Kansas
Office of the Governor
Office of Information Technology Services

POLICY AND PROCEDURE MEMORANDUM
9209.00

EFFECTIVE DATE
12/1/2014

REVIEW DATE
12/2015

1. SUBJECT: Information Security Policies, Procedures and Baselines

2. DISTRIBUTION: OITS Central Office

3. FROM: _____
Jim Clark, Secretary of Administration (Interim Chief Information Technology Officer)

4. PURPOSE: To provide detailed instruction on the implementation of information security.

5. OVERVIEW:

5.1. These procedures represent the requirements of the organization in securing the organization's computing resources and information assets. Whether it is held in hardcopy or softcopy, independently developed or provided by third parties, an information asset is any organized piece of information that is valuable to an organization.

5.2. Information assets shall be given a level of protection commensurate with its value. Measures must be taken by all to protect information from unauthorized modification, destruction, or disclosure, whether accidental or intentional, as well as to assure its confidentiality, integrity, and availability.

5.3. Organization computing resources are defined as network connectivity devices, IT Security infrastructure devices, server hardware, workstations, and mobile computing devices, as well as operating systems and application software owned, or leased by the organization.

5.4. Employees may not use organization facilities and connections to make unauthorized connections to, break into, or adversely affect the performance of other computer systems on any network. Employees shall not "test the doors" or "probe" security mechanisms at either the organization or other Internet sites unless permission is obtained first.

5.5. An information system is a functionally related group of interrelated elements working together to present a desired output, through careful definition of access and utilization permissions associated with each information system, and through judicious application of those permissions, unauthorized usage, whether intentional or unintentional, from legitimate or illegitimate users can be controlled, reduced and eliminated. The control, reduction and elimination of unauthorized usage will benefit the organization and its employees in several ways:

5.6. It will ensure that privileged information stays privileged. Protection of privileged information lessens the organizations exposure to lawsuits and other potentially damaging actions.

5.7. It ensures that information resources are always available for their intended purpose, and reduces the risk of compromise.

6. AUDIENCE AND APPLICABILITY:

6.1. This document has been written to address employees, as well as clients, partners of the organization and third parties with whom the organization may work from time-to-time. All users of information systems are required to comply with the portions of this document that are directly related to their role.

6.2. The requirements established in document are deemed to always be in effect and as such apply whether an information system user is conducting organization business internally or at an external location, (e.g. partner's location, home office etc.). Further, it applies equally to information systems that are owned and operated exclusively by the organization, or by third parties on behalf of the organization.

7. REVISION:

7.1. This document has been created to represent the security needs of the organizations information systems as they currently stand. Given that these needs are likely to change and/or grow over time; these requirements shall be appended to and updated according to the following schedule.

7.2. This document will be benchmarked against the organizational security infrastructure and operational requirements on an as needed basis, at a maximum interval of three years.

7.3. This document will be reviewed against organizational security requirements and industry standard best practices on an as needed basis, at a maximum interval of three years.

7.4. This document will be updated as per the output of the above procedures on an as needed basis, coinciding with the completion of either process.

8. ROLES AND RESPONSIBILITIES:

8.1. Chief Executive. The Chief Executive of each organization is responsible for operations, including as a subset, all IT operations for their organization. As such final and ultimate responsibility for ensuring adherence to all aspects of IT security requirements within a given organization lies with the Chief Executive of that organization.

8.2. Chief Information Technology Officer. The Chief Information Technology Officer (CITO) is responsible for all aspects of IT infrastructure and operations for the State. As such, final and ultimate responsibility for IT security, and thus for the implementation of and adherence to the requirements in this document, rests with the CITO though on-going management is delegated to the Chief Information Security Officer who acts on behalf of the CITO.

8.3. Chief Information Security Officer. The State Chief Information Security Officer (CISO) acts on behalf of the State CITO and is responsible for the development, distribution, maintenance and administration of all State level information security policies and procedures. The State CISO is also responsible for ensuring that these information security requirements are adhered to for all information systems that are owned or operated on behalf of the State of Kansas as a whole. Finally, the State CISO is also responsible for ensuring that these information security policies are adhered to for all information systems that are owned or operated on behalf of state agencies where those state agencies have no Information Security Officer.

8.4. Chief Information Officer. The Chief Information Officer (CIO) is responsible for all aspects of IT infrastructure and operations for the organization. The CIO is also responsible for IT planning, budgeting, and performance, including its information security components.

8.5. Information Security Officer. The information security officer must understand the nature and purpose of an organization’s various functions in order to ensure that appropriate and effective governance structures are developed. All decisions regarding the implementation of the security program should be the result of well-grounded organizational decisions. It is the role of the information security manager to identify and explain to stakeholders the risk to the organization’s information, present alternatives for mitigation, and then implement an approach supported by the organization.

8.6. Security Steering Committee. To some extent, security affects all aspects of an organization. To ensure that all stakeholders impacted by security considerations are involved, the steering committee shall be comprised of the organization ISO and senior representatives of affected groups. This facilitates achieving consensus on priorities and tradeoffs. It also serves as an effective communications channel and provides an ongoing basis for ensuring the alignment of the security program with business objectives.

8.7. Security Steering Committee. To some extent, security affects all aspects of an organization. To ensure that all stakeholders impacted by security considerations are involved, the steering committee shall be comprised of the organization ISO and senior representatives of affected groups. This facilitates

achieving consensus on priorities and tradeoffs. It also serves as an effective communications channel and provides an ongoing basis for ensuring the alignment of the security program with business objectives.

8.8. 8.7System and Network Administrators. Systems and Network Administrators are responsible for implementing, administering, managing and, where required, monitoring information systems of organization in accordance with the requirements of this SOP.

8.9. Database Administrators. Database Administrators are responsible for implementing, administering, managing and, where required, monitoring the databases and other structured data repositories of the organization in accordance with the requirements of this SOP.

8.10. Application and Systems Developers. Application and Systems Developers are responsible for implementing, administering, managing and, where required, monitoring in-house or custom developed software elements of information systems of the organization in accordance with the requirements of this SOP.

8.11. Data Owners and Custodians. Data Owners are responsible for the collection and protection of organization data. To achieve this, Data Owners review all information access requests and permissions as well establish data classification and retention requirements. Data Custodians work on behalf of Data Owners and are responsible for the implementation and ongoing operation of the data specific safeguards specified by the Data Owner.

8.12. Auditors. Whether organization employees or third parties, auditors are responsible for evaluating compliance. To achieve this evaluation they are to be provided full access to all facilities, personnel, information systems and records; access, actions and results shall be monitored and documented. Where applicable, auditors shall be accompanied by personnel with appropriate access for the given audit.

8.13. Human Resources. Human Resources (HR) is responsible for the administration of all personnel security requirements of this SOP. These tasks entail ensuring that roles are provided with appropriate descriptions and categorizations, that personnel hires, transfers and terminations are conducted according to SOP (including background checks), that signed forms of cyber security awareness training, access and acceptance are filed, and that appropriate sanctions are levied in the event of a violation.

8.14. Facilities Management. Facility activities play a key role in the loss or damage to operational capabilities caused be problems with premises, facilities, services or equipment.

8.15. Procurement/Acquisitions. Procurement processes have consequences for information security in terms of their role in product acquisitions. If information security is not formally addressed in the process, vulnerabilities may be introduced as a result of new equipment or services acquisitions.

8.16. Information System Users. Information System Users are responsible for performing their jobs in accordance with this SOP, and any other relevant regulatory or specific policy or procedure.

9. POLICY

9.1. Assessment and Security Planning

9.1.1. Risk and Privacy Assessment

9.1.1.1. Risk and privacy assessments are used to determine the likelihood and magnitude of harm that could come to an information system in the event of a security breach. By determining the amount of risk that exists, the organization will be in a better position to determine how much of that risk should be mitigated and what controls should be used to achieve that mitigation. Without risk and privacy assessments the potential exists that the organization might use inappropriate (either too strict or too lax) security controls to protect information systems.

9.1.1.2. Both risk and privacy assessments shall be performed for all information systems. These assessments shall address unauthorized access, use, disclosure, audit, disruption, modification and/or destruction of information or the information system itself. Further, the assessments shall identify known potential threats, the likelihood of their occurrence and the magnitude of the impact of those threats should they occur.

9.1.1.3. Both risk and privacy assessments shall be performed prior to the initial acquisition of an information system (in the event that the information system is owned/operated by the organization) or prior to initial establishment of service agreements (in the event that the information system is owned/operated by a third party on behalf of the organization). Further, risk and privacy assessments for information systems processing or storing sensitive information (PII, PHI, FTI, etc.) shall be reviewed and updated annually or whenever a significant change is made to the information system, whichever comes first. For information systems that do not process or store sensitive information, risk and privacy assessments shall be reviewed and updated every three years or whenever a significant change is made to the information system, whichever comes first.

9.1.2. Security Plan

9.1.2.1. A security plan shall be developed and implemented that includes provisions for each information system. For the purpose of the security plan, an information system is defined as a functionally related group of interrelated elements working together to present a desired output. This plan will indicate the current security stance of each information system, the intended security stance of each information system, and the steps that need to be taken to achieve this intent.

9.1.2.2. Security plans allow organizations to establish their intent regarding the on-going maintenance and/or improvement of security controls to ensure that security is always given appropriate credence in day to day operations. Without security plans the potential exists that security controls are not kept current with the protection requirements of the organization.

9.1.2.3. Security plans shall address modifications or updates to controls that are already in place as well the implementation of others. Further, it shall identify the planning process, the individuals charged with the responsibility of the planning process (including contact information) and the rationale for the planned security controls. Security plans shall be reviewed and, where required, updated on at least an annual basis or when any significant change occurs, whichever comes first.

9.1.2.4. As an addendum, where security audit and vulnerability analyses determine that deficiencies or other flaws exist in the security configuration of any information system, the security plan shall be updated immediately to include provisions for correcting these flaws and the plan shall be reviewed and, where required, updated on at least a quarterly basis until remediated or resolved.

9.2. Awareness and Training

9.2.1. Security Awareness Training

9.2.1.1. Security Awareness Training shall be conducted for all internal users (including third parties working as employees) of information systems. This training will address the purpose of IT security, the risks of failing to provide appropriate IT security as well as the manner in which information system users can uphold and enforce appropriate IT security measures.

9.2.1.2. Security awareness training ensures that users of information systems understand the security implications of their actions and increases the likelihood that information system security will not be breached, either intentionally or unintentionally, through technical measures (such as hacking) or non-technical measures (such as Social Engineering). Without such training information systems users have an increased likelihood of breaching security and have lower

individual culpability should they breach security.

9.2.1.3. All employees are required to participate in security awareness training within 90 days of hire and thereafter on an at least an annual basis. Upon completion of security awareness training all employees will be required to sign a declaration that they have completed the training, understand the purpose of the training, understand the specific procedures taught, and that they intend to abide by all applicable security policies. That signed declaration shall be filed with the Human Resources department.

9.2.1.4. The security awareness training program will be reviewed and, where required, updated on at least an annual basis. This work will ensure that program materials have the greatest level of on-going relevance with regard to the IT security requirements.

9.2.2. Security Operations Training

9.2.2.1. Security Operations Training shall be conducted for all systems and network administrators (including third parties working as employees) of information systems. This training will address the secure operation of information systems (or components of information systems) for which the employee is an administrator.

9.2.2.2. Secure operations training ensures that administrators of information systems understand the security requirements of the information systems as well as the manner in which those security requirements should be implemented and maintained. Without such training information systems have an increased likelihood of breach.

9.2.2.3. All employees that work as administrators or hold other positions with significant and relevant security operations responsibilities are required to participate in security operations training within 90 days of starting work or the deployment of a new or significantly updated/revised information system and thereafter on at least annual basis.

9.2.3. The security operations training program and accompanying materials will be reviewed and, where required, updated on at least an annual basis. This work will ensure that program and accompanying materials have the greatest level of on-going relevance with regards to IT security requirements. This review will occur prior to annual security operations training to ensure the training provided is always as current as possible.

9.3. Access Control

9.3.1. Account Management

9.3.1.1. All information system accounts shall be actively managed by appropriate administrative staff. Active management includes the acts of establishing, activating, modifying, disabling, removing, and auditing accounts from information systems.

9.3.1.2. Information system accounts are the only legitimate method by which information systems may be accessed. Without active account management, the potential exists that legitimate users can use these accounts for illegitimate purposes. Additionally, the potential exists that these accounts can be usurped and used illegitimately to access information systems.

9.3.1.3. Information system accounts are to be constructed such that they enforce the most restrictive set of rights/privileges or accesses required for the performance of tasks associated with that account. Further, to ensure separation of duties accounts shall be created such that no-one account can authorize, perform, review and audit a single transaction to eliminate conflicts of interest.

9.3.1.4. Information system accounts are to be reviewed to identify accounts with inappropriate privileges (either too high or too low) on at least an annual basis. Should information system accounts be discovered with inappropriate privileges those privileges will be manually reset to an appropriate level.

9.3.1.5. Information systems accounts are to be reviewed to identify inactive accounts. Should information system accounts that are associated with an employee or third party be discovered that have been inactive for a significant period of time, the owners of the account will be notified of pending disablement. Should the account continue to remain inactive it will be manually disabled. Inactive accounts that are not associated with an employee or third party but are associated with a system process (such as inter-system information transfer) that has been explicitly logged will not be disabled but will be reviewed on an annual basis. Inactive accounts that are not associated with employees, third parties, or system processes (including those that have not been explicitly logged) will be manually disabled.

9.3.1.6. Login attempts to information systems will be restricted such that after a set number of failed attempts within a pre-defined period of time, they will be locked out. Lockout may be automatically lifted after a pre-defined period of time or may be manually lifted through a pre-defined process.

9.3.2. Identification & Authentication (Access Enforcement)

9.3.2.1. All approved information system users must be given authorization to access information systems, and must be uniquely identified within those information systems and must present some form of acceptable identity authentication to be allowed to use any information system that houses controlled or privileged information.

9.3.2.2. The use of authorization, identification and authentication controls ensures that only known users make use of the information system. Without authorization, identification and authentication controls, the potential exists that information systems could be accessed illicitly and the confidentiality, integrity and availability of those information systems be compromised.

9.3.2.3. Prior to being granted access to an information system, users must be provided with formal authorization by an appropriate official (i.e., the owner of the information system, the custodian of the data housed within the information system or a designee of these individuals). This authorization will be based on definitive and verifiable identification of the user. Further, this authorization will be logged by the authorizing official and shared with systems and user management departments of the body that employs that user.

9.3.2.4. Once authorization has been granted, the user will be provided with a unique information system identifier. Examples of identifiers include user ids and smart cards. This identifier will be delivered to the authorized user in such a manner as to ensure that it is received only by the authorized user. Additionally, the user will be provided with a unique information system authenticator that is tied to the assigned identifier. Examples of authenticators include passwords, tokens and certificates. This authenticator will also be delivered to the authorized user in such a manner as to ensure that it is received only by the authorized user. Authentication must be cryptographically protected when stored, the solution that provides this functionality must meet the minimum specifications of FIPS 140-2.

9.3.2.5. Should an information system user’s account be disabled for any the users identifier and authenticator will also be disabled, where applicable.

9.3.2.5.1. Passwords

9.3.2.5.1.1. Passwords form the primary means of authentication. To ensure that passwords present as much security as possible, the following restrictions apply to them:

9.3.2.5.1.1.1. Passwords shall be constructed according to set requirements.

9.3.2.5.1.1.2. Passwords shall have both minimum and maximum lifespan.

9.3.2.5.1.1.3. Passwords shall not be reused for a set number of generations.

9.3.2.5.1.1.4. Passwords shall not be displayed while they are being entered.

9.3.2.5.1.1.5. Passwords shall not be transmitted in clear text.

9.3.2.5.1.1.6. Passwords shall be individually owned and kept confidential – they are not to be shared.

9.3.2.5.1.1.7. If passwords must be electronically stored, they shall not be stored in clear text.

9.3.2.5.2. Authentication Tokens

9.3.2.5.2.1. In cases where authentication tokens are used, the following restrictions apply:

9.3.2.5.2.1.1. A defined documented process must be followed for token distribution.

9.3.2.5.2.1.2. A defined documented process must be followed for token revocation.

9.3.2.5.2.1.3. A defined documented process must be followed for the handling of lost/stolen/damaged tokens.

9.3.2.5.3. Where biometric data is used for authentication:

9.3.2.5.3.1. A defined process must be followed for capturing user biometric data

9.3.2.5.3.2. A defined process must be followed for biometric revocation

9.3.2.5.3.3. A defined process must be followed for the handling of user biometric data.

9.3.3. Session Management

9.3.3.1. All communications sessions with information systems shall be both authenticated and actively managed by administrative staff. Active management includes the acts of monitoring, suspending, disabling and terminating communications to and from information systems.

9.3.3.2. Communications between components of information systems or between information systems themselves involve the transmission of information making that information susceptible to attack. Without session management, the potential exists that communications can be established or used illegitimately thereby exposing information to an increased likelihood of loss or corruption.

9.3.3.3. All information systems shall display a system use notification that indicates that the user is accessing an organization information system; that system usage is monitored, recorded and subject to audit; that unauthorized use is prohibited and subject to punitive action; that use of the information system implies consent to these controls. The system use notification will also indicate appropriate security and privacy notices. Finally this notification will be displayed until the user acknowledges it prior to completing authenticated system access.

9.3.3.4. Remote access to information systems will be strictly controlled. These controls include previous authorization of remote access privileges and the use of encrypted communications sessions. Further, all sessions must be actively monitored and must pass through managed access points. Finally, remote access is only to be used to execute privileged functions where sufficient rationale can be provided and such access will be preapproved and documented in the organization security plan.

9.3.3.5. All information systems shall impose restrictions on open sessions that are inactive for a pre-defined period of time. If the open session is established internally, the session will be locked until the session is re-authenticated. If the open session is established remotely the session will be terminated. These restrictions apply only to user accounts and not to system accounts used for inter-system communications.

9.3.3.6. All information systems shall positively and definitively identify and authenticate devices that

participate in inter-system communications prior to establishing a network connection. Appropriate authentication methods include the use of shared known information (such as MAC or TCP/IP addresses) or a defined authentication solution (such as 802.11x, EAP or Radius).

9.3.3.7. Information systems external to the control of the organization may not establish communication or access information systems unless the security controls of the third-party information system can be verified to meet the organizational security requirements. Additionally, connection agreements must be in place with the third-party host of the external information system and all communications will be both encrypted and actively monitored. Further, all such remote access to information systems must pass through defined and controlled access points. Finally information systems external to the control of the organization shall not be used for systems administration or other privileged functions without compelling reasons (such as during contingency operations) that have been documented and accepted by the organization.

9.4. Systems Configuration

9.4.1. Configuration Management

9.4.1.1. All information systems and all components of information systems shall be configured according to pre-defined, standardized configuration settings.

9.4.1.2. Standardized configuration settings allow information systems and information system components to be consistently deployed in an efficient and secure manner. Without standardized configuration settings the potential exists that information systems or information system components may be deployed that fail to meet the security requirements and may compromise the security requirements of other information systems with which they interconnect.

9.4.1.3. Systems Configuration

9.4.1.3.1. A standardized configuration will be established and maintained for all information systems and for all information system components. These baselines will indicate the specifications of information system component elements (hardware, firmware, and software), their relationship as well as the relationship of information system components, and their ownership. These baselines will be constructed such that information systems provide only essential capabilities. To achieve this, information systems must be configured for a singular purpose where possible and baselines will be reviewed and where necessary, updated on an at least annual basis.

9.4.1.3.2. Information systems will be configured according to these standards for the purpose of protecting the integrity and availability of information and applications.

9.4.1.3.3. Additionally, information systems will be configured to enforce user access restrictions. Supplemental and more restrictive controls will be used to restrict administrative access to operational and security settings, configurations and data.

9.4.1.3.4. An asset inventory of information system component elements (such as individual pieces of hardware, and software) will be maintained. This inventory will be structured such that it is searchable by both individual element and entire information system for contingency planning and operations purposes. The inventory is to be immediately updated whenever a new information system, information system component or information system component element is implemented or when an old one is retired. The asset inventory is to be reviewed and, where necessary, updated at least annually.

9.4.1.3.5. Each information system is to be provided a complete set of documentation. This documentation shall include, at a minimum, administrator and user guides for each information system component element as well as guides to the functional properties of integrated security controls. These security control guides must be detailed enough to allow for testing of the security controls.

9.4.1.4. Network Configuration

9.4.1.4.1. Information flow between information systems or components of information systems is restricted through the use of Access Control Lists, filtering and other mechanisms. Further, the authenticity of communications between information systems or information system components will make use of certificates, encryption and other mechanisms.

9.4.1.4.2. The information system that provides DNS will provide authenticated responses to requests for name resolution. These authenticated responses will be accompanied by origin and integrity artifacts (such as certificates and digital signatures). Further the information system that provides DNS will be configured for maximum fault tolerance including the use of fully redundant information system components and information system component elements.

9.4.1.4.3. Wireless networks connecting to internal networks will be restricted and may only be used where documented appropriate authorization has first been provided. Wireless networks connecting to internal networks will be actively monitored and access will be strictly controlled.

9.4.1.4.4. VoIP systems will be restricted and may only be used where documented appropriate authorization has first been provided. VoIP systems will be actively monitored and access will be strictly controlled.

9.4.1.5. Other Systems Configurations

9.4.1.5.1. The use of mobile and portable computing devices (PDA's, smart phones, cell phones, etc.) will be restricted and may only occur where documented appropriate authorization has first been provided. Where possible, the use of these devices will be actively monitored and their access to information systems strictly controlled.

9.4.1.5.2. Collaborative computing infrastructure, such as video and teleconferencing systems, will be configured so that they prohibit remote activation. Further, when these systems are in an active state (capable of receiving or transmitting information) they must provide explicit indication of that active state to local users. Examples of explicit indication include audible tones or visible "on" lights.

9.4.1.6. Change Control

9.4.1.6.1. Any change to information systems must be authorized, documented and performed in a controlled manner. They may only be made by appropriate administrative personnel that have approved access privileges.

9.4.1.6.2. Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to information systems, including upgrades and modifications.

9.4.1.6.3. All proposed information system changes will be assessed for their potential security impact prior to being made. If the security impact increases the risk that must be accepted, the changes must be revised or alternate security mitigation controls put in place prior to the change being made. After the change has been made the information system that was changed will be actively monitored for a pre-defined period of time to ensure that security has not been compromised.

9.4.2. Systems Protection.

9.4.2.1. All information systems and all components of information systems, whether they are for the exclusive internal use or publicly available, shall be protected by dedicated protection mechanisms. These requirements are equally applicable to information systems owned by the organization as well as those owned by third parties through which services are provided to the organization.

9.4.2.2. Dedicated protection mechanisms allow information systems to be provided a greater level of security than can be achieved through configuration control alone by delivering enhanced security capabilities. Without dedicated protection mechanisms the potential exists that security vulnerabilities that cannot be

mitigated by the capabilities inherent in the organization's information systems will be exploited leading to compromise of information system confidentiality, integrity and availability.

9.4.2.3. Gateway/Boundary Protection Systems

9.4.2.3.1. As limited a number of network access points as possible will be used to connect to external networks such as the Internet. Each of these network access points will be protected by boundary protection systems (generally a firewall) that monitor and control communications. These systems will be configured to deny communications by rule and allow by exception, to prevent public access to internal networks and to place controls on publicly accessible systems.

9.4.2.3.2. Where possible boundary protection systems will be configured to protect against or limit the effects of all denial of service attacks.

9.4.2.3.3. Boundary protection systems are to be deployed internally to create zones of security within the network for network segments that host information systems that are deemed to be of a critical or sensitive nature. These zones will be used wherever segmented networks are deployed.

9.4.2.4. Malware Protection Systems

9.4.2.4.1. All individual computing devices or information systems and components of information systems will be protected by malware protection systems where such solutions exist for the information system or information system component. At a minimum malware protection will be performed at the network boundary, on e-mail and other communications systems, and on all workstations, servers and other endpoints.

9.4.2.4.2. By definition, malware includes viruses, worms, spyware, adware, Trojan Horses and any other unwanted and deleterious software that may be installed on an information system component element as well as spam and other unsolicited communications.

9.4.2.5. Monitoring and Intrusion Detection and Prevention Systems

9.4.2.5.1. Each boundary (Internet) network access point will be protected by monitoring and/or intrusion detection or prevention systems that monitor events detects attacks and provides identification of unauthorized information system use. These systems will be configured to monitor both inbound and outbound communications.

9.4.2.5.2. Monitoring and intrusion detection and prevention systems may also be deployed internally to create zones of security within the network.

9.4.3. Data/Media Protection

9.4.3.1. All privileged information, whether stored in system or out of system (via information media) must be protected by data and media protection mechanisms to ensure the highest levels of confidentiality, integrity and availability. Non-privileged information will be protected to ensure the highest levels of integrity and availability.

9.4.3.2. Data and media protection mechanisms allow information to be provided a greater level of security than can be achieved with system based protection mechanisms alone. Without data and media protection mechanisms the potential exists that information assets could be exposed to an unnecessarily high level of risk, particularly in circumstances where that information is taken out of the information system.

9.4.3.3. Where data requires encryption, that encryption must be performed using a solution that meets established data standards. Further, where public key certificates are used they shall be issued by an internal certificate authority that has been cross-certified with an approved third party provider or be acquired directly from an approved third party provider.

9.4.3.4. Data Classification, to facilitate the application of appropriate data protection, all data

owners/custodians responsible for data are required to classify that data in a hierarchical system such that data that is of greater value or sensitivity can be afforded a higher level of protection than data that is of lesser value or sensitivity.

9.4.3.5. Protection of data in use

9.4.3.5.1. Only personnel that have previously been authorized are allowed to enter information into an information system. Inputs will be restricted according to granted permissions, though these restrictions may be lifted on a temporary basis based on pre-defined project responsibilities. In such circumstances, additional authorization is required and must be granted before restrictions are lifted.

9.4.3.5.2. Where possible, information systems will check entered information for accuracy, completeness, validity and authenticity. These checks will be performed as close to the point of information entry as possible and will attempt to ensure that data corruption does not occur or that entered information cannot be interpreted as system commands by the information system.

9.4.3.6. Protection of Data in Storage

9.4.3.6.1. Information systems will be configured such that they prevent unauthorized and unintended information transfer via shared system resources. Information of the highest data classification that has been used by the system will be positively removed from all systems resources (such as memory, temp and swap drives, etc.) once the use of that information is completed.

9.4.3.6.2. Where information is transferred to media that media shall be stored securely within a controlled area and access to that controlled area shall be physically restricted to authorized personnel. Further, the mechanisms that enforce those access restrictions shall collect access information and shall include the ability to audit access attempts.

9.4.3.7. Protection of Data in Transit

9.4.3.7.1. Information systems will protect the integrity and confidentiality of transmitted information using some form of session authentication and, where necessary (i.e. in the case of Personally Identifiable Information), encryption.

9.4.3.7.2. When content from the information system is output to some form of media that content and media must be handled, and stored in a secure manner.

9.4.3.7.3. When information system media is transported it shall be done so in a secure manner and only by personnel specifically authorized to do so. Further, all such transportation shall be documented.

9.4.3.7.4. Once information system media is no longer needed to store or transport system information it must be completely sanitized before either reuse or destroyed before retirement.

9.4.4. Application Protection

9.4.4.1. All applications shall be designed and implemented in as secure a manner as possible using pre-defined application development principles and procedures.

9.4.4.2. Communications between components of information systems or between information systems themselves involve the transmission of information making that information susceptible to attack. Without session management, the potential exists that communications can be established or used illegitimately thereby exposing information to an increased likelihood of loss or corruption.

9.4.4.3. The application element of all information system components is to be designed using security engineering principles, whether it is developed in house or purchased from a third party. These security engineering principles are to be applied to the entire lifecycle of the application element via a systems development life cycle methodology that includes security considerations at all stages of the life cycle. Further, development of the application element of an information system component must include the

creation and execution of a security test and evaluation plan. The results of this test and evaluation process must be documented and shared with appropriate bodies.

9.4.4.4. The application element of all information systems components will logically separate user functionality from administrative functionality such that the interface for the one cannot be used to operate the other.

9.4.5. Portable/Mobile Devices

9.4.5.1. Portable Devices represent a specific category of devices that contain data-at-rest. Many incidents involving unauthorized exposure of sensitive data are the result of stolen or lost Portable Devices. The best way to prevent these exposures is to avoid storing sensitive data on them. As a general practice, sensitive data should not to be copied to or stored on Portable Devices. However, in situations that require sensitive data to be stored on such devices, encryption reduces the risk of unauthorized disclosure in the event that the device becomes lost or stolen.

9.4.5.2. The information resource owner will specify practices to include written authorization that verifies a legitimate business need for accessing and storing sensitive information on a Portable Device and assesses the risk of unauthorized access to or loss of the data before granting permission for exceptions to this best practice.

9.4.5.3. All employees must obtain specific permission from the data owner before storing sensitive data on a Portable Device.

9.4.5.4. Sensitive information stored on Portable Devices including laptops, tablets, personal digital assistants (PDAs), Smart Phones, etc. must be encrypted using approved methods provided in this guide.

9.4.5.5. Portable Devices should not be used for long-term storage of any sensitive information.

9.4.5.6. Removable media including CD-ROMs, floppy disks, backup tapes, flash drives, etc. that contains sensitive information must be encrypted and stored in a secure, locked location.

9.4.5.7. Portable or removable media that contain sensitive data must be in the possession of an authorized employee at all times (e.g., must not be checked as luggage while in transit).

9.4.5.8. Data owners and users of Portable Devices containing sensitive data must acknowledge how they will ensure that data is encrypted and how encrypted data will be accessible by the owner in the event that an encryption key becomes lost or forgotten. Methods to meet this requirement include:

9.4.5.8.1. Maintaining an accessible copy of the data on a server managed by the organization

9.4.5.8.2. Use of whole-disk encryption technologies that provide an authorized systems administrator access to the data in the event of a forgotten key

9.4.5.8.3. Escrowing the encryption key with a trusted party designated by the data owner and the organization Information Security Officer

9.5. Systems Operation

9.5.1. Assessment Operations

9.5.1.1. Security assessments shall be performed against all information systems. Additionally, vulnerability assessments shall be performed against all information systems and web applications. Security assessments are to be performed on at least a 3 year time period and vulnerability assessments are to be performed on at least an annual basis.

9.5.1.2. Security and vulnerability assessments differ from each other in their focus. The focus of a security assessment is determining the degree to which information system security controls are correctly implemented, operating as intended and producing the desired level of security. The focus of a vulnerability

assessment is determining the weaknesses inherent in the information systems that could be exploited leading to information system breach.

9.5.1.3. Security assessments and vulnerability assessments shall be performed by independent and impartial third party on a periodic basis.

9.5.1.4. In the event that the security or vulnerability assessment discovers issues that must be corrected, the security plan shall be immediately updated with the remedial actions required to address the discovered issues. Further, the security plan shall be reviewed on an at least quarterly basis to ensure appropriate corrective actions have been taken.

9.5.2. Integrity Operations.

9.5.2.1. Information systems shall be actively monitored for integrity purposes. Integrity monitoring will be performed according to set processes.

9.5.2.2. System integrity monitoring serves as an oversight process of normal operational and maintenance processes. Without integrity monitoring, the potential exists that where adjustments to information systems, whether legitimately or illegitimately, have been made that compromise the confidentiality, integrity and/or availability of the information system that compromise may not be noted.

9.5.2.3. The security controls of information systems shall be monitored. The purpose of this monitoring will be to assess information system configuration settings, ensuring they are always within acceptable parameters as defined by the information system baseline, and identify system flaws, ensuring they are corrected in a timely manner.

9.5.2.4. Information system monitoring for integrity purposes will be supplemented with information system security alerts/advisories. Alerts/advisories will only be accepted from appropriate third parties, including information system component vendors, information security vendors and known information security advisory bodies. Before any action is taken in response to an alert/advisory it will be investigated and validated. Once validated, the alert may be circulated to appropriate State personnel and corrective action may be scheduled.

9.5.2.5. Information system error messages will be displayed to authorized personnel only. Further, these error messages will never include privileged information or information system information that, if intercepted could be used to harm the information system and/or the organization.

9.5.3. Mobile Computing

9.5.3.1. Mobile computing devices (laptops, tablets, and Smart phones) are inherently insecure and pose a significant security risk. Whether issued by the organization or personally owned, these devices easily move in and out of the network and therefore make it harder to control what users do with these devices. It is the lack of control that makes it difficult to prevent users from exposing business data to security threats either unintentionally or maliciously.

9.5.3.2. Mobile computing devices either owned by the organization or personally owned and used to conduct organization business must be used appropriately, responsibly, and ethically. The following must be observed:

9.5.3.2.1. Organization issued mobile devices are the property of the organization and must be treated, used, and safeguarded as such. If an employee damages or loses an organization-issued mobile device, the employee must notify technical support immediately to have the device de-activated.

9.5.3.2.2. Employees must obtain approval from their supervisor for each Smart Device connected to or to be used as an organization resource for conducting organization business. Once approved the request must be sent to technical support for action and a copy of the request maintained on file with personnel office.

9.5.3.2.3. Charges associated with using a mobile device issued by the organization for personal communications, including text messages, email and voice calling, counts towards the monthly consumption limit. Therefore, personal use of a mobile device issued by the organization should be minimized.

9.5.3.2.4. No employee is to use organization-owned devices for the purpose of illegal transactions, harassment, or obscene behavior, in accordance with other existing employee policies.

9.5.3.2.5. Devices must be kept up to date with manufacturer or network provided patches. At a minimum, employees shall check for updates and apply them at least once a month, security updates shall be applied as they are released.

9.5.3.2.6. Mobile devices must not be loaned to, or used by others.

9.5.3.2.7. Commonly referred to as “jail-breaking”, devices must not be modified in a way that circumvents the vendors limitations imposed upon users or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.

9.5.3.2.8. Devices must not be connected to a PC which does not have up-to-date and enabled anti-malware protection.

9.5.3.2.9. If an employee suspects that unauthorized access to organization data has taken place via a mobile device, the incident must be reported immediately.

9.5.3.2.10. Employees must report all lost or stolen Smart Devices authorized to connect to organization resources or authorized to conduct organization business, to technical support immediately.

9.5.3.2.11. When conducting organization business, the use of any cellular phone or any smart device, either hands on or hands off, while operating a vehicle is prohibited. Use of any cellular phone or any smart device, either hands on or hands off, to conduct personal business while operating an organization owned vehicle is prohibited. Prohibitions include receiving or placing calls, text messaging, surfing the Internet, receiving or responding to email, checking for phone messages, or any other purpose related to your employment; the business; customers; vendors; volunteer activities, meetings, or civic responsibilities performed for or attended in the name of the organization; or any other company or personally related activities not named here while driving. Further, if state or local laws are more restrictive, the employee must follow the appropriate law.

9.5.3.3. Secure Operation

9.5.3.3.1. In order to join a mobile computing device to organization resources, approval must be obtained. Once approved, a security policy/configuration shall be applied to the device either before or upon initial connection (for clarity, connecting smart devices to USB ports for charging is not considered joining a mobile device to organization resources). Whether an organization issued mobile computing device or personally owned, the following security settings will be applied:

9.5.3.3.2. Encryption will be enforced on device storage

9.5.3.3.3. Six character password minimum will be required to unlock smart phones and tablets; laptops shall follow authentication requirements specified in this guide

9.5.3.3.4. Ten failed logins will result in a full wipe of the encrypted device or if device is lost or stolen

9.5.3.3.5. After ten minutes of device inactivity the mobile computing device shall be locked

9.5.3.4. Personal Mobile Computing Devices

9.5.3.4.1. Personal mobile devices may not be connected to organization resources or used to conduct organization business without prior approval of the organization.

9.5.3.4.2. Before requesting authorization to join personal devices to organization resources, employees must be aware that once joined, organization security controls can render smart devices inoperable for various security events or on demand (such as in the case of a lost device). In addition, the security controls addressed previously must also be applied.

9.5.3.4.3. The organization will not assume liability for personal devices. All employees that are eligible for an organization issued mobile phone will receive an organization issued phone number.

9.5.3.4.4. The organization will not assume liability for early termination of employee paid personal mobile devices.

9.5.3.4.5. The organization will not transfer any personal phone numbers to organization issued mobile devices unless not transferring a personal phone number would negatively impact the organization.

9.5.4. Maintenance Operations

9.5.4.1. Maintenance, whether regularly scheduled or emergency in nature, shall be conducted for information systems according to set processes.

9.5.4.2. Information system maintenance is required to ensure that information systems and information systems components are always operating optimally. Set maintenance processes are required to ensure that maintenance is conducted in the most secure manner possible. Without systems maintenance the potential exists that information systems will be unable to provide appropriate information security regardless of the supplemental protection mechanisms that are used. Without systems maintenance processes the potential exists that the act of performing systems maintenance could, either directly or indirectly, compromise information system confidentiality, integrity and availability.

9.5.4.3. Routine preventative and regular maintenance (including repairs) on information system components shall be scheduled ahead of time to ensure business units have sufficient notice and that conflicts are avoided. Maintenance shall be performed in accordance with manufacturer/vendor specifications and/or organizational requirements.

9.5.4.4. Only pre-authorized personnel are allowed to perform information system maintenance. If maintenance personnel do not have sufficient access authorization, they shall be accompanied at all times by personnel that do.

9.5.4.5. Only pre-approved maintenance tools may be used in the maintenance of information systems. The use of maintenance tools shall be actively monitored.

9.5.4.6. A maintenance log shall be maintained for all information system maintenance. This log shall include:

9.5.4.6.1. The date and time of the maintenance

9.5.4.6.2. The name and organization of the person performing the maintenance

9.5.4.6.3. The name of the escort if the person performing maintenance is not a State employee

9.5.4.6.4. Description of the maintenance performed

9.5.4.6.5. List of the information system components or component elements removed/replaced

9.5.4.7. Remote maintenance must be authorized, actively monitored and audited upon completion. The requirement for remote maintenance for an information system must be made available upon system acquisition and risk mitigation techniques included in the security plan. Risk mitigation techniques shall include encrypted communications, strong authentication protocols as well as positive session termination notification.

9.5.4.8. Ongoing support capabilities for core components of critical information systems are required.

Demonstrably sufficient internal capabilities shall count as support; however sufficiency includes both experience and volume of staff. Where demonstrably sufficient internal capabilities do not exist, support contracts are mandatory and must be factored into the purchase price of information system components. Further, critical hardware must be configured for fault tolerance.

9.6. System Audit

9.6.1. System Audits

9.6.1.1. The State of Kansas requires that all information systems be configured such that they can be audited on an as-needed basis. This will be achieved through the use of information logging systems that can either be inherent or accessory to the information system.

9.6.1.2. System audits are used to determine if inappropriate actions, either intentional or unintentional, have occurred within the information system. Without system audits it can be difficult, if not impossible, to determine when a failure of the information system security or a breach of the information systems itself has occurred, the magnitude of the breach or failure, and the details of that breach or failure.

9.6.1.3. Information systems shall be configured to record, at a minimum, all system access events as well as all system administration events. The following specific data points will be collected:

9.6.1.3.1. Date of the event

9.6.1.3.2. Time of the event

9.6.1.3.3. Component of the information system affected by the event

9.6.1.3.4. Identity of the user that triggered the event

9.6.1.3.5. Outcome of the event where available

9.6.1.4. In addition to the above minimum data collection requirements, information systems must have the ability to capture additional information should it be required.

9.6.1.5. To ensure that time recordings are of the utmost relevance, all information systems, including the audit system if an accessory audit system is used, will be time synchronized with a common source on at least a daily basis.

9.6.1.6. Information systems are to be provided with sufficient primary (on-line) storage to retain a pre-defined time period’s worth of log data and sufficient secondary (off-line) storage to retain a second pre-defined time period’s worth of data. If primary storage capacity is exceeded, the information system shall be configured to immediately notify appropriate administrative personnel and continue logging by over-writing the oldest recorded logs. In the event of other logging system failures the information system will be configured to immediately notify appropriate administrative personnel but take no other automated actions.

9.6.1.7. All information systems, where the information system has the capability, shall be configured to notify appropriate administrative personnel in the event that inappropriate, unusual and/or suspicious activity is noted. In the event that automated notification fails, all system logs shall be manually reviewed according to a pre-defined period of time. Should inappropriate, unusual and/or suspicious activity be noted, it shall be fully investigated by appropriate administrative personnel and findings reported to appropriate security management personnel.

9.6.1.8. These investigative functions will be supported by a reporting capability within the information system itself or within an accessory auditing system should one be used. This reporting function will have the ability to parse all collected information to produce custom reports. In all circumstances these reports will be automatically time- stamped by the reporting system itself.

9.6.1.9. System logs are considered confidential information. As such all access to system logs and other

system audit information requires prior authorization and strict authentication whether the logs or other system audit information resides in the information system itself or in an accessory audit system. Further, any access to logs or other system audit information will be captured in those logs.

9.6.1.10. On an annual basis system audit policies and procedures will be reviewed and updated as needed.

9.7. Incident Response

9.7.1. Incident Response Security Incident Response capabilities and plans shall be developed and implemented for all information systems that house or access controlled information.

9.7.2. Incident response capabilities and plans are used to monitor and evaluate security incidents, determine the magnitude of the threat presented by these incidents, and to respond to these incidents. Without an incident response capability the potential exists that, in the event that a security incident occurs, it will go unnoticed and the magnitude of harm associated with the incident will be significantly greater than if the incident were noted and corrected.

9.7.3. The incident response capability shall include a defined plan and shall address the following stages of incident response:

9.7.3.1. Preparation

9.7.3.2. Detection

9.7.3.3. Analysis

9.7.3.4. Containment

9.7.3.5. Eradication

9.7.3.6. Recovery

9.7.3.7. Post-Incident Activity

9.7.4. Further, the use of automated tools, or a dedicated incident response management process, shall be used to aid in incident response operations. These tools must have the ability to capture incident response information, alert appropriate personnel, and provide reporting on the details of any incidents that occur.

9.7.5. All incidents will be logged and tracked in the incident response management system and the existence and nature of the incidents shall be reported to the Chief Information Security Officer.

9.7.6. To facilitate incident response operations, assign responsibility for incident handling operations to an incident response team. In the event that an incident occurs, the members of this team will be charged with executing the incident response plan and operating the incident response system. To ensure that this team is fully prepared for its responsibilities, all team members will be trained in incident response operations within 90 days of appointment to the team and thereafter on an at least annual basis.

9.7.7. Incident response is to be tested annually through the use of a table top exercise and at least every five years through the use of a full-scale test. The results of these tests will be documented, shared with the security office, IT and senior management.

9.8. Contingency Planning

9.8.1. Contingency Plans

9.8.1.1. Development of a contingency plan to address disruption to, or failure of, all information systems that house or access controlled information is required. Contingency plans may indicate that, for non-essential systems, no actions to restore functionality need be taken.

9.8.1.2. Contingency plans are used to establish the manner in which information systems will continue to be operated in the event of a catastrophic failure to the information system or any of its components. Without

contingency plans the potential exists that, should some form of catastrophic failure occur, the organization will be unprepared to recover from that failure and the unavailability of information systems will be extended.

9.8.1.3. The plan as developed will outline contingency roles and responsibilities as well as indicating the individuals assigned to those roles and responsibilities and appropriate contact information for those individuals. Where appropriate, this contingency plan will be integrated with related plans (Business Continuity Plan, Disaster Recovery Plan, Incident Response Plan, etc.) where such plans exist.

9.8.1.4. Contingency plans are to be tested annually through the use of table top exercises and at least every five years through the use of a full-scale test. The results of these tests will be documented, shared with the security office, IT and senior management.

9.8.2. Contingency Infrastructure

9.8.2.1. All activities are required to make provisions for the use of alternate infrastructure as a component of the contingency plan. This alternate infrastructure shall be broken down into three separate categories, processing facilities, storage facilities and telecommunications facilities.

9.8.2.2. Alternate or secondary infrastructure acts as a safeguard in the event that primary facilities are rendered unavailable due to some form of catastrophic failure. Without the use of alternate or secondary infrastructure the potential exists that any outage caused by the unavailability of primary infrastructure will last until the primary infrastructure can be restored to full functionality.

9.8.2.3. Alternate Processing

9.8.2.3.1. In addition to requiring the use of alternate processing facilities, alternate processing facilities must be sufficiently geographically distributed from the primary processing facility to limit the likelihood of both facilities being impacted by the same event. It is up to the discretion of the organization to determine if the alternate processing facility is sufficiently geographically distributed from the primary processing facility.

9.8.2.3.2. Further, it is required that all potential issues relating to access to the alternate processing facility be investigated and appropriate mitigation plans be drawn up to address these issues. Examples of mitigation actions include the transportation of necessary personnel to the alternate processing facility in vehicles with high access capabilities or the use of remote connections to the alternate processing facility. It is up to the discretion of the organization itself to determine if these mitigation plans are appropriate and sufficient.

9.8.2.4. Alternate storage, in addition to requiring the use of alternate storage facilities, it is also required that they be sufficiently geographically distributed from the primary storage facility to limit the likelihood of both facilities being impacted by the same event. It is up to the discretion of the organization itself to determine if the alternate storage facility is sufficiently geographically distributed from the primary storage facility.

9.8.2.5. Alternate Telecommunications, in addition to requiring the use of alternate telecommunications facilities, it is also required that the alternate telecommunications facilities make use of priority of service plans/agreements to ensure that information systems communications are always given appropriate priority. Additionally it is also required that the alternate telecommunications facilities share no common point of failure with the primary telecommunications facilities.

9.8.3. Contingency Operations

9.8.3.1. To facilitate contingency operations, assignment of designated responsibility is required for contingency operations to a contingency response team. In the event that an incident occurs, the members of this team will be charged with executing the contingency plan. To ensure that this team is fully prepared for its responsibilities, all team members will be trained in contingency operations within 90 days of appointment to the team and thereafter on an at least annual basis.

9.8.3.2. Contingency response is to be tested annually through the use of table top exercises and at least every five years through the use of a full-scale test. The results of these tests will be documented, shared with the security office, IT and senior management. These results will be used in the annual review and, where required, update of the contingency plan.

9.8.3.3. As a component of the contingency plan, information system backups will be taken on a regular basis. At a minimum full system backups will be taken monthly. For critical systems, at a minimum, additional incremental weekly backups will also be taken. A copy of each backup will be kept on site while secondary copies will be transported to offsite storage locations. These backups will be protected to ensure integrity and strict physical access controls. Further, to ensure that information systems are restorable, backups will be randomly tested such that a backup for each information system is tested at least annually. Random testing will be required for a minimum of a single tape from one complete back-up run.

9.8.3.4. In the event that an information system must be restored from a backup, before it can be declared production operational, it must be returned to a known secure state as defined by the appropriate baseline. This known secure state must include the application of all patches, hot fixes and other security control mechanisms.

9.9. Physical Security

9.9.1. Physical Access Control

9.9.1.1. Physical access controls shall be used to restrict physical access to the facilities that house information system, to the information systems within those facilities and to the display mechanisms associated with those information systems.

9.9.1.2. Physical access controls clearly indicate who is allowed to access facilities that house information systems, information systems within those facilities and or the display mechanisms associated with those information systems. Without physical access controls, the potential exists that information systems could be illegitimately physically accessed and the confidentiality, integrity and availability of the information they house compromised.

9.9.1.3. Access to facilities, information systems and information system display mechanisms will be limited to authorized personnel and that authorization shall be demonstrated through the use of authorization credentials (badges, identity cards, etc.) that have been issued by the organization.

9.9.1.4. Access will be controlled at pre-defined access points through the use of locks, guards, etc. Authorized personnel are required to authenticate themselves at these access points before facilities, information system or information system display mechanism physical access is allowed. Further, the delivery and removal of information system- related equipment will also be controlled at these access points. No equipment will be allowed to enter or leave the facility without prior authorization and all deliveries and removals will be logged.

9.9.1.5. A list of authorized personnel will be established and maintained such that newly authorized personnel are immediately appended to the list and those personnel who have lost authorization are immediately removed from the list. This list shall further be reviewed and, where necessary, updated on an at least annual basis.

9.9.1.6. In the event that visitors need access to the facilities that house information systems or to the information systems themselves, those visitors must have prior authorization, must be positively identified and must have their authorization verified before physical access is granted. Once access has been granted, those visitors must be escorted at all times and their activities monitored at all times.

9.9.1.7. Visitor access shall be recorded in a log and the log shall be reviewed monthly, at a minimum the log shall contain:

9.9.1.7.1. Name and organization of the visitor.

9.9.1.7.2. Name and organization of the person and/or system visited.

9.9.1.7.3. Purpose of the visits.

9.9.1.7.4. Date and time of arrival and departure.

9.9.1.7.5. The form of identification used for identity verification.

9.9.1.7.6. Visitors signature

9.9.2. Physical Environment Control

9.9.2.1. The use of physical environmental controls is required to ensure appropriate provisions are made to minimize environmental hazard exposure and to maximize operational availability of information systems.

9.9.2.2. Physical environmental controls clearly indicate the appropriate environmental operating parameters under which information systems should be operated. Without physical environmental controls the potential exists that the operating environment will be unsuitable to the reliable operations of State information systems leading to information system unavailability and information corruption.

9.9.2.3. Information systems will be supported by UPS power. At a minimum, sufficient UPS capacity will be provisioned to allow for an orderly shutdown of all information systems. Additionally, power equipment and power cabling shall be deployed and positioned in such a way as to minimize the likelihood of damage. Finally remote power shut-off capabilities will be provided for all information system components within information system facilities. This will allow information system components to be immediately powered down from within the information facility without direct component access. In the event of a power outage, emergency lighting that covers emergency exists and facility evacuation routes will be provided.

9.9.2.4. Core components of information systems are protected from inadvertent water damage by not being deployed within facilities such that they are not placed directly below any water conduits. This restriction will only apply to core components of information systems implemented after the publishing of this policy. Core components of information systems deployed prior to the release of this document are considered exempt from this requirement. Further a fully operable main water supply shut off valve must exist for each facility whose location must be known.

9.9.2.5. Information systems are protected from fire damage by fire detection and suppression systems. Detection systems must operate automatically and notify appropriate personnel as well as emergency responders. Suppression systems may operate manually in facilities that are staffed on a regular basis but must operate automatically in facilities that are not staffed on a regular basis. Suppression systems that activate automatically shall notify appropriate personnel and all suppression systems shall notify emergency responders.

9.9.2.6. Information systems are protected from temperature and humidity related problems. Equipment will be provisioned and monitoring will be performed to ensure that temperature and humidity within facilities that house information systems are always at acceptable levels for optimal operations.

9.10. Personnel Security

9.10.1. Privacy

9.10.1.1. General Information

9.10.1.1.1. To respect privacy is a fundamental concept. While giving out personal information on others may seem harmless, it can potentially cause significant harm to them; allowing identity fraud, vigilante action, and physical attacks as well as some far worse possibilities, which may include civil liability. It is for these reasons that sharing of personal information whether customer or colleague is prohibited unless

explicitly authorized by the organization in writing or by assignment of duties that require the employee to do so.

9.10.1.1.2. Employees authorized to share personal data must do so in a secure manner using methods outlined in this guide and prescribed by the classification of the data. The list below is inclusive, not exclusive; don't share it without first consulting with the organization Information Security Officer or Records Officer.

9.10.1.1.2.1. The real name of a person

9.10.1.1.2.2. Age

9.10.1.1.2.3. Telephone number

9.10.1.1.2.4. Place of work or employer

9.10.1.1.3. Expectation of Privacy

9.10.1.1.3.1. Privacy of electronic communications cannot be guaranteed for two reasons. First, unencrypted electronic communications, especially involving email and the Internet are not private by nature. Second, the organization routinely monitors some types of communications by employees that use email and the Internet. While passwords protect confidentiality to some extent, email and Internet messages and attachments can be read, altered or deleted by unknown parties without your permission. Employees should be aware that even when email messages or Internet files are deleted or erased it is still possible to recreate the original message or file.

9.10.1.1.3.2. The organization owns any communication or document sent via organization email or that is stored on organizational equipment. Management and other authorized staff have the right to access any material in any organization email account or on any computer at any time. Do not consider electronic communications, storage or access to be private if it is created, transmitted or stored on organization resources.

9.10.2. Acceptable Usage

9.10.2.1. Users of information systems are required to conduct themselves appropriately in regards to upholding and maintaining the security of the organization’s information systems and the information they hold. To that end it defines acceptable usage of information systems and information.

9.10.2.2. Acceptable usage policies clearly indicate what information system users are and are not allowed to do. The potential exists that, without these policies, information system users could violate information security and avoid punitive actions by claiming to not know about any restrictions in place. This can make it extremely difficult to enforce the measures outlined in the policy and ultimately lead to a complete disregard of the policy.

9.10.2.3. In a separate document, acceptable usage policies covering the following items shall issue:

9.10.2.3.1. Information System usage (which shall include software restrictions)

9.10.2.3.2. Data usage

9.10.2.3.3. Internet usage

9.10.2.3.4. E-mail usage

9.10.2.3.5. Telephone and office equipment usage

9.10.2.4. Also included within these policies will be an indication of the formal sanctions that can and will be taken against information system users that violate the acceptable usage policies or any other component of this document. Sanctions can include up to immediate and permanent dismissal with cause.

9.10.2.5. As a requirement of information system access, and as a component of security awareness training, all information system users, whether employees or third parties, will be required to provided signed acceptance of the acceptable usage policies. A copy of the signed document will be provided to the individual with the original being retained by the appropriate Human Resources department.

9.10.3. Personnel Operations

9.10.3.1. It is required that the manner in which information system users are hired, fired and transferred between positions be performed in a structured and controlled manner.

9.10.3.2. By following defined protocols regarding staffing, the users to whom it extends information system access will understand and treat that access with appropriate regard for information security. The potential exists that, without these protocols, information system users will have insufficient regard for the security of the information systems or information they use, increasing the risk that the organization is required to accept.

9.10.3.3. Activities are required to define categorizations (also known as system roles) into which all of the users of information systems must be placed. These system roles will be used for all information system users, whether they are employees or third party users, whether they work for the State itself or one of its agencies.

9.10.3.4. Each system role will have assigned to it a risk categorization. Risk categorizations will define the amount of security risk associated with any given system role. It is required that the use of appropriate personnel screening procedures and background checks when staffing positions according to the risk categorization assigned to the system role. Both system roles and risk descriptions will be reviewed and updated where required on an at least annual basis.

9.10.3.5. Upon commencement of work, employees and third party users will be required to sign appropriate access agreements (including but not limited to non-disclosure, non-compete, conflict of interest, acceptable usage, etc.). These agreements specify the user's intent to abide by the operational and security requirements of the organization. These agreements will be reviewed on an annual basis and resigned by information system users as required. Further, the agreement document(s) will be reviewed on an at least annual basis to ensure the highest level of appropriateness and applicability.

9.10.3.6. Should the user of a State information system, whether internal employee or third party user, change working location or functional system role while in the employ of the organization, the access and operational privileges of that user will be immediately reviewed and, where required, updated. This review and update will focus equally on eliminating access privileges no longer required as well as providing the net new/enhanced access required of the new functional role. As necessary, organization property, temporarily in the possession of the information system user will be returned.

9.10.3.7. Upon termination of employment, whether internal employee or third party contractor, access accounts for all information systems will immediately be suspended. All accounts, even though suspended, will be maintained for a pre-defined period of time to allow for the extraction and retention of necessary information, thereafter and where possible all accounts shall be permanently deleted. Exit interviews shall be conducted and all organization owned property (keys, ID cards, computing equipment, etc.) that had been in the temporary possession of the user shall be returned.

9.11. Secure Purchasing/Acquisition

9.11.1. Following set protocols when acquiring information systems, or information system components, ensures that expenditures are made in as wise a manner as possible in regards to the provisioning of IT security. Without such protocols, the potential exists that purchases could be made that undermine defined security requirements. Thus, the risk level faced could be increased and an additional purchase to re-establish an appropriate security level may be required.

9.11.2. The following defined protocols are required when purchasing information systems or equipment to be

used in an information system.

9.11.2.1. Before any information system, or component of an information system, is purchased, the vendor of the system or system component is required to provide documentation specifically indicating the security capabilities and requirements of the system or system component. Further, this documentation must be such that the security controls in the system can be verified by testing. This testing can be performed by the organization or a third party on behalf of either.

9.11.2.2. All information systems or components of an information system, purchased must meet the specifications of pre-defined baselines. These baselines will be distributed in a companion document. Further, where baselines have not yet been defined for a specific purchase, local IT security activities will be consulted for an appropriate guideline prior to the issuance of any purchase documents.

10. PROCDURES

10.1. Assessment & Security Planning

10.1.1. Risk and Privacy Assessment

10.1.1.1. Perform Risk Assessment.

10.1.1.1.1. A risk assessment shall be conducted on each information system (an information system is a functionally related group of interrelated elements working together to present a desired output). In addition to any identified information systems the following shall be treated as individual information systems and a risk assessment shall be conducted for each.

10.1.1.1.1.1. Organization workstation environments

10.1.1.1.1.2. Organization server environments

10.1.1.1.1.3. Organization network environments

10.1.1.1.2. Determine the amount and nature of risk to which an information system is exposed to establish the amount of risk to be mitigated and to better define the appropriate security controls required to mitigate that risk:

10.1.1.1.2.1. Threat Likelihood Classification Scheme

10.1.1.1.2.1.1. High likelihood indicates the threat-source is motivated and capable and controls are insufficient or ineffective.

10.1.1.1.2.1.2. Medium likelihood indicates the threat-source is motivated and capable but that controls may be sufficient and effective.

10.1.1.1.2.1.3. Low likelihood indicates the threats-source is motivated and capable but that controls are sufficient and effective OR the threat-source is unmotivated or incapable.

10.1.1.1.2.2. Threat Impact Classification Scheme

10.1.1.1.2.2.1. High impact indicates significant loss of assets or resources, significant damage to the organizational mission, or serious human injury or death.

10.1.1.1.2.2.2. Medium impact indicates moderate loss of assets or resources, moderate damage to the organizational mission, or human injury.

10.1.1.1.2.2.3. Low impact indicates minimal loss of assets or resources, or minimal damage to the organizational mission.

10.1.1.1.2.3. Risk Classification Scheme

10.1.1.1.2.3.1. Very High risk constitutes high likelihood and high impact. Risks of this nature have the strongest need for corrective action and resolution should be considered an emergency action.

10.1.1.1.2.3.2. High risk constitutes high likelihood and medium impact or medium likelihood and high impact. Risks of this nature have a strong need for corrective action and a corrective response plan must be developed and put in place within 30 days.

10.1.1.1.2.3.3. Medium risk constitutes high likelihood and low impact, low likelihood and high impact or medium likelihood and medium impact. Risks of this nature have a moderate need for corrective action and a corrective response plan must be developed and put in place within 90 days.

10.1.1.1.2.3.4. Low risk constitutes medium likelihood and low impact or low likelihood and medium impact. Risks of this nature have a low need for corrective action and a corrective response plan must be developed and put in place within 180 days.

10.1.1.1.2.3.5. Very Low risk constitutes low likelihood and low impact. Risk of this nature can be considered negligible and no corrective response plan is required however the risk should be reassessed annually to determine if the risk level has been elevated.

10.1.2. Perform Privacy Assessment.

10.1.2.1. Define specific and enhanced protection requirements for Personally Identifying Information (PII):

10.1.2.1.1. Identify the Information to be collected. A Privacy Impact Assessment (PIA) is required if the information processed or stored by the system is related to an individual citizen:

10.1.2.1.1.1. Review system function and determine if any aspect is citizen related.

10.1.2.1.1.2. For systems that have a citizen-related function, review the information the system stores or uses and determine if it is personally identifying information (PII).

10.1.2.1.2. Indicate the Reason for Information Collection. Define why this particular set of information must be collected and what generic purpose it will serve:

10.1.2.1.2.1. Provide rationalization for the collection of the data to ensure that data is not being collected for which a clear and definitive purpose does not exist.

10.1.2.1.3. Indicate the intended use of the information. Define the specific intended use of the collected information to ensure that the information is not being shared with other systems without a PIA first being performed on those secondary systems:

10.1.2.1.3.1. Identify all systems that will make use of the collected information to ensure that Privacy Assessment is performed for all of them.

10.1.2.1.3.2. Contact the system owners of secondary systems and inform them of the need to conduct a Privacy Assessment.

10.1.2.1.4. Indicate with whom the information will be shared. Define the intended sharing of the collected information to ensure that the information is not being shared with others without a PIA first being performed on the systems hosted by that secondary entity:

10.1.2.1.4.1. Identify all entities that will make use of the collected information to ensure

that Privacy Assessment is performed on their systems.

10.1.2.1.4.2. Contact the entity heads of alternate entities and inform them of the need to conduct a Privacy Assessment.

10.1.2.1.5. Indicate what opportunities exist to decline consent to provide information. Individuals must be provided with the opportunity to decline to have their information stored within a system or to limit the uses of that data:

10.1.2.1.5.1. Ensure Privacy Policy documents indicate that consent to provide information can be removed at any time.

10.1.2.1.6. Indicate how information will be secured. Specify both technical and non-technical controls that will be used to protect collected information:

10.1.2.1.6.1. Provide internal specifications indicating the exact controls that will be used to protect the data.

10.1.2.1.6.2. Provide external notifications indicating the generic controls that will be used to protect the data.

10.1.2.1.7. Indicate if a system of records is maintained per the Privacy Act (USC 552a). Where records of different types are catalogued in any systemic manner the existence of that catalogue must be indicated to ensure that all records are equally protected and that a PIA has been performed for all linked systems:

10.1.2.1.7.1. A system of records catalogues multiple pieces of information such that access to the first can provide contiguous access to all others. If a system of records is used, Privacy Assessment must be performed for all aspects of the data rather than the data that was collected specifically by the system.

10.2. Security Planning

10.2.1. Create a Security Plan

10.2.2. Document the requirements and security controls that will be implemented to achieve the determined security stance as a result of risk and privacy assessment:

10.2.2.1. Capture System Identification

10.2.2.1.1. Provide information to identify the system that is the target of the plan:

10.2.2.1.2. Specify both system name and a unique system identifier that will remain consistent for the life of the system.

10.2.2.1.3. Specify operational status of the system (Operational, Developmental, or in-Modification).

10.2.2.1.4. Specify system function (Major Application or General Support System).

10.2.2.1.5. Specify the system environment (physical and logical location).

10.2.2.1.6. Specify existing system interconnections (upstream and downstream).

10.2.2.2. Identify Individuals with Responsibility for the System

10.2.2.2.1. Designate an individual system owner and identify and document all relevant information about that owner:

10.2.2.2.2. Identify the owner of the system.

10.2.2.2.3. Identify the owner(s)/custodian(s) of all data stored on and/or processed by the

system

10.2.2.2.4. Identify the individual responsible for authorizing operations of and accepting risk associated with the system.

10.2.2.2.5. Identify the individual responsible for managing and maintaining the security of the system.

10.2.2.3. Determine Applicable Laws and Regulations

10.2.2.3.1. List all applicable laws, regulations, or policies that may dictate and/or affect the security of the system:

10.2.2.3.2. Include anything that impacts requirements for Confidentiality, Integrity and/or Availability.

10.2.2.4. Determine System Categorization

10.2.2.4.1. Assess and record the impact of the loss of the system as per FIPS 199:

10.2.2.4.2. Assess impact against Confidentiality, Integrity and Availability.

10.2.2.4.3. Assign a value of High, Medium or Low (as per established Risk Assessment processes).

10.2.2.4.4. Perform this task for each system component.

10.2.2.4.5. Aggregate the results of each component, recording the highest value noted for each category across all components.

10.2.2.5. Establish Appropriate Security Baseline Requirements

10.2.2.5.1. As a rule, the NIST 800-53 Moderate Baselines are to be applied to all systems. However, the organization may, at their discretion, determine that the High Baseline is appropriate for given systems depending on system requirements:

10.2.2.5.2. Review the system to determine if the Moderate Baseline is not applicable based on system requirements.

10.3. Maintain Records

10.3.1. Capture documentation appropriate to all assessment and planning processes:

10.3.1.1. Document and retain copies of the outcome of all assessments and security plans.

10.4. Awareness and Training

10.4.1. Security Awareness Training

10.4.1.1. Design and Develop an Awareness Training Program.

10.4.1.1.1. Determine needs and build programs. During the Design Phase needs are identified, a plan is developed, buy-in is secured and priorities are established:

10.4.1.1.1.1. Conduct a Needs Assessment to determine the state of awareness training and identify gaps that need to be filled.

10.4.1.1.1.2. Determine a strategy that includes the roles and responsibilities of those involved, the scope and goals, the target audience, the delivery method to be used, and the record keeping to be taken.

10.4.1.1.1.3. Establish the prioritized implementation timeline bearing in mind factors such as resource availability, organizational impact, current state of awareness training and any

external dependencies.

10.4.1.1.1.4. Define the complexity of the material to be developed such that it meets the needs of the target group and is neither too complex nor too simple to achieve the required goal.

10.4.1.1.1.5. Determine financial requirements and obtain sufficient funding to deliver the training as planned. If sufficient funding is neither available nor can be made available, the Design portion of the program may have to redeveloped accordingly.

10.4.1.1.2. Create Training Materials. Once the overall design and plan for the program has been completed and accepted the scope of awareness training topics must be established and appropriate and materials prepared:

10.4.1.1.2.1. Define a list of topics to be covered in the awareness training program such that sufficient information is shared to raise Awareness while not overwhelming the audience.

10.4.1.1.2.2. Prepare materials (e.g. presentations, hands-on sessions) that will be used during the instructional portion of the program as well as supportive materials (e.g. posters, SOPs) that will be used supportively once instruction is competed:

10.4.1.1.2.2.1. Messaging in the Awareness program should be short and simple since the audience is likely to be non- technical and simply needs to become more aware of security requirements.

10.4.2. Provide Awareness Training. Awareness Training is defined as the first level of the security learning continuum and its purpose is to focus attention on security and allow individuals to recognize security concerns in order to respond accordingly. Awareness must be provided to all users of a system:

10.4.2.1. Provide Instructive Training. Instructive training forms the core or initial thrust of the training program and is delivered in a comprehensive fashion on a periodic basis:

10.4.2.1.1. Provide sufficient scheduling flexibility to allow all identified personnel the opportunity to participate in operations training on a reasonable schedule but with minimal impact to regular tasks.

10.4.2.1.2. Deliver training via a variety of methods:

10.4.2.1.2.1. Repetition enhances understanding and adoption.

10.4.2.1.2.2. Not everyone learns best by the same technique.

10.4.2.2. Provide Training Support. Training support provides enhancements to the training program by delivering messaging around the concepts covered in the training program and is delivered on an on-going basis:

10.4.2.2.1. Training support messaging should be concise and to the point, emphasizing the core messages of the instructive training.

10.4.2.2.2. Training support messaging should be delivered by a variety of mechanisms and media to enhance visibility and up-take.

10.4.3. Security Operations Training.

10.4.3.1. Design and Develop an Operations Training Program.

10.4.3.1.1. Determine Needs and Build Programs. During the Design Phase needs are identified, a plan is developed, buy-in is secured and priorities are established:

10.4.3.1.1.1. Conduct a Needs Assessment to determine the state of operations training and identify gaps that need to be filled.

10.4.3.1.1.2. Determine a strategy that includes the roles and responsibilities of those involved, the scope and goals, the target audience, the delivery method to be used, and the record keeping to be taken.

10.4.3.1.1.3. Establish the prioritized implementation timeline bearing in mind factors such as resource availability, organizational impact, current state of operations training and any external dependencies.

10.4.3.1.1.4. Define the complexity of the material to be developed such that it meets the needs of the target group and is neither too complex nor too simple to achieve the required goal.

10.4.3.1.1.5. Determine financial requirements and obtain sufficient funding to deliver the training as planned. If sufficient funding is neither available nor can be made available, the Design portion of the program may have to redeveloped accordingly.

10.4.3.2. Create Training Materials. Once the overall design and plan for the program has been completed and accepted the scope of operations training topics must be established and appropriate and materials prepared:

10.4.3.2.1. Define a list of specific skills that participants in the operations training program are expected to learn sufficiently to apply them in both periodic and day-to-day activities.

10.4.3.2.2. Prepare materials (e.g. presentations, hands-on sessions) that will be used during the instructional portion of the program as well as supportive materials (e.g. posters, SOPs) that will be used supportively once instruction is competed:

10.4.3.2.2.1. Messaging in the Training program should be concise and to the point but detailed enough that the technical audience will be able to learn the skills necessary to implement and maintain a higher level of security.

10.4.4. Provide Operations Training. Operations Training is defined as the second level of the security learning continuum and its purpose is to provide specific skills that will allow an individual to create and maintain security in a system. Training must be provided to all users responsible for the administration and maintenance of a system:

10.4.4.1. Identify Appropriate Personnel. Identify and document those roles and personnel that hold significant system security responsibilities to ensure they receive security training.

10.4.4.1.1. Determine which roles within the organization have distinct and significant security operations responsibilities.

10.4.4.1.2. Associate personnel with those roles for the purposes of determining training needs.

10.4.4.2. Provide Instructive Training. Instructive training forms the core or initial thrust of the training program and is delivered in a comprehensive fashion on a periodic basis:

10.4.4.2.1. Provide sufficient scheduling flexibility to allow all identified personnel the opportunity to participate in operations training on a reasonable schedule but with minimal impact to regular tasks.

10.4.4.2.2. Deliver training via a variety of methods:

10.4.4.2.2.1. Repetition enhances understanding and adoption.

10.4.4.2.2.2. Not everyone learns best by the same technique.

10.4.4.3. Provide Training Support. Training support provides enhancements to be training program by delivering messaging around the concepts covered in the training program and is delivered on an on-going basis:

10.4.4.3.1. Training support messaging should be in-depth and thorough, emphasizing the processes taught during the instructive training.

10.4.4.3.2. Training support message should be delivered by a variety of mechanisms and media to enhance visibility and up-take.

10.5. Maintain Records. Capture documentation appropriate to all training processes:

10.5.1. Document and retain copies of employee completion of security awareness training.

10.5.2. Document and retain copies of employee completion of security operations training.

10.6. Access Control

10.6.1. Identification and Authentication.

10.6.1.1. Manage Identification and Authentication. Ensure that only individuals that have the pre-established right to access systems can do so:

10.6.1.1.1. Verify User Identity. To ensure that system accounts are only extended to known and trusted individuals, these individuals must be fully identified via external identity verification methods prior to the issuance of accounts:

10.6.1.1.1.1. As part of the on-boarding process, employee identity should be verified through the use of government-issued identification documents.

10.6.1.1.1.2. As part of the visitor verification process, where visitors may be provided with system access, visitor identity should be verified through the use of government-issued identification documents.

10.6.1.2. Create Unique IDs and Authenticators. Each system user is to be provided with an identifier (also known as identity or ID) and an authenticator such that they can uniquely and individually access the system:

10.6.1.2.1. Identifiers must be unique to the individual but can be common across systems.

10.6.1.2.2. Authenticators must be unique to each individual and to each systems; however a master authenticator may be used to access individual system authenticators (a single sign-on system).

10.6.1.3. Securely Distribute IDs and Authenticators. The identifiers and authenticators associated with each account must be distributed in such a manner as to ensure they are delivered only to the personnel to whom they are assigned:

10.6.1.3.1. Identifiers are to be distributed in a manner that eliminates repudiation of receipt.

10.6.1.3.2. Authenticators are to be distributed in a manner that protects their secrecy and eliminates repudiation of receipt.

10.6.1.4. Provide Lifespan Management for Authenticators. Over time, authenticators can become known (if they are first factor authenticators), or inactive/damaged/lost (if they are second factor authenticators) and so must be continually managed:

10.6.1.4.1. First factor authenticators will be provided with both a maximum and minimum lifespan and may be reset at any time at the request of the employee according to established Standards.

10.6.1.4.2. Second factor authenticators will be replaced at such point as they are lost, damaged, or fail.

10.6.1.5. Disable and Archive Inactive Identifiers. Once an identifier is no longer required, it must be disabled to prevent its use and archived to provide for potential future investigation:

10.6.1.5.1. Where account access is still required by any person, identifiers will be reset.

10.6.1.5.2. Where account access is no longer required, identifiers will be deleted along with the account.

10.6.1.6. Revoke Inactive Authenticators. Authenticators that have become known, are lost/damaged/inactive or are simply no longer required must be revoked to eliminate the potential of them being used to suborn access:

10.6.1.6.1. Where account access is still required by any person, first factor authenticators will be reset.

10.6.1.6.2. Where account access is no longer required, first factor authenticators will be deleted along with the account.

10.6.1.6.3. Second factor authenticators will be disassociated with accounts and returned to the inactive authenticator pool.

10.6.2. Account Management

10.6.2.1. Configure User Accounts

10.6.2.2. Establish the system accounts that will be used to access system in a manner that promotes and enhances security while maintaining business functionality:

10.6.2.2.1. Create User Accounts to Optimize Security

10.6.2.2.2. Users must be provided accounts for all systems that they require access to however those accounts must be created in a manner that enhances and enforces organizational security requirements:

10.6.2.2.2.1. Accounts must be created with the minimal set of permissions (also known as least privilege) as required by positional role.

10.6.2.2.2.2. Accounts must be created with the minimal set of responsibilities (also known as job segregation) as required by positional role.

10.6.2.2.2.3. Accounts must be configured to require the use of unique identifiers and authenticators.

10.6.2.2.2.4. Accounts must be configured to enforce system lockout in the event of failed authentication.

10.6.2.2.3. Review User Accounts and Account Permissions

10.6.2.2.4. Perform user account review at a pre-determined interval to ensure that users are provided with appropriate accounts and account permissions:

10.6.2.2.4.1. Validate each system user’s positional role within the organization.

10.6.2.2.4.2. Review system accounts and account permissions for each user.

10.6.2.2.4.3. Validate that each user’s account and account permissions meets the requirements established by positional role.

10.6.2.2.5. Update Accounts to Reflect Change in Requirements

10.6.2.2.6. Should account review determine that users have insufficient accounts or account permissions, the required accounts and/or permissions must be provided:

10.6.2.2.6.1. Where accounts exist but permissions are insufficient, modify the account to include appropriate permissions as per the requirements of the positional role.

10.6.2.2.6.2. Where accounts do not exist, create accounts with appropriate permissions as per the requirements of the positional role.

10.6.2.2.6.3. Review created accounts and assigned permissions to ensure they meet the requirements of the positional role.

10.6.2.2.7. Disable and Remove Extraneous Accounts and Permissions

10.6.2.2.8. Should account review determine that users have inappropriate accounts or account permissions, those accounts and/or permissions must be rescinded:

10.6.2.2.8.1. Eliminate extraneous permissions in allowed accounts.

10.6.2.2.8.2. Revoke access to, and eliminate permissions in extraneous accounts.

10.6.2.2.8.3. Review system logs to catalogue the activity of the account.

10.6.2.2.8.4. Assign short-term access with review only privileges to the user's immediate manager to allow for investigation and review of any data that may have been created or modified.

10.6.2.2.8.5. At the request of the account assignee, provide copies of any data exclusively owned by the account to the account assignee.

10.6.2.2.8.6. Upon completion of all review and investigation, permanently delete any extraneous accounts.

10.6.3. Session Management

10.6.3.1. Configure Systems for Secure Access

10.6.3.1.1. Ensure that systems are configured in such a way as to support and enhance user access and permission restrictions:

10.6.3.1.1.1. Display System Use Notification

10.6.3.1.1.2. To ensure that all users are aware that they are accessing organization owned systems and that they understand their responsibilities in regards to the use of these systems, a system use notification is to be presented at initial login.

10.6.3.1.2. Require Identifiers and Authenticators for Access

10.6.3.1.2.1. Access to systems is not only to be controlled, but auditable as well.

10.6.3.1.2.2. To that end, system access requires the use of individually assigned system identifiers and authenticators:

10.6.3.1.2.3. Configure systems to require the use of identifiers for access control. Where inherent capabilities do not exist in the system, third party tools must be used.

10.6.3.1.2.4. Configure systems to require the use of authenticators for access control. Where inherent capabilities do not exist in the system, third party tools must be used.

10.6.3.1.3. Initiate System Lock-Out

10.6.3.1.3.1. Should system authentication fail a sufficient number of times, the user that

failed authentication shall be locked out of the system for a per-determined period of time.

10.6.3.1.3.2. Should users not wish to wait the specified time period to reattempt authentication they may call the help desk and have the lock out lifted.

10.6.3.1.4. Obscure Authenticator Feedback

10.6.3.1.4.1. To limit the likelihood of authenticator information being suborned, systems are to be configured such that authenticator feedback is obscured:

10.6.3.1.4.2. Authentication information will not be shown or will not be shown in plain text while being entered.

10.6.3.1.5. Ensure Cryptographic Authentication Meets Standards

10.6.3.1.5.1. Cryptography is a valuable tool in the protection of authentication information. However, to ensure the utmost functionality, selected tools must meet set standards:

10.6.3.1.5.2. Where authentication is performed against a cryptographic module, review the cryptographic module to ensure it meets FIPS 140-2 standards.

10.6.3.1.6. Initiate Session Lock and Termination

10.6.3.1.6.1. After a pre-defined period of inactivity internally initiated system sessions must be locked and require re-authentication should further work in the system be required. Further, after a pre-defined period of inactivity externally initiated system sessions must be terminated and require re-establishing should further work within the system be required:

10.6.3.1.6.2. Internally initiated system sessions are those that are initiated from within the network of the host system.

10.6.3.1.6.3. Externally initiated system sessions are those that are initiated from outside of the network of the host system.

10.6.3.1.6.4. Session lock maintains an active session such that information in the process of being entered is not lost.

10.6.3.1.6.5. Session termination closes an active session and any information that is in the process of being entered may be lost.

10.6.3.2. Configure Systems for Secure Communication

10.6.3.2.1. Limit the potential of security threats bridging systems and of data leaking inadvertently by restricting inter-system communications:

10.6.3.2.2. Restrict Intra and Inter-System Communication by Authorization

10.6.3.2.2.1. To ensure that information is not shared inappropriately, intra and inter-system communications must be fully authorized before being established:

10.6.3.2.2.2. Define the specific communication paths and communications that will occur intra and inter-system.

10.6.3.2.2.3. Identify system owners for all involved systems and data owners for all involved data.

10.6.3.2.2.4. Obtain written sign-off on all communications by system and data owners per system.

10.6.3.2.3. Restrict Intra and Inter-System Communication by Content

10.6.3.2.3.1. To ensure that information is not shared inappropriately, intra and inter-system communications must be restricted to agreed upon content only:

10.6.3.2.3.2. Define the specific communication paths and communications that will occur both intra- and inter-system.

10.6.3.2.3.3. Define the appropriate content for each communication as specifically as possible.

10.6.3.2.3.4. Monitor communications to ensure content meets established restrictions.

10.6.3.2.4. Restrict Intra-System Communication by Authentication

10.6.3.2.4.1. Before establishing communications, system components must positively identify one another to ensure that information is only being shared by intended devices:

10.6.3.2.4.2. Systems will use hierarchical device authentication based on the risk impact assignment of the system as a whole.

10.6.4. Maintain Records.

10.6.4.1. Capture documentation appropriate to all access control processes:

10.6.4.1.1. Document and retain copies of issued user identifiers and authenticators.

10.7. Systems Configuration

10.7.1. Configuration Management

10.7.1.1. Build and Maintain a Systems Inventory

10.7.1.1.1. Create a complete list of all systems as well as components that comprise those systems. Ensure configuration specifications are included:

10.7.1.1.2. Inventory all Information Systems and Components

10.7.1.1.2.1. Systems inventories allow the organization to keep accurate track of the systems and system components. Such information is essential to ensuring that such components are appropriately protected:

10.7.1.1.2.2. Create an inventory that is keyed by system.

10.7.1.1.2.3. Catalogue specifications of all systems and system components.

10.7.1.1.2.4. Catalogue configurations of all systems and system component software.

10.7.1.2. Collect System and Component Documentation

10.7.1.2.1. System documentation is essential to providing on-going support in lieu of relying on personnel:

10.7.1.2.2. For each system and system component, collect a complete set of documentation, where possible in electronic format:

10.7.1.3. Actively Maintain Inventory

10.7.1.3.1. The inventory must be kept up to date at all times to ensure that, when consulted, the information it contains is complete and accurate:

10.7.1.3.2. When systems or system components are implemented, the information is to be appended in the inventory.

10.7.1.3.3. When systems or system components are modified in any way, the information is to

be appended in the inventory.

10.7.1.3.4. When systems or system components are removed or replaced, their information is to be removed from the inventory.

10.7.1.3.5. When configurations of systems or system components are modified in any way, the information is to be appended in the inventory.

10.7.1.3.6. When system or system component documentation is modified in any way, the information is to be appended in the inventory.

10.7.2. Perform Systems and Data Classification

10.7.2.1. In order to most efficiently protect information systems and the information they store and/or process, perform security categorization:

10.7.2.2. Identify Systems that Process or Store Information

10.7.2.2.1. Determine all systems and system components that process (including access, input, modify and/or output) or store information in any form:

10.7.2.2.2. Utilize system and information inventories.

10.7.2.3. Identify the Information Processed or Stored by the System

10.7.2.3.1. In order to be able to properly assign a security categorization to the organization's information assets, those assets must first be categorically and definitively identified and grouped by type:

10.7.2.3.2. Identify data that is related to the core services and the manner in which those services are delivered to the organization's clients.

10.7.2.3.3. Identify data that is related to the internal functions or processes of the organization itself.

10.7.2.4. Determine Security Impact Levels for Information

10.7.2.4.1. Once information assets have been identified and grouped by type, the impact to organizational security of the potential loss or destruction of those assets must be assessed:

10.7.2.4.2. Use NIST 800-60 Volume 2 to establish baseline impact levels.

10.7.2.4.3. Assess impact across all three security factors (Confidentiality, Integrity, and Availability).

10.7.2.4.4. Adjust baseline impacts according to organization specific requirements.

10.7.2.5. Assign Security Categorization to Each Information Type

10.7.2.5.1. Complete information categorization by aggregating the security impact level for each information type across all three factors according to the highest impact level assigned:

10.7.2.6. Assign Aggregate Security Categorization to Each Information System

10.7.2.6.1. Finalize the categorization process by assigning a security categorization to each information system according to the security categorization of the information stored or processed by the system:

10.7.2.6.2. For systems that house only a single type of information, assign a security categorization equivalent to that assigned to the information type.

10.7.2.6.3. For information systems that house multiple types of information, assign a security

categorization equivalent to the highest assigned to any of the information types.

10.7.3. Follow Process for Change Control

10.7.3.1. To ensure that the security that is engineered into systems and system components is maintained long term, perform changes to those systems and components in a controlled manner:

10.7.3.2. Initiate Changes via Formal Request

10.7.3.2.1. To properly control changes, requests must be made formally to allow for thorough review as well as the updating of both systems and documentation:

10.7.3.2.2. Ensure that appropriate documentation is assembled prior to request initiation including release notes, installation guides and any documented test results.

10.7.3.2.3. Submit a change request indicating the nature of the change and appropriate consent.

10.7.3.3. Perform Impact Analysis on Change

10.7.3.3.1. Prior to completing implementation plans, risks associated with the change must be assessed and any inappropriate risks must be then mitigated:

10.7.3.3.2. Establish the existence of any dependencies that may have an impact on or be impacted by the change.

10.7.3.3.3. Identify and mitigate risks associated with the change.

10.7.3.4. Provide Implementation Documentation

10.7.3.4.1. To ensure that changes are executed in a controlled manner, formal documentation that outlines roles, responsibilities and required tasks must be created and vetted by all.

10.7.3.5. Execute Controlled Test of the Change

10.7.3.5.1. Where appropriate test and development facilities exist, the change should be executed in this environment to validate the plan and identify any gaps:

10.7.3.5.2. Configure the test environment to mimic the to be changed production environment as much as possible including up and down stream dependent systems.

10.7.3.5.3. Execute the implementation in the controlled environment, noting any deficiencies with the set plan.

10.7.3.5.4. Update the plan as required reflecting lessons learned from the test implementation.

10.7.3.6. Implement the Change per the Plan

10.7.3.6.1. Execute the change according to the outlined and vetted plan:

10.7.3.6.2. Implement tasks and communications as outlined in the plan.

10.7.3.6.3. Escalate where implementation errors or plan deficiencies are noted.

10.7.3.6.4. Upon completion of change update the Systems Inventory.

10.7.3.7. Perform Post-Implementation Validation and Review

10.7.3.7.1. Once the change is finished, all systems impacted must be verified as appropriately functional and a post-implementation review completed:

10.7.3.7.2. Validate that the implementation has achieved the required change and has not yielded any unexpected results.

10.7.3.7.3. Perform a post implementation review to identify any lessons learned and to debrief staff around any deficiencies in the plan that had to be addressed during the implementation.

10.8. Systems Protection.

10.8.1. Create and maintain security infrastructure. Securely deploying systems and systems components, while beneficial, is insufficient to implementing strong security and must be supplemented with dedicated security infrastructure.

10.8.1.1. Implement network boundary protection. The network boundary forms the touch-point between the outside world and so protection mechanisms must be put in place to limit access and secure communications.

10.8.1.1.1. Determine the specific protection required.

10.8.1.1.2. Select and implement solutions according to requirements.

10.8.1.1.3. Establish standard configuration for implemented solutions.

10.8.1.1.4. Make changes as per change control processes.

10.8.1.1.5. Maintain as per maintenance processes.

10.8.1.2. Implement Anti-malware Protection. Malware (including viruses, worms, Trojan Horses, spyware and spam) represents one of the most pervasive types of security threats and can be leveraged against the organization in many ways. Protection requires appropriate solutions.

10.8.1.2.1. Determine points of protection.

10.8.1.2.2. Select and implement solutions according to the requirements.

10.8.1.2.3. Establish standard configuration for implemented solutions.

10.8.1.2.4. Make changes as per change control processes.

10.8.1.2.5. Maintain as per maintenance processes.

10.8.1.3. Implement Security Monitoring. To ensure the effectiveness of both the security controls inherent to the system as well as the security infrastructure external to the system ongoing monitoring is required.

10.8.1.3.1. Determine the nature of the monitoring information that is to be gathered and the manner in which it is to be presented.

10.8.1.3.2. Select and implement solutions according to the requirements.

10.8.1.3.3. Establish standard configuration for implemented solutions.

10.8.1.3.4. Make changes as per change control processes.

10.8.1.3.5. Maintain as per maintenance.

10.9. Data and Media Protection. The following are the procedures that support the Data and Media Protection section of the Default Security Requirements.

10.9.1. Securely Handle Data and Media. Protect data while it is in system, both in storage and use, as well as out of system in media, in both storage and transit.

10.9.1.1. Configure Transmissions for Confidentiality and Integrity Ensure both the integrity and confidentiality of electronic PII data transmissions through the use of cryptography. Cryptographic solutions must meet established standards.

10.9.1.2. Validate Data Inputs

10.9.1.2.1. Integrity of data stored by the information system is to be ensured through the use of controls on data input:

10.9.1.2.1.1. Configure systems to restrict and manage data input..

10.9.1.3. Restrict Access to Media

10.9.1.3.1. Media, in all forms, is on offline storage mechanism for data and, as such, must be protected in a manner equivalent to the data that it stores:

10.9.1.3.1.1. Where possible, protect media output devices from inappropriate access by placing them in secure locations:

10.9.1.3.1.2. Control access to media output devices placed in secure locations by requiring identified and authenticated access to those locations.

10.9.1.3.1.3. Where media output devices cannot be placed in secure locations, configure those devices to output media only when attended.

10.9.1.3.1.4. Disable local media output devices that cannot be configured to only output media when attended.

10.9.1.4. Ensure Media is Securely Stored

10.9.1.4.1. Protect any outputted media from inappropriate access by storing it securely at all times:

10.9.1.4.1.1. Place all media in locked cabinets and place those cabinets in controlled access locations.

10.9.1.4.1.2. Maintain a media access log.

10.9.1.5. Ensure Media is Securely Transported

10.9.1.5.1. Protect during transportation data that has been output to media by tracking and controlling access to that media at all times:

10.9.1.5.1.1. Before allowing media to be transported, verify that a copy of the data stored on the media exists elsewhere.

10.9.1.5.1.2. Place all media in a locked container that will protect it from environmental and man-made threats.

10.9.1.5.1.3. Maintain a media transportation log.

10.9.1.6. Ensure Media is Securely Sanitized and Disposed of

10.9.1.6.1. To provide on-going data protection once specific data points are no longer required being stored on media, that media must be properly sanitized and/or disposed of.

10.9.1.6.1.1. Securely sanitize and dispose of digital media.

10.9.1.6.1.2. Securely dispose of non-digital media.

10.9.1.7. Cloud Storage.

10.9.1.7.1. Organizational cloud storage is storage that is administered by the organization and is essentially transparent to users; it is essentially the same as network storage.

10.9.1.7.2. For the purpose of this guide, personal cloud storage refers to storage that is maintained on the Internet and administered by the employee (Dropbox, iCloud, SkyDrive,

etc.). This type of storage presents an unusually high level of risk and is therefore not authorized for business use. In the event an exception must be made a signed authorization form shall be submitted, approval authority for this exception must be approved by both the data owner and executive level management of the organization. This authorization shall be in writing and placed in the personnel file of the employee.

10.10. Application Protection

10.10.1. Apply Security Principles to Code Development

10.10.1.1. Plan for Security by Assessing Needs and Adopting Standards

10.10.1.1.1. To properly execute development in a secure manner the development team must be provided the facilities and capabilities sufficient to the task and end security needs must be established:

10.10.1.1.1.1. Perform security planning.

10.10.1.1.1.2. Perform privacy assessment.

10.10.1.1.1.3. Ensure use of secure information systems development processes.

10.10.1.2. Include Defined Security Requirements in Development/Acquisition

10.10.1.2.1. Including security inherently during the development/acquisition phase of a project ensures the tightest integration of the security controls with the least impact to system efficiency of operations:

10.10.1.2.1.1. Perform system risk assessment.

10.10.1.2.1.2. Select and document system internal security controls.

10.10.1.2.1.3. Supplement system internal security controls with external security architecture.

10.10.1.2.1.4. Engineer in security and develop controls.

10.10.1.2.1.5. Develop security documentation.

10.10.1.2.1.6. Conduct testing of functional capabilities and security capabilities of the system to ensure they meet design specifications.

10.10.1.3. Maintain Continuity of Security During Migration to Production

10.10.1.3.1. Ensure that system security is not reduced or compromised in any way during the migration to the production environment by utilizing a formal hand-off:

10.10.1.3.1.1. Integrate security by migrating the management of system security controls from the development environment into the production environment.

10.10.1.3.1.2. Assess system security.

10.10.1.4. Operate and Maintain the System According to Set Practices

10.10.1.4.1. Once implemented into the production environment the system must be operated and maintained according to established security principles:

10.10.1.4.1.1. Perform change control.

10.10.1.4.1.2. Perform system security control.

10.10.1.4.1.3. Perform patch and vulnerability management.

10.10.1.4.1.4. Perform system maintenance.

10.10.2. Maintain Records

10.10.2.1. Capture documentation appropriate to all systems configuration processes:

10.10.2.1.1. Create and maintain a systems security architecture document.

10.10.2.1.2. Create and maintain system media handling logs.

10.10.2.1.3. Create and maintain a systems component and configuration inventory.

10.10.2.1.4. Document and retain copies of SDLC requirements.

10.10.2.1.5. Document and retain copies of all system implementation plans.

10.11. Systems Operation

10.11.1. Assessment Operations

10.11.1.1. The State of Kansas requires that security assessments be performed against all information systems. Additionally, vulnerability assessments shall be performed against all information systems. Security assessments are to be performed on at least a 3 year time period and vulnerability assessments are to be performed on at least an annual basis.

10.11.1.2. Security and vulnerability assessments differ from each other in their focus. The focus of a security assessment is determining the degree to which information system security controls are correctly implemented, operating as intended and producing the desired level of security. The focus of a vulnerability assessment is determining the weaknesses inherent in the information systems that could be exploited leading to information system breach.

10.11.1.3. It is recommended that both security assessments and vulnerability assessments be performed by independent and impartial third parties on a periodic basis.

10.11.1.4. In the event that the security or vulnerability assessment discovers issues that must be corrected the security plan shall be immediately updated with the remedial actions required to address the discovered issues. Further, the security plan shall be reviewed on an at least quarterly basis to ensure appropriate corrective actions have been taken.

10.11.1.5. Perform Security Assessments

10.11.1.5.1. Security Assessments are thorough and in-depth security analyses designed to determine the security deficiencies of a system. Perform

10.11.1.5.2. Security Assessments to ascertain security concerns that may exist in a system:

10.11.1.5.2.1. Identify the Target System

10.11.1.5.2.1.1. Collect and document the information that defines the system:

10.11.1.5.2.2. Develop an Assessment Plan

10.11.1.5.2.2.1. Create a formal plan that clearly outlines the work that will be performed:

10.11.1.5.2.2.1.1. Determine the scope of assessments to be performed.

10.11.1.5.2.2.1.2. Establish a prioritized assessment schedule.

10.11.1.5.2.2.1.3. Identify and gather required skills and tools.

10.11.1.5.2.2.1.4. Creation an assessment implementation plan.

10.11.1.5.2.3. 6.1.1.3 Execute the Plan

10.11.1.5.2.3.1. Apply the developed plan to the targeted system to determine and validate the existence of security compromises:

10.11.1.5.2.3.1.1. Review the system and system documentation to determine expected security configuration and capabilities of the system:

10.11.1.5.2.3.1.2. Identify and analyze the target system through investigative techniques:

10.11.1.5.2.3.1.3. Validate vulnerabilities that may be discovered:

10.11.1.5.2.4. Securely Manage Assessment Data

10.11.1.5.2.4.1. Security assessment data contains information that, if it fell into inappropriate hands, could be used to breach the security of the system and so must be protected as critical information:

10.11.1.5.2.4.1.1. Collect data into a central repository to allow for better analysis as well as greater control of the data.

10.11.1.5.2.4.1.2. Establish defined data storage parameters, controlling access and distribution of assessment data:

10.11.1.5.2.4.1.3. Where collected assessment data must be electronically transmitted, ensure the confidentiality and integrity of the data by encrypting the transmissions or data.

10.11.1.5.2.4.1.4. When no longer required, data should be purged from systems and media should be sanitized and or disposed of according to established standards.

10.11.1.5.2.5. Analyze Assessment Data

10.11.1.5.2.5.1. To understand the findings in context, the effect to system risk impact must be determined:

10.11.1.5.2.5.1.1. Review validated assessment findings to determine the risk and cost impact on the organization:

10.11.1.5.2.6. Report on Assessment Findings

10.11.1.5.2.7. The organization must determine whether to accept the adjusted risk impact (if eligible to do so) or whether to adjust risk mitigation strategies accordingly. To facilitate this, an assessment report will be created:

10.11.1.5.2.7.1. Create a final report outlining the findings of the assessment:

10.11.1.5.2.8. Implement Controls to Mitigate Threats

10.11.1.5.2.8.1. Once appropriate risk mitigation strategies have been selected, those controls must be implemented in a planned and structured manner.

10.11.1.5.2.8.2. Note that risk acceptance may also be an acceptable strategy but acceptance of the increased risk must be documented:

10.11.1.5.2.8.2.1. Review findings reports, evaluate risk impact adjustments and accept risk or select appropriate remediation controls.

10.11.1.5.2.8.2.2. Implement remediation controls according to established

standards.

10.11.2. Integrity Operations

10.11.2.1. The State of Kansas requires information systems to be actively monitored for integrity purposes. Integrity monitoring will be performed according to set processes.

10.11.2.2. System integrity monitoring serves as an oversight process of normal operational and maintenance processes. Without integrity monitoring, the potential exists that where adjustments to information systems, whether legitimately or illegitimately, have been made that compromise the confidentiality, integrity and/or availability of the information system that compromise may not be noted.

10.11.2.3. The security controls of State information systems will be monitored. The purpose of this monitoring will be to assess information system configuration settings, ensuring they are always within acceptable parameters as defined by the information system baseline, and identify system flaws, ensuring they are corrected in a timely manner.

10.11.2.4. Information system monitoring for integrity purposes will be supplemented with information system security alerts/advisories. Alerts/advisories will only be accepted from appropriate third parties, including information system component vendors, information security vendors and known information security advisory bodies. Before any action is taken in response to an alert/advisory it will be investigated and validated. Once validated, the alert may be circulated to appropriate State personnel and corrective action may be scheduled.

10.11.2.5. Information system error messages will be displayed to authorized personnel only. Further, these error messages will never include privileged information or information system information that, if intercepted could be used to harm the information system and/or the State.

10.11.2.6. Monitor System Security Controls

10.11.2.6.1. Provide for continuous monitoring of security controls to ensure that the value of the implemented controls is not undermined and their security protection is not minimized:

10.11.2.6.2. 6.2.1.1 Identify Sources of Information

10.11.2.6.2.1. Before monitoring can be performed, the organization must determine the granularity with which monitoring of the infrastructure will be performed and configure the infrastructure to perform that monitoring:

10.11.2.6.2.1.1. Decide on the infrastructure level to be monitored.

10.11.2.6.2.1.2. Establish what information capturing capabilities exist natively to infrastructure components that could be monitored.

10.11.2.6.2.1.3. Determine which infrastructure components will be monitored to achieve the required granularity.

10.11.2.6.2.1.4. Configure monitoring capabilities to capture required information.

10.11.2.6.3. 6.2.1.2 Collect and Collate Data from All Sources

10.11.2.6.3.1. Combining monitoring information from multiple sources allows for events to be reviewed with greater context. This contextualization yields greater insight into the nature and potential results of any event:

10.11.2.6.3.1.1. Gather monitoring information from disparate systems on a periodic basis.

10.11.2.6.3.1.2. Consolidate disparate monitoring information into a central repository.

10.11.2.6.4. Analyze Aggregated Data

10.11.2.6.4.1. Once monitoring data has been collected it must be reviewed for potential threats and threat trends to determine if Incident Response processes should be activated:

10.11.2.6.4.1.1. Review monitoring data for Precursors of potential threat as well as Indicators of actual threat. Examine both individual events as well as event trend data.

10.11.3. Maintenance Operations

10.11.3.1. Plan for, and Provide Notification of, Security Operations

10.11.3.2. Ensure appropriate entities are notified prior to the initiation of scheduled security operations (Risk, Vulnerability and Security Assessments, System Audits, Contingency and Incident Response Plan Tests and solution implementations):

10.11.3.2.1. Identify Affected Systems

10.11.3.2.1.1. Collect and document the information that defines the system.

10.11.3.2.2. Issue Notification and Solicit Response

10.11.3.2.2.1. Preliminary notification allows stakeholders the opportunity to influence work and scheduling before too much time is spent developing codified plans:

10.11.3.2.2.1.1. Identify appropriate stakeholders.

10.11.3.2.2.1.2. Provide preliminary notification to stakeholders.

10.11.3.2.2.1.3. Solicit response to preliminary notification.

10.11.3.2.2.1.4. Adjust preliminary specifications accordingly.

10.11.3.3. Issue Implementation Plans and Solicit Response

10.11.3.3.1. All stakeholders must review implementation plans to ensure that the work does not inadvertently impact other operations and must provide sign-off to indicate their acceptance of the work and any intended impact:

10.11.3.3.1.1. Identify appropriate stakeholders.

10.11.3.3.1.2. Provide a detailed implementation plan to stakeholders:

10.11.3.3.1.3. Solicit response to implementation plan.

10.11.3.3.1.4. Adjust implementation plan accordingly.

10.11.3.4. Provide Update Notifications Throughout Operations

10.11.3.4.1. As work operations progress stakeholders are to be provided status notifications according to an agreed upon schedule:

10.11.3.4.1.1. Establish a notification schedule:

10.11.3.4.1.2. Follow the notification schedule as laid out during work. If work does not go as planned, ad hoc notification may be adopted.

10.11.4. Perform Patch and Vulnerability Management

10.11.4.1. Perform patch and vulnerability management to minimize the number of incidents to which the organization must respond by mitigating vulnerabilities before they can be exploited.

10.11.4.2. Monitor for Threats and Associated Remediation's

10.11.4.2.1. To ensure that treats and vulnerabilities are discovered in a timely fashion, active monitoring should be performed:

10.11.4.2.1.1. Make use of a variety of channels to monitor for threats and vulnerabilities:

10.11.4.2.1.2. Continue to monitor all channels after initial notification in the event that updated information is provided.

10.11.4.3. Prioritize Implementation of Remediation's

10.11.4.3.1. Threats and vulnerabilities should be addressed in order of their criticality, not necessarily in order of their discovery. Prioritization is essential for this:

10.11.4.3.1.1. Prioritize remediation according to established standards.

10.11.4.4. Perform Pre-Implementation Testing of Remediation's

10.11.4.4.1. Before remediation's are implemented into a production environment they are to be tested to determine if any negative impacts on the target system or other systems will occur:

10.11.4.4.1.1. Verify the authenticity and integrity of any remediation that is provided by third parties.

10.11.4.4.1.2. Perform a malware scan against any third party software remediation before testing or implementation.

10.11.4.4.1.3. Configure a test environment to match the production environment as closely as possible:

10.11.4.4.1.4. Implement the remediation into the test environment according to any pre-established standards and observe the results. If systems perform as expected proceed to production implementation. If not, seek an alternate remediation.

10.11.4.5. Deploy Prioritized and Tested Remediation's

10.11.4.5.1. After a remediation has been fully vetted is to be implemented to production systems:

10.11.4.5.1.1. Prior to implementing any remediation, follow appropriate Notification of Work processes.

10.11.4.5.1.2. Prior to implementing any remediation, follow appropriate Change Control standards.

10.11.4.5.1.3. Implement the remediation into the production environment according to the pre-established and pre-tested standards.

10.11.4.6. Verify Effectiveness of Remediation's

10.11.4.6.1. Once remediation's have been implemented to production systems, system functionality must be monitored to ensure that the remediation has had the intended effect and that no unintended effects have occurred:

10.11.4.6.1.1. Monitor the target system to ensure that the remediation is working as intended and is having no negative impact.

10.11.4.6.1.2. Monitor downstream systems of the target system to ensure that the remediation is having no negative impact.

10.11.4.6.1.3. Monitor upstream systems of the target system to ensure that the remediation

is having no negative impact.

10.11.5. Securely Maintain Systems

10.11.5.1. Prepare for Maintenance Activities

10.11.5.1.1. Prepare appropriately for system maintenance to ensure that work is carried out in a manner that does not contravene security:

10.11.5.1.1.1. Prior to performing any system maintenance, follow appropriate Notification of Work standards.

10.11.5.1.1.2. Prior to performing any system maintenance, follow appropriate Change Control standards.

10.11.5.1.1.3. Prior to performing any system maintenance, review and approve the maintenance tools to be used.

10.11.5.2. Conduct Maintenance in a Secure Manner

10.11.5.2.1. System maintenance is essential so that systems continue to operate as intended but must be conducted in a manner that neither contravenes security while being performed nor degrades security once complete:

10.11.5.2.1.1. Only pre-authorized personnel will be allowed to conduct system maintenance.

10.11.5.2.1.2. Maintenance personnel will be authenticated prior to the start of work efforts and will be accompanied at all times.

10.11.5.2.1.3. Where remote maintenance is allowed additional security measures will be utilized.

10.11.5.2.1.4. A maintenance log will be completed for all maintenance work:

10.11.5.2.1.5. Upon completion of all maintenance work the system will be reviewed to determine whether the maintenance took place as described and to ensure security has not been compromised.

10.11.6. Maintain Records

10.11.6.1. Capture documentation appropriate to all systems operations processes.

10.11.6.1.1. Document and retain copies of all system security operations notifications and implementation plans.

10.11.6.1.2. Document and retain copies of all security assessments.

10.11.6.1.3. Create and maintain systems security monitoring logs.

10.11.6.1.4. Create and maintain patch and remediation logs.

10.12. Systems Audit

10.12.1. Configure Auditing Capabilities

10.12.2. Systems Audit is used to ensure that systems are being operated in the manner according to which standards define, configure all systems to capture appropriate logging information:

10.12.3. Configure Systems to Create Log Entries

10.12.3.1. Systems must be configured to generate logs and those logs must be configured to capture required information:

10.12.3.1.1. Establish which systems require logging capabilities. Use Risk and Business Impact Analyses to help establish appropriate systems.

10.12.3.1.2. Enable system and component logging capabilities.

10.12.3.1.3. Configure logging capabilities to capture, at a minimum, all system access events and all system administrative events.

10.12.3.2. Provide Sufficient Primary and Secondary Storage

10.12.3.2.1. Ensure that logging facilities offer sufficient guidance to those investigating generated logs by providing sufficient log storage for historical review:

10.12.3.2.1.1. Systems should be configured such that logging facilities are provided with both on-line (active logs) storage and off-line (archive) storage.

10.12.3.2.1.2. Systems should be configured to transfer log data from on-line storage to off-line storage on a regular and pre-defined basis.

10.12.3.2.1.3. Verification of log transfers and validity of transferred log data should be performed before on-line log storage is cleared.

10.12.3.3. Require Authenticated Access to Logs and Logging Capabilities

10.12.3.3.1. Manage user and administrator access to logs and logging facilities to ensure the confidentiality and integrity of log information:

10.12.3.3.1.1. The number of users that have access to logs and logging facilities should be kept to a minimum. Manual authorization is recommended for the granting of access to logs and/or logging facility.

10.12.3.3.1.2. Systems should be configured to require the use of identified and authenticated access to logs and logging facilities.

10.12.3.4. Configure the System to Respond to Logging Failure

10.12.3.4.1. In the event the logging system fails for any reason, systems should be configured to take reasonable and appropriate actions.

10.12.4. Test Auditing Capabilities

10.12.4.1. Perform periodic audit capability testing to ensure that auditing capabilities continue to operate as intended:

10.12.4.2. Ensure Systems Create Appropriate Logs and Log Entries

10.12.4.2.1. To ensure the logging capabilities of the system are functioning according to specifications, regular function tests should be performed:

10.12.4.3. Ensure Authentication is Required for Log Access

10.12.4.3.1. To ensure that access to the logging capabilities of the system is appropriately secure, regular access tests should be performed:

10.12.4.4. Ensure Log Failure Triggers Appropriate Response Mechanism

10.12.4.4.1. To ensure that log system failure elicits an appropriate response, regular log failure tests should be performed.

10.12.5. Operate Auditing Capabilities

10.12.5.1. Once audit capabilities have been enabled, analyze the information generated by these

capabilities on an ongoing basis to ensure systems are being appropriately operated and that security is being maintained:

10.12.5.2. Review Logs at Predetermined Intervals

10.12.5.2.1. Logs are useful in the investigation of a previously discovered security incident and to discern previously undiscovered security incidents so regular log review should be performed

10.12.5.3. Prioritize Log Entries for Investigation

10.12.5.3.1. In order to streamline the investigation of events discovered during log review, all reviewed log entries should be assigned a prioritization.

10.12.5.4. Analyze Prioritized Log Entries

10.12.5.4.1. Once log files have been prioritized, investigation must be performed to ensure no problems, threats, vulnerabilities or violations exist or have occurred:

10.12.5.4.1.1. Examine logs for violations of the security policies.

10.12.5.4.1.2. Examine logs to ensure system configurations are in-line with established standards.

10.12.5.4.1.3. Examine logs to ensure there are no patterns of attack that may not have been detected by other means.

10.12.5.5. Respond to Logged Activities Where Required

10.12.5.5.1. As a result of the log investigation, variances, incidents and other violations may be discovered for which actions may need to be taken:

10.12.5.6. Generate and Distribute Audit Reports

10.12.5.6.1. Log files capture events that occur throughout the enterprise. In order to notify IT leaders as well as managers from other departments that may be impacted by those events, regular summary reports shall be created:

10.12.6. Maintain Records

10.12.7. Capture documentation appropriate to all systems audit processes:

10.12.7.1. Document and retain copies of the configuration of logging capabilities for each system.

10.12.7.2. Document and retain copies of the results of all tests of system logging capabilities.

10.12.7.3. Maintain copies of all reports generated as a result of log monitoring and analysis.

10.13. Incident Response

10.13.1. Build a Team and Provide Training

10.13.2. Identify Incident Response (IR) Roles

10.13.2.1. To be able to efficiently and effectively respond to incidents as they occur, a variety of skills are required. Defining roles that offer those skills ensures that appropriate personnel can be identified:

10.13.2.1.1. Identify the skills required for operation of an IR practice.

10.13.2.1.2. Identify the positional roles that provide those skills.

10.13.3. Associate Personnel with IR Roles

10.13.3.1. Once roles have been determined, individual employees must be associated with those roles according to the skill sets required of the role and available within the employee pool:

10.13.3.1.1. IR responsibilities can be called upon at any time of the day and so only those staff that are able to work within such time constraints should be considered.

10.13.3.1.2. IR responsibilities can trump the requirements of normal operations and so, unless dedicated IR staff is hired, only those staff that can be leveraged from their primary responsibilities with acceptable business impact should be considered.

10.13.3.1.3. IR responsibilities can require extreme amounts of work in compressed amounts of time and so, only those staff that can work well in such high-stress environments should be considered.

10.13.3.1.4. IR responsibilities can require the taking of quick, decisive actions based on minimal information and so only those staff that can communicate efficiently to share maximum information should be considered.

10.13.4. Identify IR Responsibilities of those Roles

10.13.4.1. Once individual employees have been associated with particular roles, it is important to define and assign specific responsibilities so that in the event of an incident all members of the team know who will be handling what.

10.13.5. Build and Deliver an IR Training Program

10.13.5.1. To ensure that all members of the IR team are able to execute their responsibilities in the most efficient manner possible a training program must be devised and delivered:

10.13.5.1.1. Determine needs and design a program accordingly.

10.13.5.1.2. Create the materials to support the delivery of the training program.

10.13.5.1.3. Provide instructive training in IR operations as per the program.

10.13.5.1.4. Provide training support materials in IR operations as per the program.

10.13.6. Build an Incident Response Capability

10.13.6.1. Incident response planning requires the identification of assets to be protected by the plan, determination of the strategies applicable to the execution of the plan and the documentation of the plan itself:

10.13.7. Create an Incident Response (IR) Plan

10.13.7.1. Develop a formal plan that outlines organizational intent in regards to incidents and the manner in which they will be handled:

10.13.7.1.1. Determine the overall purpose and scope of the IR capability.

10.13.7.1.2. Establish the goals of the IR capability and the strategies that will be used to achieve those goals.

10.13.7.1.3. Define appropriate internal and external communications requirements and mechanisms.

10.13.7.1.4. Define the metrics by which the IR capability will be measured to determine effectiveness and indicate opportunities for enhancement.

10.13.8. Develop Supporting Strategies

10.13.8.1. Once purpose and goals have been defined, strategies must be developed that allows the

organization to meet them:

10.13.8.1.1. Identify the organizational infrastructure components to be monitored (network level/system level/component level).

10.13.8.1.2. Identify and make use of pre-emptive protection mechanisms to avert incidents.

10.13.9. Acquire Tools and Resources

10.13.9.1. Incident Response requires dedicated and specialized tools for both monitoring and response tasks and these resources must be acquired prior to the occurrence of an incident:

10.13.9.1.1. Identify and acquire Monitoring resources.

10.13.9.1.2. Identify and acquire Analysis resources.

10.13.9.1.3. Identify and acquire Response resources.

10.13.10. Document the Plan

10.13.10.1. Use the information derived in the foregoing steps to create a formally documented plan that can be distributed/made available to appropriate personnel in the event that an incident occurs:

10.13.10.1.1. Include plan supporting information to provide background and context to make the plan easier to understand and implement.

10.13.10.1.2. Detail plan detection phase in order to establish processes to be followed to discover and identify incidents.

10.13.10.1.3. Detail plan analysis phase in order to indicate the measures that are to be taken to determine and understand the nature of an incident.

10.13.10.1.4. Detail plan containment and eradication phase in order to indicate the measures that are to be taken to limit the spread of an incident and eliminate the deleterious effects of the incident.

10.13.10.1.5. Detail plan recovery and post-recovery phase in order to establish a structured return to normal operations.

10.13.11. Test the Plan

10.13.11.1. To ensure the applicability of the plan and to verify that the plan can be acted upon as created, periodic testing should be performed:

10.13.11.2. Define Testing Methodologies and Tests

10.13.11.2.1. Plan testing is a critical component of IR planning as it determines the viability of the plan and identifies any gaps that may exist in the plan:

10.13.11.2.1.1. Determine the capabilities that should be included in the testing program.

10.13.11.2.1.2. Determine the manner by which testing should be conducted.

10.13.11.3. Execute Tests

10.13.11.3.1. Completion of tests requires appropriate notification throughout the organization to ensure the test achieves its desired results:

10.13.11.3.1.1. Provide notice to test participants so that they can plan workload to ensure availability for the test.

10.13.11.3.1.2. Provide notice to business and IT operations staff in the event that the plan

inadvertently impacts normal operations.

10.13.11.4. Review Test Results and Take Corrective Action

10.13.11.5. Once the test has been completed, the results should be reviewed to see if the IR plan accurately reflects the needs of the organization or if an adjustment is required.

10.13.12. Operate the plan. Should a potential threat be detected it must be analyzed to determine if an incident has occurred and then the plan must be executed to minimize the harm inflicted by the incident.

10.13.12.1. Detect incidents to identify threats. Before incidents can be responded to, they must be detected. Building standard categorizations can simplify detection and speed subsequent incident response processes.

10.13.12.1.1. Monitor systems for signs of incidents.

10.13.12.1.2. Categorize incidents according to established standards in order to establish appropriate analysis, containment, eradication and recovery processes.

10.13.13. Analyze Discovered Threats. Once incidents have been detected analysis is required to determine the appropriate manner in which to precede with subsequent incident response processes.

10.13.13.1. Investigate discovered precursors and indicators to determine if a valid threat may occur, is occurring or has occurred.

10.13.13.2. Fully document all aspects of the incident and incident response.

10.13.13.3. Prioritize the response to incidents according to potential impact.

10.13.13.4. Notify appropriate individuals within the organization once the threat has been validated and prioritized.

10.13.13.5. Contain Threats to Minimize Loss and Maintain Operations. Once incidents have been understood and response prioritized the threat associated with the incident must be contained to prevent impact to other systems and thus minimize overall impact.

10.13.13.5.1. Select a containment strategy appropriate to the incident, the impacted system and the available resources.

10.13.13.5.2. Gather evidence to allow for further investigation, as the incident progresses and once it is complete, as well as potential prosecution.

10.13.13.5.3. Where time and resources permit, identify the attacker to help stop the incident as well as to prepare for potential prosecution.

10.13.13.5.4. Eradicate Contained Threats and Recover to Normal Operations. After threats have been fully contained they must be fully removed from impacted systems and those systems must be returned to normal operational status.

10.13.13.5.4.1. Eradicate all non-evidentiary remnants of incident.

10.13.13.5.4.2. Recover affected systems and system components to pre-incident status and return to normal operations.

10.13.13.5.4.3. Maintain heightened monitoring of the affected system(s) for a period of time subsequent to an incident to ensure there are no lingering impacts.

10.13.13.6. Perform Post-Recovery Tasks. When the threats associated with an incident have been verifiably removed from the system, follow-up work must be performed.

10.13.13.6.1. Retain evidence according to predetermined standards.

10.13.13.6.2. Collect lessons learned and prepare a formal incident response report.

10.13.14. Maintain Records

10.13.14.1. Capture documentation appropriate to all incident response processes.

10.13.14.1.1. Create and maintain incident monitoring logs.

10.13.14.1.2. Document and retain copies of incident response roles, responsibilities, assigned individuals and appropriate contact information.

10.13.14.1.3. Document and retain copies of incident response training materials.

10.13.14.1.4. Document and retain copies of the incident response plan, including preparatory materials.

10.13.14.1.5. Document and retain copies of completed incident response tests.

10.14. Contingency Planning

10.14.1. Contingency Plans

10.14.1.1. Build a plan. Contingency planning requires the identification of assets to be protected by the plan, determination of the strategies applicable to the execution of the plan and the documentation of the plan itself.

10.14.1.1.1. Establish the Nature and Scope of the Plan. Contingency planning can incorporate a number of different types of plans. The organization must first decide exactly what type of planning is in-scope before commencing plan construction.

10.14.1.1.2. Determine the specific sub-plan components to be developed.

10.14.1.1.3. Conduct a Business Impact Analysis. Since it is impossible to effectively restore all systems and system functions simultaneously, the organization must determine which capabilities are the most critical in order to build a proper restoration prioritization.

10.14.1.1.3.1. Identify critical IT resources.

10.14.1.1.3.2. Identify disruption impacts and determine allowed outage times.

10.14.1.1.3.3. Develop recovery prioritization schedules.

10.14.1.1.4. Identify In-Place and Required Preventative Measures. The use of appropriate preventative measures can offset the need to initiate contingency actions and so establishing these measures is an essential component of overall contingency planning.

10.14.1.1.5. Develop a Recovery Strategy. Different types of disruptions require different types of responses and so the organization must consider building multiple response strategies into the overall contingency plan.

10.14.1.2. Document the plan. Use the information derived in the foregoing steps to create a formally documented plan that can be distributed/made available to appropriate personnel in the event that a business disruption occurs.

10.14.1.2.1.1. Provide plan supporting information to provide background and context to make the plan easier to understand and implement.

10.14.1.2.1.2. Detail notification/activation phase in order to establish processes to be followed once a disruption appears imminent or has occurred.

10.14.1.2.1.3. Detail recovery phase in order to clearly indicate the measures that are to be taken to restore systems functionality and operations.

10.14.1.2.1.4. Detail reconstitution phase in order to establish a structured return to normal operations within the primary systems and/or facilities.

10.14.1.3. Test the plan. To ensure the applicability of the plan and to verify that the plan can be acted upon as created, periodic testing is required.

10.14.1.3.1. Define testing methodologies and tests. Planned testing is a critical component of contingency planning as it determines the viability of the plan and identifies any gaps that may exist in the plan.

10.14.1.3.1.1. Determine the capabilities to be included in the testing program.

10.14.1.3.1.2. Determine the manner in which testing shall be conducted.

10.14.1.3.2. Execute tests. Completion of tests requires appropriate notification throughout the organization to ensure the test achieves its desired results.

10.14.1.3.2.1. Provide notice to test participants so that they can plan workload to ensure availability for the test.

10.14.1.3.2.2. Provide notice to business and IT operations staff in the event that the plan inadvertently impacts normal operations.

10.14.1.3.3. Review test results and take corrective action. Once the test has been completed, the results should be reviewed to see if the contingency plan accurately reflects the needs of the organization or if an adjustment is required.

10.14.2. Contingency infrastructure

10.14.2.1. No applicable procedures

10.14.3. Contingency Operations

10.14.3.1. Build a team and provide training. Contingency planning is a security control that requires specialized capabilities. Building a team ensures they are always appropriately provided for.

10.14.3.1.1. Identify Roles with Contingency Responsibilities. To be able to efficiently and effectively respond to disruptions as they occur, a variety of skills are required. Defining roles that offer those skills ensures that appropriate personnel can be identified.

10.14.3.1.2. Associate Personnel with Contingency Roles. Once roles have been determined, individual employees must be associated with those roles according to the skill sets required of the role and available within the employee pool.

10.14.3.1.3. Identify Contingency Responsibilities of those Roles. Once individual employees have been associated with particular roles, it is important to define and assign specific responsibilities so that in the event of a disruption all members of the team know who will be handling what.

10.14.3.1.4. Build and Deliver a Contingency Training Program. To ensure that all members of the contingency team are able to execute their responsibilities in the most efficient manner possible a training program must be devised and delivered.

10.14.3.1.4.1. Determine needs and design a program accordingly.

10.14.3.1.4.2. Create the materials to support the delivery of the program.

10.14.3.1.4.3. Provide instructive training as per the program.

10.14.3.1.4.4. Provide training support materials as per the program.

10.14.3.2. Backup Scheduling and Frequency. Systems and data backups are an important component of any contingency plan or contingency operations and so backups must be taken according to appropriate schedule.

10.14.3.2.1. Perform System Backup. Back systems up according to established schedules per the criticality of the given system.

10.14.4. Maintain Records

10.14.4.1. Capture documentation appropriate to all contingency planning processes.

10.14.4.1.1. Document and retain copies of contingency roles, responsibilities, assigned individuals and appropriate contact information.

10.14.4.1.2. Document and retain copies of contingency training materials.

10.14.4.1.3. Document and retain copies of the contingency plan, including preparatory materials (i.e. Business Impact Analysis output).

10.14.4.1.4. Document and retain copies of completed contingency tests.

10.15. Physical Security

10.15.1. Physical Access Control

10.15.1.1. Control Physical Access

10.15.1.1.1. Identify, Authorize and Authenticate Individuals that Require Physical Access

10.15.1.1.1.1. All individuals that will require physical access to information system components must be fully identified and authorized prior to any access being allowed and must be authenticated at the time of access:

10.15.1.1.1.1.1. Identify the roles that require both regular as well as occasional physical access and identify the individuals that fill these roles.

10.15.1.1.1.1.2. Provide standing authorization and a permanent authenticator to individuals that require regular access.

10.15.1.1.1.1.3. Require individuals that require occasional access to submit a request that must be approved prior to access being attempted or allowed.

10.15.1.1.1.1.4. Authenticate individuals with regular access requirements through the use of their assigned permanent authenticator.

10.15.1.1.1.1.5. Authenticate individuals with occasional access requirements through the use of a personal identification mechanism that includes name, signature and photograph.

10.15.1.2. Implement Physical Access Controls

10.15.1.2.1. Restrict physical access to system components and the facilities that house them through the use of physical access restrictions:

10.15.1.2.1.1. All facilities that host system components, including input and output mechanisms, must house those components in a dedicated area within that facility.

10.15.1.2.1.2. Access to the dedicated area that houses system component shall be

restricted.

10.15.1.2.1.3. Keep components of high and very high risk systems in locked cabinets within the dedicated area within the facility.

10.15.1.3. Make Use of Access Logs

10.15.1.3.1. To properly vet and maintain records of those individuals that have physically accessed information system components and the facilities that house them, an access log that captures pertinent information about each access must be maintained.

10.15.1.4. Make Use of Delivery and Removal Documentation

10.15.1.4.1. Ensure that systems components are neither illicitly removed from facilities nor are materials illicitly delivered by making use of delivery and removal orders and logs.

10.15.1.5. Monitor Physical Access to Systems

10.15.1.5.1. To ensure that physical access controls have not been breached or otherwise violated, monitoring and physical review is necessary:

10.15.1.5.1.1. All visitors are to be escorted by facilities personnel while within the facility.

10.15.1.5.1.2. Components of high risk and very high risk systems will be actively monitored via camera equipment.

10.15.2. Physical Environmental Control

10.15.2.1. Provide Environmental Controls

10.15.2.1.1. Monitor and Control Temperature and Humidity

10.15.2.1.1.1. The computing components of systems are extremely susceptible to temperature and static electricity and so air quality must be controlled:

10.15.2.1.1.2. Temperature most be controlled to prevent the overheating of system components.

10.15.2.1.1.3. Humidity must be controlled to prevent the build-up of static electricity.

10.15.2.2. Provide Secure Power Delivery

10.15.2.2.1. Power is one of the most fundamental requirements for system and therefore information availability. Ensure sufficient power protection is available.

10.15.2.3. Provide Automated Fire Response

10.15.2.3.1. Fire can cause significant damage to system components as well as present a serious threat to employees and so fire control systems must be made available.

10.15.2.4. Provide Water Shutoff

10.15.2.4.1. Though necessary for facilities operations, water can be extremely detrimental to computer systems. To minimize system unavailability caused by water damage, water control systems must be available.

10.15.2.5. Place Systems to Minimize Exposure to Hazards

10.15.2.5.1. In order to minimize the exposure of system components to environmental hazards, either natural or not in nature, system components should be placed in facilities with care.

10.15.3. Maintain Records

10.15.3.1. Capture documentation appropriate to all physical security processes:

10.15.3.1.1. Create and maintain Access Logs for all facilities that host systems or system components.

10.15.3.1.2. Create and maintain Delivery and Removal Orders and Delivery and Removal Logs for all facilities that host systems or system components.

10.15.3.1.3. Create and maintain Facilities Environmental Control Logs for all facilities that host systems or system components.

10.16. Personnel Security

10.16.1. Acceptable use. Establish Acceptable Usage Baselines. Acceptable Usage Baselines define what qualifies as appropriate and inappropriate behaviors during the course of day to day operations.

10.16.1.1. Internet and e-Mail Usage. Internet and e-mail usage must be restricted as both activities make use of public and unsecured networks.

10.16.1.2. System and Computer Usage. Systems and system components are the property of the organization.

10.16.1.3. Software and Data Usage. The software the organization provides and the data it creates and/or manipulates is the property of the organization.

10.16.1.4. Telephone Usage. The telephone system, including all telephones and fax machines, is the property of the organization.

10.16.1.5. Materials Usage. The office materials, supplies, etc. are the property of the organization and are to be used for business purposes only.

10.16.1.6. Sanctions. Violation of any of the constraints of the security policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken.

10.16.2. Personnel Operations

10.16.2.1. Establish Pre-Hiring Processes

10.16.2.1.1. Since employees will be assigned access to systems and information take steps to ensure appropriate security considerations are taken into account:

10.16.2.1.2. Create Access Agreements

10.16.2.1.2.1. To provide documented records that all personnel have, upon hire, accepted their information security responsibilities, standardized access agreements are required:

10.16.2.1.2.1.1. Formal access agreements specify the expectations placed upon employees as well as the standards to which they will be held.

10.16.2.2. Define Positional Roles

10.16.2.2.1. Utilizing role-based access methodology allows for the streamlining of on-boarding processes and the simplification of employee management which in turn enhances security:

10.16.2.2.1.1. Define roles within the organization within which personnel will be placed using additive rather than exclusive roles where possible.

10.16.2.2.1.2. Assign standardized account accesses and permissions to each role.

10.16.2.3. Establish Risk Categorizations for Each Role

10.16.2.3.1. In order to ensure that to be hired personnel are appropriate for their role from a risk management perspective, the risk associated with each role must be defined:

10.16.2.3.1.1. Review the complete set of systems to be accessed by each role.

10.16.2.3.1.2. List the established risk categorization for each of the systems to be accessed.

10.16.2.3.1.3. Set role risk categorization to be equivalent to the highest risk categorization assigned to a system the role will access.

10.16.2.4. Establish Screening Criteria for Each Categorization

10.16.2.4.1. In order to ensure that to be hired personnel are appropriate for their role from a risk management perspective they must be screened to ensure an appropriate level of trustworthiness.

10.16.2.4.1.1. Use a hierarchical scheme such that personnel hired for roles with higher risk categorizations undergo more stringent screening.

10.16.2.5. Hire Employees in a Structured Fashion

10.16.2.5.1. Upon initial hire, verify employee identity and create accounts with appropriate access rights and permissions:

10.16.2.5.2. Conduct Employee Screening

10.16.2.5.2.1. Verify that applicants offer an appropriate level of trustworthiness by checking their background as per established screening criteria.

10.16.2.5.2.1.1. Review the risk categorization of the role.

10.16.2.5.2.1.2. Conduct the appropriate screening for a role of that risk categorization.

10.16.2.5.3. Complete Access Agreements

10.16.2.5.3.1. Access agreements capture employee recognition of and consent to the rules and regulations of the organization as a whole as well as their own individual responsibilities:

10.16.2.5.3.1.1. Require all incoming employees to complete access agreements.

10.16.2.5.3.1.2. Require all access agreements be witnessed by an existing employee in either a supervisory or Human Resources role.

10.16.2.6. Provision Accounts and Permissions

10.16.2.6.1. Provide employees with the accounts and permissions they need to be able to complete their work assignments:

10.16.2.6.1.1. Review the role(s) to which the employee has been assigned and create specified accounts with the indicated privileges.

10.16.2.6.1.2. Review created accounts and assigned permissions to ensure they meet the specifications as per the role.

10.16.2.7. Transfer Employees in a Structured Fashion

10.16.2.7.1. Employees that change positions should be reviewed according to their new position and have their system accounts and permissions reviewed:

10.16.2.7.2. Conduct Employee Screening

10.16.2.7.2.1. Should an existing employee transfer to a position that carries a higher risk categorization, additional background screening is required. Additional screening is not required for transfer to a position with either an equivalent or lower risk categorization:

10.16.2.7.2.1.1. Review the risk level of the old and new roles and determine whether the risk categorization increases or decreases.

10.16.2.7.2.1.2. If risk categorization increases, conduct the appropriate screening for a role of that risk categorization.

10.16.2.7.3. Review Assigned and Required Accounts and Permissions Cross reference the accounts and permissions of the pre and post-transfer roles, documenting where adjustments need to be made:

10.16.2.7.3.1. Review positional role(s) to which the transferred employee had been assigned and catalogue accounts and permissions.

10.16.2.7.3.2. Review positional role(s) to which the transferred employee will be assigned and catalogue accounts and permissions.

10.16.2.7.3.3. Cross-reference the catalogued accounts an permissions, noting which account(s) and permissions need to be revoked/reduced, provisioning/enhanced, do not need to be adjusted.

10.16.2.7.4. Revoke Accounts and Permissions that are no Longer Valid

10.16.2.7.4.1. The accounts of transferred employees that are no longer necessary must be revoked to eliminate the possibility of illicit system access, however the data the transferred employee may have created must be preserved:

10.16.2.7.4.1.1. Revoke access to and eliminate permissions within all accounts assigned to the terminated employee.

10.16.2.7.4.1.2. Assign access with review only privileges for all accounts assigned to the transferred employee to that employee’s pre-transfer immediate manager for a pre-defined period of time.

10.16.2.7.4.1.3. During this time and at the request of the account assignee, provide copies of any data originally owned exclusively by the transferred employee to the account assignee.

10.16.2.7.4.1.4. Upon expiry of this time and at the direction of the Human Resources department of the transferred employee, permanently delete all accounts of the transferred employee.

10.16.2.7.5. Provision New Accounts and Permissions

10.16.2.7.5.1. Once the transferring employees unnecessary accounts/excess permissions in existing accounts have been removed, new accounts and permissions can be provisioned:

10.16.2.7.5.1.1. Review the role(s) to which the employee has been assigned and create specified accounts with the indicated privileges.

10.16.2.7.5.1.2. Review created accounts and assigned permissions to ensure they meet the specifications as per the role.

10.16.2.8. Terminate Employees in a Structured Fashion

10.16.2.8.1. Employee termination should include the recovery of all issued materials and the

closing of all established accounts:

10.16.2.8.2. Revoke Accounts and Eliminate Permissions

10.16.2.8.2.1. The accounts of terminated employees must be revoked to eliminate the possibility of illicit system access, however the data the terminated employee may have created must be preserved:

10.16.2.8.2.1.1. Review positional role(s) to which the terminated employee had been assigned and catalogue all accounts and permissions.

10.16.2.8.2.1.2. Revoke access to and eliminate permissions within all accounts assigned to the terminated employee.

10.16.2.8.2.1.3. Assign access with review only privileges for all accounts assigned to the terminated employee to that employee's immediate manager for a pre-defined period of time.

10.16.2.8.2.1.4. During this time and at the request of the account assignee, provide copies of any data originally owned exclusively by the terminated employee to the account assignee.

10.16.2.8.2.1.5. Upon expiry of this time and at the direction of the Human Resources department of the terminated employee, permanently delete all accounts of the terminated employee.

10.16.2.8.3. Conduct Exit Interviews

10.16.2.8.3.1. In order for the organization to understand reasons for a voluntary departure, and to ensure a terminated employee understands their ongoing responsibilities, exit interviews must be conducted:

10.16.2.8.3.1.1. Interview all employees that leave the organization, whether voluntarily or not to discuss reasons and ongoing responsibilities.

10.16.2.8.3.1.2. Provide all employees that leave the organization with copies of any non-compete, non-disclosure or other restrictive agreement documents that may have been signed and continue to be valid subsequent to the termination of employment.

10.16.2.8.4. Recover all Organizational Property Issued to the Employee

10.16.2.8.4.1. Ownership of organizational property that may have been in the possession of a terminated employee needs to be re-established and all such property must be returned in original condition, where applicable:

10.16.2.8.4.1.1. Review records to determine what property has been assigned to terminated personnel.

10.16.2.8.4.1.2. Review records to determine the specifications/configuration of property assigned to terminated personnel.

10.16.2.8.4.1.3. Recover all property that has been assigned to terminated personnel and validate that returned property meets original specifications/configuration and that aspects/components have not been removed, tampered with or otherwise negatively impacted.

10.16.3. Maintain Records

10.16.3.1. Capture documentation appropriate to all personnel security processes:

10.16.3.1.1. Maintain copies of all submission and screening documents for applicants that are hired for future reference.

10.16.3.1.2. Maintain copies of all completed access agreements.

10.16.3.1.3. Maintain copies of all provisioned system access accounts and associated permission.

10.16.3.1.4. Maintain records of all issued organization owned materials.

10.16.3.1.5. Maintain copies of all exit interview documents.

10.17. Secure Purchasing and Acquisition

10.17.1. Secure Purchasing

10.17.1.1. Include Security Requirements in Solicitation Documents

10.17.1.1.1. All Requests for Proposal, Information and/or Quotation (RFP, RFI, RFQ) documents should include system security requirements to ensure that system proposed by proponents meet the security requirements of the organization:

10.17.1.1.2. Required Security Capabilities

10.17.1.1.2.1. To ensure solutions that are acquired rather than developed meet organizational security requirements, all acquisition documents must specify the expected security capabilities of the system:

10.17.1.1.2.1.1. Include defined security requirements of the solution.

10.17.1.1.2.1.2. Review all documents prior to issuance to ensure security requirements have been included.

10.17.1.1.3. Required Design and Development Process

10.17.1.1.3.1. To ensure that solutions have been constructed using a methodology that provides definable, consistent and measurable security capabilities, all acquisition documents must specify that solution design and development processes be provided:

10.17.1.1.3.1.1. Include request for indication of the design and development process for the solution.

10.17.1.1.3.1.2. Review all documents prior to issuance to ensure design and development requirements have been included.

10.17.1.1.4. Required Test and Validation Procedures

10.17.1.1.4.1. To allow for independent testing and validation of vendor claims regarding the security capabilities of the solution, all acquisition documents must specify that the vendor must provide the testing and validation methodology and process used during solution development:

10.17.1.1.4.1.1. Include request for indication of the test and validation process used for the solution.

10.17.1.1.4.1.2. Review all documents prior to issuance to ensure test and validation requirements have been included.

10.17.1.1.5. Required Documentation

10.17.1.1.5.1. To allow for thorough independent review of all aspects of the requested solution, all acquisition documents must specify that complete system documentation is

provided:

10.17.1.1.5.1.1. Include request for solution documentation:

10.17.1.1.5.1.1.1. Solution implementation and configuration documentation.

10.17.1.1.5.1.1.2. Solution operation documentation.

10.17.1.1.5.1.2. Review all documents prior to issuance to ensure solution documentation requirements have been included.

10.17.1.2. Ensure Responses Include Required Information

10.17.1.2.1. All responses to RFP, RFI and RFQ documents should include the requested security information as well as sufficient system documentation to allow for independent verification of the security claims made:

10.17.1.2.2. Security Capabilities

10.17.1.2.2.1. To ensure that solutions that are acquired rather than developed meet the organizational security requirements, all acquisition document responses must specify the security capabilities of the proposed system:

10.17.1.2.2.1.1. Review responses to ensure that specified security capabilities are detailed.

10.17.1.2.2.1.2. Weight those responses that include the requested information positively and those that do not include requested information negatively.

10.17.1.2.3. Design and Development Process

10.17.1.2.3.1. To ensure that solutions have been constructed using a methodology that provides definable, consistent and measurable security capabilities, all acquisition document responses must specify the solution design and development processes used during the creation of the proposed system:

10.17.1.2.3.1.1. Review responses to ensure the specification of the design and development process used in solution creation is provided.

10.17.1.2.3.1.2. Weight those responses that include the requested information positively and those that do not include the requested information negatively.

10.17.1.2.4. Test and Validation Process

10.17.1.2.4.1. To allow for independent testing and validation of vendor claims regarding the security capabilities of the solution, all acquisition document responses must specify the testing and validation methodology and process used during creation of the proposed system:

10.17.1.2.4.2. Review responses to ensure the specification of the test and validation methodology and process used in solution creation is provided.

10.17.1.2.4.3. Weight those responses that include the requested information positively and those that do not include the requested information negatively.

10.17.1.2.5. Configuration and Operations Documents

10.17.1.2.5.1. To allow for thorough independent review of all aspects of the requested solution, all acquisition document responses must include complete system documentation for the proposed system:

10.17.1.2.5.1.1. Review responses to ensure that specified solution documentation is included.

10.17.1.2.5.1.2. Weight those responses that include the requested information positively and those that do not include the requested information negatively.

10.17.2. Maintain Records

10.17.2.1. Capture documentation appropriate to all acquisition processes:

10.17.2.1.1. Maintain copies of all solicitation documents for future reference.

10.17.2.1.2. Maintain copies of all solicitation response documents for future reference.

10.17.2.1.3. Maintain copies of all independent verification documents for future reference.

11. BASELINES:

11.1. Assessment & Security Planning

11.1.1. Risk and Privacy Assessment

11.1.1.1. Perform Risk Assessment. Determine the amount and nature of risk to which a system is exposed to establish the amount of risk to be mitigated and to better define the appropriate security controls required to mitigate that risk.

11.1.1.1.1. Threat likelihood classification scheme

11.1.1.1.1.1. High likelihood indicates the threat-source is motivated and capable and controls are insufficient or ineffective.

11.1.1.1.1.2. Medium likelihood indicates the threat-source is motivated and capable but that controls may be sufficient and effective.

11.1.1.1.1.3. Low likelihood indicates the threats-source is motivated and capable but that controls are sufficient and effective OR the threat-source is unmotivated or incapable.

11.1.1.1.2. Threat impact classification scheme

11.1.1.1.2.1. High impact indicates significant loss of assets or resources, significant damage to the organizational mission, or serious human injury or death.

11.1.1.1.2.2. Medium impact indicates moderate loss of assets or resources, moderate damage to the organizational mission, or human injury.

11.1.1.1.2.3. Low impact indicates minimal loss of assets or resources, or minimal damage to the organizational mission.

11.1.1.1.3. Risk classification scheme

11.1.1.1.3.1. Very High risk constitutes high likelihood and high impact. Risks of this nature have the strongest need for corrective action and resolution should be considered an emergency action.

11.1.1.1.3.2. High risk constitutes high likelihood and medium impact or medium likelihood and high impact. Risks of this nature have a strong need for corrective action and a corrective response plan must be developed and put in place within 30 days.

11.1.1.1.3.3. Medium risk constitutes high likelihood and low impact, low likelihood and high impact or medium likelihood and medium impact. Risks of this nature have a moderate need for corrective action and a corrective response plan must be developed and put in place within 90 days.

11.1.1.1.3.4. Low risk constitutes medium likelihood and low impact or low likelihood and medium impact. Risks of this nature have a low need for corrective action and a corrective response plan must be developed and put in place within 180 days.

11.1.1.1.3.5. Very Low risk constitutes low likelihood and low impact. Risk of this nature can be considered negligible and no corrective response plan is required however the risk should be reassessed annually to determine if the risk level has been elevated.

11.1.1.2. Perform Privacy Assessment. Define specific and enhanced protection requirements for Personally Identifying Information (PII).

11.1.1.2.1. Information Considered Personally Identifying.

11.1.1.2.1.1. Name information (full name, maiden name, mother's maiden name, etc.).

11.1.1.2.1.2. Personal identification numbers (social security number, passport number, driver's license number, credit card number, etc.).

11.1.1.2.1.3. Address information (both physical and electronic).

11.1.1.2.1.4. Telephone numbers (personal, mobile, business).

11.1.1.2.1.5. Personal characteristics (photographs, biometrics, medical data).

11.1.1.2.1.6. Information about personal property (title documents, etc.).

11.1.1.2.2. Information Use.

11.1.1.2.2.1. The intended usage for PII must be defined and made publicly available before any such information is collected.

11.1.1.2.2.2. Once collected PII must only be used for the purposes for which it was intended.

11.1.1.2.2.3. Must the intended usage of the PII change; permission to use the information in that manner must be explicitly sought.

11.1.1.2.2.4. Must permission not be made expressly available, collected information must not be used for revised/new purposes.

11.1.1.2.3. Information Protection

11.1.1.2.3.1. Systems that process or store PII shall be considered at least a moderate impact system and shall be protected as such.

11.1.2. Security Planning

11.1.2.1. Create a Security Plan. Document the requirements and security controls that will be implemented to achieve the determined security stance as a result of risk and privacy assessment.

11.1.2.1.1. System categorization scheme

11.1.2.1.1.1. High impact indicates significant loss of assets or resources, significant damage to the organizational mission, or serious human injury or death.

11.1.2.1.1.2. Medium impact indicates moderate loss of assets or resources, moderate damage to the organizational mission, or human injury.

11.1.2.1.1.3. Low impact indicates minimal loss of assets or resources, or minimal damage to the organizational mission.

11.1.2.1.2. System responsibility individuals. For all system responsible individuals, capture

the following information.

11.1.2.1.2.1. Name

11.1.2.1.2.2. Title and employing department

11.1.2.1.2.3. Contact Information

11.1.2.1.3. System security configuration

11.1.2.1.3.1. High impact systems should be afforded the highest level of system protection.

11.1.2.1.3.1.1. Systems should be patched and maintained on an at least weekly basis, or as often as the release of patches allows.

11.1.2.1.3.1.2. System logs should be reviewed on an at least daily basis.

11.1.2.1.3.1.3. Systems should be protected with anti-malware, data encryption and enhanced authentication solutions.

11.1.2.1.3.1.4. Systems should be placed on dedicated network segments that are provided with access controls, firewall protection and intrusion detection and prevention capabilities.

11.1.2.1.3.2. Medium impact system should be afforded a moderate level of system protection.

11.1.2.1.3.2.1. Systems should be patched and maintained on an at least monthly basis, or as often as the release of patches allows.

11.1.2.1.3.2.2. System logs should be reviewed on an at least weekly basis.

11.1.2.1.3.2.3. Systems should be protected with anti-malware and data encryption solutions.

11.1.2.1.3.2.4. Systems should be placed on networks that are provided with perimeter firewall protection and intrusion detection and prevention capabilities.

11.1.2.1.3.3. Low impact systems should be afforded a minimal level of system protection.

11.1.2.1.3.3.1. Systems should be patched and maintained on an at least quarterly basis, or as often as the release of patches allows.

11.1.2.1.3.3.2. System logs should be reviewed on an at least monthly basis.

11.1.2.1.3.3.3. Systems should be protected by anti-malware solutions.

11.1.2.1.3.3.4. Systems should be placed on networks that are provided perimeter firewall protection.

11.1.3. Maintain Records

11.1.3.1. Capture documentation appropriate to all assessment and planning processes.

11.1.3.1.1. Document and retain copies of the outcome of all risk and privacy assessments.

11.1.3.1.2. Document and retain copies of all security plans.

11.2. Awareness and Operations Training

11.2.1. Security Awareness Training

11.2.1.1.1. Design and Develop an Awareness Training Program.

11.2.1.1.1.1. Awareness Training Requirements. At a minimum, security awareness training will address the following:

11.2.1.1.1.1.1. The creation and maintenance of passwords, including the need to maintain password confidentiality.

11.2.1.1.1.1.2. Detecting, avoiding and responding to Social Engineering.

11.2.1.1.1.1.3. Detecting, avoiding and responding to Identity Theft.

11.2.1.1.1.1.4. Detecting, avoiding and responding to viruses and other malware.

11.2.1.1.1.1.5. Appropriate handling of sensitive information to ensure confidentiality and integrity.

11.2.1.1.1.1.6. Appropriate usage of the Internet, e-mail and other organization resources.

11.2.1.1.1.1.7. Appropriate usage of software, including copyright infringement and file sharing.

11.2.1.1.1.1.8. Appropriate usage of portable devices, including external storage devices and portable computing devices.

11.2.1.1.1.1.9. Appropriate usage of encryption devices.

11.2.1.1.1.1.10. Appropriate physical security measures to ensure the protection of facilities, assets and personnel.

11.2.1.1.1.1.11. Appropriate reporting, including the reporting of abuse, policy violations and suspicious activities.

11.2.1.1.2. Provide Security Awareness Training. Awareness Training is defined as the first level of the security learning continuum and its purpose is to focus attention on security and allow individuals to recognize security concerns in order to respond accordingly. Awareness must be provided to all users of a system:

11.2.1.1.2.1. Security Awareness Training Frequency and Scheduling.

11.2.1.1.2.1.1. Security awareness training shall be provided for all employees within 90 days of commencement of employment.

11.2.1.1.2.1.2. Security awareness training shall be provided thereafter for all employees on an at least annual basis. Where possible, employees will be trained together as groups.

11.2.2. Security Operations Training.

11.2.2.1. Design and Develop an Operations Training Program.

11.2.2.1.1. Operational Training Requirements. At a minimum, security operations training will address the following:

11.2.2.1.1.1. Implementation and appropriate configuration of security controls inherent to the system or system component.

11.2.2.1.1.2. Implementation and appropriate configuration of security controls external to the system or system component.

11.2.2.1.1.3. Operations of the security controls inherent to the system or system component.

11.2.2.1.1.4. Operations of the security controls external to the system or system component.

11.2.2.2. Provide Security Operations Training. Operations Training is defined as the second level of the security learning continuum and its purpose is to provide specific skills that will allow an individual to create and maintain security in a system. Training must be provided to all users responsible for the administration and maintenance of a system:

11.2.2.2.1. Positional Roles Requiring Security Operations Training. The following roles types, at a minimum, require security operations training:

11.2.2.2.1.1. Roles with application implementation and/or administration responsibilities.

11.2.2.2.1.2. Roles with server implementation and/or administration responsibilities.

11.2.2.2.1.3. Roles with desktop/laptop implementation and/or administration responsibilities.

11.2.2.2.1.4. Roles with network infrastructure implementation and/or administration responsibilities.

11.2.2.2.1.5. Roles with storage infrastructure implementation and/or administration responsibilities.

11.2.2.2.1.6. Roles with security infrastructure implementation and/or administration responsibilities.

11.2.2.2.2. Security Operations Training Frequency and Scheduling.

11.2.2.2.2.1. Security operations training shall be provided for all employees with security operations responsibilities within 90 days of commencement of employment.

11.2.2.2.2.2. Security operations training shall be provided for all employees with security operations responsibilities within 90 days of the deployment of a new or significantly revised system. Where possible, employees will be trained together as groups.

11.2.2.2.2.3. Security operations training shall be provided thereafter for all employees with security responsibilities on an at least annual basis. Where possible, employees will be trained together as groups.

11.2.3. Maintain Records

11.2.3.1. Capture documentation appropriate to all training processes:

11.2.3.1.1. Document and retain copies of employee completion of security awareness training.

11.2.3.1.2. Document and retain copies of employee completion of security operations training.

11.3. Access Control

11.3.1. Manage Identification and Authentication. Ensure that only individuals that have the pre-established right to access systems can do so:

11.3.1.1. Identity Verification. Users must be identified with government issued identifiers that include the following information:

11.3.1.1.1. Full name.

11.3.1.1.2. Signature.

11.3.1.1.3. Photograph.

11.3.1.2. User ID Construction. User identifiers (User IDs) must be constructed in a consistent manner.

11.3.1.3. User Authenticator Construction.

11.3.1.3.1. Where passwords are used as user authenticators their length and the character sets from which they are constructed must be determined by the risk categorization of the system:

11.3.1.3.1.1. Very high and high risk systems must have passwords at least twelve characters in length that make use of all four of upper case letters, lower case letters, numbers, and special characters.

11.3.1.3.1.2. Medium risk systems must either have passwords at least eight characters in length that make use of three of the four: upper case letters, lower case letters, numbers, and special characters or a minimum of sixteen characters.

11.3.1.3.1.3. Very low and low risk systems must either have passwords at least six characters in length that make use of two of the four: upper case letters, lower case letters, numbers, and special characters or a minimum or sixteen characters.

11.3.1.4. User ID and Authenticator Lifespan Management

11.3.1.4.1. User IDs must have a minimum lifespan equivalent to the term of affiliation with the organization.

11.3.1.4.2. Authenticators must have a lifespan according to the risk categorization of the system:

11.3.1.4.2.1. Very high and high risk systems must have passwords with a maximum lifespan of thirty days, a minimum lifespan of thirty days and a repeat frequency of twelve passwords.

11.3.1.4.2.2. Medium risk systems must have passwords with a maximum lifespan of sixty days, a minimum lifespan of thirty days and a repeat frequency of eight passwords.

11.3.1.4.2.3. Very low and low risk systems must have passwords with a maximum lifespan of ninety days, a minimum lifespan of fifteen days and a repeat frequency of four passwords.

11.3.2. Account Management

11.3.2.1. Configure User Accounts

11.3.2.1.1. Establish the system accounts that will be used to access the system in a manner that promotes and enhances security while maintaining business functionality:

11.3.2.1.1.1. Account Permissions and Restrictions Scheme

11.3.2.1.1.1.1. Accounts should be created with the following restrictions, by position, where applicable:

11.3.2.1.1.1.1.1. System administrative access (install, configure, modify and patch system software).

11.3.2.1.1.1.1.2. Account administrative access (creates, delete, modify accounts and permissions).

11.3.2.1.1.1.1.3. Review administrative access (review activities of other administrators).

11.3.2.1.1.1.1.4. Full content access (read, write, edit and delete data).

11.3.2.1.1.1.1.5. Limited content access (read, write and edit data).

11.3.2.1.1.1.1.6. Restricted content access (read and writes data).

11.3.2.1.1.1.1.7. Minimal content access (read data).

11.3.2.1.1.2. Account Review Scheduling and Frequency

11.3.2.1.1.2.1. Accounts should be reviewed to determine appropriateness of the accounts and the permissions of those accounts on an annual basis. This review should be structured such that one third of accounts per system are reviewed each year.

11.3.3. Session Management

11.3.3.1. Configure Systems for Secure Access. Ensure that systems are configured in such a way as to support and enhance user access and permission restrictions:

11.3.3.1.1. System Use Notification

11.3.3.1.1.1. System use notifications should, at a minimum, specify that:

11.3.3.1.1.1.1. Access is to a system owned by the organization.

11.3.3.1.1.1.2. Access to and actions within the system are monitored, recorded and may be audited.

11.3.3.1.1.1.3. Unauthorized access is not permitted and is a criminal offence.

11.3.3.1.1.1.4. System use implies consent to these strictures.

11.3.3.1.2. System Lock-Out

11.3.3.1.2.1. Session lock resulting from authentication failure should occur after five failed authentication attempts that occur within a fifteen minute time period and should last for a minimum of 30 minutes.

11.3.3.1.3. Session Lock and Termination

11.3.3.1.3.1. Session lock should apply only to sessions that are initiated by end users and not to system-initiated sessions. Session lockout should occur after twenty minutes of inactivity.

11.3.3.1.3.2. Session termination should apply only to sessions that are initiated by end users and to system-initiated sessions. Session termination should occur after twenty minutes of inactivity.

11.3.3.2. Configure Systems for Secure Communication

11.3.3.2.1. Limit the potential of security threats bridging systems and of data leaking inadvertently by restricting inter-system communications:

11.3.3.2.1.1. Intra and Inter-System Authentication

11.3.3.2.1.1.1. Systems that have very low or low risk impact should be identified by TCP/IP address.

11.3.3.2.1.1.2. Systems that have moderate risk impact should be identified by MAC and TCP/IP address.

11.3.3.2.1.1.3. Systems that have high risk impact should be identified by TCP/IP and MAC address as well as either 802.1x or Radius authentication.

11.3.3.2.1.1.4. Systems that have very high risk impact should be identified be

identified by TCP/IP and MAC address as well as both 802.1x and Radius authentication.

11.3.4. Maintain Records

11.3.4.1. Capture documentation appropriate to all access control processes:

11.3.4.1.1. Document and retain copies of issued user identifiers and authenticators. Control

11.4. Systems Configuration

11.5. Configuration Management

11.5.1. Build and Maintain a Systems Inventory. Create a complete list of all systems as well as components that comprise those systems. Ensure configuration specifications are included:

11.5.1.1. System and Component Specifications

11.5.1.1.1. Inventories should include the following specification information:

11.5.1.1.1.1. All components that form the system.

11.5.1.1.1.2. Physical specifications for all components.

11.5.1.1.1.3. Data that is stored in or used by the system.

11.5.1.1.1.4. System and data owners.

11.5.1.1.1.5. Physical location of all system components.

11.5.1.1.1.6. Indicators if components belong to multiple systems.

11.5.1.2. System and Component Configurations

11.5.1.2.1. Inventories should include the following configuration information:

11.5.1.2.1.1. Software (operating system and application) version.

11.5.1.2.1.2. Software (operating system and application) patch level.

11.5.1.2.1.3. Accounts.

11.5.1.2.1.4. Permissions of each account.

11.5.1.3. System and Component Documentation

11.5.1.3.1. Inventories should include the following documentation information:

11.5.1.3.1.1. Implementation documentation.

11.5.1.3.1.2. Configuration documentation.

11.5.1.3.1.3. Operations documentation.

11.5.1.3.1.4. Test and assessment documentation.

11.5.1.4. Inventory Update Scheduling and Frequency

11.5.1.4.1. The system inventory should be reviewed and updated on an at least annual basis.

11.5.2. Perform Systems and Data Classification. In order to most efficiently protect information systems and the information they store and/or process, perform security categorization:

11.5.2.1. Security Impact Level Scheme

11.5.2.1.1. High impact indicates significant loss of assets or resources, significant damage to the organizational mission, or serious human injury or death.

11.5.2.1.2. Medium impact indicates moderate loss of assets or resources, moderate damage to the organizational mission, or human injury.

11.5.2.1.3. Low impact indicates minimal loss of assets or resources, or minimal damage to the organizational mission.

11.5.2.2. Security Categorization Scheme

11.5.2.2.1. Assign a High categorization where at least one of confidentiality, integrity or availability is assessed an impact level of high.

11.5.2.2.2. Assign a Moderate categorization where at least one of confidentiality, integrity or availability is assessed an impact level of moderate and none are assessed an impact level of high.

11.5.2.2.3. Assign a Low categorization where confidentiality, integrity and availability are all assigned an impact level of low.

11.5.2.3. Follow Process for Change Control. To ensure that the security that is engineered into systems and system components is maintained long term, organization should perform changes to those systems and components in a controlled manner:

11.5.2.3.1. Change Documentation

11.5.2.3.1.1. An implementation plan that identifies the specific tasks to be executed prior to implementation, during implementation and subsequent to implementation.

11.5.2.3.1.2. A rollback plan that indicates the decision points at which rollback could be triggered and the tasks that will be used to return to pre-implementation status should the implementation fail.

11.5.2.3.1.3. An escalation plan that identifies the personnel to be contacted and appropriate contact information should a problem occur with the implementation that requires either deviation from the plan or the triggering of the roll back plan.

11.5.2.3.1.4. A communications plan that identifies all communications checkpoints that exist during the implementation, the parties to be contacted and the individuals responsible for establishing contact.

11.5.2.4. Impact Assessment Scheme.

11.5.2.4.1. Identify risks associated with the change or with any of the components of the change.

11.5.2.4.1.1. Identify systems that are dependent on the system undergoing change.

11.5.2.4.1.2. Identify systems that are dependent on the personnel performing the change.

11.5.2.4.1.3. Identify systems that share maintenance windows (and may not be able to be maintained) with the system undergoing change.

11.5.2.4.2. Determine risk factor by establishing the likelihood of the risk occurred versus the impact of the risk should it occur.

11.5.2.4.2.1. Very High risk constitutes high likelihood and high impact. Risks of this nature must be mitigated.

11.5.2.4.2.2. High risk constitutes high likelihood and medium impact or medium likelihood and high impact. Risks of this nature have a strong need for mitigation and are unlikely to be accepted.

11.5.2.4.2.3. Medium risk constitutes high likelihood and low impact, low likelihood and high impact or medium likelihood and medium impact. Risks of this nature have a moderate need for mitigation and may be accepted.

11.5.2.4.2.4. Low risk constitutes medium likelihood and low impact or low likelihood and medium impact. Risks of this nature have a low need for mitigation and are likely to be accepted.

11.5.2.4.2.5. Very Low risk constitutes low likelihood and low impact. Risks of this nature do not need to be mitigated.

11.5.2.4.3. Mitigate risks that are determined to have a significant enough risk factor as to impact the implementation of the change.

11.5.3. Systems Protection

11.5.3.1. Create and Maintain Security Infrastructure. Securely deploying systems and systems components, while beneficial, is insufficient to implementing strong security and must be supplemented with dedicated security infrastructure:

11.5.3.1.1. Infrastructure Components

11.5.3.1.1.1. All networks must provision a firewall at the network perimeter to monitor for and block inappropriate network traffic.

11.5.3.1.1.2. All networks must provision anti-malware on the network to monitor for and block malware (viruses, worms, spam, etc.).

11.5.3.1.1.3. All networks must provision anti-malware to the endpoint (servers, desktops and laptops) to monitor for and block malware (viruses, worms, spam, etc.).

11.5.3.1.1.4. All networks must deploy Intrusion Detection (IDS) or Intrusion Prevention (IPS) at least on the network to monitor for inappropriate network traffic that may bypass other network perimeter controls.

11.5.3.1.2. Infrastructure Component Configurations

11.5.3.1.2.1. Firewalls shall be configured to block by default and allow by exception in regards to both inbound and outbound traffic.

11.5.3.1.2.2. Enterprise anti-malware will be automatically updated on a daily basis or as frequently as is possible based on the distribution of patch and definition files from the antimalware provider.

11.5.3.1.2.3. Endpoint anti-malware will be automatically updated on a daily basis, or as frequently as is possible based on the distribution of patch and definition files from the antimalware provider.

11.5.3.1.2.4. IDS or IDP systems will be configured to monitor all inbound and outbound traffic, scanning for anomalous traffic signatures and anomalous traffic patterns. These systems will be configured to issue alerts must inappropriate traffic be detected.

11.5.4. Data/Media Protection

11.5.4.1. Securely Handle Data and Media. Protect data while it is in system, both in storage and

use, as well as out of system in media, in both storage and transit:

11.5.4.1.1. Transmission Configuration

11.5.4.1.1.1. Where possible, encrypted tunnels must be used for all electronic data transmissions.

11.5.4.1.1.2. Where encrypted tunnels cannot be used for electronic data transmissions, restricted use data must be directly encrypted prior to transmission.

11.5.4.1.2. Data Input Validation

11.5.4.1.2.1. Data should only be input by those with appropriate accounts and account permissions.

11.5.4.1.2.2. Data should only be input according to established syntax parameters.

11.5.4.1.2.3. Inputted data should be checked for accuracy, authenticity, completeness and validity by the system.

11.5.4.1.3. Data Disposal Methods

11.5.4.1.3.1. Use software or hardware delete functions to remove data from digital media that has stored non-confidential or non-restricted use data.

11.5.4.1.3.2. Use dedicated media wiping solutions to permanently remove data from digital media that has stored confidential or restricted use data.

11.5.4.1.4. Media Disposal Methods

11.5.4.1.4.1. Where digital media has reached the end of its lifespan, the media must be physically destroyed and rendered unusable before being discarded.

11.5.4.1.4.2. Where non-digital media has reached the end of its usability, the media must be physically destroyed and rendered illegible and unusable before being discarded.

11.5.5. Applications Protection

11.5.5.1. Apply Security Principles to Code Development. To ensure that information systems offer the appropriate level of security with the greatest level of efficiency, developers should engineer controls into the solution during development:

11.5.5.1.1. Standard Development Practices

11.5.5.1.1.1. Development processes should start with the creation and documentation of a secure Concept of Operations (ConOps).

11.5.5.1.1.2. Development processes should make use of documented and repeatable standards and processes.

11.5.5.1.1.3. Security training should be provided for the development team.

11.5.5.1.1.4. Quality management should be performed throughout the development process.

11.5.5.1.1.5. Code should be developed in a dedicated and secured environment.

11.5.5.1.1.6. Code should be stored in securely maintained repositories.

11.5.5.1.2. Development Training Recommendations

11.5.5.1.2.1. Development training should address all standard development practices.

11.5.5.1.3. Development Training Scheduling and Frequency

11.5.5.1.3.1. Secure code development training should be provided for all developers within 30 days of initial assignment of the individual to the development team.

11.5.5.1.3.2. Secure code development training should be provided thereafter for all developers on an at least annual basis.

11.5.5.1.3.3. Where possible, team members will be trained together as a group.

11.5.5.1.4. Quality Assurance. Code development quality assurance practices should focus on the following:

11.5.5.1.4.1. Cross-site scripting vulnerabilities.

11.5.5.1.4.2. Buffer overflows.

11.5.5.1.4.3. Race conditions.

11.5.5.1.4.4. Object model violations.

11.5.5.1.4.5. Poor user input validation.

11.5.5.1.4.6. Poor error handling.

11.5.5.1.4.7. Exposed security parameters.

11.5.5.1.4.8. Passwords in the clear.

11.5.5.1.4.9. Violations of the stated security policy..

11.5.6. Maintain Records

11.5.6.1. Capture documentation appropriate to all systems configuration processes:

11.5.6.1.1. Create and maintain a systems security architecture document.

11.5.6.1.2. Create and maintain system media handling logs.

11.5.6.1.3. Create and maintain a systems component and configuration inventory.

11.5.6.1.4. Document and retain copies SDLC requirements.

11.5.6.1.5. Document and retain copies of all system implementation plans.

11.6. Systems Operation

11.6.1. Assessment Operations

11.6.1.1. Perform Security Assessments. Security Assessments are thorough and in-depth security analyses designed to determine all security deficiencies within a system. Complete Security Assessments to establish all security concerns that may exist in a system.

11.6.1.1.1. Security Assessment Recommendations

11.6.1.1.1.1. Security assessment plans should address the following topics:

11.6.1.1.1.1.1. Whether the assessment should be external, internal or both.

11.6.1.1.1.1.2. Whether assessments should assess potential vulnerabilities or verifiable threats.

11.6.1.1.1.1.3. Whether the assessment will be performed by staff of third party experts.

11.6.1.1.1.2. System documentation to be reviewed should include:

11.6.1.1.1.2.1. System log files.

11.6.1.1.1.2.2. System configuration.

11.6.1.1.1.2.3. System rule-set.

11.6.1.1.1.3. Security assessment investigative techniques should include:

11.6.1.1.1.3.1. Network foot-printing.

11.6.1.1.1.3.2. Port and service scanning.

11.6.1.1.1.3.3. Vulnerability assessment.

11.6.1.1.1.3.4. System and account review

11.6.1.1.1.4. Security assessment validating techniques should include:

11.6.1.1.1.4.1. Penetration testing.

11.6.1.1.1.4.2. Password cracking.

11.6.1.1.1.4.3. Social engineering.

11.6.1.1.1.4.4. Permission elevation.

11.6.1.1.1.5. Security Assessment Scheduling and Frequency

11.6.1.1.1.5.1. External vulnerability assessments should be performed on an at least annual basis.

11.6.1.1.1.5.2. Internal vulnerability assessments should be performed on an at least bi-annual basis.

11.6.1.1.1.5.3. Complete security assessments should be performed on an at least tri-annual basis.

11.6.1.1.2. Security Assessment Data Management

11.6.1.1.2.1. Security assessment reports should include the following information:

11.6.1.1.2.1.1. The nature of the findings.

11.6.1.1.2.1.2. Any increased risk as a result of the findings.

11.6.1.1.2.1.3. The adjustments that must be made to system risk impact if no remediation is performed.

11.6.1.1.2.1.4. The appropriate risk mitigation techniques that could be adopted and the adjustments these will have to system risk.

11.6.1.1.2.1.5. The projected cost of proposed risk mitigation strategies.

11.6.1.1.2.2. Security assessment data should be treated as Very High risk and all systems that store such data should also be considered Very High risk. Both data and systems should be afforded appropriate protection based on this risk classification.

11.6.1.1.2.3. Assessment data should be retained according to the following schedule:

11.6.1.1.2.3.1. Raw assessment data should be retained for a period of no greater than six months or until all discovered security problems have been demonstrably resolved, whichever comes last.

11.6.1.1.2.3.2. Assessment reports should be retained for the equivalent of two full subsequent assessment periods. Reports associated with annually conducted assessments should be retained two years; reports associated with bi-annually conducted assessments should be retained four years, etc.

11.6.2. Integrity Operations

11.6.2.1. Monitor System Security Controls. Provide for continuous monitoring so as to not undermine the value of any implemented security controls and to maximize the value those controls provide:

11.6.2.1.1. Identification of Monitoring Sources

11.6.2.1.1.1. Determine at what level(s) infrastructure security monitoring will be performed:

11.6.2.1.1.1.1. Monitoring at the network level will detect threats that impact the organization but may not reveal specific information as to the specific systems or information targeted by the threat. This level of monitoring requires the least investment of effort.

11.6.2.1.1.1.2. Monitoring at the system level will detect threats that impact the system, but may not reveal specific information as to the specific information targeted by the threat. This level of monitoring requires a moderate level of effort.

11.6.2.1.1.1.3. Monitoring at the component level will detect threats that impact specific information. This level of monitoring requires the highest level of effort.

11.6.3. Maintenance Operations

11.6.3.1. Plan for, and Provide Notification of, Security Operations

11.6.3.1.1. Ensure appropriate entities within the organization are notified prior to the initiation of any security operations (Risk, Vulnerability and Security Assessments, System Audits, Contingency and Incident Response Plan Tests and solution implementations):

11.6.3.1.1.1. Notification and Work Plan

11.6.3.1.1.1.1. All works plans should include the following information:

11.6.3.1.1.1.1.1. Nature of the work.

11.6.3.1.1.1.1.2. Reason for the work.

11.6.3.1.1.1.1.3. Scheduling of the work.

11.6.3.1.1.1.1.4. Tasks involved in the work.

11.6.3.1.1.1.1.5. Contact plans to be followed during the work.

11.6.3.1.1.1.1.6. Rollback plans in the event of failure of the work.

11.6.3.1.1.1.2. All work plans should be accompanied by a notification schedule that should include the following:

11.6.3.1.1.1.2.1. The individuals to be notified.

11.6.3.1.1.1.2.2. The individuals to provide the notification.

11.6.3.1.1.1.2.3. The milestones at which notification will occur.

11.6.3.1.1.1.2.4. The method through which notification will occur (i.e., telephone

and number, e-mail and address).

11.6.3.2. Perform Patch and Vulnerability Management

11.6.3.2.1. Perform patch and vulnerability management to minimize the number of incidents to which a response may be required by mitigating vulnerabilities before they can be exploited.

11.6.3.2.1.1. Identify Patch Monitoring Sources

11.6.3.2.1.1.1. System solution vendor websites.

11.6.3.2.1.1.2. Security solution vendor websites.

11.6.3.2.1.1.3. Third party mailing lists and notification services.

11.6.3.2.1.1.4. Vulnerability scanning tools.

11.6.3.2.1.1.5. Patch management tools.

11.6.3.2.2. Patch Monitoring Frequency

11.6.3.2.2.1. Monitoring for patches should be performed in accordance with the risk categorization of the system:

11.6.3.2.2.1.1. Patches for very high and high risk systems should be monitored for on a weekly basis.

11.6.3.2.2.1.2. Patches for medium risk systems should be monitored for on a monthly basis.

11.6.3.2.2.1.3. Patches for very low and low risk systems should be monitored for on a quarterly basis.

11.6.3.2.3. Remediation Prioritization Scheme

11.6.3.2.3.1. Determine which systems are affected by threats or vulnerabilities, giving prioritization preference to those that are deemed to have a higher level of criticality.

11.6.3.2.3.2. Determine which threats or vulnerabilities have the greatest potential for causing a system impact giving prioritization preference to those that have a higher likelihood of causing an impact.

11.6.3.2.3.3. Determine which threats or vulnerabilities have the greatest potential of spreading to other systems within the organization giving prioritization preference to those that have a higher likelihood of spreading.

11.6.3.2.3.4. Determine which threats or vulnerabilities have the potential for causing the greatest amount of damage giving prioritization preference to those that have a cause a greater amount of harm.

11.6.3.2.3.5. Correlate all factors to create a master prioritization schedule. Revise this schedule each time a new threat or vulnerability is discovered.

11.6.3.3. Securely Maintain Systems

11.6.3.3.1. Perform system maintenance work in as secure a manner as possible:

11.6.3.3.1.1. Remote Maintenance

11.6.3.3.1.1.1. All active connections as well as the system being maintained should be actively monitored.

11.6.3.3.1.1.2. Remote maintenance should be performed over encrypted tunnels.

11.6.3.3.1.1.3. Tunnels should be positively terminated upon completion of all work.

11.6.3.3.2. Maintenance Logs

11.6.3.3.2.1. Maintenance logs, at a minimum, should capture the following information:

11.6.3.3.2.1.1. Affected system.

11.6.3.3.2.1.2. Date and time of scheduled maintenance.

11.6.3.3.2.1.3. Description of the work performed.

11.6.3.3.2.1.4. Listing of any equipment removed or replaced.

11.6.3.3.2.1.5. Name and organization of person performing the maintenance.

11.6.3.3.2.1.6. Identity verification mechanism used.

11.6.3.3.2.1.7. Name of escort..

11.6.4. Maintain Records

11.6.4.1. Capture documentation appropriate to all systems operations processes:

11.6.4.1.1. Document and retain copies of all security self-assessments.

11.6.4.1.2. Document and retain copies of all system security operations notifications and implementation plans.

11.6.4.1.3. Document and retain copies of all security assessments.

11.6.4.1.4. Create and maintain systems security monitoring logs.

11.6.4.1.5. Create and maintain patch and remediation logs.

11.7. Systems Audit

11.7.1. Configure Auditing Capabilities

11.7.1.1. Systems Audit is used to ensure that systems are being operated in the manner according to which standards define, and so all systems should be configured to capture appropriate logging information:

11.7.1.1.1. Log Entry

11.7.1.1.1.1. The following data points should be captured for each log event entry:

11.7.1.1.1.1.1. Date and time of the event.

11.7.1.1.1.1.2. Component of the system affected by the event (if logging at the system level rather than component level).

11.7.1.1.1.1.3. Identity information of the individual that triggered the event.

11.7.1.1.1.1.4. Information describing the outcome of the event.

11.7.1.1.2. Log Storage

11.7.1.1.2.1. Sufficient on-line storage should be provided to retain a week’s worth of logging activity.

11.7.1.1.2.2. Sufficient off-line storage should be provided to retain a year’s worth of logging activity

11.7.1.1.2.3. Log data should be automatically transferred from on-line storage to off-line

storage on a weekly basis, whether the online storage capacity is filled or not/

11.7.1.1.2.4. The integrity of transferred log data should be verified within the off-line storage before the log data is removed from online storage.

11.7.1.1.2.5. Log data should be treated as High risk and all systems that store such data should also be considered High risk. Both data and systems should be afforded appropriate protection based on this risk classification.

11.7.1.1.3. Log Failure

11.7.1.1.3.1. If system logging fails because on-line storage is filled, the system should issue an alert to appropriate administrative staff and begin overwriting logs, starting with the oldest online log information.

11.7.1.1.3.2. If system logging fails for any other reason, the information system should issue an alert to appropriate administrative staff but take no other actions.

11.7.1.2. Test Auditing Capabilities. Conduct periodic audit capability testing to ensure that auditing capabilities continue to operate as intended:

11.7.1.2.1. Audit Testing Methodologies

11.7.1.2.1.1. On-line log storage should be artificially filled to just below capacity and the system allowed to process activity until capacity is reached to observe whether an automatic transfer to off-line storage occurs and whether automatic log overwrite begins.

11.7.1.2.1.2. Log functionality should be artificially halted and the system allowed continuing operations to observe whether processing continues or is halted.

11.7.1.2.1.3. Audit Testing Scheduling and Frequency. Audit testing should be performed on an at least annual basis.

11.7.1.3. Operate Auditing Capabilities. Analyze the information generated by these auditing capabilities on an ongoing basis to ensure systems are being operated in the appropriate manner and that security is being maintained:

11.7.1.3.1. Log Review Scheduling and Frequency

11.7.1.3.1.1. Where sufficient resources exist, all logs generated for all information systems should be reviewed daily.

11.7.1.3.1.2. Where sufficient resources for full log review do not exist partial random log review should be performed:

11.7.1.3.1.2.1. A randomly determined subset of all systems should be reviewed.

11.7.1.3.1.2.2. A randomly determined subset of all log entries should be reviewed.

11.7.1.3.1.2.3. Random review should be structured such that either every system or every log entry type should be reviewed weekly and every system and every log entry type should be reviewed biweekly.

11.7.1.3.2. Log Prioritization Scheme

11.7.1.3.2.1. Events that affect systems and/or information of greater criticality and/or sensitivity should receive a higher prioritization.

11.7.1.3.2.2. Events that occur with greater frequency should receive a higher prioritization.

11.7.1.3.2.3. Events that can be correlated across multiple systems should receive a higher prioritization.

11.7.1.3.2.4. Other factors can be included in the prioritization process:

11.7.1.3.2.4.1. Time of day of the event.

11.7.1.3.2.4.2. Day of the week and/or month of the event.

11.7.1.3.2.4.3. Source of the event.

11.7.1.3.2.4.4. Newness of the event.

11.7.1.3.3. Log Response

11.7.1.3.3.1. Where systems are determined to be out of synchronization with established standards, system documentation should be checked to determine if the variance is documented and approved. If not, the system owner is to be contacted and the system should be restored to established standards.

11.7.1.3.3.2. Where security attacks have occurred the event should be considered a Security Incident and Incident Response processes should be initiated.

11.7.1.3.3.3. Where policy violations are determined to have occurred, depending on the nature of the violations, various actions may be taken:

11.7.1.3.3.3.1. Policy violation sanctions may be taken.

11.7.1.3.3.3.2. Incident Response processes may be triggered.

11.7.2. Maintain Records

11.7.2.1. Capture documentation appropriate to all systems audit processes:

11.7.2.1.1. Document and retain copies of the configuration of logging capabilities for each system.

11.7.2.1.2. Document and retain copies of the results of all tests of system logging capabilities.

11.7.2.1.3. Maintain copies of all reports generated as a result of log monitoring and analysis.

11.8. Incident Response

11.8.1. Build a Team and Provide Training

11.8.1.1. Incident Response (IR) Responsibilities

11.8.1.1.1. Communications and coordination skills are required to manage the various team members and activities and to share information with employees of the organization outside of the IR team.

11.8.1.1.2. Network management skills are required to ensure network functionality and availability during an incident as well as to understand the impact of the incident in regard to network functions.

11.8.1.1.3. Systems management skills are required to ensure system functionality and availability during an incident as well as to understand the impact of the incident in regard to system functions.

11.8.1.1.4. Security management skills are required to ensure security infrastructure functionality and availability during an incident as well as to understand the impact of the incident in regard to security functions.

11.8.1.2. IR Roles

11.8.1.2.1. IR Team Managers should be assigned primary responsibilities of coordination and communication. Secondary responsibilities can extend into the various technical areas according to the skill set of the individual.

11.8.1.2.2. IR Network Leads should be assigned primary responsibilities of network analysis and trouble-shooting. Secondary responsibilities can extend into any area according to the skill set of the individual but are likely to match best to security infrastructure management.

11.8.1.2.3. IR Systems Leads should be assigned primary responsibilities of specific system analysis and trouble-shooting. Secondary responsibilities can extend into any area according to the skill set of the individual but are likely to match best to system management of alternate systems.

11.8.1.2.4. IR Security Leads should be assigned primary responsibilities of security infrastructure analysis and trouble-shooting. Secondary responsibilities can extend into any area according to the skill set of the individual.

11.8.1.3. IR Training

11.8.1.3.1. IR training should, at a minimum, address the following:

11.8.1.3.1.1. How to recognize an incident.

11.8.1.3.1.2. How to analyze an incident.

11.8.1.3.1.3. How to contain and eradicate an incident.

11.8.1.3.1.4. How to return to normal operations.

11.8.1.3.1.5. How to communicate and escalate during an incident.

11.8.1.3.1.6. How to operate all IR tools and resources.

11.8.1.4. IR Training Scheduling and Frequency

11.8.1.4.1. IR training should be provided for all IR team members within 30 days of initial assignment of the individual to the IR team.

11.8.1.4.2. IR training should be provided thereafter for all IR team members on an at least annual basis. Where possible, team members will be trained together as a group.

11.8.2. Build an Incident Response Capability

11.8.2.1. IR Purpose and Goals

11.8.2.1.1. Decide if IR will focus on monitoring and reporting versus active response.

11.8.2.1.2. Decide if IR will focus on externally sourced incidents, internally sourced incidents or both.

11.8.2.2. IR Communications

11.8.2.2.1. The following roles should be contacted during IR activities:

11.8.2.2.1.1. State of Kansas Chief Information Security Officer.

11.8.2.2.1.2. Senior management.

11.8.2.2.1.3. Legal and compliance departments.

11.8.2.2.1.4. Public relations department.

11.8.2.2.1.5. System owners for directly affected systems.

11.8.2.2.1.6. Data owners/custodians for directly affected data.

11.8.2.2.1.7. System owners for indirectly (upstream or downstream) affected systems.

11.8.2.2.1.8. Data owners/custodians for indirectly (upstream or downstream) affected data.

11.8.2.3. IR Supporting Strategies

11.8.2.3.1. Review the results of risk and security assessments.

11.8.2.3.2. Review the results of vulnerability and patch management operations.

11.8.2.3.3. Review the results of security architecture management operations.

11.8.2.4. IR Tools and Resources

11.8.2.4.1. Monitoring resources may include:

11.8.2.4.1.1. Intrusion detection systems.

11.8.2.4.1.2. Network sniffers and traffic analyzers.

11.8.2.4.1.3. Log aggregation and management systems.

11.8.2.4.2. Analysis resources may include:

11.8.2.4.2.1. Dedicated portable workstations.

11.8.2.4.2.2. Forensics analysis software.

11.8.2.4.2.3. Recordable media.

11.8.2.4.2.4. Asset and configuration inventories.

11.8.2.4.3. Response resources may include:

11.8.2.4.3.1. Dedicated communications devices.

11.8.2.4.3.2. Contact information for all stakeholders.

11.8.2.5. IR Plan Update Scheduling and Frequency

11.8.2.5.1. IR plans should be reviewed and updated on an at least annual basis or at such time as IR testing or IR operations indicate a deficiency in the IR plan..

11.8.3. Test the Plan

11.8.3.1. IR Testing Methodologies

11.8.3.1.1. The following capabilities should be included in the IR testing program:

11.8.3.1.1.1. Recognition of externally and internally sourced incidents.

11.8.3.1.1.2. Analysis to gather incident identification information.

11.8.3.1.1.3. Application of containment and eradication tasks appropriate to the type of incident.

11.8.3.1.1.4. Restoration of normal operations.

11.8.3.1.1.5. Co-ordination and communications.

11.8.3.1.2. IR testing can be conducted in one of two ways:

11.8.3.1.2.1. o Classroom or tabletop exercises walkthrough IR operations without any IR operations occurring.

11.8.3.1.2.2. o Functional or simulation exercises recreate actual incidents and require the execution of IR operations.

11.8.3.2. IR Testing Scheduling and Frequency

11.8.3.2.1. Classroom or tabletop exercises should be performed on at least an annual basis.

11.8.3.2.2. Functional or simulation exercises should be performed on at least a tri-annual basis.

11.8.4. Maintain Records

11.8.4.1. Capture documentation appropriate to all incident response processes:

11.8.4.1.1. Document and retain copies of incident response roles, responsibilities, assigned individuals and appropriate contact information.

11.8.4.1.2. Document and retain copies of incident response training materials.

11.8.4.1.3. Document and retain copies of the incident response plan, including preparatory materials.

11.8.4.1.4. Document and retain copies of completed incident response tests.

11.9. Contingency Planning

11.9.1. Contingency Plans

11.9.1.1. Build a Plan. Contingency planning requires the identification of assets to be protected by the plan, determination of the strategies applicable to the execution of the plan and the documentation of the plan itself:

11.9.1.1.1. Critical Resources and Recovery Time Objectives. By default systems will be categorized into four groupings for recovery purposes:

11.9.1.1.1.1. Systems deemed critical upon which the operation of other critical systems depends. These systems shall have a 120 minute (2 hour) Recovery Time Objective.

11.9.1.1.1.2. Systems deemed critical upon which the operation of no other critical systems depends. These systems shall have a 480 minute (8hour) Recovery Time Objective.

11.9.1.1.1.3. Systems deemed non-critical upon which the operations of critical systems depends. These systems shall have an 8 hour (1 business day) Recovery Time Objective.

11.9.1.1.1.4. Systems deemed non-critical upon which the operation of no critical systems depends. These systems shall have a 24 hour (1 day) Recovery Time Objective.

11.9.1.1.2. Recovery Prioritization Schedule

11.9.1.1.2.1. Systems recovery prioritization shall be in accordance with established criticality and Recovery Time Objectives.

11.9.1.1.3. Contingency Plan Update Frequency and Scheduling

11.9.1.1.3.1. Contingency plans will be reviewed and updated on an at least annual basis or at such time as contingency testing or contingency operations indicates a deficiency in the contingency plan.

11.9.1.2. Test the Plan. To ensure the applicability of the plan and to verify that the plan can be

acted upon as created, periodic testing is required:

11.9.1.2.1. Contingency Testing Methodologies.

11.9.1.2.1.1. The following capabilities must be included in the contingency testing program:

11.9.1.2.1.1.1. System recovery to a primary platform from backup.

11.9.1.2.1.1.2. System recovery to a secondary platform from backup.

11.9.1.2.1.1.3. System failover from a primary system to a redundant system.

11.9.1.2.1.1.4. System failover from a primary facility to a redundant facility.

11.9.1.2.1.1.5. System performance in all circumstances.

11.9.1.2.1.1.6. Restoration of normal operations in all circumstances.

11.9.1.2.1.1.7. Co-ordination and communications.

11.9.1.2.1.2. Contingency testing can be conducted in one of two ways:

11.9.1.2.1.2.1. Classroom or tabletop exercises walkthrough contingency operations without any contingency operations occurring.

11.9.1.2.1.2.2. Functional or simulation exercises recreate actual disruptions and require the execution of contingency operations.

11.9.1.2.2. Contingency Testing Frequency and Scheduling

11.9.1.2.2.1. Classroom or tabletop exercises shall be performed on at least an annual basis.

11.9.1.2.2.2. Functional or simulation exercises shall be performed on at least a triennial basis.

11.9.2. Contingency Infrastructure

11.9.2.1. Contingency Infrastructure. Appropriate infrastructure must be put in place to provide for appropriate ongoing operations in the event of a business impacting event:

11.9.2.1.1. Contingency Infrastructure

11.9.2.1.1.1. The use of data backup and restoration is an appropriate contingency measure for circumstances where data may become corrupted but primary systems continue to be available.

11.9.2.1.1.2. The use of redundant systems in the primary location is an appropriate contingency measure for circumstances where primary systems may become unavailable but primary facilities continue to be available.

11.9.2.1.1.3. The use of redundant facilities in an alternate location is an appropriate contingency measure for circumstances where primary facilities may become unavailable. Primary and redundant facilities must be geographically disparate enough so as not to be affected by the same event.

11.9.2.1.1.4. The use of redundant power delivery systems is an appropriate contingency measure where power fluctuations may render primary or secondary processing facilities powerless. Uninterruptible power supplies must provide for at least 5 minutes of continuous operations and generators must be provided with sufficient fuel for at least 48 hours of continuous operations.

11.9.2.1.1.5. The use of redundant telecommunications links is an appropriate contingency measure for circumstances where primary links may be lost but where systems require continuous inbound and outbound network connectivity.

11.9.3. Contingency Operations

11.9.3.1. Build a Team and Provide Training. Contingency planning is a security control that requires specialized capabilities. Building a team ensures they are always appropriately provided for:

11.9.3.1.1. Contingency Capabilities

11.9.3.1.1.1. Communications and coordination skills are required to manage the various team members and activities and to share information with employees of the organization outside of the contingency team.

11.9.3.1.1.2. Network management skills are required to ensure efficient and effective migration of communications functions during a disruption.

11.9.3.1.1.3. Systems management skills are required to ensure efficient and effective migration of system functions during a disruption.

11.9.3.1.1.4. Security management skills are required to ensure efficient and effective migration of security infrastructure functions during a disruption.

11.9.3.1.2. Contingency Roles

11.9.3.1.2.1. Contingency Team Managers must be assigned primary responsibilities of coordination and communication. Secondary responsibilities can extend into the various technical areas according to the skill set of the individual.

11.9.3.1.2.2. Contingency Network Leads must be assigned primary responsibilities of network migration. Secondary responsibilities can extend into any area according to the skill set of the individual but are likely to match best to security infrastructure management.

11.9.3.1.2.3. Contingency Systems Leads must be assigned primary responsibilities of specific system migration. Secondary responsibilities can extend into any area according to the skill set of the individual but are likely to match best to system management of alternate systems.

11.9.3.1.2.4. Contingency Security Leads must be assigned primary responsibilities of security infrastructure migration. Secondary responsibilities can extend into any area according to the skill set of the individual.

11.9.3.1.3. Contingency Training Frequency and Scheduling

11.9.3.1.3.1. Contingency training shall be provided for all contingency team members within 90 days of initial assignment of the individual to the contingency team.

11.9.3.1.3.2. Contingency training shall be provided thereafter for all contingency team members on an at least annual basis. Where possible, team members will be trained together as a group.

11.9.3.2. Backup Scheduling and Frequency. Systems and data backups are an important component of any contingency plan or contingency operations and so backups must be taken according to appropriate schedule:

11.9.3.2.1. Required Backup Schedule

11.9.3.2.1.1. Those systems deemed as critical by the organization will be fully backed up on both a monthly and a weekly basis and incrementally or differentially backed up on a daily basis.

11.9.3.2.1.2. Monthly backups will be retained for 12 months, weekly backups will be retained for 5 weeks and daily backups will be retained for 7 days.

11.9.3.2.1.3. Those systems not deemed as critical by the organization will be fully backed up on a monthly basis and incrementally or differentially backed up on weekly basis. Monthly backups will be retained for 6 months and weekly backups will be retained for 2 weeks.

11.9.4. Maintain Records

11.9.4.1. Capture documentation appropriate to all contingency planning standards:

11.9.4.1.1. Document and retain copies of contingency roles, responsibilities, assigned individuals and appropriate contact information.

11.9.4.1.2. Document and retain copies of contingency training materials.

11.9.4.1.3. Document and retain copies of the contingency plan, including preparatory materials (i.e. Business Impact Analysis output).

11.9.4.1.4. Document and retain copies of completed contingency tests.

11.10. Physical Security

11.10.1. Control Physical Access

11.10.1.1. Physical threats to systems can only be managed by implementing appropriate physical security controls:

11.10.1.1.1. Roles Requiring Physical Access

11.10.1.1.1.1. Regular physical access should be provided to only those individuals that work in facilities that host systems or system components and that have a regular requirement to physically access systems:

11.10.1.1.1.1.1. Administration staff.

11.10.1.1.1.1.2. Operations staff.

11.10.1.1.1.2. Occasional physical access may be provided to any individual so long as sufficient cause can be demonstrated:

11.10.1.1.1.2.1. Temporary administrative staff.

11.10.1.1.1.2.2. Temporary operations staff.

11.10.1.1.1.2.3. Third-party administrative or operations staff.

11.10.1.1.1.2.4. Project-specific staff.

11.10.1.1.2. Physical Access Controls

11.10.1.1.2.1. All facilities that house systems and/or system components should be secured with doors that have locks.

11.10.1.1.2.2. Dedicated areas within facilities that house systems and/or systems components should be secured with doors that have pick-resistant locks.

11.10.1.1.2.3. Dedicated areas within facilities that house systems and/or systems

components should make use of access monitoring solutions.

11.10.1.1.3. Access Logs

11.10.1.1.3.1. For all individuals that access facilities, the following information should be captured and (where applicable) verified:

11.10.1.1.3.1.1. Date and time of entry.

11.10.1.1.3.1.2. Name of accessing individual and authentication mechanism.

11.10.1.1.3.1.3. Name and title of authorizing individual.

11.10.1.1.3.1.4. Reason for access.

11.10.1.1.3.1.5. Date and time of departure.

11.10.1.1.4. Delivery and Removal Orders and Logs

11.10.1.1.4.1. For all deliveries and removal of systems or system components, the following information should be captured (and where applicable) verified:

11.10.1.1.4.1.1. Date and time of delivery/removal.

11.10.1.1.4.1.2. Name and type of equipment to be delivered or removed.

11.10.1.1.4.1.3. Name and employer of the individual performing the delivery/removal and the authentication mechanism used.

11.10.1.1.4.1.4. Name and title of authorizing individual.

11.10.1.1.4.1.5. Reason for delivery/removal.

11.10.2. Physical Environmental Control

11.10.2.1.1. Provide Environmental Controls. Appropriate environmental controls are necessary to ensure the availability of systems:

11.10.2.1.1.1. Temperature and Humidity Specifications

11.10.2.1.1.1.1. The temperature of those areas within a facility that house systems or system components should be maintained between 68 and 77 degrees Fahrenheit (20 and 25 degrees Celsius).

11.10.2.1.1.1.2. The humidity of those areas within a facility that house systems or system components should be maintained between 40 and 55 percent relative humidity.

11.10.2.1.1.2. Power Delivery Specifications

11.10.2.1.1.2.1. Power cabling and power equipment should be placed within facilities such that it is protected from direct access by visitors and is sheltered from direct damage.

11.10.2.1.1.2.2. High risk and very high risk system components should be provided with redundant power connections.

11.10.2.1.1.2.3. Short-term redundant power protection should be provided in the form of an Uninterruptible Power Supply (UPS).

11.10.2.1.1.2.4. Long-term redundant power protection should be provided in the form of a dedicated generator.

11.10.2.1.1.2.5. Emergency lighting with sufficient coverage and capacity to allow for

orderly evacuation in the event of a power failure should be provided.

11.10.2.1.1.2.6. Within-facility remote shutoff capabilities for all system components should be provided in the event that the power supply must be terminated but the system is inaccessible.

11.10.2.1.1.3. Fire Response Specifications

11.10.2.1.1.3.1. Fire detection systems that automatically activate and provide notification of activation should be provided.

11.10.2.1.1.3.2. Fire suppression systems that automatically activate and provide notification of activation should be provided.

11.10.2.1.1.4. Water Protection Specifications

11.10.2.1.1.4.1. A master water shutoff valve that, at a minimum, controls water distribution to all areas that house system components should be provided.

11.10.2.1.1.4.2. Ensure that the master water shutoff valve is operational by testing on an at least monthly basis.

11.10.2.1.1.5. System and Component Placement

11.10.2.1.1.5.1. Systems and system components should be placed within facilities such that their exposure to natural hazards (external fire, external flood, tornado, etc.) is minimized.

11.10.2.1.1.5.2. Systems and system components should be placed within facilities such that their exposure to man-made hazards (vandalism, internal fire, internal flood, etc.) is minimized

11.10.3. Maintain Records

11.10.3.1. Capture documentation appropriate to all physical security processes:

11.10.3.1.1. Create and maintain Access Logs for all facilities that host systems or system components.

11.10.3.1.2. Create and maintain Delivery and Removal Orders and Delivery and Removal Logs for all facilities that host systems or system components.

11.10.3.1.3. Create and maintain Facilities Environmental Control Logs for all facilities that host systems or system components.

11.11. Personnel Security

11.11.1. Acceptable Usage

11.11.1.1. Establish Acceptable Usage Baselines. Acceptable Usage Baselines define what qualifies as appropriate and inappropriate behaviors during the course of day to day operations:

11.11.1.1.1. Internet and e-Mail Usage

11.11.1.1.1.1. Internet and e-mail usage must be restricted as both activities make use of public and unsecured networks:

11.11.1.1.1.1.1. The Internet is to be used primarily for business purposes and usage will be monitored and controlled at all times.

11.11.1.1.1.1.2. E-mail is to be used primarily for business purposes and usage will be monitored and controlled at all times.

11.11.1.1.2. System and Computer Usage.

11.11.1.1.2.1. Systems and systems components, including computers of all kinds, are the property of the organization:

11.11.1.1.2.1.1. Access to, and use of, systems and the components that form them will be monitored and controlled at all times.

11.11.1.1.3. Software and Data Usage

11.11.1.1.3.1. The software tools the organization provides and the data they create and manipulate are the property of the organization:

11.11.1.1.3.1.1. Software is to be used for its intended purpose. It is not to be copied, installed or deleted without appropriate authorization.

11.11.1.1.3.1.2. Data is to be used for its intended purpose. It is not to be copied, edited, appended to or deleted without appropriate authorization. Further such activities will be monitored and controlled at all times.

11.11.1.1.4. Telephone Usage

11.11.1.1.4.1. The telephone system, including all telephones and fax machines, is the property of the organization:

11.11.1.1.4.1.1. The telephone system, including all and analog and digital lines, will be monitored and controlled at all times.

11.11.1.1.5. Materials Usage

11.11.1.1.5.1. The office materials, furnishings and supplies provided to employees are the property of the organization and are to be used for business purposes only:

11.11.1.1.5.1.1. Generic materials (those that do not imply consent of the organization such as pens, blank paper, etc.) may be freely accessed but are not to be removed from those facilities without prior consent.

11.11.1.1.5.1.2. Specific materials (those that imply consent of the organization such as letterhead and stamps, etc.) must have restricted access and are not to be removed from the facilities without prior consent.

11.11.1.1.6. Sanctions

11.11.1.1.6.1. A Violation of any of the constraints of the security policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

11.11.1.1.6.1.1. Minor breaches will result in written reprimand.

11.11.1.1.6.1.2. Multiple minor breaches will result in suspension.

11.11.1.1.6.1.3. Serious breaches will result in termination.

11.12. Personnel Operations

11.12.1. Establish Pre-Hiring Processes. Since employees will be assigned access to systems and information, steps should be taken to ensure appropriate security considerations are taken into account:

11.12.1.1. Positional Role

11.12.1.1.1. Role definition should be based partially on employee position:

11.12.1.1.1.1. Senior management.

11.12.1.1.1.2. Middle management.

11.12.1.1.1.3. Senior non-management.

11.12.1.1.1.4. Non-management.

11.12.1.1.2. Role definition should be based partially on employee responsibility:

11.12.1.1.2.1. Administrative staff.

11.12.1.1.2.2. Non-administrative staff.

11.12.1.1.3. Role definition should be based partially on employee access requirements:

11.12.1.1.3.1. Read access.

11.12.1.1.3.2. Write access.

11.12.1.1.3.3. Edit access.

11.12.1.1.3.4. Delete access.

11.12.1.2. Risk Categorizations by Role

11.12.1.2.1. Very High risk roles constitute those that access at least one very high risk system or access mostly (greater than 50% of systems accessed) high risk systems.

11.12.1.2.2. High risk roles constitute those that access at least one high risk system or access mostly (greater than 50% of systems accessed) medium risk systems.

11.12.1.2.3. Medium risk roles constitute those that access at least one medium risk system or access mostly (greater than 50% of systems accessed) low risk systems.

11.12.1.2.4. Low risk roles constitute those that access at least one low risk system.

11.12.1.2.5. Very Low risk roles constitute those that access only very low risk systems.

11.12.1.3. Screening Criteria by Categorization

11.12.1.3.1. For very low and low risk roles, the screening process should review applicant submitted documentation and verify accuracy:

11.12.1.3.1.1. Verify employment position and term with listed employers.

11.12.1.3.1.2. Verify education with listed educational facilities.

11.12.1.3.1.3. Verify listed certifications with certifying organizations.

11.12.1.3.2. For medium risk roles, the screening process should include the tasks outlined above plus contacting at least one listed reference.

11.12.1.3.2.1. Discuss applicant’s strengths and weaknesses.

11.12.1.3.2.2. Discuss applicant’s responses to pressure situations.

11.12.1.3.3. For high risk roles, the screening process should include the tasks as outlined above plus contacting one previous supervisor/manager:

11.12.1.3.3.1. Discuss applicant’s strengths and weaknesses.

11.12.1.3.3.2. Discuss applicant’s responses to pressure situations.

11.12.1.3.4. For very high risk roles, the screening process should include the tasks as

outlined above plus a criminal background check:

11.12.1.3.4.1. Pay particular attention to activities that are indicative of questionable character or poor response to stressful situations.

11.12.2. Hire Employees in a Structured Fashion. Upon initial hire, employee identity should be verified and accounts created with appropriate access rights and permissions:

11.12.2.1. Account and Permissions Provisioning and Review

11.12.2.1.1. Account permission provisioning should be performed by one dedicated set of administrators.

11.12.2.1.2. Account and permission review should be performed by a second set of dedicated administrators.

11.12.3. Transfer Employees in a Structured Fashion. Employees that change positions within the organization should be screened according to their new position and have system account access and permissions reviewed:

11.12.3.1. Account and Permissions Revocation and Review

11.12.3.1.1. Review access to revoked accounts should be provided for no more than thirty days.

11.12.3.1.2. Data transfer orders should be provided in writing and should specify:

11.12.3.1.2.1. The data to be transferred.

11.12.3.1.2.2. The location to be transferred from.

11.12.3.1.2.3. The location to be transferred to.

11.12.3.1.2.4. The reason for the data transfer.

11.12.3.1.3. Permanent deletion orders should be provided in writing.

11.12.4. Terminate Employees in a Structured Fashion. Employee termination should include the recovery of all issued materials and the closing of all established accounts:

11.13. Maintain Records

11.13.1. Capture documentation appropriate to personnel security processes:

11.13.1.1. Maintain copies of all submission and screening documents for applicants that are hired for future reference.

11.13.1.2. Maintain copies of all completed access agreements.

11.13.1.3. Maintain copies of all provisioned system access accounts and associated permission.

11.13.1.4. Maintain records of all issued organization owned materials.

11.13.1.5. Maintain copies of all exit interview documents.