**NIST IR 8477-Based Set Theory Relationship Mapping (STRM)**
**Reference document:** Secure Controls Framework (SCF) version 2026.1
**STRM Guidance:** https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

**Focal Document:** **Vermont Data Broker Registration Act (Act 171 of 2018)**
**Focal Document URL:** https://legislature.vermont.gov/Documents/2018/Docs/ACTS/ACT171/ACT171%20As%20Enacted.pdf
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-usa-state-vt-act-171-2018.pdf

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | FINDINGS AND INTENT | See FDE for details. | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2 | PROTECTION OF PERSONAL INFORMATION | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2430 | DEFINITIONS | See FDE for details. | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2433 | ACQUISITION OF BROKERED PERSONAL INFORMATION; PROHIBITIONS | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2433(a) | Prohibited acquisition and use. | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2433(a)(1) | Prohibited acquisition and use. | A person shall not acquire brokered personal information through fraudulent means. | Functional | Subset Of | Reasonable Data Privacy Practices | PRI-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. | 10 | |
| 2433(a)(1) | Prohibited acquisition and use. | A person shall not acquire brokered personal information through fraudulent means. | Functional | Intersects With | Restrict Collection To Identified Purpose | PRI-04 | Mechanisms exist to minimize the collection of Personal Data (PD) to only what is adequate, relevant and limited to the purposes identified in the data privacy notice, including protections against collecting PD from minors without appropriate parental or legal guardian consent. | 5 | |
| 2433(a)(2) | Prohibited acquisition and use. | A person shall not acquire or use brokered personal information for the purpose of: | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2433(a)(2)(A) | Prohibited acquisition and use. | stalking or harassing another person; | Functional | Subset Of | Reasonable Data Privacy Practices | PRI-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. | 10 | |
| 2433(a)(2)(B) | Prohibited acquisition and use. | committing a fraud, including identity theft, financial fraud, or email fraud; or | Functional | Subset Of | Reasonable Data Privacy Practices | PRI-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. | 10 | |
| 2433(a)(2)(C) | Prohibited acquisition and use. | engaging in unlawful discrimination, including employment discrimination and housing discrimination. | Functional | Subset Of | Reasonable Data Privacy Practices | PRI-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. | 10 | |
| 2433(b) | Enforcement | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2433(b)(1) | Enforcement | A person who violates a provision of this section commits an unfair and deceptive act in commerce in violation of section 2453 of this title. | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2433(b)(2) | Enforcement | The Attorney General has the same authority to adopt rules to implement the provisions of this section and to conduct civil investigations, enter into assurances of discontinuance, bring civil actions, and take other enforcement actions as provided under chapter 63, subchapter 1 of this title. | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2446 | ANNUAL REGISTRATION | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2446(a) | ANNUAL REGISTRATION | Annually, on or before January 31 following a year in which a person meets the definition of data broker as provided in section 2430 of this title, a data broker shall: | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2446(a)(1) | ANNUAL REGISTRATION | register with the Secretary of State; | Functional | Intersects With | Register As A Data Controller and/or Data Processor | PRI-15 | Mechanisms exist to register as a data controller and/or data processor, including registering databases containing Personal Data (PD) with the appropriate Data Authority, when necessary. | 5 | |
| 2446(a)(2) | ANNUAL REGISTRATION | pay a registration fee of $100.00; and | Functional | Intersects With | Statutory, Regulatory & Contractual Compliance | CPL-01 | Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls. | 5 | |
| 2446(a)(3) | ANNUAL REGISTRATION | provide the following information: | Functional | Intersects With | Statutory, Regulatory & Contractual Compliance | CPL-01 | Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls. | 5 | |
| 2446(a)(3)(A) | ANNUAL REGISTRATION | the name and primary physical, e-mail, and Internet addresses of the data broker; | Functional | Intersects With | Statutory, Regulatory & Contractual Compliance | CPL-01 | Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls. | 5 | |
| 2446(a)(3)(B) | ANNUAL REGISTRATION | if the data broker permits a consumer to opt out of the data broker's collection of brokered personal information, opt out of its databases, or opt out of certain sales of data: | Functional | Intersects With | Statutory, Regulatory & Contractual Compliance | CPL-01 | Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls. | 5 | |
| 2446(a)(3)(B)(i) | ANNUAL REGISTRATION | the method for requesting an opt-out; | Functional | Intersects With | Statutory, Regulatory & Contractual Compliance | CPL-01 | Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls. | 5 | |
| 2446(a)(3)(B)(ii) | ANNUAL REGISTRATION | if the opt-out applies to only certain activities or sales, which ones; and | Functional | Intersects With | Statutory, Regulatory & Contractual Compliance | CPL-01 | Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls. | 5 | |
| 2446(a)(3)(B)(iii) | ANNUAL REGISTRATION | whether the data broker permits a consumer to authorize a third party to perform the opt-out on the consumer's behalf; | Functional | Intersects With | Statutory, Regulatory & Contractual Compliance | CPL-01 | Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls. | 5 | |
| 2446(a)(3)(C) | ANNUAL REGISTRATION | a statement specifying the data collection, databases, or sales activities from which a consumer may not opt out; | Functional | Intersects With | Statutory, Regulatory & Contractual Compliance | CPL-01 | Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls. | 5 | |
| 2446(a)(3)(D) | ANNUAL REGISTRATION | a statement whether the data broker implements a purchaser credentialing process; | Functional | Intersects With | Statutory, Regulatory & Contractual Compliance | CPL-01 | Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls. | 5 | |
| 2446(a)(3)(E) | ANNUAL REGISTRATION | the number of data broker security breaches that the data broker has experienced during the prior year, and if known, the total number of consumers affected by the breaches; | Functional | Intersects With | Statutory, Regulatory & Contractual Compliance | CPL-01 | Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls. | 5 | |
| 2446(a)(3)(F) | ANNUAL REGISTRATION | where the data broker has actual knowledge that it possesses the brokered personal information of minors, a separate statement detailing the data collection practices, databases, sales activities, and opt-out policies that are applicable to the brokered personal information of minors; and | Functional | Intersects With | Statutory, Regulatory & Contractual Compliance | CPL-01 | Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls. | 5 | |
| 2446(a)(3)(G) | ANNUAL REGISTRATION | any additional information or explanation the data broker chooses to provide concerning its data collection practices. | Functional | Intersects With | Statutory, Regulatory & Contractual Compliance | CPL-01 | Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls. | 5 | |
| 2446(b) | ANNUAL REGISTRATION | A data broker that fails to register pursuant to subsection (a) of this section is liable to the State for: | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2446(b)(1) | ANNUAL REGISTRATION | a civil penalty of $50.00 for each day, not to exceed a total of $10,000.00 for each year, it fails to register pursuant to this section; | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2446(b)(2) | ANNUAL REGISTRATION | an amount equal to the fees due under this section during the period it failed to register pursuant to this section; and | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2446(b)(3) | ANNUAL REGISTRATION | other penalties imposed by law. | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2446(c) | ANNUAL REGISTRATION | The Attorney General may maintain an action in the Civil Division of the Superior Court to collect the penalties imposed in this section and to seek appropriate injunctive relief. | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2447 | DATA BROKER DUTY TO PROTECT INFORMATION; STANDARDS; TECHNICAL REQUIREMENTS | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2447(a) | Duty to protect personally identifiable information. | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2447(a)(1) | Duty to protect personally identifiable information. | A data broker shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to: | Functional | Subset Of | Security, Compliance & Resilience Program (SCRP) | GOV-01 | Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls. | 10 | |
| 2447(a)(1)(A) | Duty to protect personally identifiable information. | the size, scope, and type of business of the data broker obligated to safeguard the personally identifiable information under such comprehensive information security program; | Functional | Subset Of | Security, Compliance & Resilience Program (SCRP) | GOV-01 | Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls. | 10 | |
| 2447(a)(1)(B) | Duty to protect personally identifiable information. | the amount of resources available to the data broker; | Functional | Subset Of | Security, Compliance & Resilience Program (SCRP) | GOV-01 | Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls. | 10 | |
| 2447(a)(1)(C) | Duty to protect personally identifiable information. | the amount of stored data; and | Functional | Subset Of | Security, Compliance & Resilience Program (SCRP) | GOV-01 | Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls. | 10 | |
| 2447(a)(1)(D) | Duty to protect personally identifiable information. | the need for security and confidentiality of personally identifiable information. | Functional | Subset Of | Security, Compliance & Resilience Program (SCRP) | GOV-01 | Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls. | 10 | |
| 2447(a)(2) | Duty to protect personally identifiable information. | A data broker subject to this subsection shall adopt safeguards in the comprehensive security program that are consistent with the safeguards for protection of personally identifiable information and information of a similar character set forth in other State rules or federal regulations applicable to the data broker. | Functional | Intersects With | Security of Personal Data (PD) | PRI-01.6 | Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD. | 8 | |
| 2447(a)(2) | Duty to protect personally identifiable information. | A data broker subject to this subsection shall adopt safeguards in the comprehensive security program that are consistent with the safeguards for protection of personally identifiable information and information of a similar character set forth in other State rules or federal regulations applicable to the data broker. | Functional | Intersects With | Reasonable Data Privacy Practices | PRI-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 | |
| 2447(b) | Information security program; minimum features | A comprehensive information security program shall at minimum have the following features: | Functional | Subset Of | Security, Compliance & Resilience Program (SCRP) | GOV-01 | Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls. | 10 | |
| 2447(b)(1) | Information security program; minimum features | designation of one or more employees to maintain the program; | Functional | Intersects With | Assigned Security, Compliance & Resilience Responsibilities | GOV-04 | Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP). | 5 | |
| 2447(b)(2) | Information security program; minimum features | identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of any electronic, paper, or other records containing personally identifiable information, and a process for evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including: | Functional | Intersects With | Risk Management Program | RSK-01 | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls. | 5 | |
| 2447(b)(2) | Information security program; minimum features | identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of any electronic, paper, or other records containing personally identifiable information, and a process for evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including: | Functional | Intersects With | Threat Intelligence Program | THR-01 | Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities. | 5 | |
| 2447(b)(2)(A) | Information security program; minimum features | ongoing employee training, including training for temporary and contract employees; | 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. | 5 | |

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| 2447(b)(2)(B) | Information security program; minimum features | employee compliance with policies and procedures; and | Functional | Intersects With | Terms of Employment | HRS-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 | |
| 2447(b)(2)(C) | Information security program; minimum features | means for detecting and preventing security system failures; | Functional | Intersects With | Security, Compliance & Resilience Controls Oversight | CPL-02 | Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership. | 5 | |
| 2447(b)(2)(C) | Information security program; minimum features | means for detecting and preventing security system failures; | 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 | |
| 2447(b)(3) | Information security program; minimum features | security policies for employees relating to the storage, access, and transportation of records containing personally identifiable information outside business premises; | 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 | |
| 2447(b)(4) | Information security program; minimum features | disciplinary measures for violations of the comprehensive information security program rules; | Functional | Intersects With | Personnel Sanctions | HRS-07 | Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures. | 5 | |
| 2447(b)(5) | Information security program; minimum features | measures that prevent terminated employees from accessing records containing personally identifiable information; | Functional | Intersects With | Onboarding, Transferring & Offboarding Personnel | HRS-01.1 | Mechanisms exist to proactively govern the following personnel management actions:(1) Onboarding new personnel (e.g., new hires);(2) Transferring personnel into new roles within the organization; and(3) Offboarding personnel (e.g., termination of employment). | 5 | |
| 2447(b)(6) | Information security program; minimum features | supervision of service providers, by: | Functional | Subset Of | Third-Party Management | TPM-01 | Mechanisms exist to facilitate the implementation of third-party management controls. | 10 | |
| 2447(b)(6)(A) | Information security program; minimum features | taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personally identifiable information consistent with applicable law; and | Functional | Intersects With | Third-Party Risk Assessments & Approvals | TPM-04.1 | Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS). | 5 | |
| 2447(b)(6)(B) | Information security program; minimum features | requiring third-party service providers by contract to implement and maintain appropriate security measures for personally identifiable information; | 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). | 5 | |
| 2447(b)(7) | Information security program; minimum features | reasonable restrictions upon physical access to records containing personally identifiable information and storage of the records and data in locked facilities, storage areas, or containers; | 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 officially designated as publicly accessible). | 5 | |
| 2447(b)(8)(A) | Information security program; minimum features | regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personally identifiable information; and | Functional | Intersects With | Security, Compliance & Resilience Controls Oversight | CPL-02 | Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership. | 5 | |
| 2447(b)(8)(B) | Information security program; minimum features | upgrading information safeguards as necessary to limit risks; | Functional | Intersects With | Periodic Review & Update of Security, Compliance & Resilience Program | GOV-03 | Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. | 5 | |
| 2447(b)(9) | Information security program; minimum features | regular review of the scope of the security measures: | Functional | Intersects With | Periodic Review & Update of Security, Compliance & Resilience Program | GOV-03 | Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. | 5 | |
| 2447(b)(9)(A) | Information security program; minimum features | at least annually; or | Functional | Intersects With | Periodic Review & Update of Security, Compliance & Resilience Program | GOV-03 | Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. | 5 | |
| 2447(b)(9)(B) | Information security program; minimum features | whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personally identifiable information; and | Functional | Intersects With | Periodic Review & Update of Security, Compliance & Resilience Program | GOV-03 | Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. | 5 | |
| 2447(b)(10)(A) | Information security program; minimum features | documentation of responsive actions taken in connection with any incident involving a breach of security; and | Functional | Intersects With | Incident Tracking Repository | IRO-09.3 | Mechanisms exist to maintain a repository where cybersecurity events and incidents document:(1) Details of the incident (e.g., category, severity, affected parties, etc.);(2) Remediation actions taken through incident closure; and(3) A summary from the Root Cause Analysis (RCA), if applicable. | 5 | |
| 2447(b)(10)(B) | Information security program; minimum features | mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personally identifiable information. | Functional | Intersects With | Root Cause Analysis (RCA) & Lessons Learned | IRO-13 | Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents. | 5 | |
| 2447(c) | Information security program; computer system security requirements | A comprehensive information security program required by this section shall at minimum, and to the extent technically feasible, have the following elements: | Functional | Subset Of | Security, Compliance & Resilience Program (SCRP) | GOV-01 | Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls. | 10 | |
| 2447(c)(1) | Information security program; computer system security requirements | secure user authentication protocols, as follows: | Functional | Subset Of | Identity & Access Management (IAM) | IAC-01 | Mechanisms exist to facilitate the implementation of identification and access management controls. | 10 | |
| 2447(c)(1)(A) | Information security program; computer system security requirements | an authentication protocol that has the following features: | Functional | Intersects With | Authenticate, Authorize and Audit (AAA) | IAC-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 | |
| 2447(c)(1)(A)(i) | Information security program; computer system security requirements | control of user IDs and other identifiers; | Functional | Intersects With | Account Management | IAC-15 | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts. | 5 | |
| 2447(c)(1)(A)(ii) | Information security program; computer system security requirements | a reasonably secure method of assigning and selecting passwords or use of unique identifier technologies, such as biometrics or token devices; | Functional | Intersects With | Authenticator Management | IAC-10 | Mechanisms exist to:(1) Securely manage authenticators for users and devices; and(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed. | 5 | |
| 2447(c)(1)(A)(iii) | Information security program; computer system security requirements | control of data security passwords to ensure that such passwords are kept in a location and format that do not compromise the security of the data they protect; | Functional | Intersects With | Protection of Authenticators | IAC-10.5 | Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access. | 5 | |
| 2447(c)(1)(A)(iv) | Information security program; computer system security requirements | restricting access to only active users and active user accounts; and | Functional | Intersects With | Account Management | IAC-15 | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts. | 5 | |
| 2447(c)(1)(A)(v) | Information security program; computer system security requirements | blocking access to user identification after multiple unsuccessful attempts to gain access; or | Functional | Intersects With | Account Lockout | IAC-22 | Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded. | 5 | |
| 2447(c)(1)(B) | Information security program; computer system security requirements | an authentication protocol that provides a higher level of security than the features specified in subdivision (A) of this subdivision (c)(1). | Functional | Intersects With | Authenticate, Authorize and Audit (AAA) | IAC-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 | |
| 2447(c)(2) | Information security program; computer system security requirements | secure access control measures that: | Functional | Intersects With | Authenticate, Authorize and Audit (AAA) | IAC-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 | |
| 2447(c)(2)(A) | Information security program; computer system security requirements | restrict access to records and files containing personally identifiable information to those who need such information to perform their job duties; and | Functional | Intersects With | Role-Based Access Control (RBAC) | IAC-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 | |
| 2447(c)(2)(B) | Information security program; computer system security requirements | assign to each person with computer access unique identifications plus passwords, which are not vendor-supplied default passwords, that are reasonably designed to maintain the integrity of the security of the access controls or a protocol that provides a higher degree of security; | Functional | Intersects With | Role-Based Access Control (RBAC) | IAC-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 | |
| 2447(c)(3) | Information security program; computer system security requirements | encryption of all transmitted records and files containing personally identifiable information that will travel across public networks and encryption of all data containing personally identifiable information to be transmitted wirelessly or a protocol that provides a higher degree of security; | Functional | Intersects With | Transmission Confidentiality | CRY-03 | Cryptographic mechanisms exist to protect the confidentiality of data being transmitted. | 5 | |
| 2447(c)(4) | Information security program; computer system security requirements | reasonable monitoring of systems for unauthorized use of or access to personally identifiable information; | 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 | |
| 2447(c)(5) | Information security program; computer system security requirements | encryption of all personally identifiable information stored on laptops or other portable devices or a protocol that provides a higher degree of security; | Functional | Intersects With | Transmission Confidentiality | CRY-03 | Cryptographic mechanisms exist to protect the confidentiality of data being transmitted. | 5 | |
| 2447(c)(6) | Information security program; computer system security requirements | for files containing personally identifiable information on a system that is connected to the Internet, reasonably up-to-date firewall protection and operating system security patches that are reasonably designed to maintain the integrity of the personally identifiable information or a protocol that provides a higher degree of security; | Functional | Intersects With | Endpoint Protection Measures | END-02 | Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices. | 5 | |
| 2447(c)(6) | Information security program; computer system security requirements | for files containing personally identifiable information on a system that is connected to the Internet, reasonably up-to-date firewall protection and operating system security patches that are reasonably designed to maintain the integrity of the personally identifiable information or a protocol that provides a higher degree of security; | Functional | Intersects With | Stable Versions | VPM-04.1 | Mechanisms exist to install the latest stable version of any software and/or security-related updates on all applicable systems. | 5 | |
| 2447(c)(7) | Information security program; computer system security requirements | reasonably up-to-date versions of system security agent software that must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-todate patches and virus definitions and is set to receive the most current security updates on a regular basis or a protocol that provides a higher degree of security; and | Functional | Intersects With | Automatic Antimalware Signature Updates | END-04.1 | Automated mechanisms exist to update antimalware technologies, including signature definitions. | 5 | |
| 2447(c)(8) | Information security program; computer system security requirements | education and training of employees on the proper use of the computer security system and the importance of personally identifiable information security. | 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 | |
| 2447(d) | Enforcement | See FDE for details. | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 3 | N/A | 9 V.S.A. § 2480b is amended to read: | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2480b | DISCLOSURES TO CONSUMERS | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2480b(a) | DISCLOSURES TO CONSUMERS | A credit reporting agency shall, upon request and proper identification of any consumer, clearly and accurately disclose to the consumer all information available to users at the time of the request pertaining to the consumer, including: | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2480b(a)(1) | DISCLOSURES TO CONSUMERS | any credit score or predictor relating to the consumer, in a form and manner that complies with such comments or guidelines as may be issued by the Federal Trade Commission; | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2480b(a)(2) | DISCLOSURES TO CONSUMERS | the names of users requesting information pertaining to the consumer during the prior 12-month period and the date of each request; and | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |

| 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 |
|---|---|---|---|---|---|---|---|---|---|
| 2480b(a)(3) | DISCLOSURES TO CONSUMERS | a clear and concise explanation of the information. | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2480b(b) | DISCLOSURES TO CONSUMERS | As frequently as new telephone directories are published, the credit reporting agency shall cause to be listed its name and number in each telephone directory published to serve communities of this State. In accordance with rules adopted by the Attorney General, the credit reporting agency shall make provision for consumers to request by telephone the information required to be disclosed pursuant to subsection (a) of this section at no cost to the consumer. | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2480b(c) | DISCLOSURES TO CONSUMERS | Any time a credit reporting agency is required to make a written disclosure to consumers pursuant to 15 U.S.C. § 1681g, it shall disclose, in at least 12 point type, and in bold type as indicated, the following notice: See FD for further details. | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2480b(d) | DISCLOSURES TO CONSUMERS | The information required to be disclosed by this section shall be disclosed in writing. The information required to be disclosed pursuant to subsection (c) of this section shall be disclosed on one side of a separate document, with text no smaller than that prescribed by the Federal Trade Commission for the notice required under 15 U.S.C. § 1681q § 1681g. The information required to be disclosed pursuant to subsection (c) of this section may accurately reflect changes in numerical items that change over time (such as the phone telephone number or address of Vermont State agencies), and remain in compliance | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2480b(e) | DISCLOSURES TO CONSUMERS | See FDE for details. | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 4 | N/A | 9 V.S.A. § 2480h is amended to read: | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 2480h | SECURITY FREEZE BY CREDIT REPORTING AGENCY; TIME IN EFFECT | See FDE for details. | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 5 | REPORTS | See FDE for details. | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 6 | ONE-STOP FREEZE NOTIFICATION | See FDE for details. | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |
| 7 | EFFECTIVE DATES | See FDE for details. | Functional | No Relationship | N/A | N/A | N/A | 0 | No applicable SCF control |