EXHIBIT A

DPS General Manual Chapters 25, *Cyber Security,* and 26, *Information Resource Policy*

CYBER SECURITY
01.25.00.00

25.01.00 PURPOSE. The Cyber Security Office (CSO) of the State of Texas Department of Public Safety (Department) manages and protects the Department's information resources and systems in accordance with the policies set forth of this chapter 25, "Cyber Security Policy", of the Departments General Manual. These policies are based on requirements contained in the Texas Administrative Code (TAC), Title 1, Part 10, Chapter 202, and other reference materials. These policies apply equally to all personnel including, but not limited to, Department employees, agents, consultants, contractors, and any third-party (non-organizational) authorized users granted access to the Department's information resources and systems. Security is a shared responsibility and affects all Divisions. A joint effort between the people using an organization's systems and information, and the organization itself, is required. The objectives of Cyber Security policies are the preservation of confidentiality, integrity, and availability of systems and information used by Department employees and contractors. Cyber Security policies and procedures provide a roadmap to employees of what to do and when to do it. Cyber Security policies are a living document that is continually updated to adapt with evolving threats, exploits, technology, business, and IT requirements and serve to ensure that all individuals within its scope understand their responsibility in reducing the risk of compromise and take appropriate security measures to safeguard DPS resources.
Violation of these policies may result in disciplinary action contained in Chapter 7A of the General Manual which may include, up to, termination of employees or a termination of employment relations (in the case of contractors or consultants). Additionally, individuals may be subject to loss of access to the Departments information resources and systems, as well as civil and criminal prosecution.
With coordination from the Cyber Policy Advisory Committee and DPS Executive approval through Executive Project Management Office, these policies have been approved and to be published in the Department General Manual.

25.02.00 DEFINITIONS.

Audit – Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Audit Event – Any observable occurrence in a network or system which is audited.

Audit Records – Chronological record of system activities, accesses, and operations performed in a given period which enable the reconstruction and examination of the sequence of events and changes within an event.

Audit Reduction – Audit reduction is a process that manipulates collected audit information (such as sorting and filtering) and organizes such information in a summary format that is more meaningful to analysts.

Authorizing Official (AO) – Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals in direct correlation to the necessity of the information system due to the Department's mission,

functions, or reputation. The Authorizing Official for the Department is the Law Enforcement Services Deputy Director.

Authority to Operate (ATO) – The official agency decision given by the Authorizing Official to authorize the operation of an information system and to explicitly accept the risk to organizational operations, assets, and individuals based on the implementation of an agreed-upon set of security controls.

Certification and Accreditation (C&A) – The comprehensive evaluation of the security features of an information system and determining the degree to which it meets its security requirements.

Collaborative Computing – modern technology tools to facilitate and enhance group work that exists through distributed technology, where individuals collaborate from remote locations.

Configuration Management – A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

Common Control – Security controls whose implementation results in a security capability that is inheritable by one or more organizational information systems. Security controls are deemed inheritable by information systems or information system components when the systems or components receive protection from the implemented controls, but the controls are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the systems or components. Examples of common controls would include security awareness training, incident response plans, physical access to facilities, and rules of behavior.

Change Control Board (CCB) – Board of key personnel who implement change control measures regarding information resources for the Department in an attempt to provide the business with stability and measured incremental change.

Chief Information Security Officer (CISO) – The individual responsible to the Department's Executive Director or designee for administering the information security function within the agency. The CISO is the agency's internal and external point of contact for all information security matters.

Criminal Justice Information Service (CJIS) – As defined in the Criminal Justice Information Service (CJIS) Security Policy is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJIS refers to the FBI CJIS provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions.

Confidential – A Data class used to label information as defined in TAC 202.1 (5) that is collected and maintained by the Department that must be protected against unauthorized disclosure and is not subject to public disclosure under the provisions of applicable state or federal law or other legal agreement.

Criticality – A measurement or description of Data importance to Department mission, operations, or individuals.

Cryptographic – pertaining to, or concerned with, cryptography. It is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.

Cryptographic Key (Key) – A parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that an entity with knowledge of the correct key can reproduce or reverse the operation, while an entity without knowledge of the key cannot. Like a physical key, it locks (encrypts) data so that only someone with the right key can unlock (decrypt) it.

Cryptography – The discipline that embodies the principle, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their modification. It is a method of writing codes so that data may be protected from unauthorized use or modification

Cybersecurity – The ability to protect or defend the use of cyberspace from cyber-attacks.

Cyber Security Operations (Cyber-OPS) – Houses an information security team responsible for monitoring and analyzing an organization's security posture on an ongoing basis. The Cyber OPS team's goal is to detect, analyze, and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes.

Data – Department-owned information in any form, including Metadata, that can be processed and is a general term meaning facts, numbers, letters, and symbols collected by various means and processed to produce information.

Data Breach – Incident that involves the unauthorized or illegal viewing, access, or retrieval of confidential data by an individual, application or service.

Data Sharing Agreement (DSA) – A formal document of agreement between the Department and another entity that specifies the conditions under which data is to be shared. Data sharing agreements typically specify what (and how) data will be shared, procedures to safeguard the data, and how the data is to be used.

Department – The Department of Public Safety of the State of Texas.

Department of Information Resources (DIR) – The Texas Department of Information Resources

Denial of Service (DoS) – The prevention of authorized access to resources or the delaying of time-critical operations.

Digital Signature – The result of a cryptographic transformation of data that, when properly implemented, provides source authentication, assurance of data integrity, and supports signatory non-repudiation. It is a type of electronic signature for encoded data that authenticates the source, assures the data's integrity, and prevents subsequent repudiation.

Distributed Denial of Service (DDoS) – A denial of service technique that uses numerous hosts to perform a cyber-attack. It is a kind of cyber threat or attack that makes systems on a computer network temporarily unusable.

Documents – A repository of documents stored by Cyber Security for the provisional impact levels associated with the Systems utilizing their Data.

Domain Name System (DNS) – A hierarchical database that is distributed across the internet that allows names to be resolved into IP addresses to locate services such as web and e-mail servers. The purpose of DNS is to translate hostnames to IP addresses.

General Support System – An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

External Agencies – A business or organization established to provide a particular service outside of the Department.

Federal Information Processing Standards (FIPS 199) – The federal government standard that establishes security categories of information systems used by the Federal Government and followed by the Department. See General Manual Chapter 26.170.00 "System Categorization" for additional guidance.

Flaw – A problem that exists in software programs that can be a security risk to information systems.

External Information System Service – An information system service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of the organizational information system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

Incident Response – The mitigation of violations of security policies and recommended practices.

Incident Response Plan – Provides a roadmap for implementing an incident response program based on the policy. The plan dictates goals for the program, including metrics for measuring the program and indicates how often incident handlers should be trained and requirements for handlers.

Incident Response Policy – Foundation of the incident response program, in which defines events considered incidents, establishes organizational structure for incident response, defines roles and responsibilities, and lists requirement for reporting incidents.

Incident Response Procedure – Provide detailed steps for responding to an incident, which should cover all phases of the incident response process. This should be based on the incident response policy and plan.

Information Assurance – Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Security Continuous Monitoring (ISCM) – Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

Information Systems – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information Systems Security Manager (ISSM) – Individual responsible for the information assurance of a program, organization, system, or enclave.

Information System Service – A capability provided by an information system that facilitates information processing, storage, or transmission. It provides (serves) data/knowledge/information.

Information Technology – Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the Department.

Interconnection Security Agreement (ISA) – An agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection.

Internal System Connection – Connection between organizational systems and separate constituent system components (i.e., connections between components that are part of the same system) including components used for system development.

Internet Control Message Protocol (ICMP) – Set of protocols that allow systems to communicate information about the state of services on other systems.

Intrusion Detection and Prevention System (IDPS) – Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents. This software constantly watches the network, identifying possible incidents, logging the information about them, and stopping the incident from occurring.

IPsec – A protocol that adds security features to the standard IP protocol to provide confidentiality and integrity services.

Least Privilege – A security principle that restricts the access privilege of authorized personnel to the minimum necessary to perform their jobs.

Malware (Malicious Code) – Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Major Application – An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All state applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and

should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

Major Modification – Any added functionality, any change in data classification, any change causing a system to become externally facing where it was not previously, or any new connections to other systems.

Metadata – Data that describes or provides information about other Data.

Minimum Security Controls – The management, operational, and technical controls prescribed for information system to protect the confidentiality, integrity, and availability of the system and its information.

Minor Application – An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system.

National Institute for Standards and Technology (NIST) – A non-regulatory federal agency within the U.S. Department of Commerce that promotes U.S. innovation and industrial. It is also a database for cybersecurity and information security related projects, publications, and news.

Network Engineer – A technology professional whose primary job duties include establishing and maintaining the connectivity of the Department's networks and network services.

Nonpublic Data – Data not available to the public or outside of the Department.

Password – A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Personal Identifying Information (PII) – As defined in the Texas Business and Commerce Code § 521.002 (1), means information that alone or in conjunction with other information identifies an individual, including an individual's: (A) name, social security number, date of birth, or government-issued identification number; (B) mother's maiden name; (C) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image; (D) unique electronic identification number, address, or routing code; and (E) telecommunication access device as defined by Texas Penal Code § 32.51.

Plan of Action and Milestones (POAM) **–** A document that identifies and details specific tasks to be accomplished. Details include resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Private Key – A cryptographic key used with an asymmetric-key (public-key) cryptographic algorithm that is not made public and is uniquely associated with an entity that is authorized to use it. In an asymmetric-key cryptosystem, the private key is associated with a public key. A private key, also known as a secret key, is like a password, a string of letters and numbers that is used to decrypt data when it is paired with a public key.

Privileged Access – A security principle allowing a user that is authorized to perform security-relevant functions that ordinary users are not authorized to perform.

Privileged User – A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. A privileged user has comparatively more authority and access to information systems than a normal user and can perform security-relevant functions.

Public – A Data class used to label information that is collected and maintained by the Department and is subject to public release under the provisions of applicable state of federal law or legal agreement and is not confidential.

Public Key – A cryptographic key used with an asymmetric-key (public-key) cryptographic algorithm that may be made public and is associated with a private key and an entity that is authorized to use that private key. In cryptography, a public key is a large numerical value that is used to encrypt data. The key can be generated by a software program, but more often, is provided by a trusted, designated authority and made available to everyone through a publicly accessible repository or directory.

Public Key Certificate – A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. A public key certificate is a digitally signed document that serves to validate the sender's authorization and name.

Public Key Infrastructure (PKI) – The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates. A PKI is a set of roles, policies, hardware, software, and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manages public-key encryption.

Regulated Data – Data that requires the Department to implement specific privacy and security safeguards as mandated by federal, state, or local law, or by a third-party agreement.

Residual Information Protection – Ensuring that any data contained in a resource is not available when the resource is de-allocated from one object and reallocated to a different object. This can be a security risk if reused resources contain data or meta-data from previous uses.

Risk Assessment – The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management that incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place.

Secret Key – A cryptographic key used by one or more (authorized) entities in a symmetric-key cryptographic algorithm; the key is not made public. It is a piece of information that is used to encrypt and decrypt data. A secret key may also be known as a private key.

Spam – Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

Security Alerts – A brief, technical notification regarding current vulnerabilities, exploits, and other security issues. Also known as an advisory, bulletin, or vulnerability note.

System Authorization Boundary – Logical groups of information resources (information and related resources such as personnel, equipment, funds, and information technology) that have the same function or mission objectives, reside in the same general operating environment, and are under the same direct management control.

Security Categorization – The process of determining the security category for information or an information system. Security categorization methodologies are described Federal Information Processing Standard (FIPS 199) and National Institute for Standards and Technology (NIST) SP 800-60.

Security Controls – Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system.

Security Control Assessment – The testing or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Security Incident – An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Sensitive – A Data class used to label information that is collected and maintained by the Department that must be protected against unauthorized disclosure, except for public release under the provisions of applicable state or federal law or as agreed upon in two-party agreements.

Server – A computer or device on a network that manages network resources. Examples include file servers (to store files), print servers (to manage one or more printers), network servers (to manage network traffic), and database servers (to process database queries).

Significant Change – Any added functionality that impacts how a security control is implemented, change in data classification or data types, change in system risk level, change causing a system to become externally facing where it was not previously, or new connections to other systems.

Software Development Life Cycle (SDLC) – Scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation, and maintenance, and ultimately its disposal that instigates another system initiation.

Texas Administrative Code (TAC) – Compilation of all state agency rules in Texas containing 16 titles, with each title representing a subject category and related agencies are assigned to the appropriate title.

Transport Layer Security (TLS) – An authentication encryption protocol widely implemented in browsers and Web Servers.

User – Individual, or (system) process, acting on behalf of an individual, authorized to access an information system.

Virtual – Refers to "Virtual Machine" (VM), which is software that allows a single host to run one or more guest operating systems.

Virus – A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting (inserting a copy of itself into and becoming part of) another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

Virtual Private Network (VPN) – Protected information system link utilizing tunneling, security controls, and endpoint translation giving the impression of a dedicated line. VPN provides a means of securely accessing resources on a network by connecting to a remote access server through the Internet or other network.

Voice over Internet Protocol (VoIP) – A term used to describe the transmission of packetized voice using the internet protocol and consists of both signaling and media protocols. VoIP provides a means of using the Internet as the transmission medium for phone calls.

Vulnerability – Refers to a flaw in a system that can leave it open to attack. A vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.

Vulnerability Management Program (VMP) – The Department framework, processes, and standards for detecting, removing, and controlling the inherent risk of vulnerabilities.

25.03.00 ROLES AND RESPONSIBILITIES

Chief Information Security Officer (CISO). The senior-level executive within the Department responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected. The CISO's responsibilities are further defined by Administrative Code § 202.21.

Computer Security Incident Response Team (CSIRT). A concrete organizational entity that is assigned the responsibility of providing the incident management capability for the Department. The team respond, analyzes, and resolves events and incidents reported by end users or are observed through a proactive network and system monitoring.

Cyber Operations (Cyber-OPS). Houses an information security team responsible for monitoring and analyzing an organization's security posture on an ongoing basis. The Cyber OPS team's goal is to detect, analyze, and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes.

Data Custodian. The person or business unit responsible for the day-to-day management of data from a business perspective and responsible for ensuring the usability and accessibility of Data.

Data Stewards. The Department personnel delegated by and responsible to the Data Owner to ensure Data is accurate, complies with Department security controls, and oversees Data sharing agreements with third parties.

Information Custodians. Person responsible for overseeing and implementing the necessary safeguards to protect the information assets, at the level classified by the Information Owner.

Information Owner. Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Information Resources Manager (IRM). The individual within a state agency who is responsible to the State of Texas for management of that agency's information resources.

Information Systems. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information that is necessary to the Department.

Information System Security Manager (ISSM). The individual providing direction and guidance in strategic operations and planning. Responsible for maintaining compliance with applicable security regulations for various classified information systems. Supports the design and successfully executes an Information Assurance security program which exceeds customer expectations and minimize security risks.

Information User. Individual or system process acting on behalf of an individual, authorized to access an information system.

System Custodian (**also Information System Custodian**). Individual responsible for overseeing and implementing the necessary safeguards to protect the information assets, at the level classified by the Information Owner.

System Owner (Information System Owner). Official responsible for the overall procurement, development, integration, modification, operation, or maintenance of an information system.

25.04.00 DATA CLASSIFICATION POLICY

04.01 Purpose. The purpose of the Data Classification policy is to establish a framework for properly classifying and managing data assets in accordance with Texas Administrative Code § 202.24(b)(1). The Department values Data and is committed to protecting it. Classifying Department Data into organized categories ensures effective, efficient, and secure usage. Data Classification establishes the official policy and standards for classifying, managing, and securing Department Data.

04.02 Scope. The Data Classification policy applies to all Department-owned Data, personnel employed or contracted by the Department, and entities accessing Department-owned Data. All Data Users must comply with this policy. This policy does not designate what Department Data can or must be released in response to a request under the Public Information Act, subpoena, court order, discovery, or other legal processes regarding the release of Department Data.

04.03 Data Management. The Department manages Data based on its associated risks and values. Data management practices must meet the appropriate levels of protection as required by state and federal regulations, consider and account for Data ethics and privacy, and accurately maintain Data to be readily available for authorized use. Cyber Security maintains the Department Data Classification policy and standards and must periodically review the Department Data Classification levels.

Metadata developed from Data utilization or storage, to include off premise storage, is the property of the Department. The Data used to develop Metadata determines its classification and management requirements.

04.03.01 Data Classifications. The Department classifies all Data using the following classes:

Public Data. Information that is collected and maintained by the Department and is subject to public release under the provisions of applicable state or federal law or legal agreement and is not confidential. However, Department personnel must review public data thoroughly before its release to ensure Confidential Data is not commingled.

Sensitive Data. Information that is collected and maintained by the Department that must be protected against unauthorized disclosure, except for public release under the provisions of applicable state or federal law or legal agreements. While these records and information may be considered "public" under state and federal regulations, a higher level of protection is needed to ensure Confidential Data is not commingled.

Confidential Data. Information as defined in 1 Texas Administrative Code § 202.1 (5) that is collected and maintained by the Department that must be protected against unauthorized disclosure and is not subject to public disclosure under the provisions of applicable state or federal law or as agreed upon in two-party agreements.

Regulated Data. Requires the Department to implement specific privacy and security safeguards as mandated by federal and state law.

04.03.02 Life Cycle. Data may be subject to reclassification through the course of its lifecycle. All Data must be stored, disposed, or destroyed in accordance with Department record retention requirements. The Department Records Management Officer maintains a record of all disposed or destroyed Data in accordance with the Department records retention requirements.

04.03.03 Security Controls. Data security controls are determined according to their classification level. Data classification security controls must include the following.

04.03.04 Roles and Responsibilities.

Information Owners:

1) Approving Data release
2) Authorizing access to Data
3) Classifying Data assets

4) Determining the corrective actions during risk reducing initiatives targeting Data and its associated systems; and

5) Ensuring Data Users and third parties, such as contractors, accessing Data are informed of Department Data classification requirements.

Data Stewards:

1) Responsible to the Data Owner

2) Ensuring overall Data quality and accuracy for business unit

3) Managing business unit's Data assets

4) Acting as the official point of contact regarding all business unit Data related initiatives

5) Ensuing Data complies with all security controls as determined by Cyber Security

6) Overseeing business unit Data sharing agreements and secure data exchange with third parties; and

7) Verifying third parties, including contractors, are compliant with Department Data Classification requirements.

Data Custodians:

1) Assisting Information Owners determine the systems, users, or third parties accessing their Data

2) Communicating with Information Owners about systems or process changes that affect their Data

3) Enforcing security controls based on Data Classification levels

4) Maintaining Data confidentiality, integrity, and availability; and

5) Participating in risk reducing initiatives.

Data Users:

1) Labeling Data, when applicable
2) Handling Data according to their Data Classification requirements; and
3) Disposing Data according to its record retention requirements.

Office of General Counsel:

1) Functions as the Department privacy office and provides legal advice in developing and maintaining Data security compliance documentation
2) Reviews Data sharing agreements; and
3) Provides Information Owners with legal guidance for classifying, releasing, and managing their Data.

Cyber Security:

1) Developing and maintaining Data security compliance documentation

2) Leading Department Data risk-reducing initiatives

3) Assisting Information Owners with determining third party compliance and Data sharing agreement compliance with Department Data classification requirements

4) Monitoring information system activity to ensure Data security control compliance; and

5) Providing Information Owners guidance for classifying, managing, and securing their Data.

04.03.05 Data Controls. Data controls must ensure Data assets remain protected throughout their lifecycles. Data Classification standards determine the requirements for Data marking, handling, duplication, mailing, disposal, and storage.

04.03.06 Access Controls. Department Data access is controlled, authorized, and granted on a need-to-know basis according to the Principle of Least Privilege. Information owners must approve all access rights to personnel. Information owners must approve the external release of Sensitive or Confidential Data unless the release is required by law. Third parties and Data sharing agreements accessing Data must be verified and compliant with Department Data Classification requirements. Data Classification standards determine the requirements for Data reading, modifying, and deleting account privileges.

1. **Transmission Controls** Printing, transmitting, and sharing Sensitive or Confidential Data must be controlled, logged, and monitored. Data Classification standards determine the Data requirements for physical printing, public transmission, and release to third parties.

2. **Audit Controls** Data Custodians must configure systems accessing Sensitive or Confidential Data to log all violation attempts and maintain audit trails to ensure Data accountability. System logs must be retained in accordance with Department records retention requirements. Data Classification standards determine the Data requirements for process logging, auditing access activity, access report retention, and classification lifecycle.
3. **Encryption Controls** Encrypted Data must comply with Department encryption policy as well as any applicable state and federal regulations. Data Classification standards determine the encryption requirements for Data in storage, at rest, transmission, and on media devices.

25.05.00 SYSTEM CATEGORIZATION

05.01 Purpose. The purpose of the System Categorization policy is to establish a risk-based framework thereby managing and reducing the Department's risk by ensuring all systems have the appropriate level of security controls. The Department must develop and implement a Risk Management Framework (RMF) in order to comply with legislative mandate in 1 Texas Administrative Code § 202.24.

05.02 Scope. The System Categorization policy applies to all systems using or storing Department owned Data and information. Third-party vendor contracts and users that use or store Department information must acknowledge and adhere to this policy. The Department must develop or adopt and adhere to a formal documented program for the categorization of information systems according to risk level by applying guidance found in this policy.

05.03 System Identification. The Department must maintain an accurate, confidential, and centrally located ledger identifying all Department owned systems and applications. System categorization guidelines determine the ledger content requirements and must include system name, environment information, status, dependencies, interconnections, criticality, sensitivity, system group, business function, locations, and owner.

05.04 System Categorization. Department System Categorization determines the minimal level of required security controls for each individual system. All Department systems must be categorized, and its minimal level of required security controls implemented. Security Categories are based on the

Department's potential impact if certain events occur which jeopardize Department data or systems needed to accomplish organizational mission, protection of assets, legal responsibilities, maintain operations, or protect individuals. Security Categories must be in conjunction with the Vulnerability Assessment and Management Standard and threat information when assessing Department risks.
The following table establishes the security objectives and impact level taxonomies used to determine the security categories of Department Systems.

Security Objectives

Security Objective	Description
Confidentiality	Preserving Authorized Restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information *A loss of confidentiality is the unauthorized disclosure of information.*
Integrity	Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity *A loss of integrity is the unauthorized modification or destruction of information.*
Availability	Ensuring timely and reliable access to and use of information *A loss of availability is the disruption of access to or use of information or an information system.*

Impact Levels

Impact Level	Description
Low	Potential losses have a limited or minor adverse effect on Department operations, information assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Moderate	Potential losses have a serious or significant adverse effect on Department operations, information assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
High	Potential losses have a severe or catastrophic adverse effect on Department operations, information assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

Security Objective Impact Matrix

Security Objective	**Potential Impact**		
	Low	*Moderate*	*High*
Confidentiality	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Security Category. The Department determines security category using a risk-based methodology to calculate potential impact for each security objective associated with the system. The Department security categories defined in the following format:

Security Category = {(Confidentiality, *impact*), (Integrity, *impact*), (Availability, *impact*)}

The Department considers all non-categorized systems to have the following security category: {(Confidentiality: High), (Integrity: High), (Availability: High)}.

Security Category Lifecycle. System categorizations may need adjustments throughout its lifecycle to reflect a more realistic view of the potential impact. The Department accomplishes system category adjustment in the following:

1) System and Information owners review the appropriateness of the potential impact levels based on the Department mission, environment, system use, and Data Sharing.

2) System and Information owners align security objective impact levels adjustment to special factors. The System Categorization guidelines determine the applicable special factors for adjusting System security categories above that of its constituent information types.

1. System and Information owners Document all adjustments to the impact levels and provide the rationale and justification for Cyber Security for approval.

05.05 Roles and Responsibilities.

Information Owners

1) Identifies the types of data utilized, stored, and transmitted by associated Department systems
2) Assigns a security impact value for the security objectives associated with the systems utilizing their data
3) Categorization of Department systems using their Data
4) Documents the provisional impact levels associated with the systems utilizing their Data; and
5) Determines the corrective actions during security control implementation.

System Owners

1) Identifies the types of data utilized, stored, and transmitted by associated Department systems
2) Assigns a security impact value for the security objectives associated with the systems utilizing their Data
3) Documents the provisional impact levels associated with the systems utilizing their Data
4) Determines the corrective actions during security control implementation
5) Implements appropriate security controls related to a system's categorization determined by Cyber Security
6) Collaborate with Information owners to categorize systems utilizing their Data; and
7) Provide the information or documentation necessary for Information owners to fulfill their responsibilities.

Cyber Security

1) Develops and maintains system categorization security compliance documentation including Department policy and guidelines
2) Test and monitor system activities to ensure security control compliance and appropriateness
3) Provides the necessary guidance to the Department for categorizing, adjusting Department systems and security control implementation
4) Approves the security category impact levels and for identified information types
5) Reviews and approves the appropriateness of the provisional impact levels based on Department guidance
6) Determines and assigns the minimal level of security controls to be implemented based on a system's categorization; and
7) Determines the System Categorization audit and adjustment schedule.

25.06.00 ACCESS CONTROL

06.01 Roles and Responsibilities.

Information Owners and Information Custodians

1) Approve user access requests prior to access request being authorized;
2) Immediately notify the Local Security Administrator when an Information User role has changed, including duty reassignments, transfers, promotions, demotions, extended absences, or

terminations. Documenting, managing, and annually reviewing access controls to information and information systems under their control to ensure:

a. Access rights requests are authorized

3. b. Access rights are restricted on the need-to-know and least privilege principles

4. c. Access rights are role-based when technically feasible; that is, permissions are assigned to roles rather than unique user identifiers

5. d. Segregation of access control roles (e.g., access request, authorization, and administration)

e. Access rights are modified or removed based on business and security requirements

f. Access to information and information systems are auditable based on access by user identifiers; and,

g. Access control policies are communicated to users through security awareness training.

06.02 User Access Management. User access management is done to ensure that authorized users and processes acting on behalf of users, can access Department-managed systems while preventing unauthorized users from accessing or modifying systems.

06.02.01 User Registration and Deactivation. There must be a formal user registration and de-registration procedure for granting access to all information systems. Information Owners must grant or revoke user access to all information systems based on a formal user registration and de-registration process.
Personnel Managers must approve user access requests prior to access request being authorized; and immediately notify the Local Security Administrator when an Information System User role has changed, including duty reassignments, transfers, promotions, demotions, extended absences, or terminations.
Deactivation of user accounts will occur after a 120-day period of an account not being used or logged into. Before deactivation, a notice will be sent to the Local Security Administrator on the 110th day stating, "(users) account has not been logged into for the previous 110 days. In accordance with the Access Control Policy, this account will be disabled on the 120th day of no usage. Please confirm with the information owner that this account is still being used or is no longer used. A lack of confirmation will result in the account being disabled."

06.02.02 User Access Provisioning. There must be a formal user accessing process to implement access or revoke access rights for all user types to all systems and services.
Information Owners and Information Custodians are responsible for the access provisioning process, including:

1) Obtaining authorization from the owner of the information system or service for the use of the information system or service; separate approval for access rights from Information Owners may also be appropriate

2) Verifying that the level of access granted is appropriate to the access policies and is consistent with other requirements such as segregation of duties

3) Ensuring that access rights are not granted (such as by service providers) before authorization procedures are completed

4) Maintaining a central record of access rights granted to user ID to access information systems and services

5) Adapting access rights of users who have changed roles or jobs and immediately removing or blocking access rights of users who have left the Department; and

6) Periodically reviewing access rights with owners of the information systems or services.

06.02.02.01 Separation of Duties. Information Owners and Information Custodians are responsible to establish one or more internal control that prevents or detects errors and irregularities by assigning to separate individuals the responsibility for initiating and recording transactions and for the custody of assets.
Information Owners and Information Custodians are responsible for documenting and implementing controls in information systems to enforce separation of duties through assigned access authorizations.

06.02.03 Management of Privileged Access Rights. A formal user accessing procedure for the allocation and use of privileged access rights must be restricted and controlled.
Information Owners and Information Custodians are responsible for allocation of privileged access rights process and must be controlled through a formal authorization procedure.

The following steps must be considered:

1) The privileged access rights associated with each system or procedure, e.g., operating system, database management system and each application and the users to whom they need to be allocated should be identified

2) Privileged access rights should be allocated to users on a need-to-use basis and an event-by-event basis, based on the minimum requirement for their functional roles

3) An authorization procedure and a record of all privileges allocated should be maintained. Privileged access rights should not be granted until the authorization procedure is complete

4) Requirements for the expiry of privileged access rights should be defined

5) Privileged access rights should be assigned to a user ID different from those used for regular business activities. Regular business activities should not be performed from privileged ID

6) The competencies of users with privileged access rights should regularly be reviewed to verify if they are in line with their duties

7) Specific procedures should be established and maintained to avoid the unauthorized use of generic administration user IDs, according to systems' configuration capabilities; and

8) For generic administration user IDs, the confidentiality of privileged access information should be maintained when shared (e.g., changing passwords frequently and as soon as possible when a privileged user leaves or changes job, communicating them among privileged users with appropriate mechanisms).

06.02.04 Management of Privileged Access Information of Users. A procedure for the allocation of privileged access information must be controlled through a formal management process.

Information Owners and Information Custodians are responsible for process allocation of privileged access information that must include the following requirements:

1) Users should be required to sign a statement to keep personal privileged access information confidential and to keep group or shared privileged access information solely within the members of the group; this signed statement may be included in the terms and conditions of employment

2) Procedures should be established to verify the identity of a user before providing new, replacement, or temporary privileged access information

3) Temporary privileged access information should be given to users in a secure manner; the use of external parties or unprotected (clear text) email messages should be avoided

4) Temporary privileged access information should be unique to an individual and should not be guessable

5) Users should acknowledge receipt of privileged access information; and

6) Default vendor privileged access information should be altered following installation of systems or software if the systems or software are DPS-owned, created, or developed and not owned by a third-party or contractor.

06.02.05 Review of User Access Rights. Information Owners and Information Custodians are responsible for implementing a formal procedure for the periodic review of user access rights. Information users should be granted minimum user access rights to perform their roles based on the need-to-know principle.

User access rights must be reviewed and reauthorized:

1) Annually, or more frequently depending on the value of the information system

2) When a role changes as a result of the promotion, demotion, transfer, or other change that may affect access requirements; and

3) When new systems and applications are deployed by the Department.

06.03 SYSTEM AND APPLICATION ACCESS CONTROL

06.03.01 Information Access Restriction. Access to information systems functions and information must be restricted in accordance with the access control policy.

06.03.01.01 Information Access Controls. Information Owners and Information Custodians are responsible for ensuring the implementation of the access control policy for their business applications. Every information system must have an access control policy that specifies access permissions for information and system functions. The access control policy must identify the information and system functions accessible by various classes of users.

The application and information section of the access control policy must specify:

1) The information to be controlled

2) The system functions to be controlled; and,

3) The roles authorized to access the resources/information and what types of access are permitted (e.g., Create, Read, Update/Write, Delete, Execute) based on business need.

06.03.01.02 System Configuration. Information system access controls must be configurable to allow Information Custodians to modify access permissions without making code changes.
System utilities or functions that can bypass user access controls must be specified in the access control procedure. Access to these utilities and functions must be restricted.

06.03.01.03 Publicly Accessible Information. Information that is publicly accessible must be segregated from non-public information.

06.03.01.04 Segregation of Sensitive Information Systems. Information Owners and Information Custodians must follow the System Categorization Policy (GM 25.06.00). The information system classification level determines the controls beyond baseline standards that must be followed.

06.03.01.05 Information Flow Enforcement. Information Owners and Information Custodians are responsible for developing a procedure to address the configuration of the information system to enforce approved authorizations for controlling the flow of information within the system and between authorized interconnected systems.

06.03.02 Secure Log-on Procedure. Access to information systems must use a secure logon procedure.

06.03.02.01 System Use Notification. All systems must use Department logos containing approved wording and must provide prompts as needed. Information system must display to users a notification before granting access to the system that provides privacy and security notices consistent with applicable federal and state laws.

06.03.02.02 Unsuccessful Logon Attempts Information Owners must ensure that Information Custodians configure logon processes to:

1) Record unsuccessful logon attempts

2) Allow a limited number (no more than three) of unsuccessful logon attempts

3) Limit the minimum and maximum time allowed for the logon procedure. If exceeded, the system should terminate the logon; and,

4) Force a time delay or reject further logon attempts if the limited number of consecutive unsuccessful logon attempts is reached.

06.03.02.03 Previous Logon Notification. The information system must notify the user, upon successful logon to the system, of the date and time of the last logon.

06.03.02.04. Session Control The information system limits the number of concurrent sessions for each account.

06.03.02.05. Session Lock Department systems must timeout sessions or require a re-authentication process after 30 minutes of inactivity.

06.03.02.06 Password Transmission. Information Owners and Information Custodians must ensure logon processes are configured to prevent transmission of passwords in clear text.

06.03.03 Use of Privileged Utilities Programs. Use of system utility programs must be restricted and tightly controlled.

Information Owners and Information Custodians must restrict access to system utility programs by:

1) Defining and documenting authorization levels

2) Restricting the number of users with access to system utility programs

3) Annually reviewing the status of users with permission to use system utility programs

4) Requiring a secure logon process

    a) Identify system utility programs in use and log usage; and

    b) Removing or disabling redundant or obsolete system utilities and system software.

06.03.04 Access Control to Program Source Code. Access to DPS-owned program source code must be restricted.

Information Owners and Information Custodians must implement procedures to control access to program source code, program source libraries, and related documentation for information systems by:

1) Restricting access by privileged users on a need to access basis

2) Authorizing modifications to program source code, program source libraries, and related documentation

3) Ensuring change control procedures are followed when maintaining and copying program source libraries

4) Maintaining access audit logs

5) Using a controlled central repository for storing program source code and libraries that is isolated from operational information systems; and,

6) Securely protecting and storing media containing program source code, program source libraries, and related documentation.

06.05 Network Management. Information Custodians must enable network services needed to support business requirements (for example, by explicitly enabling needed services and disabling unneeded services). Access to network services will be controlled at network perimeters, routers, gateways, workstations, and servers.

Information system network access must be restricted to the authorized users and systems, using the principle of least privilege, as defined in the access control policies for the information system.

06.05.01 Management Controls and Processes. Information Custodians must document processes for management of network access, including:

1) Documentation and review of implemented network access controls

2) Identification of threats, risks, and mitigation factors associated with network services; and

3) Testing of network access controls to verify correct implementation.

06.05.02 Remote Access. Access to the Department network and internal networks via external connections from local or remote location must not be automatically granted with network or system access. Systems must be available for on- or off-site remote access only after explicit request is made by the user and approved by the manager for the system in question. With a Department approved business need and prior Department management approval, authorized users of agency computer systems and data repositories must be permitted to connect remotely to those systems through secure authenticated and carefully managed access methods. The minimum method for remote access must consists of using a Virtual Private Network (VPN) and minimum security controls required for connection to networks (such as anti-virus software, firewalls, and user and system authentication requirements).

06.05.03 Wireless Access. Such wireless technologies include microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (such as EAP/TLS, PEAP), which provide credential protection and mutual authentication. In certain situations, wireless signals may radiate beyond the confines and control of Department controlled facilities.
Network Engineers must ensure these steps for secure wireless access:

1) Establish usage restrictions and implementation guidance for wireless access

2) Monitor for unauthorized wireless access to the information system

3) Authorize wireless access to the information system prior connections; and

4) Enforce requirements for wireless connections to the information system.

Network Engineers must ensure the Service Set Identifiers (SSID) values are changed from the manufacturer setting. Some networks should not include organizational or location information in the SSID. The prohibition and periodically monitor any unauthorized installation or use of Wireless Personal Area Networks on state organizational IT systems by individuals without approval of the Department.

06.05.04 Mobile Devices. Information Owners and Information Custodians must establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for DPS controlled mobile devices; and authorize connections of mobile devices to Department Information systems.

06.06 Use of External Information Systems. Information Owners and Information Custodians must establish terms and conditions, including types of applications that can be accessed from external information systems, security category of information that can be processed, stored, or transmitted, use of VPN and firewall technologies, the use and protection against vulnerabilities of wireless technologies, physical security maintenance, and the security capability of installed software are to be updated.

06.07 Information Sharing. Information Owners and Information Custodians must enable secure information sharing between authorized users and trusted third parties as required by the Department

by ensuring the recipient has similar to or better than Department controls in place around the information being shared.

06.08 Portable Storage Devices. Information Owners and Information Custodians must restrict the use of Department-controlled portable storage devices by authorized individuals on external information systems. These portable storage devices must be encrypted, so if lost, any information on them can be rendered useless.

06.09 Publicly Accessible Content. Information Owners and Information Custodians must designate individuals authorized to post information onto a publicly accessible information system. Training of authorized users to ensure that publicly accessible information does not contain nonpublic information. Review proposed content of information prior to posting onto publicly accessible information system to ensure that nonpublic information is not included. Review the content on the publicly accessible information system for nonpublic information and remove such information, if discovered.
06.10 Access Control Decisions The Information Owner must establish procedures to ensure access control decisions are applied to each access request prior to access enforcement.

25.07.00 AUDIT AND ACCOUNTABILITY

07.01 Purpose. The purpose of this policy is to provide the framework by which information system audit and accountability procedures must be conducted. This framework is based on the framework provided by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 4. Agency employees, contractors, and third-party personnel accessing information systems are accountable for any actions taken on a system that requires authentication and authorization to gain access. Audit events, when combined with access control procedures, ensure all actions can be traced to a unique user to establish accountability.

Audit events from systems, applications, and services also provide key information and potential indicators of compromise and are critical to have from a security monitoring and investigation standpoint.

This policy should be viewed as a set of minimum security controls that must be implemented to establish a consistent baseline of security. Additional requirements may apply depending on the needs of the Information Owner or System Owner, the type and categorization of the data being processed, stored, or transmitted by the system, and any applicable state and federal laws, executive orders, directives, policies, regulations, standards, and guidance.

07.02 Scope. This policy applies to all Department information systems that process, store, or transmit sensitive, confidential, or regulated information, or that make access control decisions. This includes information systems used, managed, or operated by a contractor, another agency, or another organization on behalf of the agency. Information Owners are responsible for ensuring that contractors comply with all applicable requirements and that all requirements are in the contract signed with the contractor (whether contractors hired through WorkQuest, DIR, or other employment agency or through a competitively posted solicitation as a vendor).

The intended audience of this policy is:

1) Information Owners and System Owners responsible for the implementation of new information systems; and
2) System Owners or System Custodians responsible for the operations of existing information systems.

07.03 Audit Events. Information Owners and System Owners must identify events that are relevant to the security and compliance of the Information Systems and the environments in which they operate. At a minimum, Information Systems must be configured to record and retain the following audit events:

1) Successful and unsuccessful log-on attempts
2) Attempts to create, modify, disable, or remove a user account
3) Attempts to access, create, write, delete, or change permission on a user account, file, directory, or other System resource
4) Attempts to change account passwords
5) All actions by privileged (administrative) accounts; and
6) Attempts for users to access, modify, or destroy the audit log.

07.04 Content of Audit Records. Information system audit records must contain the following content, at a minimum:

1) The type of event that occurred
2) The date and time the event occurred
3) The software or hardware component of the information system where the event occurred
4) The source of the event (such as the IP address)
5) The identity of the user/subject associated with the event; and
6) The outcome (success or failure) of the event.

07.05 Audit Storage Capacity and Retention. Information Owners and System Owners must ensure audit records are retained until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes, such as after-the-fact investigations of security incidents.

1) Audit records for the events identified in Section 03.01 must be retained in accordance with information-specific retention policies and compliance requirements.
    a) In the absence of specific policies, audit records must be retained for at least one year.
    b) All record retention must be in accordance with General Manual Chapter 21: *Records and Information Policies.*

2) Information Systems must have enough storage capacity allocated to ensure the retention of all audit records for the required time period without loss.

07.06 Response to Audit Processing Failures. Information Owners and System Owners must ensure alerting procedures are in place in the event of an audit processing failure. Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

1) Information Systems must be configured to alert the System Custodian immediately and automatically in the event of an audit processing failure.

2) System Custodians must immediately take action to restore the regular functionality of any systems experiencing an audit processing failure.

3) Information Systems must be configured to automatically alert the System Custodian when the allocated storage capacity reaches a percentage of maximum storage capacity.
   a) This value must be pre-defined in such a way that ensures an audit processing failure does not occur due to a lack of storage space

4) The Information Owner and System Owner must select one of the following specific actions, subject to the approval of Cyber Security, for the information system to invoke in the event of audit failures, if an alternate audit capability does not exist:
   a) Shutdown the information system or halt processing
   b) Overwrite the oldest records; or
   c) Stop generating audit records.

07.07 Audit Review, Analysis, and Reporting. Information Owners and System Owners must ensure processes are in place to regularly review and analyze audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, and report any findings to the appropriate Department personnel.

1) Information Owners and System Owners, in collaboration with Cyber Security, must define events that may indicate inappropriate or unusual activity and who should receive event notifications.
   1) Examples may include:
      i) Password lockouts after repeated failed login attempts
      ii) Successful or failed login attempts outside business hours
      iii) Adding, deleting, or modifying user accounts or groups
      iv) Adding users to privileged groups
      v) Clearing event logs; or
      vi) Changing or disabling services or configurations.

2) Information systems, alone or in conjunction with another system, must be configured to perform automated review and analysis of audit records for the defined events and automatically alert appropriate personnel.
   1) If this is not possible, Information Owner and System Owner must determine the frequency of manual audit reviews and develop procedures for audit review, analysis, and reporting.

3) Individuals engaged in the review or analysis of audit records, or who receive alert notifications, must immediately notify Cyber Security of any findings that may indicate a security incident.

4) System Custodians must provide any audit logs as requested by Cyber Security or other appropriate Department personnel.

07.08 Audit Reduction and Report Generation. Information Owners and System Owners must ensure information systems provide an audit reduction and report generation capability. Audit reduction is a process that manipulates collected audit information (such as sorting and filtering) and organizes such information in a summary format that is more meaningful to analysts.

1) Information systems, alone or in conjunction with another system, must be configured to provide audit reduction and report generation capabilities for the list of auditable events defined in 03.01 “Audit Events” with the content defined in 03.02 “Content of Audit Records.”
    a) Information Owners and System Owners must be able to define additional auditable events to be included in audit reports.
    b) Audit reports must be available on-demand to support audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents.
    c) Audit reports must not alter the original content or time ordering of audit records.

07.09 Time Stamps. Information Owners and System Owners must ensure information systems use time stamps for audit records that are sufficient for effective event correlation.

1) Information systems must be configured to:
    a) Use internal system clocks to generate time stamps for audit records; and
    b) Record time stamps for audit records that can be mapped to UTC and are accurate to within one second. If these requirements are not possible, Cyber Security must review and grant an exemption to the requirements.

07.10 Protection of Audit Information. Information Owners and System Owners must ensure that audit records and audit tools are protected from modification, deletion, and unauthorized access.

1) Information systems must have the appropriate controls in place to protect against unauthorized changes to audit records and tools:
    a) Only users who have an explicit, documented need are authorized access to audit records or the management of audit functionality.
    b) Unless the user’s job function explicitly requires otherwise, all authorized users must be granted read-only access to all audit information.

07.11 Policy Implementation. Information Owners and System Owners must develop appropriate processes, and procedures to comply with the Audit and Accountability policy.

25.08.00 SYSTEM AND SERVICES ACQUISITION POLICY

08.01 Purpose. The purpose of this policy is to ensure system security is planned and managed throughout a system's life cycle, from initial planning to design, implementation, operation, and disposal. The System and Services Acquisition policy includes the following controls: allocation of resources, acquisition process, system documentation, system development life cycle, and other security measures to protect information, applications, and services.

Additional security requirements can be found in the Cyber Security Standards Library on SharePoint.

08.02 Scope. This policy applies to all Department information and information systems including those used, managed, or operated by a contractor, vendor, third-party user, another agency, or another organization on behalf of the Department.

The intended audience of this policy is:

- Information Owners and System Owners responsible for the implementation of new information systems,
- System Owners or System Custodians responsible for the operations of existing information systems,
- Cyber Security and IT personnel responsible for oversight and management of Department information systems.

08.03 Allocation of Resources. Information Owners and System Owners must coordinate with Cyber Security to determine the security requirements for an Information System or Information System Service and ensure adequate resources are available to meet those requirements. Resources include personnel and funding required for the initial acquisition as well as sustainment of the system or service.

08.04 System Development Life Cycle. Information Technology and Cyber Security must implement and manage a System Development Life Cycle (SDLC) for Department information systems that incorporate the following information security considerations:

1) Defines and documents information security roles and responsibilities throughout the SDLC,
2) Identifies individuals having information security roles and responsibilities, and
3) Integrates information security risk management processes into SDLC activities.

08.05 Acquisition Process. Information Owners and System Owners, in conjunction with Procurement and Contract Services, must include security functional requirements and/or specifications as a part of the acquisition process for information systems or information system services per applicable state or federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

08.06 System Documentation. System documentation helps personnel understand the implementation and continued operation of security controls. Any manual configurations or processes that are needed for the secure operation of the system should be documented.
Information Owners and System Owners must obtain or develop administrator and user documentation for information systems and services. System documentation must be protected from unauthorized exposure and made available to authorized personnel.

08.07 Security And Privacy Engineering Principles. Information Technology and Cyber Security must apply information system security and privacy engineering principles in the specification, design, development, implementation, and modification of information systems.

08.08 External Information System Services. External information system services are provided by an external provider or contractor, and the Department has no direct control over the implementation of the required security controls or the assessment of control effectiveness.
When using an external service provider, Information Owners and System Owners, in conjunction with Cyber Security, must:

1) Require that providers of external information system services comply with organizational information security requirements and applicable federal laws, policies, regulations, and standards
2) Define and document DPS oversight and user roles and responsibilities concerning external information system services; and

3) Employ processes to monitor security control compliance by external service providers on an ongoing basis.

08.09 Developer Configuration Management. Information Technology personnel responsible for the development of information systems, system components, or system services must perform configuration management during information system design, development, implementation, and operation.

08.10 Developer Testing and Evaluation. Information Technology personnel responsible for the development of information systems, system components, or system services must coordinate with Cyber Security to conduct a security assessment of the system before production implementation that includes:

1) Performing testing and evaluation of security functions,
2) Producing evidence of the results of the security testing/evaluation,
3) Implementing a verifiable flaw remediation process, and
4) Correcting flaws identified during security testing/evaluation.

08.11 Unsupported System Components. Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts. An example of unsupported components includes when vendors no longer provide critical software patches or product updates, which can result in an opportunity for adversaries to exploit weaknesses in the installed components. Information Owners and System Owners must:

1) Replace information system components when support for the components is no longer available from the developer, vendor, or manufacturer, or
2) If there is no replacement for the unsupported system, provide justification and document Cyber Security approval for the continued use of unsupported system components required to satisfy mission or business needs.

08.12 Policy Implementation. Responsible parties must develop appropriate processes and procedures to comply with the System and Services Acquisition policy.

25.09.00 SYSTEM AND COMMUNICATIONS PROTECTION POLICY

09.01 Purpose. The purpose of this policy is to implement Departmental security control requirements which:

1) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) externally and internally and
2) Promote effective information security within the Department.

Additional security requirements can be found in the Cyber Security Standards Library.

09.02 Scope. This policy applies to all Department information and information systems including those used, managed, or operated by a contractor, another agency, or another organization on behalf of the Department.

The intended audience of this policy is:

- Information Owners and System Owners responsible for the implementation of new information systems,
- System Owners or System Custodians responsible for the operations of existing information systems, and
- Cyber Security and IT personnel responsible for oversight and management of Department information systems.

09.03 Application Partitioning. Information Owners and System Owners must ensure that the system separates user functionality from information system management functionality physically and/or, logically.

Information system management functionality includes, but is not limited to, functions necessary to administer databases, network components, workstations, servers, or applications, and requires privileged user access.

09.04 Information in Shared Resources. Information Owners and System Owners must ensure that systems are configured to prevent unauthorized and unintended information transfer via shared system resources (e.g., registers, main memory, hard disks). This is also referred to as residual information protection or object reuse.

Any information produced by prior users must not be available to any current users after those resources have been released back to the information system.

09.05 Denial of Service Protection. Information Owners and System Owners must ensure that an information system is protected from the effects of a Denial of Service (DoS) attack. A DoS attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor.

09.06 Boundary Protection. Boundary Protection is the monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of device such as gateways, routers, firewalls, guards, and encrypted tunnels.
Information Owners and System Owners must ensure that the following measures are in place for boundary protection for networks and information systems:

1) Network devices to monitor and control communication at the external boundary of the network or information system, and at defined internal boundaries.
2) A subnetwork to separate all publicly accessible systems from internal systems.
3) All connections to or from external networks or information systems go through a managed interface, such as a firewall, gateway, router, or other device, before accessing the network or information system.

09.07 Transmission Confidentiality and Integrity. Information Owners and System Owners must ensure that systems protect the confidentiality and/or integrity of transmitted information as required based on the data classification and as specified by the Data Classification policy.

This applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines).

09.08 Network Disconnect. System Owners and Custodians responsible for managing network connection settings must ensure network connections, such as VPN connections, are terminated at the end of a session or after a defined period of inactivity.

Once a network connection has been terminated, there must be a re-authentication process to re-establish access.

09.09 Cryptographic Key Establishment and Management. A cryptographic key is essentially a piece of information, such as a password, that is used to control an encryption and decryption process. Anyone with access to a key will have access to any data encrypted with that key.

System Owners and Custodians responsible for cryptographic key management processes must manage cryptographic keys in a secure manner for the entire key lifecycle in accordance with applicable state, local, and federal regulatory standards for key generation, distribution, storage, access, and destruction.

09.10 Cryptographic Protection. Cryptography can be used to support a variety of security solutions including, for example, the protection of confidential information (confidentiality) or the provisioning of digital signatures (integrity).

System Owners and Custodians must implement the required cryptographic uses (confidentiality or integrity) and the type of cryptography required for each use in accordance with the data classification and applicable state and federal laws, executive orders, directives, policies, cyber standards, and guidance.

09.11 Collaborative Computing Devices. Collaborative computing devices include, for example, networked white boards, cameras, and microphones.

System Owners and Custodians responsible for the oversight of collaborative computing devices must ensure the following:

a. Devices must only allow remote activation through a method authorized by the IT Division.
b. Devices must provide a light or signal for users physically present to show that the device is activated.

09.12 Public Key Infrastructure (PKI) Certificates. System Owners and Custodians responsible for cryptographic key management processes must ensure that all public key certificates are obtained from trusted vendors or providers.

09.13 Mobile Code. Cyber Security and IT must develop standards for mobile code based on the potential for the code to cause damage to the systems if used maliciously. Mobile code standards must:

1) Define acceptable and unacceptable mobile code and mobile code technologies (e.g., Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript);
2) Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies on servers, workstations, and mobile devices; and

3) Authorize, monitor, and control the use of mobile code within Department information systems.

09.14 Voice over Internet Protocol. System Owners and Custodians responsible for Voice over Internet Protocol (VoIP) technologies must:

a. Establish usage restrictions and implementation guidance for VoIP based on the potential to cause damage to information systems if used maliciously, and
b. Authorize, monitor, and control the use of VoIP within the Department's networks.

09.15 Secure Name / Address Resolution Service.
System Owners and Custodians responsible for Domain Name System (DNS) technologies must implement secure name/address resolution services. Information systems that provide name/address resolution services must be fault tolerant to enhance redundancy and eliminate single points of failure.

09.16 Session Authenticity. Information Owners and System Owners must ensure information systems protect the authenticity of communications sessions. This establishes confidence in the ongoing identities of other parties and in the validity of information transmitted at both ends of the session.

09.17 Process Isolation. Information Owners and System Owners must ensure information systems maintain a separate execution domain for each executing process. This can be done, for example, by assigning each process a separate address space within the system's core processing capability.

Process isolation ensures that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process.

09.18 Policy Implementation. Information Owners and System Owners must develop appropriate processes, and procedures to comply with the System and Communications Protection policy.

25.10.00 SYSTEM AND INFORMATION INTEGRITY POLICY

10.01 Purpose. The purpose of this policy is to define the requirements for system and information integrity security controls. Additional security requirements can be found in the Cyber Security Standards Library. These security controls focus on timely identification and remediation of system vulnerabilities (e.g., software flaws or coding errors) to ensure the integrity of systems and the information they process and store. Security controls include system monitoring, reporting, updating, patching, scanning, and remediation to correct information and information system flaws, provide protection from malicious code, and monitor information system security alerts and advisories.

10.02 Scope. This policy applies to all Department information and information systems, to include information and information systems used, managed, or operated by a contractor, another agency, or another organization on behalf of the Department.

The intended audience of this policy is:

- Information Owners and System Owners responsible for the implementation of new information systems,
- System Owners or System Custodians responsible for the operations of existing information systems, and

- Cyber Security and IT personnel responsible for oversight and management of Department information systems.

10.03 Flaw Remediation. Flaw remediation is the process of identifying and correcting software flaws that may pose a security risk to the Department. To conduct flaw remediation, in accordance with the Vulnerability Management Program standard:

Cyber Security must:

1) Identify information system flaws through various means for all systems in development and production.
2) Report the discovery of a system flaw to System Owners and/or Custodians.
3) Indicate risk level in vulnerability scan reports. If not indicated, a high-risk level must be assumed.
4) Track and verify flaw remediation actions.

System Owners and/or Custodians must:

1) Identify information system flaws through various means for all systems in development and production.
2) Report the discovery of a system flaw found in a production system, or a flaw that cannot be corrected prior to a system moving into production, to Cyber Security.
3) Correct information system flaws.
4) Install security-relevant software updates (e.g., patches, services packs, and hot fixes).
5) Complete testing of software updates related to flaw remediation for effectiveness and potential side effects before installation on production systems, when possible.

10.04 Malicious Code Protection. Malicious code, or malware, is software that is used by cyber-attackers to disrupt, damage, or gain unauthorized access to a computer system. Information systems can be protected against malicious code with anti-virus software and other reputation-based technologies.

Information Owners and System Owners must ensure that information systems employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code. Information system entry and exit points include, for example, firewalls, e-mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Cyber Security and the Information Technology Division must oversee and manage malicious code protection technologies for Department-managed systems.

10.05 Information System Monitoring. Information system monitoring capabilities are achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Information systems must be monitored to ensure attacks are detected and prevented or mitigated to reduce the impact on Department systems.

Cyber Security and the Information Technology Division must manage information system monitoring technologies for Department-owned networks. Cyber Security is responsible for monitoring and oversight of these network monitoring technologies to ensure attacks, indicators of potential attacks, and unauthorized connections are detected.

Information Owners utilizing a network owned and managed by a contractor or external entity must ensure monitoring technologies and procedures are in place for systems storing, processing, or transmitting Department data.

10.06 Security Alerts, Advisories, and Directives. Cyber Security must receive information system security alerts, advisories, and directives from designated external organizations on an ongoing basis, and generate internal communication and dissemination as deemed necessary.

Information Owners and Custodians, in coordination with Cyber Security, must implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance as required.

10.07 Software, Firmware, and Information Integrity. Integrity is the process of guarding against unauthorized information modification or destruction. Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering or malware).

System Owners and Custodians must ensure the information system employs integrity verification tools to detect unauthorized changes to software, firmware, and information.

10.08 Spam Protection. Spam email is commonly used to conduct email fraud or phishing designed to trick users. Spam email may also deliver malware through file attachments or scripts or contain links to websites hosting malware. Cyber Security must oversee and manage spam protection mechanisms to detect and take action on unsolicited email messages sent to a user's DPS email address.

Users should:

1) Avoid opening spam emails and never respond to them or click on links in the messages, and
2) Send all suspected spam emails to Cyber Security for review, as an attachment, at: spam@dps.texas.gov.

10.09 Information Input Validation. Input validation is the process of testing information input supplied by a user or application for compliance against a defined standard. Examples include defining a character length for a text field or a minimum and maximum value range for a numerical field. An input validation attack occurs when an attacker deliberately enters malicious input with the intention of confusing an application and causing it to carry out some unplanned action or exploit a vulnerability.

Information Owners and System Owners must ensure that information systems are configured to check the validity of information inputs, when possible, to help ensure accurate and correct inputs and to prevent attacks.

10.10 Error Handling. The structure and content of information system error messages should be carefully considered to ensure the error messages cannot be used maliciously by cyber-attackers.

Information Owners and System Owners must ensure that systems generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.

10.11 Information Handling and Retention. Both information within the information system and output from the information system must be handled and retained in accordance with applicable laws, directives, policies, regulations, standards, and operational requirements.

Information handling guidelines can be found in General Manual Chapter 26 Annex – Data Classification Standards.

Information retention requirements can be found in General Manual Chapter 21: Records and Information Policy.

10.12 Memory Protection. System memory is the place where a computer holds current programs and data that are in use. The main purpose of memory protection is to prevent unauthorized program code from accessing memory and impacting the confidentiality, integrity, or availability of the system and/or data.

Information Owners and System Owners must ensure safeguards are implemented to protect information system memory from unauthorized code execution.

10.13 Policy Implementation. Information Owners and System Owners must develop appropriate processes and procedures to comply with the System and Information Integrity policy.

25.11.00 INCIDENT RESPONSE POLICY

11.01 Purpose. The purpose of the Incident Response Policy is to ensure that security incidents are reported to Cyber Security and that the Department maintains effective security incident response capabilities. Incident response procedures must be followed for security incidents that threaten the confidentiality, integrity, or availability of the Department's assets, information systems, and the networks that deliver the information. Incident response procedures must include reporting requirements from applicable state and federal laws, executive orders, directives, regulations, standards, and guidance. A process of continual improvement should be applied to the response, monitoring, evaluating, and overall management of information security incidents.

For further guidance on this policy, see the Incident Response Standard.

11.02 Scope. This policy applies to all employees and non-Departmental personnel (contractors, vendors, and third-party users) accessing Department information and/or information systems. This includes systems used, managed, or operated by a contractor, another agency, or another organization on behalf of the Department.

11.03 Incident Response Training. Cyber Security must provide security incident response training to personnel with specific assigned security roles and responsibilities. Training must occur before being assigned an incident response role or responsibility and then annually thereafter, or sooner if required by information system changes.

Cyber Security must ensure that general incident response roles and responsibilities are included as part of required security awareness training for all personnel.

11.04 Incident Response Testing. Cyber Security must coordinate testing of security incident response capabilities, determine the incident response effectiveness, and document the results. Testing must occur annually, or sooner if required by information system changes. Testing requirements will be based on the incident response plan tasks and responsibilities once they are developed for each information system or network.

11.05 Incident Handling. Cyber Security must implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, recovery, and lessons learned.

Priority: Security incident response activities can take priority over normal duties and may require that standard processes be circumvented in the interest of time. Cyber Security Analysts under the direction of the CSIRT Team Leader or Cyber Management (e.g., Cyber Security Operations Manager, ISSM, and CISO) are authorized to perform the actions identified in this paragraph.

Security Incident handling activities must be coordinated with contingency planning activities. Lessons learned from ongoing security incident handling activities must be incorporated into incident response procedures, training, and testing exercises and implemented accordingly.

11.06 Incident Monitoring and Reporting. Cyber Security must track and document information system security incidents on an on-going basis and share this information with the appropriate stakeholders identified in the Incident Response Plan.

All personnel are required to report suspected security incidents to Cyber Security immediately. Personnel can report incidents by emailing GRP_Cyber_Security@dps.texas.gov during normal business hours or by calling the OIC afterhours at 512-424-2139.

Cyber Security will follow up with the reporting individual in a timely manner based on the scope of the issue and information received.

Cyber Security is responsible for coordinating communications with internal stakeholders, outside organizations, and law enforcement, as well as reporting incidents to local, state, or federal law officials as required by applicable statutes and regulations.

11.07 Incident Response Assistance. Cyber Security is responsible for providing security incident response support, advice, and assistance to information system users for handling and reporting security incidents.

Assistance may include providing reporting instructions, opening, and tracking incident response tickets, providing forensic services, and advising users on remediation actions.

11.08 Incident Response Plan. Cyber Security must develop an Incident Response Plan that:

a) Serves as a roadmap to handle security incidents
b) Describes the incident response process
c) Documents the incident response team's roles, resources, and responsibilities
d) Provides a high-level approach for how the incident response process fits into the overall organization

e) Meets the unique requirements of the Department related to mission, size, structure, and functions
f) Defines reportable incidents
g) Provides metrics for measuring the incident response capability of the Department
h) Defines the resources and management support needed to effectively maintain the incident response capability; and
i) Is reviewed and approved by the executive leadership of all stakeholders.

The Incident Response Plan must be distributed to incident response personnel with defined roles and responsibilities.

Cyber Security must review the Incident Response Plan annually, or sooner if required by information system changes.

Cyber Security, in conjunction with Information Technology, must update the Incident Response Plan to address system or organizational changes or problems encountered during plan implementation, execution, or testing. Updates must be communicated to incident response personnel with defined roles and responsibilities.

The Incident Response Plan must be protected from unauthorized disclosure and modification.

11.09 Policy Implementation. Information Owners and System Owners must develop appropriate processes and procedures to comply with the Incident Response policy.

25.12.00 ASSESSMENT, AUTHORIZATION, AND MONITORING POLICY

12.01 Purpose. This policy is intended to minimize risk to the agency by ensuring all new information systems have explicit Authority to Operate (ATO) at an acceptable risk level to the Department as determined and approved by the Authorizing Official. Additionally, existing networks and information systems will be continuously assessed, monitored, and evaluated for any new or emerging risks. For those networks or information systems in which a risk is identified, a Plan of Action and Milestones (POAM) must be created to correct any identified weakness or deficiency. Should this weakness or deficiency result in a Significant Change to the overall system risk level, then that system must be re-authorized to operate by the Authorizing Official.

12.02 Roles and Responsibilities. This policy pertains to all the Department's information and information systems, to include information and information systems used, managed, or operated by a contractor or subcontractor, another governmental entity, or any entity or organization on behalf of the agency.

The intended audience for this policy is:

a) Information Owners and System Owners responsible for the implementation of new information systems
b) System Owners responsible for operating existing information systems; and
c) Cyber Security and IT personnel responsible for oversight and management of Department information systems.

12.03 Security Control Assessments. Security Control Assessments are a critical component of the system assessment and authorization process. These assessments aid the authorization process by testing and evaluating the overall effectiveness of the control implementation for an information system.

Security Control Assessments also identify weaknesses and deficiencies in system design and development, ensure the Department is meeting information security and privacy requirements, and provide essential risk information required to make informed decisions of acceptable risk as part of the system authorization process.

Cyber Security conducts security control assessments as determined by the required controls outlined in the Texas Cybersecurity Framework Agency Security Plan (ASP). Security control implementation status is documented in the System Security Documentation (SSD) for an information system.

Information Owners and System Owners must notify Cyber Security, initiate a Security Control Assessment, and provide any requested security documentation needed to complete the Security Control Assessment:

d) For any new information system
e) Every three years after the initial authorization for systems with no known security vulnerabilities
f) Every year after the initial authorization for systems with known security vulnerabilities that have a documented risk acceptance and POAM
g) When a Significant Change is made to the system; or
h) After the discovery of a serious security violation which raises questions about the validity of an earlier security authorization.

Cyber Security will:

a) Select the appropriate assessor or assessment team for the type of assessment to be conducted. Assessors should possess the technical skills and knowledge required to perform the type of assessment required
b) Develop a Security Control Assessment Plan which outlines:
    (1) Security controls under assessment
    (2) Procedures to determine effectiveness of controls and
    (3) The assessment environment, team, and roles and responsibilities
c) Ensure that the Security Control Assessment Plan is reviewed and approved by the Cyber Security Risk Manager prior to conducting the assessment
d) Conduct an assessment of the information system security to determine if the controls are operating as intended and producing the desired outcome
e) Produce a security control assessment report that documents the results of the assessment; and
f) Provide the results of the security control assessment report to the Authorizing Official, CISO, Information Owner, and System Owner.

Assessment reports may use results from the following to satisfy the security control assessment requirement:

a) Initial or ongoing system authorization
b) Continuous monitoring
c) System development life cycle activities; or
d) Previous control assessments if the results are still valid and can be updated with additional information as needed.

12.04 Risk Assessment. Risk Assessments allow the Department to review an information system's overall risk to the agency by identifying threats to and vulnerabilities of the system and determining the likelihood and magnitude of harm that would arise from any unauthorized access, use, disclosure, disruption, modification, or destruction of the system. The risk assessment also factors in potential risk to the Department from any information the system may process, store, or transmit.
As part of the Security Control Assessment, Information Owners and System Owners must:

a) Conduct a Risk Assessment of the information system which includes:
   (1) Identifying any system threats and vulnerabilities
   (2) Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, and the information it processes, stores, or transmits, and any related information; and
   (3) Determining the likelihood and impact on individuals arising from the processing of Personally Identifiable Information (PII), sensitive personal information, or biometric data
b) Review and update the risk assessment:
   (1) Every three years after the initial authorization for systems with no known security vulnerabilities
   (2) At least every year after the initial authorization for systems with known security vulnerabilities that have a documented risk acceptance and POAM
   (3) When Significant Change is made to the system or any changes that may impact the security or privacy of the system; or
   (4) After the discovery of a serious security violation which raises questions about the overall system risk.

Cyber Security will:

a) Integrate any organizational risk management results and decisions with the results from the system risk assessment.
b) Document the risk assessment results in the System Security Documentation (SSD) and the System Authorization documentation.
c) Provide the risk assessment results to the Authorizing Official, CISO, Information Owner, and System Owner.

12.05 Plan of Action and Milestones. The System Owner must develop a plan of action and milestones (POAM) for tracking remediation activities when a weakness or deficiency is discovered in an information system. The POAM must include activities to help reduce or eliminate known system vulnerabilities and be updated regularly (and at least annually) based on any findings from control assessments, independent audits and reviews, or continuous monitoring activities.
Cyber Security will include a copy of the POAM in the information system's authorization package for approval by the Authorizing Official.

12.06 Information Exchange. Information exchange between two or more systems that may have differing security controls, privacy controls, or data classifications can bring additional risk to the Department. Information exchange can occur between systems that are internal or external to the Department and can vary in the type of information exchange connections.
Information exchange risk and the controls needed to mitigate that risk are determined by Information Owners and Cyber Security and must be approved by the DPS CISO and the DPS Authorizing Official. The following must take place when initiating information exchange between two or more systems:

a) If the information exchange occurs solely within Department resources (not an external party such as a governmental entity or a contractor), the Information Owners involved in the information exchange need to agree upon and document the security controls, security and privacy requirements, interface characteristics, data classifications, and the impact level of the information being communicated in the security documentation for each system. Information Owners must ensure that the security documentation is up-to-date and remains relevant. As part of their review, Information Owners should determine if there is a continued need for the information exchange. Information Owners should terminate information exchange connections or activities when no longer needed or when an identified risk cannot be mitigated or accepted.

b) If the information exchange occurs between a Department resource and an external party (includes other governmental entities or contractors), the Information Owners need to document the information exchange through an agreement approved by Cyber Security and OGC Privacy Counsel (such as the Cyber Exhibit, the Interconnection Security Agreement (ISA), Data Sharing Agreement (DSA), or other approved agreement). The Information Owners must document the security controls, security and privacy requirements, interface characteristics, data classifications, and the impact level of the information being communicated for each agreement. Information Owners must ensure associated agreements are up-to-date and remain relevant and that external parties are complying with all requirements. As part of their review, Information Owners should determine if there is a continued need for the information exchange. Information Owners should terminate the agreement with the external party as well as the information exchange connections or activities when no longer needed or when an identified risk cannot be mitigated or accepted.

12.07 Internal Systems Connections. Internal system connections are connections between organizational systems and separate constituent system components (that is connections between components that are part of the same system) including components used for system development. System Owners and System Custodians must document the interface characteristics, security and privacy requirements, data classifications, and the impact level of the information communicated for each internal connection. System Owners must provide this documentation in the information system authorization package for approval by the Authorizing Official.

Internal system connections must be reviewed periodically as required for ongoing system authorization and terminated when no longer needed or when an identified risk cannot be mitigated or accepted.

12.08 Authorization. Prior to the implementation of a new information system or the implementation of a Significant Change to an existing system, that system must first be granted authority to operate (ATO). Authority to operate is an explicit statement and acceptance of risk to the Department's operations, assets, and individuals based on how well an information system implements the agreed upon security controls.

This acceptance of risk and authorization is granted by the Authorizing Official for the Department.

Authorization is required and must be documented:

a) For any new information system.
   (1) The Authorization process should be initiated during the acquisition/development phase of the system development life cycle and at least 90 days prior to implementation to allow time for security control assessment activities.
   (2) The information system must be given final authorization by the Authorizing Official prior to being implemented for use by DPS.
b) For any existing information system that is undergoing a Significant Change.
   (1) Prior to implementing a Significant Change, the information system must be given final authorization by the Authorizing Official.

System authorization documentation must be reviewed, updated, and reauthorized:

a) Every three years for systems with no known security vulnerabilities,
b) At least every year for systems with known security vulnerabilities that result in elevated risk,
c) When a Significant Change occurs.

12.09 Continuous Monitoring. Maintaining ongoing awareness of an information system's security, control effectiveness, and overall risk level requires that information systems are assessed and monitored on a regular basis using well defined methodologies. This continuous monitoring also supports the Department in making timely risk management decisions including ongoing authorization decisions.

Common activities can cause changes to systems or the environments of operation and can have a significant impact on the security and privacy posture of systems. Examples include installing or disposing of hardware, making changes to configurations, and installing patches outside of the established configuration change control process. Monitoring should be in place for unauthorized changes due to attacks or errors, as well as authorized changes that impact the security or privacy posture of systems.

Cyber Security and the Information Technology Division will develop, implement, and maintain a Department-wide continuous monitoring strategy for information systems. System Owners and System Custodians must adhere to the requirements identified in the continuous monitoring strategy. This strategy will include the following:

a) Establishing system-level metrics that should be monitored through configuration management, change management, or other activities
b) Establishing how often information systems should be monitored and assessed for security control effectiveness
c) Ongoing assessments of security controls
d) Ongoing monitoring of system-level metrics
e) Analysis of information generated by control assessments and monitoring
f) Risk response actions to address the control assessment and monitoring analysis; and
g) Reporting of the security and privacy status of the system to meet ongoing system authorization requirements.

12.10 Penetration Testing. To further identify vulnerabilities that could be exploited to cause harm to the system or the Department, Cyber Security will conduct penetration testing on information systems or system components on an ongoing basis. This type of testing goes beyond automated vulnerability scanning and attempts to duplicate the actions of adversaries to provide a more in-depth analysis of security- and privacy-related weaknesses or deficiencies.
To implement a penetration testing program for Department information systems, Cyber Security will:

a) Identify information systems or system components on which the Department will conduct penetration testing.
b) Establish rules of engagement, including roles and responsibilities for conducting penetration tests and addressing findings.
c) Conduct or coordinate penetration testing for these systems or system components on a periodic basis as determined by system risk level.

25.15.00 PROHIBITED TECHNOLOGIES

15.01 Purpose. All state agencies are required to ban the application TikTok and other prohibited technologies from all state-owned and state-issued devices and networks to protect these state-owned and state-issued assets. Throughout this policy, "Prohibited Technologies" will refer to TikTok and any additional prohibited hardware or software.

15.02 Scope. This policy applies to all full-time and part-time Department employees as well as contractors, paid or unpaid interns, and users of state networks. All are responsible for complying with this policy.

15.03 State Owned Devices. The use or download of prohibited technologies, applications, or websites is prohibited on all state-owned and state-issued devices, including cell phones, tablets, desktop and laptop computers, and other internet capable devices.
The Department will identify, track, and control state-owned devices to prohibit the installation of or access to all prohibited applications. This includes the various prohibited applications for mobile, desktop, or other internet capable devices.
The Department will implement the security controls listed below:

a) Restrict access to "app stores" or non-authorized software repositories to prevent the install of unauthorized applications.
b) Maintain the ability to remotely wipe non-compliant or compromised mobile devices.
c) Maintain the ability to block mobile devices with unauthorized software from accessing the Department's resources. The Department will notify the device owners that their device is blocked and inform them how to remediate the problem.
d) Deploy secure baseline configurations for mobile devices, as determined by DPS Cyber Security.

15.04 Personal Devices Used for State Business. Employees and contractors may not install or operate prohibited applications or technologies on any personal device that is used to conduct state business. State business includes accessing any state-owned data, applications, email accounts, non-public facing communications, VoIP, SMS, video conferencing, CAPPS, Texas.gov, and any other state technologies, databases, or applications.

15.05 Identification of Sensitive Locations. Sensitive locations must be identified, catalogued, and labeled. A sensitive location is any location, physical or logical (such as video conferencing or electronic meeting rooms) that is used to discuss confidential, sensitive, or regulated information, including information technology configurations, criminal justice information, financial data, personally identifiable data, sensitive personal information, or any data protected by federal or state law. Unauthorized devices such as personal cell phones, tablets, or laptops may not enter sensitive locations, which includes any electronic meeting room labeled as a sensitive location.
Visitors granted access to secure locations are subject to the same limitations as contractors and employees on unauthorized personal devices when entering secure locations. Employees must ensure that any visitor complies with this policy.

15.06 Network Restrictions. DIR has blocked access to prohibited technologies on the state network. To ensure multiple layers of protection, the Department implemented additional network-based restrictions to include:

a) Configuring agency firewalls to block access to statewide prohibited services on all agency technology infrastructures, including local networks, WAN, and VPN connections.
b) Prohibiting personal devices with prohibited technologies installed from connecting to agency or state technology networks, infrastructure, or state data.
c) If the Director approves an exception, providing a separate network for access to prohibited technologies for law enforcement purposes.

15.07 Ongoing and Emerging Technology Threats. To provide protection against ongoing and emerging technological threats to the state's sensitive information and critical infrastructure, DPS and DIR will regularly monitor and evaluate additional technologies posing concerns.
The website that lists all prohibited technologies, including apps, software, hardware, or technology providers is published at https://dir.texas.gov/information-security/prohibited-technologies. New technologies will be added to the list after consultation between DIR and DPS. The Department must implement the removal and prohibition of any listed technology.

15.08 Limited Exceptions. Exceptions to the ban on prohibited technologies may only be approved by the Director. This authority may not be delegated. All Director-approved exceptions to the TikTok prohibition or other statewide prohibited technologies must be reported to DIR.
Exceptions to the policy will only be considered when the use of prohibited technologies is required for a specific business need, such as enabling law-enforcement investigations. Those granted an exception to use a prohibited technology must only use that technology on devices that are not used for any other state business and that do not connect to state networks. Cameras and microphones must be disabled on devices for exception-based use, unless otherwise permitted in the approved exception.

INFORMATION RESOURCE POLICY
01.26.00.00

26.05.00 Purpose

The Information Technology Division (ITD) of the Texas Department of Public Safety (Department) manages and protects the Department's information resources in accordance with the policies of this Chapter 26, "Information Resource Policy," of the Department's General Manual.

These policies are based on requirements contained in Texas Administrative Code Title 1, Part 10, Chapter 202 and related reference material. These policies apply equally to all personnel including, but not limited to, the Department's employees, agents, consultants, and all other authorized users granted access to the Department's information resources. Furthermore, these policies apply to all information generated by the Department's information resource functions, through the time of its transfer of ownership to any entity outside the Department or its proper disposal/destruction.

Violation of these policies may result in disciplinary action contained in Chapter 7A of the General Manual which may include termination of employees or a termination of employment relations in the case of contractors or consultants. Additionally, individuals may be subject to loss of access to the Department's information resources, as well as civil and criminal prosecution.

"Information" is defined as any and all data, regardless of form, that is created, contained in, or processed by the Department, or the Department's communications networks or the Department's storage devices.

"Information resources" includes any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing websites, or receiving, storing, managing, or transmitting electronic data. These devices include, but are not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDAs), smart phones, pagers, distributed processing systems, network-attached and computer-controlled laboratory equipment (such as embedded technology), telecommunication resources, network environments, telephones, fax machines, and printers. Additionally, information resources include the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

The discipline of information resources governance deals primarily with the connection between the business focus and information resources management of an organization. This discipline highlights the importance of information resources related matters in organizations and states that strategic information resources management decisions should be made by the executive management of the organization, rather than by the Chief Information Officer or other information resources managers.

26.10.00 DEFINITIONS, KEY ROLES, AND RESPONSIBILITIES

10.01 Abuse of privilege. When a user willfully performs an action prohibited by Department policy or law, even if technical controls are insufficient to prevent the user from performing the action.

10.02 Backup. A copy of files and applications made to avoid loss of data and facilitate recovery in the event of a system crash.

10.08 Data Owner. A delegated person or business unit responsible for setting the overall strategic direction of a specific data asset. They ensure the collection is developed, maintained, and utilized in accordance with Department strategic goals.

10.10 Electronic mail system. Any computer software application that allows electronic mail to be communicated from one computing system to another.

10.11 Email. Abbreviation for electronic mail, which consists of messages sent over any electronic media by a communications application. Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

10.12 Information Resources Manager (IRM). The individual within a state agency who is responsible to the State of Texas for management of that agency's information resources. The designation of an agency IRM is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state agency's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement security policies, procedures, practice standards, and guidelines to protect the information resources of the agency. If an agency does not designate an IRM, the title defaults to the agency's Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

The Department's Executive Director has designated the ITD Division Chief as the IRM for the Department.

10.13 Internet. A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and colleges. The Internet is the present "information superhighway."

10.14 Intranet. A private network for communications and sharing of information like the Internet but is accessible only to authorized users within an organization. An organization's Intranet is usually protected from external access by a firewall.

10.15 Local Area Network (LAN). A data communications network spanning a limited geographical area, a few miles at most. It provides communication between computers and peripherals at relatively high data rates and relatively low error rates.

10.16 Metadata. Data that describes or provides information about other Data.

10.19 Offsite backup storage. Based on data criticality, offsite backup storage should be in a geographically different location from the Department's campus so that a single disaster could not destroy both the production data and the backup data. For less than critical data, removing the backup media from the building and storing it in another secured location on the Department's campus may be appropriate.

10.20 Owner. The manager or agent responsible for the function supported by the information resources. The owner administers the program that uses the resources, making the owner responsible for both business results of that system and for establishing controls that provide for resource security. Where appropriate, ownership may be shared by managers of different Department Divisions.

10.24 Project Management (PM). The discipline of organizing and managing resources (such as people) in such a way that the project is completed within defined scope, quality, time, and cost constraints. A project is a temporary and one-time endeavor undertaken to create a unique product or service, which brings about beneficial change or added value.

10.25 Production system. A computer application that has been implemented for business use, as contrasted to a test system, which is a computer application using test data that has not been implemented. When addressing the security of a production system, the hardware, software, physical, procedural, and organization components must be considered.

10.26 Program Manager. Assigned information resources ownership; responsible for the information used in carrying out program(s) under their direction and provides appropriate direction to implement defined security controls and procedures. The Division Chief is generally designated as the Program Manager.

10.28 Removable Media Devices. Computing devices capable of storing Data and designed to be removed from a system while the system is operating. *Removable Media Devices include but are not limited to floppy disks, flash memory drives, memory cards, cameras, MP3 players, portable hard drives, and optical disks.*

10.29 Security Administrator. A person charged with monitoring and implementing security controls and procedures for a system. Whereas each agency will have one Information Security Officer, ITD technical management may designate a number of Security Administrators.

10.31 Server. A computer program that provides services to other computer programs in the same, or another, computer. A computer running a server program is frequently referred to as a server, though it may also be running other client (and server) programs.

10.32 Service Level Agreement (SLA). A Service Level Agreement is a formal negotiated agreement between the application or system owners and ITD. It records the common understanding about services, priorities, and responsibilities with the main purpose to agree on the level of service committed to a system or application within the Department. For example, it may specify the levels of availability, serviceability, performance, operation, or other attributes of the service ITD provides to the application or system owners.

10.33 System Administrator. The person responsible for the effective operation and maintenance of information resources, including implementation of standard procedures and controls to enforce the Department's information resource policy.

10.34 System Development Life Cycle (SDLC). A set of procedures to guide the development of production application software and data items. A typical SDLC includes design, development, quality assurance and acceptance testing, implementation, and maintenance.

10.35 Technical Manager. An assigned ITD employee who is both a custodian of information resources and provider of technical facilities and support services to owners and users of information; assists the Program Manager in the selection of cost effective controls to be used to protect information resources; is responsible for executing the monitoring techniques and procedures for detecting, reporting, and investigating breaches in the security of information resources.

10.36 Trojan Horse. Destructive programs, usually viruses or worms that are hidden in an attractive or innocent-looking piece of software, such as a game or graphics program. Users may receive a Trojan horse by email or on a diskette, often from another unknowing user. Also, a user may be urged to download a file with a Trojan horse from a website or bulletin board.

10.37 User. The user is any person who has been authorized to read, enter, or update information by the owner of the information. The user has the responsibility to (1) use the information resource only for the purpose specified by the owner, (2) comply with controls established by the owner, and (3) prevent disclosure of confidential or sensitive information. The user is the single most effective control for providing adequate security.

10.38 Vendor. A company or individual that contracts with the Department to provide information resources (goods or services).

10.39 Virus. A program that attaches itself to an executable file or vulnerable application and causes problems that range from annoying to extremely destructive. It could also be a surreptitious program to quietly gather and forward sensitive or financial information, passwords, or compromise other information critical to the operational integrity of the system without being detected. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allow users to generate macros.

10.40 World Wide Web (WWW). A system of Internet hosts that support documents formatted in HTML (HyperText Markup Language). These documents contain links to other documents (hyperlinks) and to audio, video, and graphic images. Users can access the Web with special applications called browsers, such as Netscape, Navigator, and Microsoft Internet Explorer.

10.41 Worm. A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. Some worms are security threats, disrupting networks by overloading them. A worm is similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors.

26.15.00 ACCEPTABLE USE

15.01 Purpose. Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Thus this "Acceptable Use Policy" is established to achieve the following:

1. To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.

2. To establish prudent and acceptable practices regarding the use of information resources.

3. To educate information resource users of their responsibilities regarding the use of information resources.

15.02 Acceptable Use Policy. Following constitutes the "Acceptable Use Policy" for the Department's information resources. For more details see 26.110.02 "Email Acceptable Use Policy" and 26.115.03 "Internet and Intranet Acceptable Use Policy."

1. Electronic files created, sent, received, or stored on information resources that are owned, leased, administered by the Department, or otherwise under the custody and control of the Department are the property of the Department.

2. The Department's electronic files (see #1) are not private. The Department's electronic files may be accessed by authorized Department personnel at any time without knowledge of the file's user or owner, regardless of whether the file is encrypted, password protected, or marked as confidential.

Use of information resources constitutes consent by the user to access by authorized Department representatives.

Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards.

3. Computer systems and electronic files are subject to inspection at any time.

4. Storage devices that are connected to Department's information resources are subject to inspection for compliance with Department policy at any time. The connection of a portable storage or computing device to the Department's information resources constitutes consent by the user to the inspection of the device, even if that device is not owned by the Department.

5. The Department's information resources are Department property and are made available to employees and select third parties for authorized State of Texas business use.

6. All persons granted access to the Department's information resources will complete an orientation and will adhere to the following requirements:

a) Users must report any weaknesses in the Department's computer security, any incidents of possible misuse or violation policy to the proper authorities by contacting the appropriate management.

b) Users must not attempt to access any data or programs contained on the Department's systems for which they do not have authorization or explicit consent of the Department.

c) Users must not divulge dial-up or dial-back modem phone numbers to anyone.

d) Users must not share their Department account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (for example, Smartcard), Internet Protocol (IP) address, computer name or similar information or devices used for identification and authorization purposes. Users must not make unauthorized copies of copyrighted software.

e) Users must not use shareware or freeware software without the ITD approval unless it is on the Department's standard software list.

f) Users must not purposely engage in activity that may harass, threaten or abuse others; degrade the performance of information resources; deprive an authorized Department user access to a resource; obtain extra resources beyond those allocated; or circumvent computer security measures.

g) Users must not download, install, or run programs or utilities that reveal or exploit weaknesses in the security of a system. For example, Department users must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on information resources (other than in the course of an official investigation where this aspect of the investigation has the explicit approval of the Department or in the course of network management by an authorized ITD employee).

h) Department information resources must not be used for personal benefit.

i) Users must not intentionally access, create, store or transmit material that the Department may deem to be offensive, indecent or obscene (other than in the course of an official investigation where this aspect of the investigation has the explicit approval of the Department).

j) Access to the Internet from a Department-owned, home-based, computer must adhere to all the same policies that apply to use from within Department facilities. Employees must not allow family members or other non-employees to access Department-owned computer systems.

k) Users must not otherwise engage in acts against the objectives, mission, or programs of the Department as specified in its governing documents or in its rules, regulations and procedures.

l) Users are responsible for changing their password in compliance with the Department's password policy.

7. As a convenience to the Department's employees, incidental use of information resources may be permitted by a group's management as a privilege (not a right). The following restrictions apply:

a) Incidental personal use of electronic mail, Internet access, fax machines, printers, copiers, and so on, is restricted to the Department's approved users; it does not extend to family members or other acquaintances.

b) Incidental use must not result in direct costs to the Department.

c) Incidental use must not interfere with the normal performance of an employee's work duties, as defined by the employee's supervisor. Incidental use should not exceed a time period comparable to reasonable daily lunch and break times.

d) Incidental personal use of Department resources is permitted but must not be excessive or inappropriate as determined solely by the Department. Inappropriate use includes hacking, pirating software, disrupting others' work activities, using Department resources for non-Department commercial activities, soliciting or distributing literature for outside entities, disclosing confidential information of the Department or third parties, sending inappropriate email, accessing inappropriate websites (such as those advocating hate or violence, posting or sharing any racist, sexist, threatening, illegal or otherwise objectionable material such as those containing sexually explicit material, gambling, or promoting illegal activities), or using Department resources in a way that violates Department policies contained in the General Manual or state law.

e) No files or documents may be sent or received that may cause legal action against, or embarrassment to, the Department.

f) Storage of personal email messages, voice messages, files and documents within the Department's information resources must be kept to a minimum.

g) All messages, files, and documents – including personal messages, files and documents – located on Department information resources are owned by the Department, may be subject to open records requests, and may be accessed in accordance with this policy.

26.20.00 ACCOUNT MANAGEMENT

20.01 Purpose. The purpose of this policy is to: (1) protect access to DPS's information technology (IT) systems and applications; (2) prevent unauthorized access to IT resources; (3) define the roles and responsibilities of user account management; (4) ensure accountability and compliance with standards and procedures; and (5) require training.

Information resources residing at or administered by DPS are strategic and vital assets. Access to these resources must be appropriately managed. DPS must protect its information resources based on risk against accidental or unauthorized access, disclosure, modification, or destruction. DPS must ensure the availability, confidentiality, and integrity of these resources while avoiding creation of unjustified obstacles to conducting business in order to safely achieve DPS's mission, goals, and objectives.

Access to DPS's Active Directory account must be restricted to authorized users only, based on the principle of least privilege. The LSA agrees to comply with the LSA user agreement, this policy, and any additional requirements given to the LSA by ITD. The LSA user agreement states the process for granting and suspending authorized access. The Division and its LSA will verify account validity and access authority.

Access will be granted to resources only as necessary to perform an employee's official job duties and always in compliance with Texas and federal laws as well as Department rules, policies, and procedures.

20.02 Scope. This policy applies to all Active Directory accounts owned, leased, operated, or under the custodial care of DPS; all Active Directory accounts owned, leased, operated, or under the custodial care of third parties operated on behalf of DPS; and all individuals accessing, using, holding, or managing DPS's information resources on behalf of DPS.

20.03 Compliance with Confidentiality Requirements. Information that is collected related to the Division's Information Security Program is confidential in accordance with Texas Government Code Section 552.139.

20.04 Local Security Administrator. A Local Security Administrator (LSA) is a Department employee who is authorized and assigned the task to submit network and system access requests for other members of their area of responsibility. The LSA attends meetings regarding data security—whether it applies to the TLE domain or mainframe—to assist them in fulfilling the duties of an LSA. The LSA is a representative and point of contact for individuals in their area of responsibility who require modifications to access rights. The LSA is approved by their Chief, Assistant Chief, Regional Director, or designee, and is capable of performing all tasks regarding access requests and communicating changes to all affected areas/individuals within their area of responsibility as provided for in this Account and LSA Management policy. LSA responsibilities and duties are provided below.

20.05 Security Principles. Each Division's LSA will provide access privileges to Active Directory accounts based on the principle of Least Privilege. The Division will determine how much privilege is required based on its needs.

The Division and its LSA must comply with security requirements and appropriately grant access privileges for accounts under its control. Human Resources must independently verify that background checks have been completed successfully before the Division may grant access to any Department system or application.

The LSA must formally document requests and approvals for user and special accounts and access privileges.

Application and service accounts must be used only for the access originally authorized for them. Access to the password of such accounts will be restricted to authorized ITD administrators or application developers only.

Users must change the initial password from LSA upon initial access to account. New Application and Service accounts must change passwords at least once per year or when an administrator who has knowledge of the password leaves. Non-expiring passwords will no longer be issued. Exceptions must be justified by the Division and approved by the CISO and ITD Division Chief.

Passwords for application and service accounts that are changed yearly must meet increased length and complexity requirements. These passwords must have a minimum length of 12 alphanumeric characters and contain at least two upper case characters, two lower case characters, two numeric characters, and two special characters.

All accounts, including third-party accounts, accessing DPS's Active Directory will be issued a unique account and identifier (ACID).

Users will be held accountable for all actions initiated from accounts issued to them.

All users must sign the DPS's Computer Security Statement-Notice to Employee before access is given to an account.

If a user needs a remote access account, the user and their Division Chief or Division Assistant Chief must sign the DPS's Remote Access User Policy Statement and submit it to an ITD Security/System Administrator in addition to other requirements of the account management process.

All accounts must be uniquely identifiable using the assigned username.

All default passwords for accounts must be constructed in accordance with the DPS's password policy.

Any account that has not been accessed within 30 days of creation will be disabled.

20.06 LSA Responsibilities And Duties. LSA will read this policy, perform, and be held accountable for the responsibilities and duties assigned, as follows:

1) Attends LSA training as provided for in this policy.

2) Reviews user account requests and verifies, by submitting the service request, that all requirements for the requested access have been met and ensures that Human Resources has independently verified that background checks have been completed successfully.

3) Verifies that user accounts have received appropriate authorization from the business owner to access data within their scope of responsibility based on data sensitivity and risk, and through use of appropriate administrative, physical, and technical safeguards including the following:
    a. Ensures that data owner has authorized access to Confidential Data to those employees who need access for the performance of the employees' job responsibilities.
    b. An employee may not access Confidential Data if it is not required for the employee's job function.

4) Submits a service ticket using DPS's ticketing system to create, modify, or deactivate network accounts or groups.

5) Reviews quarterly user account reports from Account Management and submits appropriate request(s) in order to validate user access and authorization and maintain compliance with security policy. Request(s) for updates should be completed **within 15 business days**.

6) Submits, **within five business days,** an appropriate request to disable user access, when a user takes extended leave or is suspended.

20.06 Account Management Security Policy. The Department account management policy shall consist of the following:

1) All accounts created must have an associated request and approval that is appropriate for the Department system or service.

2) All users must sign the Department's Computer Security Statement-Notice to Employee before access is given to an account.

3) If a user needs a remote access account, the user and their Division Director or Assistant Division Director must sign the Department's Remote Access User Policy Statement and submit it to an ITD Security/System Administrator in addition to other requirements of the account management process.

4) All accounts must be uniquely identifiable using the assigned username.

5) All default passwords for accounts must be constructed in accordance with the Department's password policy.

6) All accounts must have a password expiration that complies with the Department's password policy. Process accounts may be exempted from this policy with the approval of the ITD Division Director.

7) Any account that has not been accessed within 30 days of creation will be disabled.

8) System Administrators, Security Administrators, or other designated staff:

    a. Are responsible for removing the no longer authorized accounts of individuals that change roles within the Department or are separated from their relationship with the Department.

b. Must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes, and permission changes.

c. Must have a documented process for periodically reviewing existing accounts for validity.

d. Are subject to independent audit review.

e. Must provide a list of accounts for the systems they administer when requested by authorized Department management.

f. Must cooperate with authorized Department management who are investigating security incidents.

20.07 LSA Responsibilities And Duties. LSA will read this policy, perform, and be held accountable for the responsibilities and duties assigned, as follows:

1) Attends LSA training as provided for in this policy.

2) Reviews user account requests and verifies, by submitting the service request, that all requirements for the requested access have been met and ensures that Human Resources has independently verified that background checks have been completed successfully.

3) Verifies that user accounts have received appropriate authorization from the business owner to access data within their scope of responsibility based on data sensitivity and risk, and through use of appropriate administrative, physical, and technical safeguards including the following:
    a. Ensures that data owner has authorized access to Confidential Data to those employees who need access for the performance of the employees' job responsibilities.
    b. An employee may not access Confidential Data if it is not required for the employee's job function.

4) Submits a service ticket using DPS's ticketing system to create, modify, or deactivate network accounts or groups.

5) Reviews quarterly user account reports from Account Management and submits appropriate request(s) in order to validate user access and authorization and maintain compliance with security policy. Request(s) for updates should be completed **within 15 business days**.

6) Submits, **within five business days,** an appropriate request to disable user access, when a user takes extended leave or is suspended.

LSAs are responsible for the accuracy, completion, and proper authorizations of all of their requests.

20.08 New LSA Procedures. User provisioning requires the following procedures:

1) An existing LSA submits a new LSA request within the ITSM tool.

2) New LSA reads and agrees to comply with LSA responsibilities and duties.

3) Assistant Chief/Chief/Regional Director approves or denies request.

4) Once approved, the ITSM tool grants the access automatically.

5) Account Management grants the access within Active Directory for other LSA rights.

6) A separate LSA user agreement will be developed. LSAs must agree annually to the user agreement.

The LSA user agreement, ITSM tool reference documents, LSA training materials, and LSA related processes and workflows can be found at the secure LSA SharePoint site.

LSA may contact the Account Management team by email at data-security@dps.texas.gov.

20.09 Account Management Responsibilities And Duties. The Account Management team will read this policy, perform, and be held accountable for the responsibilities and duties assigned, as follows:

1) Process user account action requests as submitted by the LSA.

2) Provide quarterly user access reports to LSAs that allow the LSA to verify legitimacy, authorization, and appropriate attributes of such accounts.

3) Review, on a monthly basis, the following high-level administrative groups and sends report of Enterprise, Schema, and Domain admin members to IT and Cyber Executive Management:
    a. Enterprise Admins;
    b. Schema Admins;
    c. Domain Admins;
    d. Account Operators (if present);
    e. Server Operators (if present);
    f. Print Operators (if present);
    g. DHCP Administrators; and
    h. DNS Admins.

4) Manage accounts based on user's employment status (such as FMLA).
    a. Disable account after 90 days in which user has not changed the password.
    b. Terminate accounts 60 days after account has been disabled, but not before 150 days since user has changed password, unless an exception exists (for example, FMLA or military leave.)
    c. Disable user domain admin account after 30 days if not logged in.
    d. Disable accounts included on the monthly HR Termination Report.
    e. Issues a new ACID for users who return to DPS after prior employment at DPS.
    f. Reviews and disables an account that it discovers is no longer eligible for access.

5) Take whatever appropriate action that it deems necessary to ensure the security and integrity of DPS's information resources.

6) Perform regular account audits.

7) Provide training materials to LSAs.

20.10 Administrative And Special Access. The Administrative and Special Access provisions govern the creation, use, monitoring, control, and removal of accounts with special access privilege. Technical support staff, security administrators, system administrators, and others may have special access account privilege requirements that differ from everyday users. The fact that these administrative and special access accounts have a higher level of access means that granting, controlling, and monitoring these accounts is extremely important to an overall security program.

The Administrative and Special Access provisions require that:

1) DPS Division Chiefs must submit, to ITD, a list of personnel requiring a special access account for their systems that are connected to the DPS's network.

2) All users must sign the DPS's Computer Security Statement-Notice to Employee before access is given to an account.

3) All users of administrative/special access accounts must have account management instructions, documentation, training, and authorization.

4) Each individual that uses administrative/special access accounts must refrain from abuse of privilege and may only do investigations under the direction of the CISO.

5) Each individual that uses administrative/special access accounts must use the account privilege most appropriate with work being performed (for example, user account vs. administrator account).

6) Each account used for administrative/special access must meet the DPS's password policy.

7) The password for a shared administrator/special access account must change when an individual with the password leaves the section or DPS, or upon a change in the vendor personnel assigned to the DPS contract.

8) In the case where a system has only one administrator there must be a procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.

9) When special access accounts are needed for internal or external audit, software development, software installation, or other defined need, they must be:
   a. Authorized by the ITD Division Chief or the Director;
   b. Created with a specific expiration date; and
   c. Removed when work is complete.

20.11 Oversight And Compliance. The data owner must exercise due diligence to ensure the accuracy, legitimacy, and authorization of the user access accounts requested.

LSA will submit a ticket to have a new user account created. LSA must provide user's supervisor and HR's approval of employment and background check. The approvals will be automated in the ticketing system. Once all approvals have been received, the Account Management team will process the request.

LSAs exercise primary oversight and compliance verification of user account provisioning. The Account Management team provisions user accounts as specified in the LSA user account request. When the Account Management team receives a request, it is expected that LSAs have already properly verified the legitimacy and authorization of a user account request.

20.12 Audit And Logging. Users accounts will be audited at least once annually. User access to information resources and data, as well as significant system events, must be logged by the Information System.

Account access audit logs must be protected from unauthorized access or modification.

Account access audit logs must be retained for an appropriate period of time based on DPS's Records Management Retention Schedule.

20.13 LSA Training. ITD will ensure that LSA training is delivered and tracked. All LSAs will receive:

1) Initial training that will, at minimum, identify duties and responsibilities, common threats, regulatory and DPS requirements regarding the acceptable use and security of information resources, proper handling of Confidential data, security incident notification, and procedures as provided for in this policy.

2) Refresher training annually, unless changes require more frequent training, that will focus on LSA duties and proper workflow process and procedures, any updates to training since the previous training, and other elements identified to ensure that all LSAs perform their duties consistently and as provided for in this policy.

3) LSAs are encouraged to consult training resources provided by Account Management. Account Management responds to frequent calls and emails from LSAs when questions or problems arise.

The method of delivery and scheduling of training will be determined by the ITD Division Chief or designee. See General Manual, Chapter 26, 26.60.02 Security Training Policy.

20.14 Disciplinary Action. Employees whose duties and responsibilities are provided for in this policy understand and agree that their use of DPS's information resources is conditioned upon their agreement to comply with this policy and that violations of this policy may result in disciplinary action in accordance with DPS's applicable rules, policies, and procedures, up to and including termination of employment.

20.15 Related Information. Other related policies that may be developed in support of this policy or as required by state or federal law, regulations, and DPS. General Manual Chapter 25 and Chapter 26. All informative data for Local Security Administrators is located on a secure SharePoint site.

26.25.00 ACCOUNT MANAGEMENT PRINCIPLES.

Proper management and use of user accounts are basic requirements for protecting DPS's information resources. All users who create or request access accounts for applications, networks, or systems are required to request, approve, and manage the accounts in accordance with this policy. Access to an information resource may not be granted by another user without the permission, proper authorization, and approval of the appropriate data owner of that resource.

25.02 DPS employs a de-centralized model of user account management in which the local security administrators verify the legitimacy and authorization of user accounts and submit requests in DPS's ticketing system to be provisioned by the Account Management team.

25.03 The success of DPS's user account provisioning process depends on the accuracy and validity of the user account requests created, submitted, and audited by the local security administrators. The local security administrators provide the primary security control over the accounts which they process and must ensure that access requests are properly vetted, authorized, and appropriate to the user's job duties (in accordance with the principle of Least Privilege) as provided for in this policy.

25.04 All Active Directory accounts will follow the ITD account creation process. DPS's ticketing system will document who is associated with the account, the purpose for which the account was created, the specific privileges assigned to the account, verification of successful background investigation, and the name of the business or data owner or supervisor who approved the account.

25.05 LSA will review user accounts on a quarterly basis for validity of access privileges and may modify, disable, or terminate access as necessary to comply with this policy. Account Management will send report listing accounts and users to LSA to review for accuracy and proper authorization as required by needs of its Division.

25.06 Changes in rights for an account provided only for a limited time will be reviewed and disabled according to the nature of the changes. To be granted, data owner must provide all information regarding start and ending of permissions.

25.07 User accounts assigned to contractors will be set to expire according to the contract's expiration date. LSA will note the contract expiration date on the user access request.

25.08 Accounts of users on extended leave (more than 90 days) or accounts that have not been accessed in more than 90 days will be disabled.

25.09 Accounts of users whose employment status, roles, or security requirements with DPS have changed must be updated to comply with the authorization and privileges of the new status. The user's manager should notify the appropriate LSA to request the immediate modification of accounts assigned to employees whose employment status has changed. New privileges and access must be authorized and approved by the business owner or user's manager, and the LSA must review the new access request for compliance with provisions of this policy.

25.10 Account Management will monitor accounts to see if the existing 90-day password has not changed; if password has not been changed, Account Management will disable such accounts. Existing user accounts and access privileges will be reviewed to detect dormant accounts and accounts with excessive privileges.

25.11 Access will be immediately terminated, modified, or disabled when a user is terminated or ceases to have a legitimate reason to access DPS's information resources, including any "emergency requests" for access. The user's manager should notify the appropriate LSA to request such accounts be

immediately terminated, modified, or disabled. Examples of emergency requests include accounts that Account Management deems:

1) A security risk that, if not immediately processed, exposes DPS or its operations to a significant security risk; and

2) An impact to a business process that, if not immediately processed, exposes DPS or its operations to imminent failure or adversely affects production operations.

25.12 Accounts which are found to have been granted access improperly or not in accordance with this policy will be reviewed and modified, disabled, or terminated as required to ensure the security of DPS's information resources. The Account Management team may take whatever appropriate action that it deems necessary to ensure the security and integrity of DPS's information resources. Examples of such action include modifying, disabling, or terminating the account.

25.13 All access requests for changes to existing permissions will be documented using DPS's ticketing system in place.

26.30.00 CHANGE MANAGEMENT

30.01 Purpose. Change management is the process of controlling modifications to hardware, software, firmware, and documentation to ensure that information resources are protected against improper modification before, during, and after system implementation.

A change can be any of the following ways the Department's information resources may be impacted:

- Implementation of new capabilities
- Interruption of service
- Repair of existing capabilities
- Removal of existing capabilities

The purpose of the Department's "Change Management Policy" is to manage changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of information resources. The Department's information resources infrastructure is expanding and continuously becoming more complex. There are more people dependent upon the network, more client machines, upgraded and expanded administrative systems, and more application programs. As the interdependency between information resources grows, the need for a strong change management process is essential. From time to time each information resource element requires an outage for planned upgrades, maintenance, or fine-tuning. Additionally, unplanned outages might occur that may also result in upgrades, maintenance, or fine-tuning. Managing these changes is a critical part of providing a robust and valuable information resources infrastructure.

30.02 Change Management Policy. The Department's "Change Management Policy" consists of the following:

1. Every change to Department information resources (such as operating systems, computing hardware, networks, and applications) is subject to this "Change Management Policy" and must follow the Department's change management procedures.

2. All changes affecting computing environmental facilities (such as air-conditioning, water, heating, plumbing, electricity, and alarms) need to be reported to or coordinated with the ITD Infrastructure and Operations Assistant Division Chief responsible for the Department's change management process.

3. The Change Management Committee is composed of both ITD and Division representatives and a leader appointed by ITD management. The Change Management Committee meets regularly at Change Reviews to review (approve, deny, or delay) change requests, coordinate scheduling of changes, and to ensure that communications are being satisfactorily performed.

4. A formal written change request must be submitted for all changes.

Exception for an unauthorized emergency change: When an unauthorized immediate response is needed to prevent widespread service disruption, an "unauthorized emergency change" may be enacted. However, this change must be documented before the next Change Review as required by the Department's change management procedures.

Exception for authorized unscheduled change: If an emergency problem occurs, and there is no time to gather the Change Management Committee for a Change Review, but the leader of the Change Management Committee or the ITD Division Chief/Assistant Division Chief/designate approves the verbal change request, it is called an "authorized unscheduled change" and may be enacted. However, this change must be documented before the next Change Review as required by the Department's change management procedures.

5. All change requests must be submitted, (see #4 for exceptions), in accordance with the Department's change management procedures so that the Change Management Committee has time to review the request, access risks, and make the decision to approve, deny, or delay the request.

6. Each change request, (see #4 for exceptions), must receive formal Change Management Committee approval before proceeding with the change. A change with the approval of the Change Management Committee, in advance of the change being enacted, is called a "scheduled change."

7. The leader of the Change Management Committee may deny a change request for reasons including, but not limited to, inadequate planning (no project implementation plan, no back out plan, and so forth) the timing of the change will negatively impact a key business process such as year-end accounting, or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays, or during special events.

8. The ITD Division Chief and/or Assistant Division Chief will resolve any items that are escalated to them and will have veto power over all change requests.

9. Customer notification must be completed for each scheduled or authorized unscheduled change, (see #4 for exceptions) following the steps contained in the Department's change management procedures.

10. A Change Review must be completed within five (5) business days for each change.

11. If the scheduled change does not occur on the scheduled date, the Change Review committee must approve the new date.

12. A change management log must be maintained for all changes. The log must contain, but is not limited to:

a) Date of submission and date of change
b) Owner and custodian contact information
c) Nature of the change
d) Indication of success or failure

13. All Department information systems must comply with the Department's information resources change management process that meets the minimum standards outlined above.

26.35.00 DISASTER RECOVERY AND CONTINGENCY PROGRAM

35.01 Purpose. To accomplish its mission, DPS must ensure that its essential functions and time-critical operations are performed efficiently and with minimal disruption. This policy provides guidance for implementing contingency and disaster recovery programs and processes to support essential functions. DPS's ITD Disaster Recovery program and the Enterprise Risk Management Continuity of Operations (ERM-COOP) program collaboratively established the Division's responsibilities in the deployment of continuity of operations, contingency plans, and IT-supported disaster recovery. Additionally, IT works with ERM-COOP, Cyber Security, and the Divisions to establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for DPS information systems to ensure the availability of critical information resources and continuity of operations in emergency situations or disasters.

In accordance with guidance from Federal Emergency Management Agency (FEMA), Texas Department of Information Resources (DIR), Disaster Recovery Institute International, Criminal Justice Information Services (CJIS) and National Institute of Standards and Technology (NIST) Contingency, a sound disaster recovery and contingency program guides the orderly and expeditious restoration of the Department's mission-critical systems, services, responsibilities, and applications in an outage. A core responsibility of Cyber security and ITD is protecting information technology assets from unauthorized access, disclosure, modification, or destruction, whether accidental or deliberate, as well as supporting the availability, integrity, utility, authenticity, and confidentiality of the Department's information.

A COOP plan identifies and documents the processes and methods needed by each Division to continue essential agency functions during an incident affecting information systems, employees, contractors, agents, or DPS locations.

35.02 Disaster Recovery and Contingency Program . As further defined in Section 35.03, DPS, through its different roles, will maintain a comprehensive disaster recovery, contingency, and continuity program that addresses the following:

1. Review policy annually on disaster recovery, contingency, and continuity of operations according to state guidelines and industry best practices
2. Establish Division Resiliency Liaisons.
3. Establish incident management team concepts to support Department incidents.
4. Develop continuity plans and tools.
5. Regularly perform a business impact analysis (BIA) by identifying DPS essential functions and critical systems. The BIA will determine acceptable lengths of disruption to normal processes that DPS can tolerate for each business function.

6. Perform risk assessments to determine threats that can adversely affect business functions, the damage potential, the timescale needed to restore functions, and the controls that can reduce the risk of impact.
7. Develop operational, tactical, continuity and contingency technical recovery tools and guidelines to support performance for all essential functions and systems.
8. Develop contingency procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.
9. Review and update the current contingency planning procedures on an annual basis.
10. Coordinate with all program and support areas that perform essential functions and critical systems to develop strategically aligned continuity procedures, contingency plans, and recovery strategies.
11. Develop and maintain the DPS Disaster Recovery Plan; this plan will complement the agency ERM-COOP plan and specify how information systems that support essential functions and critical systems are restored or maintained.
12. Provide the contingency plans in an accessible format to authorized personnel and store a copy of the plan in secured locations.
13. Conduct periodic tests and exercises of planning material to identify operational issues or gaps in procedures for restoring or maintaining essential functions and critical systems during disruptions.
14. Ensure that DPS employees, contractors, and agents understand the procedures and that after-action reviews are performed with corrective action plans developed post-test or exercise.
15. Review disaster recovery and contingency plans after each disruption and at least annually, to keep them up-to-date and document the date that revisions are adopted.
16. Follow the established continuity plans during continuity activation, response, and recovery.
17. Provide staff with appropriate awareness and operational training to implement, disaster recovery, contingency, and continuity roles and responsibilities.
18. Work with other governmental entities, contractors, and other partners to develop preparedness activities and coordinate support during incidents.

35.03 Disaster Recovery and Contingency Program Roles and Responsibilities.

All Divisions are responsible in varying degrees for continuity and disaster recovery planning, preparedness, and execution. These responsibilities may include the following:

1. Provide information for planning
2. Participate in training and exercises to enhance DPS's readiness to implement continuity and disaster recovery processes
3. Implement continuity and disaster recovery plans and procedures during activation; and
4. Perform other duties deemed necessary to support essential functions. Such participation may require an alternate shift pattern, assignment, or location.

In addition, the following roles have specific responsibilities.

1) DPS Divisions are expected to support disaster recovery, continuity, and contingency efforts in the following ways:
   a) Provide leadership and support during incidents.
   b) Advocate for and provide available funding and strategic direction to disaster recovery, contingency, and continuity preparedness planning and procedures.
   c) Review and approve high-level DPS disaster recovery, contingency, and continuity deliverables.
   d) Resolve issues brought to their attention by the DPS Resiliency Core Group or a Resiliency Liaison.

e) Consult with the ITD Disaster Recovery and ERM-COOP and act on its recommendations, including the decision whether to accept or mitigate identified risks.
f) Provide direction and participate in preparedness training and exercises designed to enhance DPS's disaster recovery, contingency, and continuity response.

2) DPS disaster recovery and ERM-COOP Executive Sponsors (ITD, Cyber, and IOD Chiefs) ensure that DPS disaster recovery, contingency, and continuity goals and objectives are strategically aligned and consistent with DPS goals, objectives, and policy. They should also ensure that disaster recovery contingency and continuity objectives, deliverables, and schedules are met on time and within scope in the following ways:
   a) Advocate for, secure resources, and provide strategic direction to DPS disaster recovery, contingency, and continuity programs.
   b) Review and approve disaster recovery, contingency, and continuity deliverables and submit to the Deputy Directors or the Director as necessary.
   c) Resolve issues escalated by the DPS disaster recovery, contingency, and continuity program and make formal decisions on recommendations.

3) DPS Resiliency Core Group (ITD DR, Cyber, Data Management, and Enterprise Risk Management) ensures that the purpose, objectives, and deliverables of DPS disaster recovery and continuity planning are completed on time and within scope of agency goals in the following ways:
   a) Coordinate assignments and projects that contribute to completion of disaster recovery, contingency, and continuity objectives and plans, and submit deliverables for approval.
   b) Convene meetings of the DPS Resiliency Liaisons and create ad hoc workgroups as necessary to meet planning and preparedness objectives.
   c) Identify issues, risks, and opportunities that may affect disaster recovery, contingency, and continuity preparedness or response and escalate to Division Chiefs, the Deputy Directors, or the Director for resolution as necessary.
   d) Coordinate the development of plans, tools, Standard Operating Guidelines (SOG), and templates in support of comprehensive and collaborative disaster recovery, contingency, and continuity planning and operations.
   e) Collaborate with business partners and customers to meet DPS ITD disaster recovery, contingency and continuity objectives.
   f) Advocate for the DPS disaster recovery, contingency and continuity program and seek appropriate resources.
   g) Develop and implement the disaster recovery, contingency, and continuity training and exercise program.

4) The Resiliency Liaison collaborates with the ITD Disaster Recovery Team, and ERM-COOP to ensure that the deliverables align with DPS's guiding principles and objectives, and that they are completed on time and within scope by the following actions:
   a) Complete DPS disaster recovery or ERM-COOP objectives and submit deliverables for approval. Participate in periodic program tests and exercises, After-Action Reviews, and corrective action plan implementation.
   b) Convene staff meetings to develop their disaster recovery and continuity programs and plans. This may include the development of program or division specific essential function Standard Operating Guidelines (SOG), technical recovery guides, and other tactical or technical documents.
   c) Identify staff to serve on Emergency Relocation Groups (ERGs), to support implementation of essential functions' continuity.
   d) Analyze threats, risks, and opportunities that may affect the disaster recovery and ERM-COOP program or plans; and provide recommendations to the Resiliency Liaison's chain of command.

e) Assist in developing and implementing training to support agency disaster recovery and ERM-COOP objectives.
f) Collaborate in the development of agency disaster recovery and continuity plans and procedures.

5) DPS Divisions must provide up-to-date and complete information regarding agency-wide disaster recovery and contingency program development, division continuity plans and function-specific Standard Operating Guidelines. This includes the completion of the Business Impact Analysis, risk assessment, mitigation strategies, and ITD disaster recovery and contingency support. Additional responsibilities are as follows:
   a) Ensure that all contractors and external parties identify and develop appropriate disaster recovery, contingency, and continuity capabilities; and that the capabilities support DPS's essential functions and are in compliance with any contractual requirements.
   b) Participate in training and exercises to support DPS's ability to implement disaster recovery, contingency, and continuity operations.
   c) Collaborate with ITD in strategic planning to develop future program plans and in identifying funding sources.
   d) Should data be restored from electronic backup (due to disaster recovery, hardware failure, data corruption, or other event), ITD will notify the affected Division and the records management office. The division records management owner must review restored data and ensure that all records are handled in accordance with records retention requirements.

6) ITD leads the evaluation of applications designated as mission critical by the Division Chief or designee owning the application. ITD will inform the Division Chief of all risks and opportunities identified during gap analysis and provide potential solutions and associated costs for consideration. If necessary, ITD will escalate these issues to the Deputy Directors or the Director for a final decision. ITD discharges these responsibilities as follows:
   a) Oversee and coordinate the development, maintenance, and distribution of DPS Disaster Recovery Plans (DRPs), Information System Contingency Plans (ISCPs), and Technical Recovery Guidelines.
   b) Implement disaster recovery and contingency program.
   c) Document, manage, and coordinate ITD application incidents and outages.
   d) Collaborate with Cyber Security for outages related to information system security threats.
   e) Coordinate with DPS ERM-COOP to provide ITD support for continuity preparedness activities and operations.

26.40.00 SECURITY INCIDENT MANAGEMENT

40.01 Purpose. The Department's "Security Incident Management Policy" describes the requirements for dealing with computer security incidents. Security incidents include, but are not limited to: detection of a virus, worm, or Trojan horse; unauthorized use of computer accounts and computer systems; and improper use of information resources as outlined in "Email Acceptable Use Policy," "Internet and Intranet Acceptable Use Policy," and "Acceptable Use Policy."

40.02 Security Incident Management Policy

1. The Department's Computer Incident Response Team (CIRT), members have pre-defined roles and responsibilities that can take priority over normal duties.

2. Whenever a security incident, such as a virus, worm, hoax email, hacking tool, altered data, and so forth is suspected or confirmed, the appropriate security incident management procedures must be followed. An immediate notification must be made to the CISO.

3. The CISO is responsible for notifying the IRM and the CIRT and initiating the appropriate incident management action including restoration as defined in the incident management procedures.

4. The CISO is responsible for determining the physical and electronic evidence to be gathered as part of the security incident investigation.

5. The appropriate technical resources from the CIRT are responsible for monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.

6. The CISO, working with the IRM, will determine if a widespread Department communication is required, the content of the communication, and how best to distribute the communication.

7. The appropriate technical resources from the CIRT are responsible for communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.

8. The CISO is responsible for initiating, completing, and documenting the incident investigation with assistance from the CIRT.

9. The CISO is responsible for reporting the incident to the:

a) IRM and CRIT

b) Department of Information Resources as outlined in TAC 202

c) Local, state or federal law officials as required by applicable statutes and/or regulations

10. If it is determined that a user is engaged in unapproved activities that pose an immediate threat to the Department's network, the CISO may immediately suspend the user's access pending resolution of the threat. The CISO must notify the IRM immediately upon taking such action.

11. The CISO is responsible for coordinating communications with outside organizations and law enforcement.

12. In the case where law enforcement is not involved, the affected Division Chief will recommend disciplinary actions pursuant to Chapter 7A, General Manual.

13. In the case where an outside law enforcement agency is involved, the CISO will act as the liaison between any outside law enforcement agencies and the Department.

26.45.00 NETWORK CONFIGURATION SECURITY

45.01 Purpose. The purpose of the Department's "Network Configuration Security Policy" is to establish the rules for the maintenance, expansion, and use of the network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of the Department's information.

45.02 Network Configuration Security Policy

1. ITD owns and is responsible for the Department's network infrastructure and will manage further developments and enhancements to this infrastructure.

2. To provide a consistent network infrastructure capable of supporting new networking developments, all cabling must be installed by the Building Program Bureau or an approved contractor.

3. All network connected equipment must be configured to a specification approved by ITD.

4. All hardware connected to the Department's network is subject to ITD management and monitoring standards.

5. The ITD Division Chief or designee must approve any changes to the configuration of active network management devices.

6. The Department's network infrastructure supports a well-defined set of approved networking protocols. ITD Division Chief or designee must approve any use of non-sanctioned protocols.

7. The networking addresses for the supported protocols are allocated, registered, and managed centrally by the ITD Division Chief or designee.

8. All connections of the network infrastructure to external third-party networks are the responsibility of the ITD Division Chief or designee. This includes connections to external telephone networks.

9. Firewalls must be installed and configured following the ITD Firewall Implementation Standard documentation.

10. The use of internal firewalls by individual entities is not permitted without the written authorization from the ITD Division Chief or designee.

11. Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the Department's network without the approval of the ITD Division Chief or designee.

12. Users must not install network hardware or software that provides network services without the approval of the ITD Division or designee.

13. Users are not permitted to alter network hardware in any way.

45.03 Vulnerability Assessment. The CISO will be responsible for establishing an annual information resource vulnerability assessment and specific focus areas for the assessment will be based on the results of the security risk assessment.

26.50.00 PASSWORDS

50.01 Purpose. User authentication is a necessary means to control who has access to an information resource system. Access gained by a non-authorized entity damages/breaches information confidentiality, integrity, and availability, which may result in the loss or revenue, data, or trust, and/or may cause a liability or embarrassment to the Department. The purpose of the Department's "Password Policy" is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation

50.02 Password Policy. The purpose of the password policy is to establish uniform and enterprise-wide practices to create, manage and maintain passwords to ensure expected levels of access security. The policy outlines requirements for creation of strong passwords, protection of those passwords, and password change frequency.

The following must be followed unless permission is granted by the Department's CISO or CIO:

1) All passwords, including initial passwords, must be constructed, and implemented according to the following Department information resource rules:

    a) A password must be changed at least every 90 days

    b) Passwords must be changed immediately if the user knows or suspects their account has been compromised

    c) Passwords for default accounts must be changed at first use if the capability exists. If the capability does not exist, it should be documented that the default password was not changed and the reason for not changing it.

2) Passwords must be a minimum of eight (8) characters chosen from at least three of the following elements:

    a) Uppercase characters

    b) Lowercase characters

    c) Numeric characters

    d) Special characters (i.e. $, ^, #, @, etc.).

3) Passwords must not contain Department business terms, personal details, such as family names, social security number, geographical locations, common acronyms, slang, or date of birth.

4) Users must generate a new unique password that does not reuse any portion of the last 10 iterations of their password.

5) Passwords must be treated as confidential information.

6) Passwords must not be written down or discussed, unless through an encrypted source or program, such as LastPass.

7) When stored, passwords must be encrypted.

50.02.01 Use of Privileged Access Information. Users must be required to follow good security practices in the selection and use of passwords.

50.02.02 Initial Use Password. All user passwords provisioned should be changed at initial login.

50.02.03 Password Confidentiality. User passwords are confidential and must be treated as such; users must not share or reveal passwords. Users that share or intentionally reveal his/her password is accountable for the unauthorized user's actions.

50.02.04 Password Write-Down. The only time it is safe to write a password down (electronically) is if it is stored in an encrypted format. If left in plain text, it is essentially compromised the moment the user leaves it unattended because the user cannot prove it was not compromised.

50.02.05 Change Passwords after Disclosure. Users must immediately change their passwords that are suspected of being disclosed or known to have been disclosed. Cyber Security must be notified when passwords have been suspected of being disclosed to be monitored for a brief period of time.

50.02.06 Password Difficult-to-Guess. Users must select passwords that are difficult-to-guess and must not select passwords that are:

1) Words in a dictionary

2) Agency business terms

3) Derivatives of user IDs

4) Common character sequences, such as "123456"

5) Personal details, such as spouse's name, automobile license plate, social insurance number (Canada), social security number (U.S.A.), and date of birth; or,

6) Parts of speech, such as proper names, geographical locations, common acronyms, and slang.

06.04.07 Elevated Privilege Users. Users with elevated accounts (i.e., Administrator accounts) must use a minimum of 12-character password and, follow the rules as set forth in **26.50.01.**

26.55.00 PHYSICAL ACCESS

55.01 Purpose

The granting, controlling, and monitoring of the physical access to information resources facilities is extremely important to an overall security program. The purpose of the Department's "Physical Access Policy" is to establish the rules for the granting, control, monitoring, and removal of physical access to information resource facilities.

55.02 Physical Access Policy

1. All physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.

2. Physical access to all information resources restricted facilities must be documented and managed.

3. All information resources facilities must be physically protected in proportion to the criticality or importance of their function at the Department.

4. Access to information resources facilities must be granted only to Department support personnel and contractors whose job responsibilities require access to that facility.

5. The process for granting card and/or key access to information resources facilities must include the approval of the manager responsible for the facility.

6. Each individual that is granted access rights to an information resources facility must receive emergency procedures training for the facility and must sign the appropriate access and non-disclosure agreements.

7. Requests for access must come from the applicable Department owner or custodian of the information resource that resides in the facility.

8. Access cards and/or keys must not be shared or loaned to others.

9. Access cards and/or keys that are no longer required must be returned to the appropriate manager for return to security. Cards must not be reallocated to another individual bypassing the return process.

10. Lost or stolen access cards and/or keys must be reported to the manager responsible for the information resources facility.

11. All information resources facilities that allow access to visitors will track visitor access with a sign in/out log.

12. A replacement charge may be assessed for access cards and/or keys that are lost, stolen, or are not returned.

13. Card access records and visitor logs for information resources facilities must be kept for routine review based upon the criticality of the information resources being protected.

14. The manager responsible for the information resources facility must ensure the removal of the card and/or key access rights of individuals that change roles within the Department or are separated from their relationship with the Department.

15. Visitors must be escorted in card access-controlled areas of information resources facilities.

16. The manager responsible for the information resources facility must review access records and visitor logs for the facility every one hundred and eighty days and investigate any unusual access.

17. The manager responsible for the information resources facility must review card and/or key access rights for the facility every ninety days and ensure removal of access for individuals that no longer require access.

26.60.00 SECURITY TRAINING

60.01 Purpose. Understanding the importance of computer security and individual responsibilities and accountability for computer security are paramount to achieving organization security goals. This can be accomplished with a combination of general computer security awareness training and targeted, product specific training. The philosophy of protection and specific security instructions needs to be taught, and reinforced, to computer users. The security awareness and training information needs to be continuously upgraded and reinforced. The purpose of the Department's "Security Training Policy" is to describe the requirements that ensure that each user of the Department's information resources receives adequate computer security training.

60.02 Security Training Policy

1. All new users must complete an approved security awareness training class prior to, or at least within 30 days of, being granted access to any Department information resources.

2. All users must sign an acknowledgement stating they have read and understand the Department's requirements regarding computer security policies and procedures.

3. All users (employees, consultants, contractors, temporaries, and so forth.) must be provided with training and supporting reference materials to assist them in protecting the Department's information resources.

4. ITD will prepare, maintain, and distribute one or more information security manuals that concisely describes the Department's information resource security policies and procedures.

5. All users must complete an annual computer security training class and pass the required examination.

6. ITD will develop and maintain a communications process to be able to communicate new information resource security program information, security program information, security bulletin information, and security items of interest.

26.65.00 SOFTWARE LICENSING

65.01 Purpose. End-user license agreements are used by software and other information resource companies to protect their valuable intellectual assets and to advise information resource users of their rights and responsibilities under intellectual property and other applicable laws. The purpose of the Department's "Software Licensing Policy" is to establish the rules for licensed software use on Department owned information resources.

65.02 Software Licensing Policy

1. The Department provides a sufficient number of licensed copies of software such that workers can get their work done in an expedient and effective manner. Management must make appropriate arrangements with the involved vendor(s) through ITD for additional licensed copies if and when additional copies are needed for business activities.

2. Third party copyrighted information or software that the Department does not have specific approval to store and/or use must not be stored on Department systems or networks. Systems administrators will remove such information and software unless the involved users can provide proof of authorization from the rightful owner(s).

3. Third party software in the possession of the Department must not be copied unless such copying is consistent with relevant license agreements and prior management approval of such copying has been obtained, or copies are being made for contingency planning purposes.

4. A list of software authorized for installation on Department owned computers may be found on the Intranet. Any specialized software not appearing on this list must be approved by the Division Chief where the software will be utilized and kept on file with ITD.

5. All employees utilizing Department owned software must read and understand the Department's "Software Licensing Policy."

26.70.00 COMPUTER VIRUS DETECTION

70.01 Purpose. The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents. ITD is responsible for determining which virus detection software will be installed and used on the Department's computer equipment. The purpose of the Department's "Computer Virus Detection Policy" is to describe the requirements for dealing with computer virus, worm, and Trojan Horse prevention, detection and cleanup.

70.02 Computer Virus Detection Policy

1. All workstations, whether connected to the Department's network or standalone, must use the Department's ITD approved virus protection software and configuration. The virus detection software should be executed every time the workstation is turned on. All diskettes will be virus checked before data is loaded from the diskette to the workstation.

2. The virus protection software must not be disabled or bypassed.

3. The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.

4. The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.

5. Each file server attached to the Department's network must use ITD approved virus protection software and setup to detect and clean viruses that may infect file shares.

6. Each email gateway must use ITD approved email virus protection software and must adhere to the ITD rules for the setup and use of this software.

7. Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the ITD Service Desk. If an employee thinks there is a virus on their workstation, they should call and advise the Help Desk. The Help Desk will inform the CISO and support the CISO with ITD Service Desk staff if necessary.

8. To minimize any confusion, users should only regard email alerts concerning viruses that originate from the CISO as genuine.

9. ITD will keep the most current version of the approved virus detection software installed on the Department's computer equipment.

26.75.00 NETWORK ACCESS

75.01 Purpose. The Department's network infrastructure is provided as a central utility for all users of Department information resources. It is important that the infrastructure, which includes cabling and the associated "active equipment," continues to develop with sufficient flexibility to meet the Department's demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services. The purpose of the Department's "Network Access Policy" is to establish the rules for the access and use of the network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of the Department's information resources.

75.02 Network Access Policy

1. Users are permitted to use only those network addresses issued to them by ITD.

2. All remote access (dial in services or VPN) to the Department will be either through an approved modem pool or Internet Service Provider (ISP).

3. Remote users may connect to Department owned information resources only through an ISP and using protocols approved by the Department.

4. Users inside the Department firewall may not be connected to the Department's network at the same time a modem is being used to connect to an external network.

5. Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the Department's network without ITD approval.

6. Users must not install network hardware or software that provides network services without ITD approval.

7. Non-Department owned computer systems that require network connectivity must be approved by the ITD Division Chief and must conform to ITD Standards.

8. Users must not download, install, or run security programs or utilities that reveal weaknesses in the security of a system. For example, Department users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the Department's network infrastructure.

9. Users are not permitted to alter network hardware in any way.

26.80.00 PORTABLE COMPUTING DEVICES

80.01 Purpose. Portable computing devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices ever more desirable to replace traditional desktop devices in a wide number of applications. However, the portability offered by these devices may increase the security exposure to groups using the devices. The purpose of the Department's "Portable Computing Devices Security Policy" is to establish the rules for the use of mobile computing devices and their connection to the network. These rules are necessary to preserve the integrity, availability, and confidentiality of Department's information resources.

80.02 Portable Computing Devices Security Policy

1. Only Department approved portable computing devices may be used to access the Department's information resources.

2. Portable computing devices must be password protected.

3. Department information should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all sensitive Department owned information must be encrypted using approved encryption techniques.

4. Department owned information must not be transmitted via wireless to or from a portable computing device unless ITD approved wireless transmission protocols and approved encryption techniques are utilized.

5. All remote access (dial in services) to the Department must be either through an approved modem pool or Internet Service Provider (ISP).

6. Non-Department owned computer systems that require network connectivity must conform to ITD standards and must be approved in writing by the ITD Division Chief.

7. Unattended portable computing devices must be physically secure. Users must not leave portable computing devices unattended in vehicles unless the portable computing device is secured in the Department installed locking mechanism during the employee's tour of duty. After the employee's tour of duty, the portable computing device may be secured in the locked trunk of the automobile or in the locked toolbox/bed cover of a pickup truck equipped with a lockable toolbox/bed cover.

8. Portable computing devices will not remain in vehicles that have been left at a business for repairs or servicing.

08.03 Mobile Device Use

This document outlines the conditions the Texas Department of Public Safety (TXDPS) requires for the use of mobile devices. By signing this agreement, the user agrees to abide by the TXDPS Rules of Behavior and Cyber Security Policies (ref. DPS General Manual, Chapter 26, *Information Management Service)* for the use of mobile devices. It is the user's responsibility to ensure they understand and follow the established policies for the protection, storage, and handling of all TXDPS Data. This includes Personally Identifiable Information (PII), Criminal Justice/Intelligence (CJIS), Health Insurance Portability

and Accountability Act (HIPAA), and Payment Card Industry (PCI) data. In addition, the following rules apply to any mobile devices that access TXDPS information systems.
The user understands and agrees to the following:

- TXDPS will install a security profile on all mobile devices. The security profile may affect an application's usability, functions, or features. If the user experiences application issues, they must not attempt to remove, disable, or bypass any security settings enabled by TXDPS. The user must report the application issues to the helpdesk for troubleshooting.

- If any tampering with the mobile device security profile is attempted or it is discovered that the user has made unauthorized modifications, TXDPS will immediately wipe and disable the mobile device.

- The user will only purchase, download, or install applications on the mobile device that are for official work-related business. The user's supervisor must formally approve the purchase, download, or installation prior to the application being loaded on the device. If the user violates TXDPS policy and purchases, downloads, or installs any applications without approval, TXDPS will not be responsible for the cost and the application will be removed when it is discovered.

- There is no expectation of privacy for any data processed, stored, or transmitted on the mobile device. TXDPS can access and audit all data on the mobile device at any time without any notice to the user.

- TXDPS may recall the mobile device for audit and accountability at any time. Mobile devices that are not returned by the required timeframe will be remotely wiped and disabled.

- The processing of government data on non-government devices is highly discouraged; however, it is understood that emergencies may necessitate this practice. The user will make every attempt to use TXDPS devices to process, download, or store government data. If an emergency arises that requires the user to process government data on a non-government device, the user is responsible for the protection, storage, and handling in accordance with TXDPS Policy.

- TXDPS can remotely wipe devices at any time with or without notice to the user, and they are not liable for any loss of data or applications resulting from a remote wipe.

- The user is prohibited from taking a TXDPS issued mobile device outside of the United States (US) for personal travel unless the user's Deputy Assistant Director /Major approves the request. If a device is approved for use on personal travel outside the US, the user will send the following information via email to the Office of Cyber Security (Grp_Cyber_Security@dps.texas.gov prior to leaving the country:

    - Dates of travel
    - Countries of travel including stopovers and layovers
    - Identification of any sensitive data that will be on the mobile device during travel
    - Copy of Deputy Assistant Director/Major Approval (approval via email is acceptable)
    - Compliance with additional security requirements such as maintaining possession of the device at all times, disabling Wi-Fi and Bluetooth services, and any other security controls imposed by TXDPS

In addition, if the user extends their travel beyond the original travel dates an updated email with the new dates of travel must be sent to the above email address. Upon return to the US, the mobile device will be sanitized and re-imaged to protect the department's information. Travel outside of the US that is for official TXDPS business is exempt from this process.

26.85.00 SECURITY MONITORING

85.01 Purpose. Security monitoring is a method used to confirm that the implemented security practices and controls are being adhered to and are effective. Security monitoring consists of activities such as the review of:

1. Automated intrusion detection system logs
2. Firewall logs
3. User account logs
4. Network scanning logs
5. Application logs
6. Data backup recovery logs
7. Help desk logs
8. Other logs and error files

The purpose of the Department's "Security Monitoring Policy" is to ensure that information resource security controls are in place, effective, and not being bypassed. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities. This early identification can help to block the wrongdoing or vulnerability before harm can be done, or at least to minimize the potential impact. Other benefits include: audit compliance, service level monitoring, performance measuring, limiting liability, and capacity planning.

85.02 Security Monitoring Policy

1. Automated tools will provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible, a security baseline will be developed, and the tools will report exceptions. These tools will be deployed to monitor:

a) Internet traffic

b) Electronic mail traffic

c) LAN traffic, protocols, and device inventory

d) Operating system security parameters

2. The following files will be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:

a) Automated intrusion detection system logs

b) Firewall logs

c) User account logs

d) Network scanning logs

e) System error logs

f) Application logs

g) Data backup and recovery logs

h) Help desk trouble tickets

i) Telephone activity – call detail reports

j) Network printer and fax logs

3. The following checks will be performed at least annually by assigned individuals:

a) Password complexity requirements based on current industry standards (within limits of the operating systems)

b) Unauthorized network devices

c) Unauthorized personal Web servers

d) Unsecured sharing of devices

e) Unauthorized modem use

f) Operating system and software licenses

4. Any security issues discovered will be reported to the CISO for follow-up investigation.

26.90.00 SERVER HARDENING

90.01 Purpose. Servers are depended upon to deliver data in a secure, reliable fashion. There must be assurance that data integrity, confidentiality and availability are maintained. One of the required steps to attain this assurance is to ensure that the servers are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service. The purpose of the Department's "Server Hardening Policy" is to describe the requirements for installing a new server in a secure fashion and maintaining the security and integrity of the server and application software.

90.02 Server Hardening Policy

1. A server must not be connected to the Department's network until it is in an ITD accredited secure state and the network connection is approved by the ITD Division Chief.

2. The server hardening procedures provide the detailed information required to harden a server and must be implemented for ITD accreditation. Some of the general steps included in the server hardening procedure include:

a) Installing the operating system from an ITD approved source.

b) Applying vendor supplied patches.

c) Removing unnecessary software, system services, and drivers.

d) Setting security parameters, file protections, and enabling audit logging.

e) Disabling or changing the password of default accounts.

3. ITD will monitor security issues, both internal to the Department and externally, and will manage the release of security patches on behalf of the Department.

4. ITD will test security patches against ITD core resources before release, where practical.

5. ITD may make hardware resources available for testing security patches in the case of special applications.

6. Security patches must be implemented by ITD within the specified timeframe by automated delivery such as System Management Server (SMS) or similar application.

26.95.00 SYSTEM DEVELOPMENT

95.01 Purpose. The number of application software errors and the resulting cost of business disruption and service restoration continues to escalate world-wide. The purpose of the Department's "System Development Policy" is to describe the requirements for developing and/or implementing new software for the Department.

95.02 System Development Policy

ITD is responsible for developing, maintaining, and participating in a System Development Life Cycle (SDLC) for the Department's system development projects. All software developed in-house which runs on production systems must be developed according to the SDLC. A typical SDLC includes design, development, quality assurance and acceptance testing, implementation, and maintenance. This methodology ensures that the software will be adequately documented and tested before it is used for critical Department information.

1. All production systems must have designated owners and custodians for the critical information they process. ITD must perform yearly risk assessments of production systems to determine whether the controls employed are adequate.

2. All production systems must have an access control system to restrict who can access the system as well as restrict the privileges available to these users. A designated access control administrator (who is not a regular user on the system in question) must be assigned for all production systems.

3. Where resources permit, there should be a separation between the production, development, and test environments. This will ensure that security is rigorously maintained for the production system, while the development and test environments can maximize productivity with fewer security restrictions. Where these distinctions have been established, development and test staff must not be permitted to have access to production systems. Likewise, all production software testing must utilize sanitized information.

4. All application-program-based access paths other than the formal user access paths must be deleted or disabled before software is moved into production.

5. All production systems must have a Service Level Agreement that specifies the levels of availability, serviceability, performance, operation, or other attributes.

26.100.00 VENDOR ACCESS

100.01 Purpose. Vendors play an important role in the support of hardware and software management, and operations for customers. Vendors authorized by the ITD Division Chief may remotely view, copy and modify data and audit logs, correct software and operating systems problems, monitor and fine tune system performance, monitor hardware performance and errors; modify environmental systems, and reset alarm thresholds. Setting limits and controls on what can be seen, copied, modified, and controlled by vendors will eliminate or reduce the risk of loss of data, loss of trust, and liability or embarrassment to the Department. The purpose of the Department's "Vendor Access Policy" is to establish the rules for vendor access to the Department's information resources and support services, vendor responsibilities, and protection of Department's information resources.

100.02 Vendor Access Policy

1. Vendors must comply with all applicable Department policies, practice standards and agreements, including, but not limited to:

a) Safety policies

b) Privacy policies

c) Security policies

d) Auditing policies

e) Software licensing policies

f) Acceptable use policies

2. Vendor agreements and contracts must specify:

a) The Department information that the vendor should have access to.

b) How Department information is to be protected by the vendor.

c) Acceptable methods for the return, destruction, or disposal of Department information in the vendor's possession at the end of the contract.

d) That the Vendor must only use Department information and information resources for the purpose of the business agreement.

e) That any other Department information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others.

3. The Department will provide an ITD point of contact for the vendor. The point of contact will work with the vendor to make certain the vendor is in compliance with these policies.

4. Each vendor must provide the Department with a list of all employees working on the contract. The list must be updated and provided to the Department within 24 hours of staff changes.

5. Each on-site vendor employee must acquire a Department identification badge that will be displayed at all times while on Department premises. The badge must be returned to the Department when the employee leaves the contract or at the end of the contract.

6. Each vendor employee with access to Department owned sensitive information must be cleared to handle that information.

7. Vendor personnel must report all security incidents directly to the appropriate Department personnel.

8. If vendor management is involved in Department security incident management, the responsibilities and details must be specified in the contract.

9. Vendor must follow all applicable Department change control processes and procedures.

10. Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate Department management.

11. All vendor maintenance equipment on the Department's network that connects to the outside world via the network, telephone line, or leased line, and all Department IR vendor accounts will remain disabled except when in use for authorized maintenance.

12. Vendor access must be uniquely identifiable and password management must comply with the Department's "Password Policy" and "Administrative and Special Access Policy." Vendor's major work activities must be entered into a log and available to Department management upon request. Logs must include, but are not limited to, such events as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.

13. Upon departure of a vendor employee from the contract for any reason, the vendor will ensure that all sensitive information is collected and returned to the Department or destroyed within 24 hours.

14. Upon termination of contract or at the request of the Department, the vendor will return or destroy all Department information and provide written certification of that return or destruction within 24 hours.

15. Upon termination of contract or at the request of the Department, the vendor must surrender all Department owned Identification badges, access cards, equipment, and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented and authorized by Department management.

16. Vendors are required to comply with all State and Department auditing requirements, including the auditing of the vendor's work.

17. All Department owned software used by the vendor in providing service to the Department must be properly inventoried and licensed.

26.105.00 INFORMATION RESOURCE SECURITY POLICY DEVELOPMENT AND MAINTENANCE

105.01 Purpose. The Department's information resource security policies provide the techniques and methodology to protect the Department's information resource assets. These security policies were developed by interpreting HIPAA, TAC 202 and other legislation and legal requirements, understanding business needs, evaluating existing technical implementations, and by considering the cultural environment. However, there will be valid reasons to develop and maintain the information resource security policies. For example, these security policies may be impacted by changing technology, threats, legislation, and business requirements. The purpose for the Department's "Policy for Developing and Maintaining the Information Resource Security Policies" is to explain why and how to create new and revise existing information security policies.

105.02 Policy for Developing and Maintaining the Information Resources Security Policies

The following policy explains why and how to change information security policies.

1. **Changing Environment.** The business, technical, cultural, and legal environment of the Department, as it relates to information technology use and security, is constantly changing. The information resource security policies will be revised as needed to comply with changes in law or administrative rules or to enhance its effectiveness.

2. **Technology Neutral.** The information resource security policies are technology neutral and apply to all aspects of information resources. It is possible however, that emerging technologies or new legislation could impact these policies in the future.

3. **Change Drivers.** A number of factors could result in the need or desire to change the information resource security policies. These factors include, but are not limited to:

a) Annual review of established policies

b) New legislation

c) Newly discovered security threat or vulnerability

d) New technology

e) Audit report

f) Business requirements

g) Cost/benefit analysis

h) Cultural change

4. **Ownership and Approval.** The information resource security policies are owned by the Department's Executive Director. This responsibility has been delegated to the Information Resource Manager (IRM). The Executive Director, IRM, or designate, is the only authority that can approve modifications to the information resource security policies.

5. **Change Process.** Updates to the Department's information resource security policies, which include establishing new policies, modifying existing policies, or removing policies, can result from three different processes:

a) At least annually, CISO, or designate, will review the information resource security policies for possible addition, revision, or deletion. An addition, revision, or deletion is created if it is deemed appropriate.

b) Every time new information resource technology is introduced into the Department a security assessment must be completed. The result of the security assessment could necessitate changes to the information resource security policies before the new technology is permitted for use at the Department.

c) Any user may propose the establishment, revision, or deletion of any practice standard at any time. These proposals should be directed to the CISO, who will evaluate the proposal and make recommendations to the IRM.

6. **Change Distribution and Notification.** Once a change to information resource security policies has been approved by the IRM, or designate, the following steps will be taken as appropriate to properly document and communicate the change:

a) The appropriate information resource Web pages will be updated with the change

b) Training and compliance materials will be updated to reflect the change

c) The changes will be communicated using standard communication methods such as interoffice memorandum or newsletters.

7. **Policy Exceptions.** Policy exception provisions provide a methodology used to document variations from the rules of the information resource security policies. Following are examples:

a) Allowing a desktop modem if the information resource security policies states desktop modems are not permitted

b) Giving an individual elevated privileges in comparison to another individual with similar responsibilities

The steps for permitting and documenting an exception are:

a) Any user of the Department's information resources may apply for an exception through their chain of command to the CISO.

b) A request for an exception is received by the CISO along with a business case for justifying the exception.

c) The CISO analyzes the request and the business case and determines if the exception should be accepted, denied, or if it requires more investigation.

d) If more investigation is required, the CISO and ITD technical staff determine if there is a cost-effective solution to the problem that does not require an exception.

e) If there is not an alternate cost-effective solution, and the risk is minimal, the exception may be granted. The CISO maintains a file of all exceptions granted.

f) Each exception must be re-examined annually.

g) Any exception request that is rejected may be appealed to the IRM.

26.110.00 EMAIL

110.01 Purpose. It is the policy of the Department to provide for the efficient, economical, and effective management of electronic mail records in accordance with Texas Administrative Code (TAC), Chapter 13, Sections 6.91-6.97 (State Agency Bulletin Number One, Electronic Records Standards and Procedures). TAC Chapter 13, Section 6.92(c), provides that "the agency head or designated records management officer must administer a program for the management of records created, received, retained, used or disposed on electronic media." The Department has adopted this "Email Policy" for that purpose; and to prescribe guidelines and procedures for the management of electronic mail consistent with the Electronic Records Standards and Procedures; and in the interest of cost-effective and efficient record-keeping, including long-term records retention for the Archives of the State. Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. This policy is established to achieve the following:

a) To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.

b) To establish prudent and acceptable practices regarding the use of email.

c) To educate individuals using email with respect to their responsibilities associated with such use.

The purpose of the Department's "Email Policy" is to establish the rules for the use of Department email for the sending, receiving, or storing of electronic mail. For more details, especially with regards to privacy, see 26.15.02 "Acceptable Use Policy" and 26.115.02 "Privacy" (Internet and Intranet).

110.02 Email Acceptable Use Policy

1. The following activities are prohibited by policy:

a) Sending email that is intimidating or harassing.

b) Using email for any personal monetary interests or gain.

c) Using email for purposes of political lobbying or campaigning.

d) Violating copyright laws by inappropriately distributing protected works.

e) Posing as anyone other than oneself when sending email, except when authorized to send messages for another when serving in an administrative support role.

f) The use of unauthorized email software.

2. Personal email should not impede the conduct of state business; only incidental amounts of employee time—time periods comparable to reasonable lunch and break periods during the day—should be used to attend to personal matters. Racist, sexist, threatening, or otherwise objectionable language is strictly prohibited. Email should not be used for any personal monetary interests or gain. Employees should not subscribe to mailing lists or mail services strictly for personal use. Personal email should not cause the state to incur a direct cost in addition to the general overhead of email. The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:

a) Sending or forwarding chain letters.

b) Sending unsolicited messages to large groups except as required to conduct agency business.

c) Sending excessively large messages.

d) Sending or forwarding email that is likely to contain computer viruses.

3. All sensitive Department material transmitted over any external network will be encrypted utilizing an encryption standard established by ITD.

4. All user activity on Department information resource assets is subject to logging and review.

5. Electronic mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the Department or any unit of the Department unless appropriately authorized (explicitly or implicitly) to do so. Individuals must not send, forward or receive confidential or sensitive Department information through non-Department email accounts. Examples of non-Department email accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, and email provided by other Internet Service Providers (ISP).

6. Individuals will send, forward, receive and/or store confidential or sensitive Department information only on mobile devices approved by the Department. Examples of mobile devices include, but are not limited to, Personal Data Assistants, two-way pagers, and cellular telephones.

7. Personal use of email is a privilege, not a right. Abuse of the privilege may result in appropriate disciplinary action. Employees need to keep in mind that all email is recorded and stored along with the source and destination. Management has the ability and right to view employees' email. Recorded email messages are the property of the Department and therefore the taxpayers of the State of Texas. Thus, they are subject to the requirements of the Texas Public Information Act and the laws applicable to State records retention. Employees should be aware that when sending an email message of a personal nature, there is always the danger of the employees' words being interpreted as official agency policy or opinion. Therefore, when an employee sends a personal email, especially if the content of the email could be interpreted as an official agency statement, the employee should use the following disclaimer at the end of the message:

"This email contains the thoughts and opinions of (employee name) and does not represent official Texas Department of Public Safety's policy."

If the content of the email contains sensitive or confidential information the employee may use the following message at the end of the message:

"This message contains information which is confidential. Unless you are the addressee (or authorized to receive for the addressee), you may not use, copy, or disclose to anyone the message or any information contained in the message. If you have received the message in error, please advise the sender by reply email and delete the message."

8. Retention Requirements: All email sent or received by the Department is considered a state record. Therefore, all email messages must be retained or disposed of according to the Department's retention schedule. The Department's approved retention schedule lists the record series that agency records may be categorized under and the retention period for each series. It is the content and function of an email message that determines the retention period for that message. Email systems must meet the retention requirements found in TAC 6.94(e). Email generally (but not always, see the Texas State Records Retention Schedule for more information) fall into several common record series categories. These are:

a) Administrative Correspondence, 1.1.007. Incoming/outgoing and internal correspondence, in any format, pertaining to the formulation, planning, implementation, interpretation, modification, or redefinition of the programs, services or projects of the Department and the administrative regulations, policies and procedures that govern them. Only the administrative correspondence of executive staff, Division Chiefs, program heads and board or commission members require archival review. Retention: 4 years.

b) General Correspondence, 1.1.008. Non-administrative incoming/outgoing and internal correspondence, in any media, pertaining to or arising from the routine operations of the policies, programs, services, or projects of the Department. Retention: 2 years.

c) Transitory Information, 1.1.057. Records of temporary usefulness that are not an integral part of a records series of the Department, that are not regularly filed within the Department's record-keeping system, and that are required only for a limited period of time for the completion of an action by an official or employee of the Department or in the preparation of an on-going records series. Transitory records are not essential to the fulfillment of statutory

obligations or to the documentation of Department functions. Examples of transitory information are routine messages (can be recorded on any medium, such as hard copy message slips or in an electronic format as voice mail); internal meeting notices; routing slips; incoming letters or memoranda of transmittal that add nothing of substance to enclosures; and similar routine information used for communication, but not for the documentation, of a specific Department's transaction. Retention: AC (after purpose of record has been fulfilled).

9. User Responsibilities: It is the responsibility of the user of the email system, with guidance and training from the Records Management Officer, to manage email messages according to the Department's retention schedule. It is the responsibility of the sender of email messages within the agency's email system and recipients of messages from outside the Department to retain the messages for the approved retention period. Names of sender, recipient, date/time, as well as any attachments must be retained with the message. Except for listserv mailing services, distribution lists must be able to identify the sender and recipient of the message.

Examples.

Example 1: DPS supervisor sends an email describing a new major regulatory enforcement policy to DPS employees. The DPS supervisor who sent the email is responsible for retaining the email according to the record retention schedule. For the DPS supervisor, the email is "administrative correspondence" with a retention period of four years. The email may be kept in an electronic format or printed out. The recipient of the email has received a copy of the email and should keep the email for as long as it is useful, but it is not the original record subject to the retention law and should not be kept longer than the retention period of the official record.

Example 2: DPS employee sends an email to co-workers arranging transportation to an in-service training program. The email does not need to be kept at all. It is "transitory information" and may be deleted immediately.

Example 3: DPS supervisor sends an email regarding work schedules and procedures for the coming month to employees. The DPS supervisor who sent the email is responsible for retaining the email according to the record retention schedule. For the DPS supervisor, the email is "general correspondence" with a retention period of 2 years. The email may be kept in electronic format or printed out. The recipient of the email has received a copy of the email and should keep the email for as long as it is useful, but it is not the original record that is subject to the retention law and should not be kept longer than the retention period of the official record.

Example 4: DPS supervisor receives an email from a member of the public that is general correspondence. The DPS supervisor who receives the email is responsible for retaining the email according to the record retention schedule for general correspondence.

10. Maintenance of Electronic Mail: Records created using an email system may be saved for their approved retention period by one of the following:

a) Print message and file in appropriate hard copy file.

b) Place in folders and save on personal network drive or C: drive.

c) Save to recordable media.

d) Transfer to an automated records management software application.

e) Managed at the server by an automated classification system.

11. Disposition of Electronic Mail: The process for the legal disposition of state records (including electronic mail) is subject to the same documentation requirements as any other format or medium. Agency personnel and RMLs should follow the same procedure in filling out a disposition log as with paper records to adequately document disposition and destruction of electronic records. See General Manual, Chapter 21.01.04 – Procedures (3) Final Disposition of Records. Section 6.95 of the Electronic Records Standards and Procedures (relating to the Final Disposition of Electronic State Records) states that:

a) b. "An electronic state record that is an archival record must be maintained by the agency through hardware and software migrations and upgrades as authentic evidence of the state's business in accessible and searchable form, except as otherwise determined by the state archivist."...And;

b) d. "A state agency must establish and implement procedures that address the disposition of an electronic mail record by staff in accordance with its approved records retention schedule and, specifically, must establish guidelines to enable staff to determine if an electronic mail record falls under transitory information (records series item number 1.1.057) on the agency's approved records retention schedule in order to encourage its prompt disposal after the purpose of the record has been fulfilled."...

12. Email standards for signature block and automatic reply message: An email signature is a block of text that is appended to the end of a sent email message. Generally, a signature block is used to provide the recipient with necessary contact information to include the sender's name, business contact information, or web site URL. An automatic reply is a message the user can have automatically sent out in response to every e-mail that comes into the account during a timeframe specified by the user.

All e-mail correspondence sent using the DPS system, sent both internally and externally, should be treated as an official form of communication and must present a professional image.

The signature block for any non-personal e-mails sent using the DPS system may only contain the sender's name, title, department or office, agency name, address, work phone and fax contact information, work email, link to agency website or other contact information regarding the agency and any necessary disclaimer language authorized under related policy.

Automatic Reply messages may only contain pertinent, work related information.

The signature block and Auto Reply messages may not include any of the following: background images, animations, emoticons (i.e. smiley faces, hearts, etc.), logos (sport team, product logos, etc.), graphics with the exception of approved DPS related insignias, personal contact information (i.e. personal phone numbers, personal email addresses or websites), quotes, sayings, or other superfluous language.

Example One: The following is an example of an acceptable e-mail signature block:

Author's name
Title (optional)
Department or office
Texas Department of Public Safety

Your address (optional)
Phone: (xxx) xxx-xxxx (optional)
FAX: (xxx) xxx-xxxx (optional)
Cell: (xxx) xxx-xxxx (optional)
www.dps.texas.gov (optional)

Example Two: The following is an example of an acceptable auto reply message:

> "I will be out of the office from December 23rd through January 2nd. If you need immediate assistance please contact my supervisor, Jane Doe, at (123)456-7890 or Jane.Doe@dps.texas.gov"

26.115.00 INTERNET AND INTRANET

115.01 Purpose. Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. The Department's "Internet and Intranet Policy" is established to achieve the following:

a) To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.

b) To establish prudent and acceptable practices regarding the use of the Internet.

c) To educate individuals who may use the Internet, the Intranet, or both with respect to their responsibilities associated with such use.

For more details, see 26.15.02 "Acceptable Use Policy" and 26.15.02 "Email Acceptable Use Policy."

115.02 Privacy. Electronic files created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of the Department are not private and may be accessed by Department employees at any time without knowledge of the information resource user or owner. Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards.

115.03 Internet and Intranet Acceptable Use Policy

1. All software used to access the Internet must be part of the Department's standard software suite or approved by the CISO. This software must incorporate all vendor provided security patches.

2. All files downloaded from the Internet must be scanned for viruses using the approved ITD distributed software suite and current virus detection software.

3. All software used to access the Internet must be configured to use the firewall http proxy server.

4. All sites accessed must comply with the Department's acceptable use policies. The Internet path record is the property of the Department and, therefore, the taxpayers of the State of Texas.

Employees should be mindful that information concerning Internet use may be subject to disclosure under public information laws.

5. All user activity on Department owned information resource assets is subject to logging and review. Employees need to keep in mind that all Internet usage is recorded and stored, along with the source and destination within the computer's cache and registry. Employees have no rights to privacy with regard to Internet use. Management has the ability and right to view employees' usage patterns and take action to assure that Department Internet resources are devoted to maintaining the highest levels of productivity.

6. Supervisors should work with employees to determine the appropriateness of using the Internet for professional activities and career development (written permission needed).

7. Each employee using the Internet must identify themselves honestly, accurately, and completely (including one's Department affiliation and function, where requested). However, criminal investigators, while performing assigned duties involved in a criminal investigation, are exempt from the identification requirement of this policy for security reasons.

8. Content on all Department websites must comply with the Department's acceptable use policies.

9. Divisions must make all public websites accessible and compliant with law and standards promulgated by the Department of Information Resources (DIR) and the World Wide Web Consortium. Each Division Chief will appoint a representative to review that Division's Web content every ninety days and provide any approved Web content changes to ITD for posting. In addition, the following policies govern all proposed changes to the Department's website:

a. All DPS employees (or contracted vendors) creating, making changes to, or requesting new or additional Web content, for both internal or external websites, must have their Division Chief's approval and will coordinate through the ITD Web team. Any approved changes to the Department's websites will be made by authorized ITD personnel only.

b. Any approved changes will conform to authorized design templates and programming standards approved by the ITD Division Chief.

c. All vendors contracted by the Department to create and maintain authorized Web pages will conform to established design templates and programming standards established by ITD and will make all public websites accessible and compliant with laws and standards promulgated by the DIR and the World Wide Web Consortium.

10. No offensive or harassing material may be made available via Department websites.

11. Business related purchases are subject to Department procurement rules.

12. No personal commercial advertising may be made available via Department websites.

13. Department Internet access may not be used for personal gain or non-Department personal solicitations.

14. No Department data will be made available via Department websites without ensuring that the material is available to only authorized individuals or groups.

15. All sensitive Department material transmitted over external network must be encrypted.

16. Users must be mindful that electronic files that are original records are subject to records retention rules just like paper documents.

17. The following addresses incidental use of Internet and Intranet.

a) Incidental personal use of Internet access is restricted to approved users; it does not extend to family members or other acquaintances.

b) Incidental use must not result in direct costs to the Department.

c) Incidental use must not interfere with the normal performance of an employee's work duties and will be defined by the employee's supervisor. Incidental use should not exceed a time period comparable to reasonable daily lunch and break times.

d) No files or documents may be sent or received that may cause legal liability for, or embarrassment to, the Department.

e) Storage of personal files and documents within the Department's information resources should be minimal.

f) All files and documents – including personal files and documents – are owned by the Department, may be subject to open records requests, and may be accessed in accordance with this policy.

g) Incidental personal use of Department resources is permitted but must not be excessive or inappropriate as determined solely by the Department. Inappropriate use includes hacking, pirating software, disrupting others' work activities, using Department resources for non-Department commercial activities, soliciting or distributing literature for outside entities, disclosing confidential information of the Department or third parties, sending inappropriate email, accessing inappropriate websites (such as those advocating hate or violence, posting or sharing any racist, sexist, threatening, illegal or otherwise objectionable material such as those containing sexually explicit material, gambling, or promoting illegal activities), or using Department resources in a way that violates Department policies contained in the General Manual or state law.

26.125.00 ELECTRONIC BACKUP

125.01 Purpose. Electronic backups are a business requirement to enable the recovery of data and applications in the case of events such as natural disasters, system disk drive failures, espionage, data entry errors, or system operations errors. The purpose of the Department's Backup/Disaster Recovery Plan Policy is to establish the rules for the backup and storage of electronic Department information.

125.02 Electronic Backup Policy

1. The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner.

2. The Department backup and recovery process for each system must be documented and periodically reviewed.

3. The vendor(s) providing offsite backup storage for the Department must be cleared to handle the Department's most sensitive classification category for the information stored.

4. Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally backup media must be protected in accordance with the Department's most sensitive classification category for the information stored.

5. An automated process must be implemented to verify the success of the Department's electronic information backup. Also, the automated process must have reports whose output

a) Describes the contents of any backup tape including the date(s) the system(s) was backed up and the retention period(s)

b) Lists the tape number(s) of any system for a particular backup date.

In the box with each set of offsite storage backup tapes will be a report listing the contents of each backup tape. ITD headquarters will keep a copy of this report until the tapes return to ITD for reuse.

6. Backups must be periodically tested to ensure that they are recoverable.

7. Signature cards held by the offsite backup storage vendor(s) for access to the Department's backup media must be reviewed annually or when an authorized individual leaves the Department.

8. Procedures between the Department and the offsite backup storage vendor(s) must be reviewed annually.

26.130.00 WIRELESS ACCESS

130.01 Purpose. Wireless access to the Department's network must be secured properly to deliver data in a secure, reliable fashion. There must be assurance that data integrity, confidentiality and availability are maintained. One of the required steps to attain this assurance is to ensure that all wireless access devices are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service. The ITD Division Chief will be responsible for implementing and maintaining the wireless access policy for the Department.

To ensure the technical coordination required to provide the best possible wireless network for the Department, ITD will be solely responsible for the deployment and management of 802.11 and related wireless standards access points on the Department's network. No other entity may deploy 802.11 or related wireless standards access points without authorization from the ITD Division Chief.

This policy provides the structure for a Department-wide solution for the implementation of wireless technology, which includes centralized determination of identity, authentication, and appropriate levels of security for access to and use of wireless technology.

Wireless in the Local Area Network using the IEEE 802.11 standard is a fast-emerging technology. Current 802.11 wireless technologies are by nature easy to deploy, but they must be very carefully planned, deployed, and managed in a centralized fashion to ensure basic functionality, maximum bandwidth, and a secure network.

Current 802.11 wireless technologies deploy a very low power signal in a frequency band divided into only three (3) non-overlapping channels. The primary purpose of these channels is not so much to provide separate networks, but to ensure that adjacent access points with slightly overlapping areas of coverage do not interfere with each other. In the normal case, it is necessary to use all three channels in an integrated fashion as a single unified network to achieve an optimal design. It is therefore not feasible to allow individuals to install their own access points without centralized coordination, due to the resulting signal interference and greatly degraded performance to the common wireless network.

The Wireless Policy provides guidelines regarding the following:

a) The central deployment by ITD of 802.11 and related wireless standards access points.

b) The provision of wireless service by ITD for the Department.

c) The management by ITD of 802.11 and related wireless standards access.

130.02 Wireless Access Policy

1. **ITD deployment of 802.11 and related wireless standards access points.** ITD will be solely responsible for the deployment and management of 802.11 and related wireless standards access points for the Department. No other entity may deploy 802.11 or related wireless standards wireless access points without approval from the ITD Division Chief.

2. **Provision of wireless service by ITD.** ITD will offer a standard wireless deployment plan that will meet the needs of most Department information resource users wishing to construct and operate wireless services. The ITD Division Chief will work with Division Chiefs to accommodate any special needs they may have within the technical constraints of the wireless technology, understanding that all requests may not be technically feasible.

3. **Management by ITD of 802.11 and related wireless standards access points.** ITD will ensure that all wireless services deployed by the Department will adhere to Department-wide standards for access control. ITD will manage the wireless spectrum in a manner that ensures the greatest interoperability and roaming ability for all information resource users wishing to use wireless technology, and, using the Enterprise Directory, will centralize the process of determining identity, authentication, and appropriate levels of security for access to and use of wireless technology. ITD reserves the right to minimize interference to the common wireless network, and will work with the Division Chiefs to reconfigure or shut down any Division's wireless networks that interfere with the common wireless network.

130.03 Procedures and Guidelines

1. ITD will advise the IT Board on wireless plans, deployment strategies, and management issues.

2. Any Division wishing to work with ITD to deploy wireless access must contact ITD by phoning the ITD Service Desk to begin the process. The purchase must be approved by the ITD Division Chief or designate to ensure the hardware and software meet Department standards.

3. In the case of existing wireless technology deployments that use the same or interfering spectrums, ITD will work with the Divisions in question to minimize interference to the common wireless network.

4. All sensitive data being transmitted across a wireless network should be encrypted.

26.135.00 INSTANT MESSAGING POLICY

1. Employees will not download/install any instant messaging software without specific authorization in writing from the Department's IRM or a Division Chief.

2. Employees authorized to use instant messaging technologies will not download any illegal and/or unauthorized copyrighted content. The IRM or Division Chief must approve in writing the use of instant messaging technology to download copyrighted material in writing. The Department must follow appropriate state and federal laws and guidelines when copying, storing, or transferring copyrighted material.

3. This policy applies to instant messaging used within the Department and instant messaging used conjointly with the Internet and does not supersede any state or federal laws, or any other agency policies regarding confidentiality, information dissemination, or standards of conduct.

4. Authorized state network users should keep in mind that all instant messaging can be recorded and stored along with the source and destination. Users have no right to privacy with regard to instant messaging. Management has the ability and right to view employees' instant messaging. Recorded instant messages are the property of the Department and may be subject to the requirements of the Texas Public Information Act and the laws applicable to state records retention.

5. Instant messaging is not authorized for personal use.

6. Generally instant messaging should be used only for legitimate state business; however, brief, and occasional instant messaging of a personal nature may be sent and received if the use complies with this policy.

7. Use of instant messaging is a privilege, not a right. As such, the privilege may be revoked at any time and for any reason. Abuse of the privilege may result in appropriate disciplinary action.

8. If authorized for usage on state systems, instant messaging may be used for any routine official business communication that is not normally filed for recordkeeping, such as a communication that is temporarily needed only for an employee to complete an action.

9. Do not use instant messaging to conduct any state business that would require the content to be saved as a state record. Instant messaging may not be used to document a statutory obligation or Department decision, and instant messaging should not be used when the resulting record would normally be retained for record keeping purposes.

10. Accessing, viewing, downloading, uploading, transmitting, printing, copying, posting, or sharing any racist, sexist, threatening, sexually explicit, obscene, or otherwise objectionable material (for example, a visual, textual, or auditory entity) is strictly prohibited.

26.140.00 PEER-TO-PEER FILE SHARING

140.01 Purpose. Peer-to-Peer File Sharing (P2P) programs can be used to share any type of electronic files. To accommodate these legitimate file downloads, the State of Texas does not ban P2P programs from its networks. However, the purpose of the Department's "Peer-to-Peer File Sharing Policy" is to avoid problems such as the following:

P2P programs is the primary channel for malware distribution. One of the primary misuses of P2P technology has been copying of commercial music, movies, and video games for personal enjoyment. These activities on state government systems generally violate the U.S. Copyright.

P2P file-sharing programs increase the connectivity between computers connected to a common P2P network. This heightened connectivity can expose computers to risks beyond those raised by other Internet activities. P2P programs also have a high incidence of being misconfigured to share more folders than the user originally intended. Because P2P file-sharing programs allow all types of electronic data sharing, every computer file in the shared space becomes accessible to every other user on the P2P network. A P2P user who chooses to share a folder containing a music collection may not be aware that he or she is also sharing every personal document that might be stored in the same location.

Viruses and worms can multiply on these P2P networks and enter into a user's computer through a P2P file sharing program. The vast majority of viruses, adware, and Spyware use P2P networks as a primary distribution network. Moreover, free P2P client software often includes adware and backdoors that can be exploited by malware and hackers.

140.02 Peer-to-Peer Policy.

1. Employees of the Department will not download, install, or use any P2P software on DPS computers, networks, or mobile devices (PDA) without specific written authorization from the Department's IRM.

2. Authorized P2P users will use P2P technologies for official state business only.

3. Authorized P2P users will be trained on P2P policy, monitoring, and enforcement.

4. State government computer systems or networks (as well as those operated by contractors on the government's behalf) must not be used to download illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of acceptable use policy, if done without permission of the copyright owner:

a) Copying and sharing images, music, movies, or other copyrighted material using P2P technology.

b) Making unlicensed copies of a CD or DVD for others.

c) Posting or plagiarizing copyrighted material.

d) Downloading any copyright-protected files which you have not already legally procured (for example, licensed copies of software, MP3s, movies).

5. Copyright law applies to a wide variety of works and covers much more than what is listed above.

26.145.00 PROJECT MANAGEMENT

145.01 Purpose. Information Technology project success is greatly enhanced when project management disciplines are used. The Department will use project management discipline when identifying and developing information resource solutions for the Department's initiatives.

The Department's project management process is administered by the Enterprise Project Management Office located in the Administration Division of the agency. Projects exceeding the minimum thresholds, as specified by the Texas Department of Information Resources (DIR), must comply with the additional requirements of the DIR Texas Project Delivery Framework (Framework). The DIR Framework requires executive sponsor and authorization by the director of the agency as well as additional project approval and reporting requirements.

To meet the standards required by the Department and DIR, ITD partners with the Enterprise Project Management Office to provide guidance for developing project management documentation. Request for project management assistance should be directed to the Enterprise Project Management Office.

Sometimes it becomes necessary or advantageous to have changes in the approved project requirements, schedule, or resources. Also, sometimes a vendor contract needs changing. These project change requests must follow the policies and procedures maintained by the Enterprise Project Management Office.

26.150.00 WORK REQUEST

150.01 Purpose. ITD is constantly performing tasks requested by the Department's Divisions. Tasks that are a direct response to a problem are governed by 26.155.02 "Problem Management Policy." Some tasks are routine tasks, not requiring work requests because the tasks are part of an established repeatable procedure, like an operator running a nightly job. Therefore, a "work request" pertains to a Division's requests for ITD work outside the scope of project management, problem management, and routine tasks.

Examples of work requests include:

a) An ad hoc report using an already implemented database

b) A technology refresh for ten workstations

The Department's "Work Request Policy" serves both the requesting Division and ITD by providing an automated methodology/tracking system that enables:

a) A Division designate to request ITD to perform a task involving information resources.

b) ITD management to assign the task to the person in ITD who will do the work

c) Authorized Department staff (including the requestor) to view the work request to determine to whom the work as been assigned, the estimated completion date, and whether the work has been completed.

150.02 Work Request Policy

Following are the ITD responsibilities:

1. Developing/publishing procedures for completing a work request.

2. Prioritizing work requests.

3. When a work request competes for the same resources as an enterprise project priority must be given to the enterprise project. If resource(s) are unavailable to work on the 'work request' ITD contacts the requestor and suggests that the requestor submit the request as a project request to the EPMO. Then, ITD management closes the uncompleted work request, indicating that it was uncompleted.

4. Providing potential alternatives or suggesting existing possibilities as a solution.

5. Recommending information resource solutions to meet the customer's business requirements.

6. Evaluating and providing resources to complete work requests.

7. Tracking the progress of open work requests.

8. Providing an automated method of tracking work requests.

9. Creating and maintaining documentation of applications developed by ITD.

10. Ensuring confidentiality and security of the customer's data.

11. Providing customer notification on completed work requests.

12. Requiring written authorization from the customer prior to making changes to the production environment.

Following are the Division Chief's designate(s) responsibilities:

1. Following the ITD procedures when initiating work requests.

2. Ensuring that the Division approves any work request submitted to ITD.

3. Submitting work requests using the on-line services ITD provides for work requests.

4. Identifying required output (reports), if any.

5. Participating in the design and testing of the requested task, if applicable.

6. Supplying data elements of the records, examples of reports, lists, and totals, if applicable.

26.155.00 PROBLEM MANAGEMENT

155.01 Purpose. Indications of information resource problems include outages, error messages, performance degradation, usability complaints, failure in procedures, unclear or missing procedures, wait states, missing or late output, poor quality output, erroneous output, undocumented messages, and customer questions/complaints. The purpose of the "Problem Management Policy" is to manage problems effectively and efficiently regarding the Department's information resources, so that each Division receives the level of service agreed upon in their Service Level Agreement (SLA) with ITD. Therefore, the Department's users can call the ITD 24-hour Service Desk to have their information resource problems immediately resolved, or escalated, tracked and resolved in an expeditious manner with an acceptable balance of risk, resource/service effectiveness, and minimal disruption to the user. Some of the most important objectives of the Problem Management Policy are:

a) Establish procedures that provide for the timely response to customer requests for information and assistance with problems.

b) Establish procedures that enable customers to report all problems easily and accurately.

155.02 Problem Management Policy

Following are the ITD responsibilities:

1. Staff a 24 x 7 ITD Service Desk to provide professional and courteous assistance to information resource problems and questions. The phone number is for 424-5432 for calls local to Austin and 1-866-866-7700 for toll-free calls. During business hours (7am to 5pm) the ITD Service Desk checks the e-mail address, Help Desk Issues.

2. Using appropriate methods, such as network monitoring, to determine information resource problems or potential problems before the users encounter the problems.

3. If a user's question/problem cannot be immediately resolved, ensure that sufficient data is logged into the Department's on-line problem software to define the problem, as well as to aid in cause determination, severity determination, escalation, notification, meaningful problem reporting, and statistical analysis.

4. ITD management must ensure that problems are handled with expedient escalation to relevant ITD staff, vendors, and contractors. ITD management must also ensure that timely notification is sent to the correct individuals and groups, both within and outside the Department.

Following are the Department's user responsibilities with regards to placing ITD Service Desk calls:

1. Identify yourself completely. Provide your first and last name, department, telephone number, location, and Access ID (ACID), for example, ab00088. Your information will be verified and entered into a problem tracking database so that your problem can be tracked to a satisfactory resolution.

2. Know as much as possible about the problem you are experiencing. The ITD Service Desk technician will ask you to provide information such as error messages, the operating system, and the software application (for example, Word, Excel, Access, CICS, and so forth).

3. Be prepared to assist the ITD Service Desk technician in basic troubleshooting. Be close to the computer screen or device to follow simple diagnostic steps. It is often possible to remedy problems over the phone, speeding up the resolution process for everyone.

4. The ITD Service Desk technician will work with you to help resolve your problem. If necessary, a problem ticket will be generated and referred to a specialist who will contact you. Your problem will be assigned a number. Please retain this number for future reference.

5. When requesting a password reset, ITD Service Desk technicians are required to speak to the owner of the account to verify personal information. If someone other than the owner (for example, supervisor, co-worker) calls, the technicians are instructed to not reset the password without authorization from the CISO. The CISO may choose to require written authorization from the user's Division Chief or a designate.

26.160.00 INFORMATION RESOURCE PROCUREMENT

160.01 Purpose. The Department has initiated an effort to implement information resource governance as a key component in the establishment of a Department enterprise architecture. Enterprise architecture is the organizing logic for business processes and information resource infrastructure reflecting the integration and standardization requirements of the Department's operating model. An enterprise architecture should respond to the need to align information resource investments with the Department's strategic plan. The primary purpose of creating an enterprise architecture is to ensure that business strategy and information resource investments are aligned. As such, enterprise architecture allows traceability from the business strategy down to the underlying technology.

160.02 Policy. To ensure compatibility with the Department's enterprise architecture and ensure compliance with all Department of Information Resources (DIR) rules and regulations, all information resource purchases, excluding those made by the purchasing card, will require the ITD tracking form be completed. The form and all associated purchasing documents will be reviewed and approved ITD personnel.

General Manual Chapter 26 Annex – Data Classification Standards				
General Information				
ORGANIZATION Texas Department of Public Safety				
Date Adopted XX/XX/XXXX				
Data Classification Levels	**Public**	**Sensitive**	**Confidential**	**Regulated**
Definition	A Data class used to label information that is collected and maintained by the Department and is subject to public release under the provisions of applicable state or federal law or legal agreement and is not Confidential.	A Data class used to label information that is collected and maintained by the Department that must be protected against unauthorized disclosure, except for public release under the provisions of applicable state or federal law or other legal agreements.	A Data class used to label information as defined in Texas Administration Code § 202.1 (5) that is collected and maintained by the Department that must be protected against unauthorized disclosure and is not subject to public disclosure under the provisions of applicable state or federal law or other legal agreement.	A Data class that requires the Department to implement specific privacy and security safeguards as mandated by the federal and state law.
Examples	Public Data may include but is not limited to the following examples: • Department publications • Press releases • Public web postings	Sensitive Data may include but is not limited to the following examples: • Employee Records • Gross Salary Information • PII	Confidential Data may include but is not limited to the following examples: • Computer Vulnerability Reports • Protected draft communications • Net salary information	Regulated Data may include but is not limited to the following examples: • Social Security numbers • Credit card data • Tax information
Security Controls				
Roles and Responsibilities	**Public**	**Sensitive**	**Confidential**	**Regulated**
Data Custodian	Ensure systems support access controls which enforce data classification	Ensure systems support access controls which enforce data classification	Ensure systems support access controls which enforce data classification	Ensure systems support access controls which enforce data classification
Data Owner	• Identify the classification level of data	• Identify the classification level of data	• Identify the classification level of data	• Identify the classification level of data

	• Review audit logs	• Review audit logs • Ensure Users are aware of data classification requirements	• Review audit logs • Ensure Users are aware of data classification requirements	• Review audit logs • Ensure Users are aware of data classification requirements
Information Security Officer	• Develop and maintain information security policies procedures, and guidelines • Provide guidance on data classifications	• Develop and maintain information security policies, procedures, and guidelines • Provide guidance on data classifications	• Develop and maintain information security policies, procedures, and guidelines • Provide guidance on data classifications	• Develop and maintain information security policies, procedures, and guidelines • Provide guidance on data classifications
Legal and/or Privacy Office (Public Information Officer)	• Develop and maintain privacy policies, procedures, and guidelines • Provide guidance on data classifications	• Develop and maintain information privacy policies, procedures, and guidelines • Provide guidance on data classifications	• Develop and maintain information privacy policies, procedures, and guidelines • Provide guidance on data classifications	• Develop and maintain information privacy policies, procedures, and guidelines • Provide guidance on data classifications
Users	N/A	• Identify, and Label where appropriate, Data • Properly Dispose of Data	• Identify, and Label where appropriate, Data • Properly Dispose of Data	• Identify, and Label where appropriate, Data • Properly Dispose of Data
Data Controls	**Public**	**Sensitive**	**Confidential**	**Regulated**
Marking	N/A	• Mark document and Metadata as such • Special handling instructions must be provided	• Mark document and Metadata as such • Special handling instructions must be provided • Each page of printed sheets • Front and back covers, and title page if bound	• Mark documents and meta data Sensitive or Confidential as necessary • Special handling instructions must be provided • Each page of printed sheets • Front and back covers, and title page if bound
Handling	N/A	N/A	Confidential data must only be given to those persons with	Confidential data must only be given to those persons with

			authorization and a need to know	authorization and a need to know
Duplication	N/A	Information to be duplicated for business purposes or in response to an "Open Records" request only	Personnel can duplicate confidential documents with Data Owners authorization	Personnel can duplicate confidential documents with Data Owners authorization
Mailing	N/A	N/A	N/A	• Confirmation of receipt required • May required double packaged delivery. Outside of the package is not marked. Inside paperwork is appropriately marked.
Storage of hardcopy	• Store in compliance with records retention policy	• Store in compliance with records retention policy • Documents should be locked up when not in use	• Store in compliance with records retention policy • Documents should be locked up when not in use	• Store a compliance with records retention policy • Documents should be locked up when not in use
Storage on fixed media	N/A	• Access is password controlled	• Access is password controlled • Encryption required	• Access is password controlled • Encryption required
Storage on removable media	N/A	Encryption required	Encryption required	Encryption required
Access Controls	**Public**	**Sensitive**	**Confidential**	**Regulated**
Granting Access Rights	No Restrictions	Data owner only	Data Owner only	Data Owner only
Read Access	• Data Owner defines permissions by User and role	• Data Owner defines permissions by User and role	• Information owner defines permissions by User and role • Access highly restricted or controlled	• Information owner defines permissions by User and role • Access highly restricted or controlled

Update Access	• Data Owner defines permissions by User and role	• Information owner defines permissions by User and role • Controls needed for processes and transactions that are susceptible to fraudulent or other unauthorized activities	• Data Owner defines permissions by User and role • Controls needed for processes and transactions that are susceptible to fraudulent or other unauthorized activities	• Information owner defines permissions by User and role • Controls needed for processes and transactions that are susceptible to fraudulent or other unauthorized activities
Delete Access	• Data Owner defines permissions by User and role	• Data Owner defines permissions by User and role	• Data Owner defines permission by User and role • Controls needed for processes and transactions that are susceptible to fraudulent or other unauthorized activities	• Information owner defines permissions by User and role • Controls needed for processes and transactions that are susceptible to fraudulent or other unauthorized activities
Transmission Controls	**Public**	**Sensitive**	**Confidential**	**Regulated**
Print Controls	No restrictions	Data Owner define permissions	Output routed to pre-defined printer and monitored, or secure printing enabled	Output routed to pre-defined printer and monitored, or secure printing enabled
Transmission by public network	No restrictions	Encryption Recommended	Encryption Required	Encryption Required
Release to Third Parties	No restrictions	No restrictions	Data Owner Approval and Non-Disclosure Agreement	Data Owner Approval and Non-Disclosure Agreement
Audit Controls	**Public**	**Sensitive**	**Confidential**	**Regulated**
Tracking Process by Log	N/A	N/A	Recipients, Copies Made, Locations, Addresses, Those Who Viewed, and Destruction	Recipients, Copies Made, Locations, Addresses, Those Who Viewed, and Destruction

Auditing access activity	N/A	IT system should be configured to log all violation attempts. Audit trails should be maintained to provide for accountability of modifications to information resources and for all changes to automated security and access rules	IT system should be configured to log all violation attempts. Audit trails should be maintained to provide for accountability of modifications to information resources and for all changes to automated security and access rules	IT system should be configured to log all violation attempts. Audit trails should be maintained for accountability of modifications to information resources and for all changes to automated security and access rules
Retention criteria for Access Reports	Logs must be retained in accordance with records retention guidelines	Logs must be retained in accordance with records retention guidelines	Logs must be retained in accordance with records retention guidelines	Logs must be retained in accordance with records retention guidelines
Retention criteria for Access Reports	N/A	The Data Owner determines retention of violation logs	Data Owner determines retention of violation logs	Data Owner determines retention of violation logs
Classification review cycle timeframe	Review and affirm date must be set but flexible	Review and affirm date must be set but flexible	Data Owner must review and affirm all info classification and User rights, not to exceed 1 year	Data Owner must review and affirm all info classification and User rights, not to exceed 1 year
Encryption Controls	**Public**	**Sensitive**	**Confidential**	**Regulated**
Data in storage on premises	N/A	N/A	N/A	Encryption per regulation requirements
Data in storage off premises	N/A	Encryption required	Encryption required	Encryption per regulation requirements
Data in internal transmission	N/A	Encryption recommended	Encryption required	Encryption per regulation requirements
Data in external transmission	N/A	Encryption required	Encryption required	Encryption per regulation requirements
Data in Removable Media Devices	N/A	Encryption required	Encryption required	Encryption per regulation requirements