NIST 800-53 Abbreviated

(Based on the TX CSF)

Small and Medium Business & Education K-12

Built to balance cybersecurity with the realities of the market

#	FUNCTIONAL AREA	SECURITY OBJECTIVE	MINERVA	NIST 800-53	DEFINITION/OBJECTIVE	ROAD MAP INFORMATION
2.1	Identify	Privacy & Confidentiality	PC-1	AP-02	Ensuring the appropriate security of retained information and approved sharing under defined conditions with required safeguards and assurance. Includes the requirements of HIPAA, Texas Business & Commerce Code, and agency defined privacy policies that include and expand upon regulatory and legal requirements for establishing contractual/legal agreements for appropriate and exchange and protection.	1) Ensuring the appropriate security of retained information and approved sharing under defined conditions with required safeguards and assurance. 2) Check for appropriate Identity Access Mgmt. (IAM) i.e. Onboarding & Off boarding processes, Principle of Least Privilege Access. 3) Establish and adhere to data retention policy. 4) Adherence to data protection requirements of FERPA, Texas Business & Commerce Code, Texas Education Code and entity defined privacy policies. 5) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 6) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			PC-2	AR-01		
			PC-3	AR-03		
			PC-4	AR-07		
			PC-5	AR-08		
			PC-6	CA-03		
			PC-7	DI-01		
			PC-8	DI-02		
			PC-9	DM-01		
			PC-10	DM-02		
			PC-11	DM-03		
			PC-12	IP-01		
			PC-13	IP-02		
			PC-14	IP-03		
			PC-15	SC-08		
			PC-16	SI-07		
			PC-17	SE-01		
			PC-18	TR-01		
			PC-19	TR-02		
			PC-20	TR-03		
			PC-21	UL-01		
			PC-22	UL-02		
2.2	Identify	Data Classification	DC-1	CM-08	Data classification provides a framework for managing data asse and information resources based on utility to the organization, intrinsic financial value and impact of loss and other associated risks. To apply the appropriate levels of protection as required by state and federal law as well as proprietary, ethical, operational, a privacy consideration, data, whether electronic or printed, must b classified. The data owner should consult with the Information Security organization and legal counsel on the classification of data as Restricted, Confidential, Agency-Internal, or Public. Consistent use of data classification reinforces with users the expected level of protection of data assets in accordance with required security policies.	1) Establish a documented Data Classification policy which clearly define levels of classification. 2) Data Owners should consult with ITS and legal counsel regarding data classification on information not governed by federal, state or local regulations including FERPA, Texas Business & Commerce Code, Texas Education Code. 3) Review data and its classification on a regular basis to assure compliance. 4) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 5) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			DC-2	CM-10		
			DC-3	MP-03		
			DC-4	MP-04		
			DC-5	PL-04		
			DC-6	PM-05		
			DC-7	RA-02		
			DC-8	SE-01		
2.3	Identify	Critical Information Asset Inventory	AI-1	CM-08	Identification and prioritization of all of the organization's information assets so that they are prioritized according to criticality to the business, so that protections can be applied commensurate with the asset's importance.	1) Identification and prioritization of all the organization's information assets so that they are prioritized per criticality to t business impact, measure of risk and ability to implement including hardware (servers, workstations, laptops, networking infrastructure), software and where sensitive and critical information assets are located (i.e. Databases) and what application(s) have access. 2) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 3) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			AI-2	CA-03		
			AI-3	CP-02		
			AI-4	PL-08		
			AI-5	RA-02		
			AI-6	PM-05		
2.4	Identify	Enterprise Security Policy, Standards and Guidelines	PS-2	AP-01	Maintain the organization's security policy framework, standards, and guidelines. Defines the acceptable use policy for agency information resources. Contributes to the definition of enterprise standards and secure configuration standards to ensure alignment to security specifications and risk management requirements. There will be situations where the strict application of an information security standard would significantly impair the functionality of a service. The exception management process provides a method for evaluating the risks associated with non-compliant conditions and tracking the exception until expiration.	1) Ensure organizations security policy framework and standards including a violation policy and process are in place and regularly maintained. 2) Include an Exception Policy to handle exceptions as the they may arise which includes a procedure to track and rectify any exemptions. No exemptions should be permanent. 3) Establish a regularly updated formal acknowledgement process for users to sign off on reviewing and acknowledgment and adherence to the policies. 4) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 5) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			PS-3	AR-01		
			PS-4	AT-01		
			PS-5	AU-01		
			PS-6	CA-01		
			PS-7	CM-01		
			PS-8	CP-01		
			PS-10	DM-01		
			PS-11	IA-01		
			PS-12	IR-01		
			PS-13	MA-01		
			PS-14	MP-01		
			PS-15	PE-01		
			PS-16	PL-01		
			PS-17	PM-01		
			PS-18	PM-02		

			PS-19	PM-03		
			PS-20	PM-04		
			PS-21	PS-01		
			PS-22	RA-01		
			PS-23	SA-01		
			PS-24	SC-01		
			PS-25	SI-01		
			PS-26	DI-01		
			PS-27	UL-01		
2.5	Identify	Control Oversight and Safeguard Assurance	OA-1	AU-01	Catalog the security activities that are required to provide the appropriate security of information and information resources throughout the Enterprise. Evaluate the control activities that have been implemented in terms of maturity, scope/breadth of implementation, effectiveness or associated deficiency to assure required protection levels as specified by security policy, regulatory/legal requirements, compliance mandates, or organizational risk thresholds. Ensure that control activities are performed as required and performed in a manner that is auditable and verifiable. Identify control activities that are not implemented or are not effective at achieving the defined control objectives. Oversee the implementation of required controls to ensure ongoing audit readiness and effective control implementations.	1)Provide the appropriate security of information and information resources throughout the Enterprise. 2)Review controls and maturity of the 40 controls provided in the Information Security Plan. 3) Self-evaluation of maturity and scope of implementation commensurate to Data Classification. 4) Implement a third-party risk assessment program on a periodic time frame. 5) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 6) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			OA-2	AU-02		
			OA-3	CA-06		
			OA-4	CA-07		
			OA-5	PM-11		
2.6	Identify	Information Security Risk Management	RM-1	RA-01	The assessment and evaluation of risk within the information resources and technology to ensure that business operations are capable of delivering programs and services efficiently and effectively within acceptable tolerances potential negative outcomes.	1) Establish and maintain Information Risk Management policy and processes. 2) Identify risks related to controls not meeting established due diligence and develop a Road Map for remediation including budget analysis 3) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 4) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			RM-2	RA-02		
			RM-3	RA-03		
			RM-4	PM-01		
			RM-5	PM-12		
			RM-6	PM-16		
2.7	Identify	Security Oversight and Governance	OG-1	AR-01	The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly.	1) Establish Security Oversight and Governance Board (including organization leadership team) to ensure enterprise security strategy adheres to enterprise business strategies and overall goals. 2) SOGB should meet on regular basis to review Information Security Program, identified risk and remediation strategies and progress. 3) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 4) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			OG-2	PM-08		
			OG-3	PM-09		
			OG-4	PM-11		
			OG-5	PM-03		
			OG-6	PM-07		
			OG-7	SA-02		
2.8	Identify	Security Compliance and Regulatory Requirements Mgmt	CR-1	AR-06	Monitor the legislative and industry landscape to ensure security policy is updated in consideration of changes that are pertinent or applicable to the organization. Facilitate any validation audits, assessments or reporting that is necessary to assure compliance to applicable laws, regulations, or requirements. Includes the HIPAA Privacy Office(r), IRS Safeguard Reviews, and responses to third party inquiries into the security of the organization.	1) Monitor legislative landscape to ensure adherence to requirements of FERPA, Texas Business & Commerce Code, Texas Education Code and agency defined privacy policies. 2) Facilitate any validation audits, assessments or reporting that is necessary to assure compliance to applicable laws, regulations, or requirements (i.e. Filing of Information Security Plan on even years per SB 1597). 3) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 4) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			CR-2	CA-07		
			CR-3	IA-07		
			CR-4	AU-11		
			CR-5	RA-02		
2.9	Identify	Cloud Usage and Security	CS-1	AC-20	The assessment and evaluation of risk with the use of "cloud" technologies including Software as a Service (SAAS), Platform as a Service (PAAS), and Information as a Service (IAAS), to ensure that business operations are capable of delivering programs and services efficiently and effectively within acceptable tolerances potential negative outcomes.	1)The assessment and evaluation of risk with the use of "cloud" technologies to ensure that business operations can deliver programs and services efficiently and effectively within acceptable tolerances potential negative outcomes. 2)Negotiation of acceptable levels of security should be included in the contract negotiation process. 3) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 4) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			CS-2	SA-09		
			CS-3	SC-04		
			CS-4	CA-02		
			CS-5	CA-07		
			CS-6	CA-08		
			CS-7	RA-03		
			CS-8	RA-05		
			CS-9	SI-02		
			CS-10	SI-04		
			CS-11	SI-05		
2.1	Identify	Security Assessment and Authorization/ Technology Risk Assessments	AS-1	AP-02	Evaluate systems and applications in terms of design and architecture in conjunction with existing or available controls to ensure that current and anticipated threats are mitigated within acceptable risk tolerances. Includes an analysis of in-place systems periodically or when significant change occurs as well as the analysis of the introduction of new technology systems.	1) Evaluate systems and applications in terms of design and architecture in conjunction with existing or available control to ensure that current and anticipated threats are mitigated within acceptable risk tolerances. 2) Establish a governance-based authorization/acceptance of risk review process which includes executive sign-off 3) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 4)The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			AS-2	AR-02		
			AS-3	CA-01		
			AS-4	CA-02		
			AS-5	CA-03		
			AS-6	CA-09		
			AS-7	PM-9		
			AS-8	PM-10		
			AS-9	PM-11		
			AS-10	RA-01		

			AS-11	RA-03		
			AS-12	RA-05		
			AS-13	SI-04		
2.11	Identify	External Vendors and Third-Party Providers	TP-1	AR-03	Evaluation of third-party providers and external vendors to ensure security requirements are met for information and information resources that will be transmitted, processed, stored, or managed by external entities. Includes contract review as well as the development of service level agreements and requirements.	1) Evaluation of third-party providers and external vendors to ensure security requirements are met for information and information resources that will be transmitted, processed, stored, or managed by external entities commensurate to ove Information Security strategies. 2) In addition to the development of SLA levels, contract should include information security platform items considered essential for doing business with the organization (i.e. background check of 3rd party employees working with organization data. 3) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 4) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			TP-2	CA-03		
			TP-3	SA-09		
			TP-4	AC-20		
			TP-5	UL-02		
2.43	Identify	*Secure Application Development	AP-1	AR-07	Ensuring that the code and processes that go into developing applications are as secure as possible. Includes not only the application's processes, but the processes used in the development of the application.	1) Ensure coding and processes that go into developing applications are secure. For example: compliance with OWASP Application Security Verification Standard 2) If the application is being developed by a third party, ensure secure coding practices are included in the contract. For example: compliance with OWASP Application Security Verification Standard 3) The organization should have a documented, secure application framework, and employees are generally aware of and follow the framework. 4) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 5) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			AP-2	SA-03		
			AP-3	SA-10		
			AP-4	SA-11		
			AP-5	DM-03		
2.44	Identify	*Beta Testing	BT-1	CA-08	Validating that projects and systems are secure and vulnerabilities are identified prior to implementation in a production environment. May also be known as End User Acceptance Testing.	1) Beta testing procedures exists and is uniform across the agency, and projects and systems are regularly tested before implementation in a production environment. 2) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 3) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			BT-2	SI-02		
			BT-3	DM-03		
			BT-4	PM-14		
2.45	Identify	*Penetration Testing	PT-1	CA-08	A simulated attack on a system, performed to evaluate the strengths and weaknesses of the system's security. The attack simulates internal and/or external users and attempts to overcome the system's defenses to obtain unauthorized access.	1) Ensure Penetration Testing procedures are uniform across the organization and systems are regularly tested. 2) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 3) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			PT-2	SI-02		
			PT-3	PM-14		
			PT-4	CA-05		
2.46	Identify	Vulnerability Testing	VT-1	RA-05	Scanning a system for known vulnerabilities, quantifying the vulnerabilities' risk levels based on the system's exposure to the and preparing risk plans for each vulnerability.	1) Ensure our Vulnerability Program procedures are uniform across the organization and systems are regularly tested. 2) Identified Vulnerabilities should be prioritized by risk and remediated based the priority of the risk. 3) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 4) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			VT-2	SI-02		
			VT-3	PM-14		
			VT-4	CA-05		
2.12	Protect	Enterprise Architecture, Roadmap & Emerging Technology	RM-1	PL-08	An enterprise information security architecture that is aligned with Federal, State, Local and agency data security and privacy requirements. The integration of information security requirements and associated security controls into the information security architecture helps to ensure that security considerations are addressed early in the system development life cycle and are directly and explicitly related to mission/business processes. Using a roadmap and emerging technology evaluation process, the Information Security Program will stay abreast of th continued evolution of security solutions, processes, and technology to identify continuous, ongoing ways to deliver technology and information securely.	1) Establish and maintain an information security architecture and roadmap to reach organizational expectation and due diligence levels. 2) Using a roadmap and emerging technology evaluation process, the Information Security Program can stay abreast of t continued evolution of security solutions, processes, and technology to identify continuous, ongoing ways to deliver technology and information securely. 3) Re-evaluate and modify roadmap on a regular basis 4) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 5) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			RM-2	PM-06		
			RM-3	PM-07		
			RM-4	SA-01		
			RM-5	SA-02		
			RM-6	SC-22		
			RM-7	SI-01		
			RM-8	SI-12		
			RM-9	SA-10		
			RM-10	SA-03		
2.13	Protect	Secure System Services, Acquisition and Development	AD-1	AR-07	Ensure that the development and implementation of new systems meets the requirements necessary to assure the security of information and resources.	1) Ensure that the acquisition or development and implementation of new secure system services meets the requirement necessary to assure the security of information and resources as outlined in the Enterprise Security Architecture Plan. 2) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 3) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			AD-2	SA-03		
			AD-3	SA-04		
			AD-4	SA-08		
			AD-5	SA-11		
			AD-6	SA-05		
2.14	Protect	Security Awareness and Training	ST-1	AT-01	Define, prepare, deliver, and facilitate an ongoing awareness campaign utilizing a wide variety of mediums and delivery mechanisms to effectively and constantly educate the organization on security related information, threats, and technology risks.	1) Establish a Security Awareness Policy. 2) Define, prepare, deliver, and facilitate an ongoing Security Awareness campaign utilizing a wide variety of mediums an delivery mechanisms to effectively and constantly educate the organization on security related information, threats, and technology risks based on roles performed in the organization (i.e. privileged users (admins, DBA's), executive users, programmers, contractors and end users). 3) Role based training can consist of information as determined appropriate to perform job function from online training, instructor lead training or simple PowerPoint presentation. 4) Ensure that every employee, contractor, intern and affiliate is aware of the organization's approach and policies to protecting the assets and information within your organization. 5) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 6) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			ST-2	AT-02		
			ST-3	AT-03		
			ST-4	AT-04		

2.15	Protect	Privacy Awareness and Training	PT-1	AR-05	Define, prepare, deliver, and facilitate an ongoing awareness campaign utilizing a wide variety of mediums and delivery mechanisms to effectively and constantly educate the organization on privacy requirements and information related to the protection of privacy risks and protections.	1) Define, prepare, deliver, and facilitate an ongoing Privacy Awareness campaign utilizing a wide variety of mediums and delivery mechanisms to effectively and constantly educate the organization on security related information, threats, and technology risks based on roles performed in the organization (i.e. privileged users (admins, DBA's), executive users, programmers, contractors and end users). 2) Role based training can consist of information as determined appropriate to perform job function from online training, instructor lead training or simple PowerPoint presentation. 3) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 4) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
2.16	Protect	Cryptography	CR-1	SC-12	Establish the rules and administrative guidelines governing the use of cryptography and key management in order to ensure that data is not disclosed or made inaccessible due to an inability to decrypt.	1) Encryption of mobile laptops, removeable media, data bases and files which may contain sensitive information as defined by the organizational Data Classification Policy commensurate to the protection of information from unauthorized access. 2) Implement HTTPS encryption with Strict Transport Security (HSTS) using TLS 1.2 or higher on all public facing website and applications on locally managed services and with 3rd parties via contract language updates. 3) Implement encryption in transit between Internet gateways to application and data base servers. 4) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 5) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			CR-2	SC-13		
2.17	Protect	Secure Configuration Management	SM-1	CM-01	Ensure that baseline configurations and inventories of information systems (including hardware, software, firmware, and documentation) are established and maintained throughout the respective system development life cycles. Establishes and enforces security configuration settings for information technology products employed in information systems. Ensures all systems are operating under configurations that have been agreed upon according to organizational risk management.	1) Ensure that baseline configurations and inventories of information systems (including hardware, software, firmware, and documentation) are established and maintained throughout the respective system development life cycles. 2) Ensures all systems are operating under configurations that have been agreed upon per organizational risk management and changes have been documented in the change management process. 3) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 4) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			SM-2	CM-02		
			SM-3	CM-03		
			SM-4	CM-04		
			SM-5	CM-05		
			SM-6	CM-06		
			SM-7	CM-07		
			SM-8	CM-08		
			SM-9	CM-09		
			SM-10	CM-10		
			SM-11	CM-11		
			SM-12	SA-10		
2.18	Protect	Change Management	CM-1	CA-06	Establishes a set of rules and administrative guidelines to manage changes in a rational and predictable manner. In addition it provides for the necessary documentation of any changes made so as to reduce any possible negative impact to the Users of IR systems. Changes include, but are not limited to implementation of new functionality, interruption of service, repair of existing functionality, and the removal of existing functionality.	1) Establish a Change Management Policy and processes. 2) Include monitoring and auditing for compliance within the organization commensurate to the organization Enterprise Security Architecture. 3) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 4) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			CM-2	CM-01		
			CM-3	CM-02		
			CM-4	CM-03		
			CM-5	CM-04		
			CM-6	SA-10		
			CM-7	CM-05		
2.19	Protect	Contingency Planning	CP-1	CP-01	Plans for emergency response, backup operations, and post-incident occurrence recovery for information systems are established, maintained and effectively implemented to ensure theavailability of critical information resources and continuity of operations in emergency situations. Backing up data and applications is a business requirement. It enables the recovery of data and applications in the event of loss or damage (natural disasters, system disk and other systems failures, intentional or unintentional human acts, data entry errors, or systems operator errors).	1) Ensure plans for emergency response, backup operations, and post-incident occurrence recovery for information systems are established, maintained and effectively implemented to ensure the availability of critical information resource and continuity of operations in emergency situations. 2) Backing up data and applications is a business requirement. Utilize tabletop exercises to test for gaps in plan and adj accordingly. 3) Implement a regular testing component to ensure the processes and plans work at anticipated. 4) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 5) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			CP-2	CP-02		
			CP-3	CP-03		
			CP-4	CP-04		
			CP-5	CP-06		
			CP-6	CP-07		
			CP-7	CP-08		
			CP-8	CP-09		
			CP-9	CP-10		
			CP-10	IR-08		
			CP-11	PE-17		
2.2	Protect	Media	MD-1	MP-01	The protection of digital and non-digital information system media, the assurance that access to information on information system media is limited to authorized users, and requirements that information system media is sanitized or destroyed before disposal or release for reuse. The requirement that safeguards are in place to restrict access to Information system media which includes both digital media (e.g., systems, diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives and other portable mass storage devices, compact disks, and digital video disks) and non-digital media (e.g., paper, microfilm). This standard applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices) as well as data center systems and servers.	1) Ensure that access to information on information system media is limited to authorized users, and requirements that information system media is sanitized or destroyed before disposal or release for reuse. 2) The requirement that safeguards are in place to restrict access to Information system media which includes both digital media (e.g., systems, diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives and other portable mass storage devices, compact disks, and digital video disks) and non-digital media (e.g., paper, microfilm). 3) Include end security protection which can monitor USB devices and alert for unauthorized devices plugged into the US which might be used to extract information. 4) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 5) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			MD-2	MP-02		
			MD-3	MP-03		
			MD-4	MP-04		
			MD-5	MP-05		
			MD-6	MP-06		
			MD-7	MP-07		
			MD-8	PM-05		
			PP-1	MA-02		

2.21	Protect	Physical and Environmental Protection	PP-2	PE-01	Assure that physical access to information systems, equipment, and the respective operating environments is limited to authorize individuals. Protect the physical locations and support infrastructure for information systems to ensure that supporting utilities are provided for to limit unplanned disruptions. Protect information systems against environmental hazards and provide appropriate environmental controls in facilities containing information systems.	1) Ensure physical access to information systems, equipment, and the respective operating environments as well as paper copies of sensitive information is limited to authorized individuals using guards or receptionist and card reader access doors to areas where sensitive information may be accessible. 2) Keeping infrastructure closets such as switches locked is essential. 3) Protect information systems against environmental hazards and provide appropriate environmental controls in facilities containing information systems. 4) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 5) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			PP-3	PE-02		
			PP-4	PE-03		
			PP-5	PE-04		
			PP-6	PE-05		
			PP-7	PE-06		
			PP-8	PE-09		
			PP-9	PE-10		
			PP-10	PE-11		
			PP-11	PE-12		
			PP-12	PE-13		
			PP-13	PE-14		
			PP-14	PE-15		
			PP-15	PE-16		
2.22	Protect	Personnel Security	PS-1	PS-01	Ensuring that individuals responsible for agency information are identified and their responsibilities are clearly defined. Any individuals occupying positions of responsibility within the agency (including third-party service providers) are trustworthy and meet established security criteria for those positions. Ensuring that information resources are protected during and after personnel actions such as terminations and transfers. Employing formal sanctions for personnel failing to comply with security policies and procedures.	1) Individuals occupying positions of responsibility (including third-party service providers) should be trustworthy and meet established security criteria for those positions including background checks. 2) Job description and responsibility should be clearly defined. 3) Establish on-boarding processes which utilize the principle of least privilege promoting minimal user profiles to perform their assigned jobs. 4) Establish processes for handling internal job transfers to verify access to proper resources are applied. 5)Establish off-boarding processes to remove access to all resources and properly removing User ID's. 6) Establish violation disciplinary action policies to formalize sanctions for personnel filing to comply with documented security policies and established procedures. 7) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 8) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			PS-2	PS-02		
			PS-3	PS-03		
			PS-4	PS-04		
			PS-5	PS-05		
			PS-6	PS-06		
			PS-7	PS-07		
			PS-8	PS-08		
			PS-9	MA-05		
2.23	Protect	Third-Party Personnel Security	TS-1	AC-20	Requires all third-party providers to comply with all security policies and standards. Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. Establishes personnel security requirements including roles and responsibilities with limits on access requirements defined in accordance to least privileged and data minimization methodologies. Monitors providers for compliance.	1) Require all third-party providers to comply with all security policies and standards. 2) Establishes personnel security requirements including roles and responsibilities with limits on access requirements defined in accordance to least privileged and data minimization methodologies. 3) Monitor all providers for compliance. 4) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 5) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			TS-2	PS-01		
			TS-3	PS-02		
			TS-4	PS-03		
			TS-5	PS-04		
			TS-6	PS-07		
			TS-7	MA-05		
2.24	Protect	System Configuration Hardening & Patch Management	PM-1	CM-03	Ensure that systems are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and service disruptions by configuring operation systems and software with appropriate parameters. Includes the removal of default accounts/passwords, disablement of unnecessary protocols/ports/services, and the ongoing distribution and installation of service packs/patches.	1)Establish a patch management program to patch workstations and servers in a timely manner. 2)Configure Operation Systems and software with the appropriate parameters to prevent unauthorized access or use and to minimize service disruptions. 3)Include the removal of or changed default accounts and passwords. Disable unnecessary services, ports and protocol 4) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 5)The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			PM-2	MA-01		
			PM-3	MA-02		
2.25	Protect	Access Control	AC-01	AC-02	Processes used to ensure access to applications, servers, databases, and network devices in the environment is limited to authorized personnel. Access is to be limited to authorized users, processes acting on behalf of authorized users, or authorized devices. Authorized users are further limited to the types of transactions and functions that they are permitted to exercise. Session limits, lockout features for failed login attempts, account expirations and disabling unused accounts are controls that provide access control.	1) Establish processes to ensure access to applications, servers, databases and network devices in the environment is limited to authorized personnel based on least privileges through documented on-boarding procedures. 2) Establish session limits, lockout features for failed login attempts, auto screen locking features. 3)Establish account expirations and disable unused accounts in a timely manner. 4) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 5) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			AC-02	AC-03		
			AC-03	AC-04		
			AC-04	AC-05		
			AC-05	AC-06		
			AC-06	AC-07		
			AC-07	AC-08		
			AC-08	AC-11		
			AC-09	AC-12		
			AC-10	AC-14		
			AC-11	AC-17		
			AC-12	AC-18		
			AC-13	AC-19		
			AC-14	AC-20		
			AC-15	AC-21		
			AC-16	AC-22		
			AC-17	IP-02		

			AC-18	CM-05		
			AC-19	MP-02		
			AC-20	AC-01		
2.26	Protect	Account Management	AM-1	AC-01	Account Management establishes the standards for the creation, monitoring, control, and removal of accounts. A request process for accounts that includes authorization, approval for access by data owners, and acknowledgement of the user of their responsibilities are controls that assure proper account management. Periodic reviews of access entitlements as well as prompt removal of access during role change or employment termination are also controls that are part of account management.	1) Establish Account Management Policies, standards and processes for the creation, monitoring, control, and removal o accounts. 2) The request process for accounts that includes authorization, approval for access by data owners, and acknowledgement of the user of their responsibilities are controls that assure proper account management. 3) Also include periodic review of access entitlements and prompt removal of access during role change or employee termination. 4) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 5) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			AM-2	AC-02		
			AM-3	IA-01		
			AM-4	IA-02		
			AM-5	IA-04		
			AM-6	IA-05		
			AM-7	IA-07		
			AM-8	IA-08		
2.27	Protect	Security Systems Management	SS-1	SI-04	The design, implementation, configuration, administration, maintenance, monitoring, and ongoing support of security systems used to enforce security policy and provide security services. Systems include firewalls, Intrusion Prevention Systems (IPS), Internet Proxy Servers, Security Information and Event Management (SIEM) systems, and other control enforcement or monitoring systems.	1) The design, implementation, configuration, administration, maintenance, monitoring, and ongoing support of security systems should be used to enforce security policy and provide security services. Security systems include firewalls, Intrusion Prevention Systems (IPS), Internet Proxy Servers, Security Information and Event Management (SIEM) systems, and other control enforcement or monitoring systems. 2) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 3) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			SS-2	SI-04		
			SS-3	SA-04		
			SS-4	SA-10		
			SS-5	CM-02		
			SS-6	CM-03		
			SS-7	CM-06		
			SS-8	CM-07		
			SS-9	PL-08		
2.28	Protect	Network Access and Perimeter Controls	PC-1	AC-01	Network equipment such as servers, workstations, routers, switches and printers should be installed in a manner that prevents unauthorized access while limiting services to only authorized users. A perimeter should be established to delineate internal systems and prevent unauthorized external parties from tampering, attempting access or connecting without approved remote access methods.	1) Establish Identity Access Management (IAM) for On-boarding and Off-boarding processes. 2) Establish Identity Access Management (IAM) for Remote access (i.e. VPN, Citrix). 3) Establish Identity Access Management (IAM) for Wireless Access. 4) Establish Identity Access Management (IAM) for Firewall rule sets. 5) Establish Identity Access Management (IAM) for Network switch configuration (best practice). 6) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 7) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			PC-2	AC-02		
			PC-3	AC-03		
			PC-4	AC-17		
			PC-5	AC-20		
			PC-6	SC-07		
			PC-7	SC-10		
2.29	Protect	Internet Content Filtering	IC-1	AC-03	The enforcement of controls used to block access to Internet websites based upon categories of content, application types and granular application functions, time of day or amount of utilization, or the dynamically updated reputation of the destination. Bandwidth Preservation – The Local Area Network (LAN) and Wide Area Network (WAN) resources within the Agency locations are limited and heavily utilized for conducting business. The Bandwidth Preservation aspect of Internet Content Filtering i designed to remove unnecessary bandwidth usage from the network by blocking access to sites that are not business related and consume excessive bandwidth. Inappropriate Content – The Internet contains content that is inappropriate in nature and unacceptable for access in the workplace. The Inappropriate Content service within the Internet Content Filtering function is intended to support the Management and Human Resources policies to provide a non-threatening or offensive workplace environment. Additionally, the Inappropriate Content service provides management and monitoring tools for the enforcement of waste and abuse of state resources. Malware and Cyber-threat Prevention- Internet content is often used to propagate malware and cyber-threats. Even the most popular Internet sites have become infected and used to spread malicious code. The Malware and Cyber-Threat Prevention aspect of Internet Content Filtering is designed to prevent the infection and spread of malware through Internet content.	1) Establish Information Security Policies to provide a non-threatening or an offensive workplace environment. 2) Utilize the Internet Content Filtering function to support the Information Security policies to provide a non-threatening o offensive workplace environment. 3) Utilize the Internet Content Filtering function to prevent the infection and spread of malware throughout our infrastructure and end points devices. 4) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 5) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			IC-2	SC-22		
			IC-3	SC-07		
			IC-4	CM-07		
			IC-5	SC-39		
			IC-6	AC-17		
			IC-7	SC-20		
			IC-8	SC-21		
			IC-9	Cp-08		
			IC-10	AC-18		
2.3	Protect	Data Loss Prevention	DL-1	AU-11	Solution designed to detect and prevent potential data breach incidents where sensitive may be disclosed to unauthorized personnel by malicious intent or inadvertent mistake. Detection o data at risk can be performed while in use at the endpoint, while i motion during transmission across the network, and while at rest on data storage devices.	1) Data Loss Prevention (DLP) should be implemented to monitor and detect sensitive information at risk while in use at t endpoint, while in motion during transmission across the network, and while at rest on data storage devices. 2) Implementation of DLP will help in detection against unauthorized access or exposure internally and externally during exfiltration attempt. 3) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 5)The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			DL-2	SC-07		
			DL-3	SC-08		
			DL-4	SC-12		
			DL-5	SC-13		
			DL-6	IR-05		
			DL-7	SI-04		
			DL-8	SI-06		
			DL-9	PS-03		
			DL-10	AC-05		
2.31	Protect	Identification & Authentication	IA-1	AC-01	The verification of the claimed identity of users, processes, or devices as a prerequisite to permitting access. Verification can b performed by accepting a password, a Personal Identification Number (PIN), smart card, biometric, token, exchange of cryptographic keys, etc. Passwords are the most common authentication factor used in the identification process for users. Password standards establish the rules for the creation, length	1) Establish an Account Management or Identity and Access Management (IAM) Policy for verification of the claimed identity of users, processes, or devices as a prerequisite to permitting access. 2) Establish a Password Policy for verification accepting a password, or a Personal Identification Number (PIN), smart ca biometric, token, exchange of cryptographic keys, etc. 3) Consider implementing multi-factor authentication (MFA) to reduce the threat of compromised account information. 4) Passwords are the most common authentication factor used in the identification process for users. 5) Password standards establish the rules for the creation, length and complexity requirements, distribution, retention and periodic change as well as suspension or expiration of authenticators. 6) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its
			IA-2	AC-02		
			IA-3	IA-01		
			IA-4	IA-02		
			IA-5	IA-03		
			IA-6	IA-04		

			IA-7	IA-05	and complexity requirements, distribution, retention and periodic change as well as suspension or expiration of authenticators.	compliance. 7)The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
			IA-8	IA-06		
			IA-9	IA-07		
			IA-10	IA-08		
2.32	Protect	Spam Filtering	SF-1	SI-08	As digital messaging (e-mail, cellular messaging, etc.) has become an integral part of the business process, its abuse has also grow This abuse often is manifested as "SPAM" or "junk" messaging which has the potential to, beyond its annoying nature, slow- down and/or clog the infrastructure required to process electronic messages. In addition, "SPAM" is often used as a transmission vehicle in the migration of malicious code infections. To limit the effects of "SPAM", messages will be examined for content and filtered as required.	1) "SPAM" or "junk" messaging which has the potential to, beyond its annoying nature, slow-down and/or clog the infrastructure required to process electronic messages. "SPAM" is often used as a transmission vehicle in the migration malicious code infections. To minimize the effects of "SPAM", messages should be examined for content and filtered as required. 2) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 3) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
2.33	Protect	Portable & Remote Computing	RC-1	AC-17	Computing is no longer limited to traditional workstations. Mobile computing has introduced tablets, smartphones, handhelds and other computing devices designed to be portable and facilitate productivity for remote users. Traditional controls still apply in many areas, but additional considerations must be made for portable devices and the specific configuration and enforcement of controls will likely require special consideration.	1) Establish a Portable or Mobile Computing Policy to address this rapidly changing environment. Portable or Mobile computing has introduced tablets, smartphones, handhelds and other computing devices designed to be portable and facilitate productivity for remote users. 2) Traditional controls still apply in many areas, but additional considerations must be made for portable devices and the specific configuration and enforcement of controls will likely require special consideration. 3) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 4) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.
			RC-2	AC-18		
			RC-3	CP-08		
			RC-4	SC-07		
			RC-5	SC-20		
			RC-6	SC-21		
			RC-7	SC-22		
			RC-8	SC-39		
			RC-9	SC-18		
2.34	Protect	System Communications Protection	CO-1	PM-15	The control, monitoring, management and protection of communications and transmissions between information systems. Includes network architecture considerations, inventory of confidential and restricted data transmissions, permitted inbound and outbound Internet communications, permitted inbound and outbound extranet and intranet communications, as well as communications between agencies. Establishes the requirements for protections such as link encryption, secure file transmission protocols, retention of files on source and destination systems, integrity validation, and restrictions for access at all levels (i.e. user/process, system, and network).	1) Application Architecture should include how the application communicates with end users, servers, databases and transmissions between information systems. 2) The control, monitoring, management and protection of communications and transmissions between information systems should include network architecture considerations, inventory of confidential and restricted data transmissions, permitted inbound and outbound Internet communications, permitted inbound and outbound extranet and intranet communications, as well as communications between approved external entities. 3) Establish the requirements for protections such as link encryption, secure file transmission protocols, retention of files on source and destination systems, integrity validation, and restrictions for access at all levels (i.e. user/process, system, and network). 4) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 5) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis. 6) Implement HTTPS encryption with Strict Transport Security (HSTS) using TLS 1.2 or higher on all public facing website and applications on locally managed services and with 3rd parties via contract language updates.
			CO-2	SC-01		
			CO-3	SC-02		
			CO-4	SC-04		
			CO-5	SC-05		
			CO-6	SC-08		
			CO-7	SC-21		
			CO-8	SC-10		
			CO-9	SC-12		
			CO-10	SC-13		
			CO-11	SC-15		
			CO-12	SC-17		
			CO-13	SC-18		
			CO-14	SC-19		
			CO-15	SC-20		
			CO-16	SC-22		
			CO-17	SC-23		
			CO-18	SC-39		
			CO-19	SI-05		
2.42	Protect	* System Currency	SC-1	SA-03	Ensures that the necessary knowledge, skills, hardware, software and supporting infrastructure are available at a reasonable cost t support information systems operation. Includes the monitoring and planning of future system developments that enable the organization to leverage modern technology and reduce technical debt.	1) Establish a documented information systems currency policies and modernization roadmap exist and are developed with appropriate stakeholder input. 2)Ensure standards exist for maintaining the organizationally defined level of currency. 3)Exceptions to currency should be documented and a roadmap or plan for modernize outdated components is documented and adhered to. 4) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 5) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.
			SC-2	CA-06		
			SC-3	MA-06		
			SC-4	PL-01		
			SC-5	PL-02		
			SC-6	SA-22		
2.35	Detect	Vulnerability Assessment	VA-1	RA-05	Assessment and monitoring of vulnerability detection and remediation including patch management processes, configuration management, system, database and application security vulnerabilities. Test and evaluate security controls and security defenses to ensure that required security posture levels are met. Perform and/or facilitate ongoing and periodic penetration testing of security defenses. Evaluate results of various penetration tests to provide risk-based prioritization of mitigation.	1) Establish a documented vulnerability assessment management program. 2) The vulnerability assessment management program should include regular assessments and monitoring of vulnerability detection and remediation including patch management processes, configuration management, system, database and application security vulnerabilities. 3) Test and evaluate security controls and security defenses to ensure that required security posture levels are met. 4) Establish a tracking process to measure the effectiveness of the program. 5) Perform and/or facilitate ongoing and periodic penetration testing of security defenses. 6) Evaluate results of various penetration tests to provide risk-based prioritization of mitigation. 7) Re-test to validate the mitigation worked as anticipated. 7) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 8) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.
			VA-2	SI-05		
			VA-3	SI-02		

2.36	Detect	Malware Protection	MP-1	SI-03	The prevention, detection and cleanup of Malicious Code (including virus, worm, Trojan, Spyware and other similar variants). Protection is accomplished at varying layers including the host, at the network, or at the gateway perimeter. Protection mechanisms must be updated periodically and frequently to address evolving threats and monitored to provide manual intervention where required.	1) Establish a Malicious Code Policy to reflect the management intent to prevent, detect, protect and cleanup malicious code in your environment. 2) Protection is accomplished at varying layers including at the host, at the network, and/or at the gateway perimeter. 3) Protection mechanisms must be updated periodically and frequently to address evolving threats and monitored to provide manual intervention where required. 4 The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 5 The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations a regular basis.
2.37	Detect	Security Monitoring and Event Analysis	MA-1	SI-04	Analysis of security events and alerts as detected by the array of security enforcement devices and log collection facilities implemented throughout the Enterprise environment. System level events include server operating system security and system logs. Application level events include web application logs, application access logs, and other application associated log events. Security monitoring and analysis includes alert configuration and generation, event correlation as well as defining and distributing periodic reports and event statistical analysis. Also includes analysis of events from the Internet content filtering system, SPAM prevention system, email encryption system, and other security control devices to ensure appropriate protections of information and information resources. Security Monitoring and Event Analysis can include advanced functionality used to detect fraud within program areas and ensure client identity protection by collecting and analyzing data access correlated with system events information. The limits of this function are limited only by the data sources that are compiled and the resources devoted to the data analysis.	1) Establish a Security Monitoring and Event Analysis (SIEMS) program to include advanced functionality used to detect fraud within program areas and ensure client identity protection by collecting and analyzing data access correlated with system events information. This function is limited only by the data sources and the resources devoted to the data analysis. 2) Analyze security events and alerts as detected by the array of security enforcement devices and log collection facilities implemented throughout the Enterprise environment. System level events include server operating system security and system logs. 3) Include web application logs, application access logs, and other application associated log events where feasible restrained only by limited resources. 4) Also, include analysis of events from the Internet content filtering system, SPAM prevention system, email encryption system, and other security control devices to ensure appropriate protections of information and information resources where feasible. 5) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 6) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.
			MA-2	SI-05		
			MA-3	SI-07		
			MA-4	PM-14		
			MA-5	SI-11		
			MA-6	CA-07		
			MA-7	SC-05		
			MA-8	SC-07		
2.41	Detect	* Audit Logging	AL-1	AU-01	Ensures that the necessary knowledge, skills, hardware, software and supporting infrastructure are available at a reasonable cost t support information systems operation. Includes the monitoring and planning of future system developments that enable the organization to leverage modern technology and reduce technical debt.	1) Establish documented logging policies and standards which are enforced throughout the organization. 2) Ensure logs are stored for the appropriate retention periods and periodically checked for accuracy and adherence to defined policies. 3) Verify there are sufficient controls in place to provide auditable evidence for system transactions and that key records available for a sufficient amount of time. 4) Establish and document responsibility for notifying and escalating incidents to appropriate personnel and coordinating activities to ensure timely isolation and containment, impact analysis, and any resulting remediation / resolution requirements. 5) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 5) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.
			AL-2	AU-02		
			AL-3	AU-03		
			AL-4	AU-04		
			AL-5	AU-05		
			AL-6	AU-06		
			AL-7	AU-07		
			AL-8	AU-08		
			AL-9	AU-09		
			AL-10	AU-11		
			AL-11	AU-12		
2.38	Respond	Cyber-Security Incident Response	SI-1	IR-01	Establishes an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, recovery, and response activities. The Incident Response program is used to track, document, and report incidents to appropriate officials and/or authorities.	1) Establish an Incident Response policy and program with the handling capability for information systems that includes adequate preparation, detection, analysis, containment, recovery, and response activities. 2) The Incident Response program is used to track, document, and report incidents to appropriate officials and/or authorities. 3) Consider including Texas Department of Information Resources' (DIR) Incident Response Team Redbook (http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Incident%20Response%20Template%202018.pdf) as a guide in your incident response program. 4) The Incident Response program should also include the ability to implement changes in protection processes to take advantage of lessons learned from your experiences. 5) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 6) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.
			SI-2	IR-02		
			SI-3	IR-03		
			SI-4	IR-04		
			SI-5	IR-05		
			SI-6	IR-06		
			SI-7	IR-07		
			SI-8	IR-08		
			SI-9	CP-01		
			SI-10	CP-02		
			SI-11	CP-09		
			SI-12	CP-10		
2.39	Respond	Privacy Incident Response	PI-1	SE-01	Management of events, issues, inquiries, and incidents when detected or reported to include all phases from investigation through resolution. Responsible for notifying and escalating incidents to appropriate personnel and coordinating activities to ensure timely isolation and containment, impact analysis, and a resulting remediation / resolution requirement. Incidents include but may not be limited to privacy breach, loss, theft, unauthorized access, malware infections, and occurrences of negligence, human error, or malicious acts.	1) Privacy Incident Response includes the management of events, issues, inquiries, and incidents when detected or reported to include all phases from investigation through resolution. 2) Incidents include but may not be limited to privacy breach, loss, theft, unauthorized access, malware infections, and occurrences of negligence, human error, or malicious acts. 3) Establish and document responsibility for notifying and escalating incidents to appropriate personnel and coordinating activities to ensure timely isolation and containment, impact analysis, and any resulting remediation / resolution requirements. 4) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 5) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.
			PI-2	SE-02		
			PI-3	IP-04		
2.4	Recover	Disaster Recovery Procedures	DR-1	CP-02	Managing the recovery of data and applications in the event of loss or damage (natural disasters, system disk and other system failures, intentional or unintentional human acts, data entry errors or systems operator errors).	1) Establish a Backup and Disaster Recover policy and program to maximize your efforts to protect your resources during disaster utilizing the identification and prioritization of all the organization's information assets so that they are prioritize per criticality to the business. 2) Managing the recovery of data and applications in the event of loss or damage (natural disasters, system disk and other systems failures, intentional or unintentional human acts, data entry errors, or systems operator errors). 3) Regularly perform tabletop and disaster recovery exercises to determine the gaps in your documented process and provide assurances that your resources can be restored in a timely manner as they are prioritized per criticality to the business. 4) Perform regular backup restoration testing to validate backups and restoration process. 5) The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 6) The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.
			DR-2	CP-09		
			DR-3	CP-10		
			DR-4	IR-04		
			DR-5	IR08		

support@v3cybersecurity.com

OR

V3 Cybersecurity, Inc.

9838 Old Baymeadows Rd. #335

Jacksonville, FL 32256