Texas Cybersecurity Framework (TCSF)
40 Security Control Objectives and Definitions

Functional Area	Security Objective	Definition
IDENTIFY	Privacy and Confidentiality	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.
	Data Classification	Data classification provides a framework for managing data assets 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, and privacy considerations, data, whether electronic or printed, must be 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.
	Critical Information Asset Inventory	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 assets importance.
	Enterprise Security Policy, Standards and Guidelines	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.
	Control Oversight and Safeguard Assurance	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.

Functional Area	Security Objective	Definition
	Information Security Risk Management	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.
	Security Oversight and Governance	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.
	Security Compliance and Regulatory Requirements Management	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.
	Cloud Usage and Security	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.
	Security Assessment and Authorization / Technology Risk Assessments	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.
	External Vendors and Third Party Providers	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.
PROTECT	Enterprise Architecture, Roadmap and Emerging Technology	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 the continued evolution of security solutions, processes, and technology to identify continuous, ongoing ways to deliver technology and information securely.

Functional Area	Security Objective	Definition
	Secure System Services, Acquisition and Development	Ensure that the development and implementation of new systems meets the requirements necessary to assure the security of information and resources.
	Security Awareness and Training	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.
	Privacy Awareness and Training	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.
	Cryptography	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.
	Secure Configuration Management	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.
	Change Management	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.
	Contingency Planning	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 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).
	Media	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

Functional Area	Security Objective	Definition
		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.
	Physical and Environmental Protection	Assure that physical access to information systems, equipment, and the respective operating environments is limited to authorized 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.
	Personnel Security	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.
	Third-Party Personnel Security	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.
	System Configuration Hardening and Patch Management	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.
	Access Control	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.

Functional Area	Security Objective	Definition
		Session limits, lockout features for failed login attempts, account expirations and disabling unused accounts are controls that provide access control.
	Account Management	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.
	Security Systems Management	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.
	Network Access and Perimeter Controls	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.
	Internet Content Filtering	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 is 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.

Functional Area	Security Objective	Definition
	Data Loss Prevention	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 of data at risk can be performed while in use at the endpoint, while in motion during transmission across the network, and while at rest on data storage devices.
	Identification and Authentication	The verification of the claimed identity of users, processes, or devices as a prerequisite to permitting access. Verification can be 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 and complexity requirements, distribution, retention and periodic change as well as suspension or expiration of authenticators.
	Spam Filtering	As digital messaging (e-mail, cellular messaging, etc.) has become an integral part of the business process, its abuse has also grown. 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.
	Portable and Remote Computing	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.
	System Communications Protection	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).
	Information Systems Currency	Ensures that the necessary knowledge, skills, hardware, software, and supporting infrastructure are available at a reasonable cost to support information systems operations. Includes the

Functional Area	Security Objective	Definition
		monitoring and planning of future system developments that enable the organization to leverage modern technology and reduce technical debt.
DETECT	Vulnerability Assessment	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.
	Malware Protection	The prevention, detection and cleanup of Malicious Code (including virus, worm, Trojan, Spyware and other similar variants). Protection is accomplished at varying layers including at 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.
	Security Monitoring and Event Analysis	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.
	Audit Logging and Accountability	Processes, policies, and procedures that enable organizations to establish an accurate and verifiable record of system relevant actions whether manual or automated for investigatory and accountability purposes.
RESPOND	Cyber-Security Incident Response	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.

Functional Area	Security Objective	Definition
	Privacy Incident Response	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 any resulting remediation / resolution requirements. 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.
RECOVER	Disaster Recovery Procedures	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).