN, VLAN, firewalls, switches, endpoints, etc.
TS-2.3	Network Traffic	Establish a policy to use layer 3 switches/devices to manage Network Traffic, to include the following: • Enable port security. • Disable unused switch ports or transfer to a separate, non-functional VLAN. • Disable Simple Network Management Protocol (SNMP) if it is not in use. • Use SNMP v3 at a minimum, with strong passwords for community strings.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	• Use device administrator credentials with strong passwords. • If enabled ports are enabled and/or on a functioning VLAN, use physical ethernet cable locks. • Network-based access control (e.g., 802.1X). • If layer 2 switches are still in use, confirm that a higher layer network communications device is providing network isolation and traffic control. • Restrict the use of non-switched devices such as hubs and repeaters.
TS-2.3	Network Traffic	Establish a policy to use layer 3 switches/devices to manage Network Traffic, to include the following: • Enable port security. • Disable unused switch ports or transfer to a separate, non-functional VLAN. • Disable Simple Network Management Protocol (SNMP) if it is not in use. • Use SNMP v3 at a minimum, with strong passwords for community strings.	Functional	Intersects With	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	8	• Use device administrator credentials with strong passwords. • If enabled ports are enabled and/or on a functioning VLAN, use physical ethernet cable locks. • Network-based access control (e.g., 802.1X). • If layer 2 switches are still in use, confirm that a higher layer network communications device is providing network isolation and traffic control. • Restrict the use of non-switched devices such as hubs and repeaters.
TS-2.4	Firewall Access Control List	Establish and regularly review a policy and process to separate external networks (WANs) from the internal networks) by using stateful inspection firewalls), to include the following: • Create an Access Control List (ACL). • Regularly review ACLs. • Generate logs for all traffic and configuration changes. • Regularly review logs. Apply the following configurations: • Deny all WAN traffic to any internal network other than to explicit hosts that reside on the DMZ. • Deny all incoming and outgoing network requests by default. • Block malicious sites at external and internal firewall level. • Enable only explicitly defined outgoing requests by specific protocol and destination. • For externally accessible hosts, only allow incoming requests to needed ports. • Restrict unencrypted communication protocols (e.g., Telnet, FTP, etc.). • Manage core services with a dedicated service or management network (e.g., DNS, antivirus, logging, etc.).	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	• Anti-spoofing filters. • Permit only authorized IP addresses and block unnecessary network traffic at the Firewall. • Regularly review the list of approved incoming and outgoing requests. • All attempts to access malicious web addresses are logged and monitored. • Deploy a Web Application Firewall (WAF) in front of Internet facing web applications and APIs. • Block the following: • Non-routable IP addresses over external ports. • User Datagram Protocol (UDP) or Internet Control Message Protocol (ICMP) echo requests. • Unused ports and services.
TS-2.4	Firewall Access Control List	Establish and regularly review a policy and process to separate external networks (WANs) from the internal networks) by using stateful inspection firewalls), to include the following: • Create an Access Control List (ACL). • Regularly review ACLs. • Generate logs for all traffic and configuration changes. • Regularly review logs. Apply the following configurations: • Deny all WAN traffic to any internal network other than to explicit hosts that reside on the DMZ. • Deny all incoming and outgoing network requests by default. • Block malicious sites at external and internal firewall level. • Enable only explicitly defined outgoing requests by specific protocol and destination. • For externally accessible hosts, only allow incoming requests to needed ports. • Restrict unencrypted communication protocols (e.g., Telnet, FTP, etc.). • Manage core services with a dedicated service or management network (e.g., DNS, antivirus, logging, etc.).	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: 1) At least annually. 2) When required due to so, or 3) As part of system component installations and upgrades.	5	• Anti-spoofing filters. • Permit only authorized IP addresses and block unnecessary network traffic at the Firewall. • Regularly review the list of approved incoming and outgoing requests. • All attempts to access malicious web addresses are logged and monitored. • Deploy a Web Application Firewall (WAF) in front of Internet facing web applications and APIs. • Block the following: • Non-routable IP addresses over external ports. • User Datagram Protocol (UDP) or Internet Control Message Protocol (ICMP) echo requests. • Unused ports and services.
TS-2.4	Firewall Access Control List	Establish and regularly review a policy and process to separate external networks (WANs) from the internal networks) by using stateful inspection firewalls), to include the following: • Create an Access Control List (ACL). • Regularly review ACLs. • Generate logs for all traffic and configuration changes. • Regularly review logs. Apply the following configurations: • Deny all WAN traffic to any internal network other than to explicit hosts that reside on the DMZ. • Deny all incoming and outgoing network requests by default. • Block malicious sites at external and internal firewall level. • Enable only explicitly defined outgoing requests by specific protocol and destination. • For externally accessible hosts, only allow incoming requests to needed ports. • Restrict unencrypted communication protocols (e.g., Telnet, FTP, etc.). • Manage core services with a dedicated service or management network (e.g., DNS, antivirus, logging, etc.).	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	5	• Anti-spoofing filters. • Permit only authorized IP addresses and block unnecessary network traffic at the Firewall. • Regularly review the list of approved incoming and outgoing requests. • All attempts to access malicious web addresses are logged and monitored. • Deploy a Web Application Firewall (WAF) in front of Internet facing web applications and APIs. • Block the following: • Non-routable IP addresses over external ports. • User Datagram Protocol (UDP) or Internet Control Message Protocol (ICMP) echo requests. • Unused ports and services.
TS-2.4	Firewall Access Control List	Establish and regularly review a policy and process to separate external networks (WANs) from the internal networks) by using stateful inspection firewalls), to include the following: • Create an Access Control List (ACL). • Regularly review ACLs. • Generate logs for all traffic and configuration changes. • Regularly review logs. Apply the following configurations: • Deny all WAN traffic to any internal network other than to explicit hosts that reside on the DMZ. • Deny all incoming and outgoing network requests by default. • Block malicious sites at external and internal firewall level. • Enable only explicitly defined outgoing requests by specific protocol and destination. • For externally accessible hosts, only allow incoming requests to needed ports. • Restrict unencrypted communication protocols (e.g., Telnet, FTP, etc.). • Manage core services with a dedicated service or management network (e.g., DNS, antivirus, logging, etc.).	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	• Anti-spoofing filters. • Permit only authorized IP addresses and block unnecessary network traffic at the Firewall. • Regularly review the list of approved incoming and outgoing requests. • All attempts to access malicious web addresses are logged and monitored. • Deploy a Web Application Firewall (WAF) in front of Internet facing web applications and APIs. • Block the following: • Non-routable IP addresses over external ports. • User Datagram Protocol (UDP) or Internet Control Message Protocol (ICMP) echo requests. • Unused ports and services.
TS-2.4	Firewall Access Control List	Establish and regularly review a policy and process to separate external networks (WANs) from the internal networks) by using stateful inspection firewalls), to include the following: • Create an Access Control List (ACL). • Regularly review ACLs. • Generate logs for all traffic and configuration changes. • Regularly review logs. Apply the following configurations: • Deny all WAN traffic to any internal network other than to explicit hosts that reside on the DMZ. • Deny all incoming and outgoing network requests by default. • Block malicious sites at external and internal firewall level. • Enable only explicitly defined outgoing requests by specific protocol and destination. • For externally accessible hosts, only allow incoming requests to needed ports. • Restrict unencrypted communication protocols (e.g., Telnet, FTP, etc.). • Manage core services with a dedicated service or management network (e.g., DNS, antivirus, logging, etc.).	Functional	Intersects With	Data Flow Enforcement - Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	5	• Anti-spoofing filters. • Permit only authorized IP addresses and block unnecessary network traffic at the Firewall. • Regularly review the list of approved incoming and outgoing requests. • All attempts to access malicious web addresses are logged and monitored. • Deploy a Web Application Firewall (WAF) in front of Internet facing web applications and APIs. • Block the following: • Non-routable IP addresses over external ports. • User Datagram Protocol (UDP) or Internet Control Message Protocol (ICMP) echo requests. • Unused ports and services.
TS-2.4	Firewall Access Control List	Establish and regularly review a policy and process to separate external networks (WANs) from the internal networks) by using stateful inspection firewalls), to include the following: • Create an Access Control List (ACL). • Regularly review ACLs. • Generate logs for all traffic and configuration changes. • Regularly review logs. Apply the following configurations: • Deny all WAN traffic to any internal network other than to explicit hosts that reside on the DMZ. • Deny all incoming and outgoing network requests by default. • Block malicious sites at external and internal firewall level. • Enable only explicitly defined outgoing requests by specific protocol and destination. • For externally accessible hosts, only allow incoming requests to needed ports. • Restrict unencrypted communication protocols (e.g., Telnet, FTP, etc.). • Manage core services with a dedicated service or management network (e.g., DNS, antivirus, logging, etc.).	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5	• Anti-spoofing filters. • Permit only authorized IP addresses and block unnecessary network traffic at the Firewall. • Regularly review the list of approved incoming and outgoing requests. • All attempts to access malicious web addresses are logged and monitored. • Deploy a Web Application Firewall (WAF) in front of Internet facing web applications and APIs. • Block the following: • Non-routable IP addresses over external ports. • User Datagram Protocol (UDP) or Internet Control Message Protocol (ICMP) echo requests. • Unused ports and services.
TS-2.4	Firewall Access Control List	Establish and regularly review a policy and process to separate external networks (WANs) from the internal networks) by using stateful inspection firewalls), to include the following: • Create an Access Control List (ACL). • Regularly review ACLs. • Generate logs for all traffic and configuration changes. • Regularly review logs. Apply the following configurations: • Deny all WAN traffic to any internal network other than to explicit hosts that reside on the DMZ. • Deny all incoming and outgoing network requests by default. • Block malicious sites at external and internal firewall level. • Enable only explicitly defined outgoing requests by specific protocol and destination. • For externally accessible hosts, only allow incoming requests to needed ports. • Restrict unencrypted communication protocols (e.g., Telnet, FTP, etc.). • Manage core services with a dedicated service or management network (e.g., DNS, antivirus, logging, etc.).	Functional	Intersects With	Human Reviews	NET-04.6	Mechanisms exist to enforce the use of human reviews for Access Control Lists (ACLs) and similar roles on a routine basis.	5	• Anti-spoofing filters. • Permit only authorized IP addresses and block unnecessary network traffic at the Firewall. • Regularly review the list of approved incoming and outgoing requests. • All attempts to access malicious web addresses are logged and monitored. • Deploy a Web Application Firewall (WAF) in front of Internet facing web applications and APIs. • Block the following: • Non-routable IP addresses over external ports. • User Datagram Protocol (UDP) or Internet Control Message Protocol (ICMP) echo requests. • Unused ports and services.
TS-2.5	Content & Production Networks	Establish and regularly review a process to isolate the Content & Production Networks from Non-Content & Non-Production Networks (e.g., office network, DMZ, content transfer, Internet, etc.) to include the following: • Physical air gap and/or Logical segmentation via layer 2 or layer 3 VLAN ACLs. • Prohibit bridging or dual-homed networking (physical network bridging) or computer systems between Content & Production Networks and Non-Content & Non-Production Networks.	Functional	Intersects With	Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production Technology Assets, Applications and/or Services (TAAS).	8	• Regularly review configurations. • Update upon significant changes.
TS-2.6	Firewall Management	Establish and regularly review a policy and process for Firewall Management, to include the following: • Provision Firewall users based on the Principle of Least Privilege (PLP). • Apply Change Control Best Practices (CS-5.0). • Restrict Firewall Management from the Internet or WAN. • Subscription to anti-virus, sandbox, and intrusion detection updates. • Configure alerts for key security events.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	• Regularly review role access. • Regularly review alert configuration. • Update upon changes.
TS-2.6	Firewall Management	Establish and regularly review a policy and process for Firewall Management, to include the following: • Provision Firewall users based on the Principle of Least Privilege (PLP). • Apply Change Control Best Practices (CS-5.0). • Restrict Firewall Management from the Internet or WAN. • Subscription to anti-virus, sandbox, and intrusion detection updates. • Configure alerts for key security events.	Functional	Intersects With	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	5	• Regularly review role access. • Regularly review alert configuration. • Update upon changes.
TS-2.6	Firewall Management	Establish and regularly review a policy and process for Firewall Management, to include the following: • Provision Firewall users based on the Principle of Least Privilege (PLP). • Apply Change Control Best Practices (CS-5.0). • Restrict Firewall Management from the Internet or WAN. • Subscription to anti-virus, sandbox, and intrusion detection updates. • Configure alerts for key security events.	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	5	• Regularly review role access. • Regularly review alert configuration. • Update upon changes.
TS-2.6	Firewall Management	Establish and regularly review a policy and process for Firewall Management, to include the following: • Provision Firewall users based on the Principle of Least Privilege (PLP). • Apply Change Control Best Practices (CS-5.0). • Restrict Firewall Management from the Internet or WAN. • Subscription to anti-virus, sandbox, and intrusion detection updates. • Configure alerts for key security events.	Functional	Intersects With	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	5	• Regularly review role access. • Regularly review alert configuration. • Update upon changes.
TS-2.7	Intrusion Detection & Prevention Systems	Establish and regularly review a policy and process to deploy network-based Intrusion Detection & Prevention Systems (IDS & IPS), to include the following: • Configure the systems to alert and block suspicious network activity. • Basic border gateway services (e.g., gateway anti-virus, URL filtering, etc.). • Regularly update attack signature definitions. • Log all activity and configuration changes.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	• Host-based Intrusion Detection Systems • Utilize virtual patching.
TS-2.7	Intrusion Detection & Prevention Systems	Establish and regularly review a policy and process to deploy network-based Intrusion Detection & Prevention Systems (IDS & IPS), to include the following: • Configure the systems to alert and block suspicious network activity. • Basic border gateway services (e.g., gateway anti-virus, URL filtering, etc.). • Regularly update attack signature definitions. • Log all activity and configuration changes.	Functional	Intersects With	Host Intrusion Detection and Prevention Systems (HIDS / HIPS)	END-07	Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS), or similar technologies, to monitor for and protect against anomalous host activity, including lateral movement across the network.	5	• Host-based Intrusion Detection Systems • Utilize virtual patching.

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Relationship	STRM Relationship	SCF Control	SCF #	Control Description	Strength of Relationship	Notes
TS-2.7	Intrusion Detection & Prevention Systems	Establish and regularly review a policy and process to deploy network-based Intrusion Detection & Prevention Systems (IDS & IPS) to include the following: • Configure the systems to alert and block suspicious network activity • Basic border gateway services (e.g., gateway anti-virus, URL filtering, etc.) • Regularly update attack signature definitions • Log all activity and configuration changes	Functional	Intersects With	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	5	• Host-based Intrusion Detection Systems • Utilize virtual patching
TS-2.7	Intrusion Detection & Prevention Systems	Establish and regularly review a policy and process to deploy network-based Intrusion Detection & Prevention Systems (IDS & IPS) to include the following: • Configure the systems to alert and block suspicious network activity • Basic border gateway services (e.g., gateway anti-virus, URL filtering, etc.) • Regularly update attack signature definitions • Log all activity and configuration changes	Functional	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5	• Host-based Intrusion Detection Systems • Utilize virtual patching
TS-2.8	Internet Access	Establish and regularly review a policy and process for Internet Access in content & production networks, and all systems that process or store digital content, to include the following: • Prohibit directly accessing unauthorized Internet sites, resources, or services	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	• Prohibit direct email access • For a business case that requires Internet Access from the production network, apply the following: • Explicitly allow protocols and ports (e.g., layer 2/3 ACLs) that require connections to services • Use proxy servers to broker access • Restrict Internet Access to shared storage solutions for isolated web browsing/email access • Utilize isolation tools via a virtual environment separate from the production network • For use of Keyboard/Video/Mouse (KVM) solution for web browsing and/or email access • Confirm machine is not connected to the production network • Confirm that any physical ports not in use are properly locked down
TS-2.8	Internet Access	Establish and regularly review a policy and process for Internet Access in content & production networks, and all systems that process or store digital content, to include the following: • Prohibit directly accessing unauthorized Internet sites, resources, or services	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	• Prohibit direct email access • For a business case that requires Internet Access from the production network, apply the following: • Explicitly allow protocols and ports (e.g., layer 2/3 ACLs) that require connections to services • Use proxy servers to broker access • Restrict Internet Access to shared storage solutions for isolated web browsing/email access • Utilize isolation tools via a virtual environment separate from the production network • For use of Keyboard/Video/Mouse (KVM) solution for web browsing and/or email access • Confirm machine is not connected to the production network • Confirm that any physical ports not in use are properly locked down
TS-2.8	Internet Access	Establish and regularly review a policy and process for Internet Access in content & production networks, and all systems that process or store digital content, to include the following: • Prohibit directly accessing unauthorized Internet sites, resources, or services	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	5	• Prohibit direct email access • For a business case that requires Internet Access from the production network, apply the following: • Explicitly allow protocols and ports (e.g., layer 2/3 ACLs) that require connections to services • Use proxy servers to broker access • Restrict Internet Access to shared storage solutions for isolated web browsing/email access • Utilize isolation tools via a virtual environment separate from the production network • For use of Keyboard/Video/Mouse (KVM) solution for web browsing and/or email access • Confirm machine is not connected to the production network • Confirm that any physical ports not in use are properly locked down
TS-2.8	Internet Access	Establish and regularly review a policy and process for Internet Access in content & production networks, and all systems that process or store digital content, to include the following: • Prohibit directly accessing unauthorized Internet sites, resources, or services	Functional	Intersects With	Direct Internet Access Restrictions	NET-06.5	Mechanisms exist to prohibit, or strictly-control, Internet access from sensitive/regulated data enclaves (secure zones).	5	• Prohibit direct email access • For a business case that requires Internet Access from the production network, apply the following: • Explicitly allow protocols and ports (e.g., layer 2/3 ACLs) that require connections to services • Use proxy servers to broker access • Restrict Internet Access to shared storage solutions for isolated web browsing/email access • Utilize isolation tools via a virtual environment separate from the production network • For use of Keyboard/Video/Mouse (KVM) solution for web browsing and/or email access • Confirm machine is not connected to the production network • Confirm that any physical ports not in use are properly locked down
TS-2.8	Internet Access	Establish and regularly review a policy and process for Internet Access in content & production networks, and all systems that process or store digital content, to include the following: • Prohibit directly accessing unauthorized Internet sites, resources, or services	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	3	• Prohibit direct email access • For a business case that requires Internet Access from the production network, apply the following: • Explicitly allow protocols and ports (e.g., layer 2/3 ACLs) that require connections to services • Use proxy servers to broker access • Restrict Internet Access to shared storage solutions for isolated web browsing/email access • Utilize isolation tools via a virtual environment separate from the production network • For use of Keyboard/Video/Mouse (KVM) solution for web browsing and/or email access • Confirm machine is not connected to the production network • Confirm that any physical ports not in use are properly locked down
TS-2.9	Remote Access	Establish and regularly review a policy and process for Remote Access to all environments, to include the following: • Utilize VPN and configure to prohibit split tunneling • Allow only authorized remote access to content transfer systems • Disable or limit the functionality of clipboard to prevent unauthorized data transfer (e.g., global settings by remote access applications) • Segregate production network through a remote connection via client approved remote access • Enable AES-256 encryption at a minimum • Terminate remote sessions upon 15 minutes of inactivity • Apply the MPA Content Security Best Practices • Application Configuration Guidelines (Content) (TS-1.17) • Application Configuration Guidelines (In-House Developed) (TS-1.18) • Authentication (TS-1.8) • Firewall Management (TS-2.6) • Remote Sites & Locations (OP-2.1) • Systems Configuration (TS-1.3)	Functional	Subset Of	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	10	• Use of corporate owned devices when content is stored locally on the endpoint device • Use secure methods for remote access (e.g., SSH, HTTPS, etc.) • Use a Firewall to segregate the WAN (Internet) from the internal network used to access content • Document Remote Access Infrastructure or Network Topology Diagrams • Utilize email streaming applications to avoid content transfer to production devices • Configure the wireless access point/controller to broadcast only within the required range • Port-based network access control (e.g., 802.1X framework for wireless networking) • Lightweight Directory Access Protocol (LDAP) server (e.g., Active Directory) to manage user accounts • Public Key Infrastructure (PKI) to generate and manage client and server certificates • Configure WPA2 or WPA3 with CCM (AES) • Actively scan for rogue wireless access points and alert upon detection
TS-2.10	Web Filtering	Establish and regularly review a process for Web Filtering, to address the following: • Peer-to-peer file sharing • Malware and ransomware • Malicious sites	Functional	Subset Of	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	10	• Use DNS filtering
TS-2.11	Wireless Networks	Establish and regularly review a policy and process for managing Wireless Network configurations in all environments, to include the following: • Disable WPA2 Enterprise (AES) and/or WPA3 SAE • Change default administrator login credentials • Change default network name Service Set Identifier (SSID) and use non-company, non-production names • Set a complex wireless access point passphrase and change regularly • Remote Authentication Dial-In User Service (RADIUS) for authentication (does not apply to guest networks) • Disconnect wireless Network Interface Cards (NICs) from production computers • Segregate guest networks • Redirect guest networks to access only the Internet	Functional	Intersects With	Wireless Access Authentication & Encryption	CM-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking communications by implementing secure and strong encryption.	8	• Use WPA2 Enterprise (AES) • MAC address filtering and disable wireless MAC addresses of production devices • Configure the wireless access point/controller to broadcast only within the required range • Port-based network access control (e.g., 802.1X framework for wireless networking) • Lightweight Directory Access Protocol (LDAP) server (e.g., Active Directory) to manage user accounts • Public Key Infrastructure (PKI) to generate and manage client and server certificates • Configure WPA2 or WPA3 with CCM (AES) • Actively scan for rogue wireless access points and alert upon detection
TS-2.11	Wireless Networks	Establish and regularly review a policy and process for managing Wireless Network configurations in all environments, to include the following: • Disable WPA2 Enterprise (AES) and/or WPA3 SAE • Change default administrator login credentials • Change default network name Service Set Identifier (SSID) and use non-company, non-production names • Set a complex wireless access point passphrase and change regularly • Remote Authentication Dial-In User Service (RADIUS) for authentication (does not apply to guest networks) • Disconnect wireless Network Interface Cards (NICs) from production computers • Segregate guest networks • Redirect guest networks to access only the Internet	Functional	Intersects With	Guest Networks	NET-02.2	Mechanisms exist to implement and manage a secure guest network.	8	• Use WPA2 Enterprise (AES) • MAC address filtering and disable wireless MAC addresses of production devices • Configure the wireless access point/controller to broadcast only within the required range • Port-based network access control (e.g., 802.1X framework for wireless networking) • Lightweight Directory Access Protocol (LDAP) server (e.g., Active Directory) to manage user accounts • Public Key Infrastructure (PKI) to generate and manage client and server certificates • Configure WPA2 or WPA3 with CCM (AES) • Actively scan for rogue wireless access points and alert upon detection
TS-2.11	Wireless Networks	Establish and regularly review a policy and process for managing Wireless Network configurations in all environments, to include the following: • Disable WPA2 Enterprise (AES) and/or WPA3 SAE • Change default administrator login credentials • Change default network name Service Set Identifier (SSID) and use non-company, non-production names • Set a complex wireless access point passphrase and change regularly • Remote Authentication Dial-In User Service (RADIUS) for authentication (does not apply to guest networks) • Disconnect wireless Network Interface Cards (NICs) from production computers • Segregate guest networks • Redirect guest networks to access only the Internet	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	5	• Use WPA2 Enterprise (AES) • MAC address filtering and disable wireless MAC addresses of production devices • Configure the wireless access point/controller to broadcast only within the required range • Port-based network access control (e.g., 802.1X framework for wireless networking) • Lightweight Directory Access Protocol (LDAP) server (e.g., Active Directory) to manage user accounts • Public Key Infrastructure (PKI) to generate and manage client and server certificates • Configure WPA2 or WPA3 with CCM (AES) • Actively scan for rogue wireless access points and alert upon detection
TS-2.11	Wireless Networks	Establish and regularly review a policy and process for managing Wireless Network configurations in all environments, to include the following: • Disable WPA2 Enterprise (AES) and/or WPA3 SAE • Change default administrator login credentials • Change default network name Service Set Identifier (SSID) and use non-company, non-production names • Set a complex wireless access point passphrase and change regularly • Remote Authentication Dial-In User Service (RADIUS) for authentication (does not apply to guest networks) • Disconnect wireless Network Interface Cards (NICs) from production computers • Segregate guest networks • Redirect guest networks to access only the Internet	Functional	Intersects With	Wireless Networking	NET-13	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	8	• Use WPA2 Enterprise (AES) • MAC address filtering and disable wireless MAC addresses of production devices • Configure the wireless access point/controller to broadcast only within the required range • Port-based network access control (e.g., 802.1X framework for wireless networking) • Lightweight Directory Access Protocol (LDAP) server (e.g., Active Directory) to manage user accounts • Public Key Infrastructure (PKI) to generate and manage client and server certificates • Configure WPA2 or WPA3 with CCM (AES) • Actively scan for rogue wireless access points and alert upon detection
TS-2.12	Cloud Service Provider & Cloud Service Consumer	Establish and regularly review a process for configuring applications and infrastructure for Cloud Service Providers (CSPs) & Cloud Service Consumers (CSCs), to include the following: • Define user and intra-tenant user access • Segregate access through appropriate physical or logical controls	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with strong encryption.	5	• In accordance with local laws, regulations, and agreements • Monitor segmentation between intra-tenant access
TS-2.12	Cloud Service Provider & Cloud Service Consumer	Establish and regularly review a process for configuring applications and infrastructure for Cloud Service Providers (CSPs) & Cloud Service Consumers (CSCs), to include the following: • Define user and intra-tenant user access • Segregate access through appropriate physical or logical controls	Functional	Intersects With	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud environments.	5	• In accordance with local laws, regulations, and agreements • Monitor segmentation between intra-tenant access
TS-2.13	Network Connections	Establish and regularly review a process to monitor, encrypt, and restrict Network Connections to only authorized and authorized connections, to include the following: • Detect unauthorized connections • Remove unauthorized connections	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5	• Log all unauthorized connections in log management system • Regularly review Network Connections for number of unauthorized connections, how they were removed, trends, patterns, etc.