**TITLE 1 GENERAL GOVERNMENT ADMINISTRATION**
**CHAPTER 12 INFORMATION TECHNOLOGY**
**PART 20 INFORMATION SECURITY OPERATION MANAGEMENT**

**1.12.20.1 ISSUING AGENCY.** Department of Information Technology.
[1.12.20.1 NMAC - N/E, 04/14/2010]

**1.12.20.2 SCOPE.** This rule applies to all executive branch agencies, and any other state entity which utilizes the state information technology (IT) infrastructure, contractors and subcontractors and any other non-state government staff members, and outsourced third parties, who have access to, store, or manage state government information on site at a state agency or off-site, as approved by a state agency.
[1.12.20.2 NMAC - N/E, 04/14/2010]

**1.12.20.3 STATUTORY AUTHORITY.** NMSA 1978 Section 9-27-6 F (3) and 9-27-6 I (1).
[1.12.20.3 NMAC - N/E, 04/14/2010]

**1.12.20.4 DURATION.** Permanent.
[1.12.20.4 NMAC - N/E, 04/14/2010]

**1.12.20.5 EFFECTIVE DATE.** April 14, 2010, unless a later date is cited at the end of a section.
[1.12.20.5 NMAC - N/E, 04/14/2010]

**1.12.20.6 OBJECTIVE.** The purpose of this rule is to establish security operation management practices for executive branch agencies and any other state entity which utilizes the state information technology (IT) infrastructure in the operation of their information technology (IT) systems and infrastructure/networks. This rule encompasses all systems, automated and manual, for which the state has administrative responsibility, including systems managed or hosted by third parties on behalf of a state agency.
[1.12.20.6 NMAC - N/E, 04/14/2010]

**1.12.20.7 DEFINITIONS.** Defined terms apply to this rule and all other rules promulgated by the secretary and adopted by the information technology commission.

**A.** **"Act"** means the Department of Information Technology Act, NMSA 1978 9-27-1 et seq.

**B.** **"Agency"** means an executive branch agency of the state or any other state entity which uses the state IT infrastructure.

**C.** **"Architectural configuration requirement (ACR)"** means the technical specifications for information architecture and information technology system purchases for agencies.

**D.** **"CIO"** means chief information officer and refers to the secretary of the department as chief information officer of the state or any agency CIO.

**E.** **"Commission"** means the information technology commission.

**F.** **"Department or DoIT"** means the department of information technology.

**G.** **"Exception"** means a request, limited in scope and duration, granted by the department allowing an agency an exclusion from compliance with a rule, ACR or guideline.

**H.** **"Firewall"** means a part of a computer system or network designed to block unauthorized access while permitting authorized communications. It is a device or set of devices which is configured to permit or deny computer based applications based upon a set of rules and other criteria.

**I.** **"Individual"** means a natural person, a human being.

**J.** **"Information owner"** means the individual or individuals held managerially and financially accountable for a dataset and who have legal ownership rights to a dataset even though the dataset may have been collected/collated/disseminated by another party.

**K.** **"Information security officer ("ISO")** means a senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy and program to ensure information assets are adequately protected

**L.** **"Information technology ("IT")** means computer hardware, software and ancillary products and services including: systems design and analysis, acquisition, storage and conversion of data; computer programming, information storage and retrieval, voice, radio, video and data communications, requisite systems, simulation and testing, and related interactions between users and information systems.

**M.** **"Information technology project"** means the purchase, replacement, development or modification of an IT component or system.

**N.** **"IT asset"** means all elements of software and hardware found in an IT environment.

**O.** **"Malicious code"** is the term used to describe any code in any part of a software system or script intended to cause undesired effects, security breaches or damage to a system. Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors, and malicious active content.

**P.** **"Network segregation"** means controlling the security of networks by dividing them into separate secure networks. Security measures can then be applied to further segregate the network environments.

**Q.** **"Password"** means a secret series of characters that enables a user to access a file, computer, or program. On multi-user systems, each user must enter his or her password before the computer will respond to commands. The password helps ensure that unauthorized users do not access the computer. In addition, data files and programs may require a password.

**R.** **"Person"** means an individual, association, organization, partnership, firm, syndicate, trust, corporation, and every legal entity.

**S.** **"Portable computing devices or removable media devices"** means, but is not limited to, removable media such as thumb or USB drives, external hard drives, laptop or desktop computers, mobile/cellular phones, smartphones or personal digital assistants (PDA's) owned by or purchased by agency employees, contract personnel, or other non-state user(s).

**T.** **"Privileged accounts"** means accounts required for systems to function; they are frequently used by system administrators in their performance of their job duties. These special system privileges are primarily used when major changes to the system are necessary by administrators.

**U.** **"Rule"** means any rule promulgated by the department for review and approval by the commission which requires compliance by executive agencies and any other state user of the state IT infrastructure.

**V.** **"Secretary"** means the secretary of the department of information technology.

**W.** **"Segregation of security duties"** means disseminating the tasks and associated privileges for a specific business process among multiple users to reduce the potential for damage from the actions of one person. IT staff should be organized in a manner that achieves adequate separation of duties in the agency.

**X.** **"State"** means New Mexico, or, when the context indicates a jurisdiction other than New Mexico, any state, district, commonwealth, territory, or possession of the United States.

**Y.** **"State CIO"** means the cabinet secretary of the department of information technology.

**Z.** **"State information architecture"** means a logically consistent set of principles, policies and standards that guides the engineering of state government’s information technology systems and infrastructure in a way that ensures alignment with state government’s business needs.

**AA.** **"State information technology strategic plan"** means the information technology planning document for the state that spans a three-year period.

**BB.** **"Virtual private network ("VPN")** means a network that uses a public telecommunication infrastructure, such as the internet, to provide remote offices or individual users with secure access to their organization's network. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

[1.12.20.7 NMAC - N/E, 04/14/2010]

**1.12.20.8 DOCUMENTATION OF SECURITY OPERATIONS:**

**A.** All agency IT technical operations shall have documented security operating instructions, management processes, and formal incident management procedures in place that define roles and responsibilities of individuals who operate or use agency IT technical operations and facilities.

**B.** Where one agency provides a server, application, or network services to another agency, operational and management responsibilities shall be coordinated by the CIOs of both agencies.

**C.** All agencies shall develop procedures for conducting background investigations on IT employees or contractors as required by state law, NMSA 1978 9-27-6 C (15) and D.

[1.12.20.8 NMAC - N/E, 04/14/2010]

**1.12.20.9 SEGREGATION OF SECURITY DUTIES:** Segregation of duties is required to reduce the risk of accidental or deliberate damage to the state or agency IT system through misuse by a person or persons. In small agencies in which separation of duties is difficult to achieve, with the approval of DoIT, the agency shall implement

compensatory controls including, but not limited to, actively monitoring its IT operations, audit trails, and by regularly documented management supervision.
[1.12.20.9 NMAC - N/E, 04/14/2010]

**1.12.20.10 NETWORK MANAGEMENT:** All agencies shall implement a range of network controls to maintain security in its trusted, internal network, and to ensure the protection of connected services and networks. Such controls help prevent unauthorized access and use of the agencies' private networks. The following controls, at minimum, shall be implemented:

**A.** individuals with operational responsibility for networks shall be separate from those with computer operations responsibility; responsibilities and procedures for remote access shall be established;

**B.** controls, such as data encryption, shall be implemented to safeguard data integrity and the confidentiality of data passing over public networks (internet);

**C.** all client-based VPN connections shall have split tunneling disabled; VPN connections to the agency are only permitted from agency managed VPN devices;

**D.** agencies' networks shall implement private address routing to public addresses when sending over the internet to minimize the exposure of public routable addresses;

**E.** firewall policies shall be configured to accept only inbound and outbound data traffic which is required based on business needs; all other data traffic should be denied;

**F.** firewall policies shall take into account the source and destination of the traffic in addition to the content;

**G.** data traffic with invalid or private addresses shall be default blocked from delivery;

**H.** proposed modifications to network and security equipment must be requested and approved for implementation through the agency change management procedure;

**I.** to prevent unauthorized modifications of the firewall configuration, the firewall administrator must review the firewall configuration quarterly;

**J.** any form of cross-connection, which bypasses the firewall, is strictly prohibited;

**K.** remote firewall administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access;

**L.** details of firewall, and security devices type, software versions, and configuration data will not be disclosed without the permission of the agency CIO;

**M.** agencies shall define security zones and create logical entities and rules for what comprises permissible data and network traffic between different agency business units; and

**N.** agencies shall perform network segmentation to control the flow of data between hosts on different segments of the network to provide enhanced security, network performance, and connectivity.
[1.12.20.10 NMAC - N/E, 04/14/2010]

**1.12.20.11 PRIVILEGED ACCOUNTS MANAGEMENT:** The issuance and use of privileged accounts in agencies shall be restricted and controlled by system administrator management in the agency.

**A.** Agencies shall develop processes to ensure that if a privilege account is issued, the use of such privileged accounts is monitored by the manager of system administration, or the CIO.

**B.** Agencies shall promptly investigate any suspected misuse of these accounts by the manager of system administration or DoIT or an agency approved independent contractor.

**C.** Agencies shall change passwords of system privileged accounts no less than every 60 days.
[1.12.20.11 NMAC - N/E, 04/14/2010]

**1.12.20.12 ACCESS CONTROL POLICY:** To preserve the integrity, confidentiality, and availability of the system and the data, the agency's information assets shall be protected by logical as well as physical access control mechanisms commensurate with the value and sensitivity of the system, the ease of recovery of the assets and the direness of consequences, legal or otherwise, if the loss or compromise were to occur.

**A.** Agencies' CIOs are responsible for determining who shall have access to sensitive and protected information resources within the agency. Access privileges shall be granted by the CIO in accordance with the particular user's role and job responsibilities in the agency.

**B.** Agency enforcement of its access control policy shall be verified during an independent annual risk assessment which shall be performed by DoIT or a DoIT approved contractor.
[1.12.20.12 NMAC - N/E, 04/14/2010]

**1.12.20.13 OPERATING SYSTEM ACCESS CONTROL:**

**A.** Access to agency operating system code, commands and services shall be restricted to individuals with specialized skills such as systems programmers, database administrators, network, and security administrators who require access to perform their daily job responsibilities.

**(1)** Each of these individuals who are given access shall have assigned to them a unique privileged account (user ID).

**(2)** User IDs shall not disclose nor provide any indication of the user's supervisor, manager, administrator, or privilege level.

**B.** To allow administrator activities to be tracked to the individual responsible for the work or changes to the system, such as system programmers, database administrators, network administrators and security administrators, a second user ID shall be provided for use when the particular individual performs necessary business transactions unrelated to his or her regular job functions (operating system, database, network and security functions), such as accessing an employee's electronic records.

**C.** Under some agency specific circumstances, where there is a clear business requirement or system limitation, the use of a shared user ID/password for a group of users or a specific job can be used by obtaining written approval by the agency ISO and agency CIO. In such situations, additional controls shall be implemented by the agency to ensure accountability of the device operating system is maintained.

**D.** Where technically feasible, default administrator accounts shall be renamed, removed, or disabled. The default passwords for these accounts shall be changed if the account is retained, even if the account is renamed or disabled.

[1.12.20.13 NMAC - N/E, 04/14/2010]

**1.12.20.14 APPLICATION ACCESS CONTROL:**

**A.** Access to agency business and systems applications shall be restricted to those individuals who have an identified business need to access those applications or systems in the performance of their job responsibilities.

**B.** Access to source code for applications and systems shall be restricted; any such access shall be further restricted so that only authorized agency staff and agency supervised contractors can access those applications and systems for which they directly provide support.

[1.12.20.14 NMAC - N/E, 04/14/2010]

**1.12.20.15 NETWORK ACCESS CONTROL:** Access to an agency's trusted internal network shall require all agency authorized users to authenticate themselves through use of an individually assigned user ID or other agency approved authentication mechanism (e.g., password, token, smart card). Network controls shall be developed and implemented by the agency to ensure that an authorized user can access only those network resources and services necessary to perform their assigned job responsibilities.

[1.12.20.15 NMAC - N/E, 04/14/2010]

**1.12.20.16 USER AUTHENTICATION FOR EXTERNAL CONNECTIONS (REMOTE ACCESS CONTROL):**

**A.** To maintain information security, agency must require through published policies and procedures consistent with these rules, that individual accountability shall be maintained at all times, including during remote access.

**B.** Connection to the agency's networks shall be provided in a secure manner to preserve the integrity of the network, to preserve the data transmitted over that network, and to maintain the availability of the network. Security mechanisms shall be in place to control remote access to agency systems and networks from fixed or mobile locations.

**C.** Approval for any such remote connection shall first be obtained from the agency management and the agency CIO or ISO. Prior to approval being granted, the CIO shall review the request to determine what needs to be accessed and what method of access is desired and document the risks involved and technical controls required for such connection to take place.

**D.** Because of the level of risk inherent with remote access, the agency shall require use of a stronger password or another comparable method of protection prior to allowing connection to any agency network. Users shall be informed that all sessions performed remotely are subject to periodic and random monitoring by the agency.

**E.** When accessing an agency network remotely, identification and authentication of the user shall be performed by the remote access system (VPN) in such a manner as to not disclose the password or other authentication information that could be intercepted and used by a third-party.

**F.** All remote connections to an agency computer shall be made through managed central points-of-entry or "common access point." Using this type of entry system to access an agency computer provides simplified and cost effective security, maintenance, and support.

**G.** Vendors which may be provided access to agency computers or software, will be required to have individual accountability. For any agency system (hardware or software) for which there is a default user ID or password that came with the system for use in set up or periodic maintenance of the system , that account shall be disabled until the user ID is needed and requested. Any activity performed while a vendor user ID is in use shall be logged on the remote access system by an external logger. Since such maintenance accounts are not regularly used, the vendor user ID shall be disabled, the password changed, and other controls shall be implemented by the agency to prevent or monitor unauthorized use of these privileged accounts during periods of inactivity.

**H.** In special cases wherein servers, storage devices, or other computer equipment has the capability to automatically connect to a vendor in order to report problems or suspected problems, the agency ISO shall review any such connection and process to report certain events back to the system's manufacturer for performance "tuning" to ensure that such connectivity does not compromise the agency or other third-party connections.

**I.** Agency personnel will only be allowed to work from a remote location upon authorization by the CIO and agency management. Once approved, appropriate arrangements shall be made pursuant to agency written policy and procedures, consistent with this rule, to ensure the work environment at the remote location provides adequate security for transmission of agency data and protection of computing resources. The agency shall identify to the user the appropriate protection mechanisms necessary to protect against theft of agency equipment, unauthorized disclosure of agency information, misuse of agency equipment, unauthorized access to the agency internal network, or facilities by anyone besides the specifically identified and approved user, including family and friends. To ensure the proper security controls are in place and all state security standards are followed, the agency will approve remote access after consideration and documentation of their review following:

**(1)** the physical security of the remote location, including the use of any portable devices at any location other than an employee's approved work station;

**(2)** the method of transmitting information given the sensitivity of agency's internal system; and

**(3)** clearly defined business continuity procedures, including the capability of backing up critical information.

**J.** The following access system controls shall be implemented. Agency ISO or CIO shall monitor and audit their use:

**(1)** a definition of the type of information accessed (such as sensitive or confidential information under HIPAA) and the systems and services that the remote user is authorized to access;

**(2)** procedures and end user system requirements for secure remote access, such as authentication tokens or passwords, shall be documented by the agency including provisions for revocation of authorization and return of equipment to the agency;

**(3)** access system support and usage procedures provided to the users;

**(4)** implementation of suitable network boundary controls to prevent unauthorized information exchange between agency networks connected to remote computers and externally connected networks, such as the internet; such measures shall include firewalls and intrusion detection techniques at the remote location; and

**(5)** physical security of the equipment used for remote access (e.g. such as cable locking device, or locking computer cabinet/secure storage area).

[1.12.20.16 NMAC - N/E, 04/14/2010]

**1.12.20.17 DEDICATED NETWORK CONNECTIONS:**

**A.** The internet is inherently insecure, access to the internet is prohibited from any device that is connected (wired or wireless) to any part of the state network unless such access is authorized via exception signed by the state CIO. Such access includes accounts with third-party internet service providers.

**B.** Any dedicated network connection from the agency network to any external network (either within or outside state government) shall be first approved in writing by the DoIT.

**C.** Dedicated network connections shall be allowed after the requesting agency has presented its proposed network architecture for approval by the DoIT; DoIT will approve if the proposal has acceptable security controls and procedures in place, and appropriate security measures have been implemented by the agency to protect state network resources. The agency shall perform a risk analysis of the connection to ensure that the connection to

the external network shall not compromise the agency's private network. The agency may require that additional controls, such as the establishment of firewalls and a DMZ (demilitarized zone) be implemented between the third-party connection and the agency.

**(1)** The business case for the dedicated connection is still valid and the dedicated connection is still required.

**(2)** The security controls are in place (e.g., filters, rules, access control lists) are current and are functioning correctly.

**D.** The dedicated connection to the agency network shall be accomplished by the agency in a secure manner to preserve the integrity of the agency network, preserve the integrity of the data transmitted over that network, and the availability of the network to the agency. Security requirements for each connection shall be assessed individually and permission to use such connection shall be driven by the specific business needs of the agency. Only agency CIO-approved and qualified staff or agency CIO-approved and qualified third-party shall be permitted to use sniffers or similar technology on the network to monitor operational data and security events.

**E.** The agency ISO or designee shall every six (6) months review external network connections, audit trails and system logs for abuses and anomalies.

**F.** Any agency-approved third-party network or workstation connection to an agency network shall:

**(1)** have written justification in the form of a clear business case provided to the agency CIO for any such network connection;

**(2)** sign an agency non-disclosure agreement ("NDA"); the non-disclosure agreement shall be signed by a duly appointed representative from the third-party organization who is legally authorized to sign such an agreement;

**(3)** have equipment in place that conforms to this rule and any other applicable state security standards, complies with the agency's technical architecture, and be approved in writing by the agency CIO; and

**(4)** use encryption to ensure the confidentiality and integrity of any sensitive or confidential data passing over the external network connection.

[1.12.20.17 NMAC - N/E, 04/14/2010]

**1.12.20.18 NETWORK SEGREGATION:** When an agency desires to connect its network to any other third party network or its network becomes a segment on a larger network, controls shall be in place to prevent access by users from other connected networks to sensitive areas of the agency's private network. Such connection must first be approved by the agency CIO. Firewalls or other agency approved technologies shall be implemented to control access to secured resources on the trusted agency network. If any such third party network connections are contemplated, the agency CIO must first approve and receive approval from the state CIO.

[1.12.20.18 NMAC - N/E, 04/14/2010]

**1.12.20.19 WIRELESS NETWORKS, BLUETOOTH, AND RADIO FREQUENCY IDENTIFICATION:**

**A.** No wireless network or wireless access point shall be installed prior to an agency performed risk assessment and the written approval of the agency CIO.

**B.** Suitable controls, such as media access control (MAC), address restriction, authentication, and encryption, shall be implemented by the agency to ensure that a wireless network or access point cannot be exploited to disrupt agency information services or to gain unauthorized access to agency information. When selecting wireless technologies, such as 802.11x or its predecessors or its successor, wireless network security features on the equipment shall be available and implemented at the time of deployment.

**C.** Access to systems that hold sensitive information or the transmission of protected or sensitive information via a wireless network is not permitted unless and until appropriate and adequate measures have been implemented and approved by the state CIO. Such measures shall include authentication, authorization, encryption, access controls, and logging.

[1.12.20.19 NMAC - N/E, 04/14/2010]

**1.12.20.20 USER REGISTRATION AND MANAGEMENT:**

**A.** A user management process shall be established, documented and provided to all IT staff of the agency which outlines and identifies all aspects of user management including the generation, distribution, modification, and deletion of user accounts. This process shall ensure that only authorized individuals have access to agency applications and information and that such users only have access to the resources required to perform authorized services.

**B.** The user management process shall include the following sub-processes:

**(1)** how to enroll new users;

**(2)** how to remove user IDs;

**(3)** how to grant a "privileged account" to a user;

**(4)** how to remove "privileged accounts" from a user;

**(5)** how the agency defines "periodic review" of "privileged accounts";

**(6)** how the agency defines "periodic review" of users enrolled in any state IT system;

**(7)** how to assign a new authentication token (e.g. password reset processing); and

**(8)** how proper enforcement of user management shall be verified during an independent annual risk assessment.

**C.** The appropriate information owner or other authorized officer shall make requests for the registration and granting of any data access rights.

**D.** For applications that interact with individuals who are not employees of the agency, including but not limited to employees of other state agencies, approved contractors or approved vendors, the information owner is responsible for ensuring an appropriate user management process is implemented. Standards for the registration of such external users shall be defined by the agency CIO, to include what credentials shall be provided to prove the identity of the user requesting registration, validation of the request, and the scope of access that may be provided.
[1.12.20.20 NMAC - N/E, 04/14/2010]

**1.12.20.21 USER PASSWORD MANAGEMENT:** Password protocols shall be developed consistent with state standards and implemented to ensure all authorized individuals accessing agency resources follow 1.12.11 NMAC Enterprise Architecture. Such password protocols shall be mandated by automated system controls whenever possible. Password protocols should include, but not be limited to:

**A.** compliance with 1.12.11.16 NMAC (Security Password rule);

**B.** prohibiting the storage of passwords in clear text;

**C.** prohibiting the use of passwords that could be easily guessed or subject to disclosure through a dictionary attack;

**D.** direction for keeping passwords confidential;

**E.** prohibiting any and all password sharing;

**F.** directing users to change passwords at regular intervals;

**G.** direction for changing temporary passwords at the first logon;

**H.** enforcing the implementation standard password formats to include a mix of alphabetic, numeric, special, and upper/lower case characters;

**I.** automated logon processes which must be approved by agency CIO;

**J.** implementing state password standards and protocols on agency computing resources; and

**K.** verifying proper enforcement of password management by the agency during an annual independent risk assessment.
[1.12.20.21 NMAC - N/E, 04/14/2010]

**1.12.20.22 PROHIBITION OF USE OF PERSONAL COMPUTING DEVICES ON STATE EQUIPMENT OR SYSTEMS:**

**A.** Connecting any computing device not owned by the state of New Mexico to a state network or to any state computing device is prohibited unless authorized in writing by the agency CIO.

**B.** Installation of any software, executable or other file to any state computing device is prohibited if that software, executable, or other file was downloaded by, is owned by, or was purchased by an employee or contractor with his or her own funds.

**C.** Installation of downloaded software, executables, or other files to any state computing device is prohibited when downloaded or installed by an employee or contractor for personal use. Downloaded software, executable, or other files include, but are not limited to: SKYPE, music files or other software, and personal photos.
[1.12.20.22 NMAC - N/E, 04/14/2010]

**1.12.20.23 VULNERABILITY SCANNING:**

**A.** All state owned computing devices that are, or will be, accessible from outside the agency network shall be scanned by DoIT, DoIT-approved contractor or DoIT-approved agency IT staff for vulnerabilities and weaknesses prior to installation on the state network and following any changes made to the software, operating system, or configuration.

**B.** For both internal and external systems, scans shall be performed at least annually by DoIT or a DoIT-approved contractor to ensure that no major vulnerabilities have been introduced into the environment. The frequency of additional scans shall be determined by the agency ISO; such determination shall depend upon the criticality and sensitivity of the information on the system.

**C.** Network vulnerability scanning shall be conducted after any new network software or hardware has been installed and after major configuration changes have been made on critical and essential agency systems.

**D.** Output from the scans shall be reviewed immediately by the agency IT staff or agency ISO and the results communicated to the agency CIO.

**E.** Any vulnerability detected as a result of a scan shall be immediately evaluated for risk and actions shall be taken by the agency to mitigate such risk.

**F.** Tools used to scan for vulnerabilities shall be updated quarterly to ensure that any recently discovered vulnerabilities are included in any scans.

**G.** If an agency has outsourced a server, application, or network services to another agency, the responsibility for vulnerability scanning shall be coordinated by both agencies.

**H.** Anyone authorized to perform vulnerability scanning shall have its process defined, documented, tested, and followed at all times to minimize the possibility of disruption of services. Reports of exposures to vulnerabilities shall immediately be forwarded to the agency CIO and agency general counsel.

**I.** Any vulnerability scanning other than that performed by an agency ISO shall be conducted only by qualified individuals or organizations contracted with or otherwise authorized in writing by the agency's CIO.
[1.12.20.23 NMAC - N/E, 04/14/2010]

**1.12.20.24 PENETRATION AND INTRUSION TESTING:** All state computing infrastructures that provide information through a public network, either directly or through another dedicated circuit, and that provide information externally (such as through the world-wide web), shall be subject to annual independent penetration analysis and intrusion testing by qualified, independent third-party contractor approved by DoIT.

**A.** Penetration analysis and testing shall be used to determine whether:

**(1)** a user can make an unauthorized change to an application;

**(2)** a user can access the application and cause it to perform unauthorized tasks;

**(3)** an unauthorized individual can access, destroy or change any data;

**(4)** an unauthorized individual may access the application and cause it to take actions unintended by the application designer(s).

**B.** The output of the penetration testing and intrusion testing shall be reviewed by the agency ISO and any vulnerability detected shall be evaluated for risk and steps taken to mitigate the risk.

**C.** Any tools used to perform the penetration testing shall be kept updated to ensure that recently discovered vulnerabilities are included in any future testing.

**D.** Where an agency has outsourced a server, application, or network services to another agency, independent penetration testing shall be coordinated by both agencies.

**E.** Only an individual or individuals authorized in writing by the agency shall perform penetration testing. The agency ISO shall notify DoIT security staff two business days prior to any penetration test. Any attempt by the agency to perform penetration testing without prior notice to DoIT shall be deemed an unauthorized access attack which shall be reported to the state CIO.

**F.** All documents pertaining to security penetration tests, security investigations, security data and reports shall be categorized as sensitive and protected from public disclosure. Counsel for the agency shall review and approve such information to ensure compliance with state law.
[1.12.20.24 NMAC - N/E, 04/14/2010]

**1.12.20.25 PROTECTION AGAINST MALICIOUS CODE:**

**A.** Software and any other mechanism to prevent intrusions shall be implemented across agency systems to prevent as well as detect the introduction of malicious code. The introduction of malicious code can cause serious damage to networks, workstations, and business data.

**B.** Agency users shall be informed of the dangers of unauthorized or malicious code.

**C.** Agency shall implement controls to, first, detect and then prevent any computer virus from being introduced to the agency environment. The types of controls and frequency of updating signature files shall be dependent on the value and sensitivity of the information at risk.

**D.** For most agency workstations, virus signature files shall be kept updated by the agency system administrator. On host systems or servers, the signature files shall be updated when the virus software vendor's signature files are updated and made available.
[1.12.20.25 NMAC - N/E, 04/14/2010]

**1.12.20.26 SYSTEM SECURITY CHECKING:**

**A.** Systems that process or store sensitive or confidential information or services that provide support for critical services shall undergo technical security reviews by agency system administrators to ensure compliance with implementation standards and rules as promulgated by DoIT and check for vulnerabilities to threats discovered subsequent to the review. Technical reviews of systems and services essential to the support of critical agency functions shall be conducted by agency system administrators at least once every year. Random reviews of all systems and services shall be conducted at least once every 24 months.

**B.** Any deviations from expected or required results, as defined by the agency CIO or ISO which are detected by the technical security review shall be reported to the agency CIO and the agency ISO and shall be corrected immediately. Agency staff shall also be advised of such deviations and agency shall investigate deviations (including the review of system activity log records, if necessary) and provide results of investigation to agency ISO and CIO.
[1.12.20.26 NMAC - N/E, 04/14/2010]

**1.12.20.27 PORTABLE DEVICES AND REMOVABLE MEDIA:**

**A.** All state owned portable computing resources and removable media shall be secured to prevent compromise of confidentiality or integrity of information. All portable computing devices and removable media must be protected by a password.

**B.** No portable and removable media computing devices may store or transmit sensitive information without suitable protective measures approved by the agency CIO.

**C.** An agency user of portable computing devices such as notebooks, PDAs, laptops, and mobile phones, Smartphones, or any other such then current portable devices, shall obtain the approval from the agency CIO to use and such approval shall be based on satisfactory documentation that the requirements for physical protection, access controls, cryptographic techniques, back-ups, malware and malicious codes protection and the rules associated with connecting portable devices to networks and guidance on the use of these devices in public places have been met.

**D.** Agency users shall be instructed that when using portable computing devices or removable media in public places, meeting rooms and other unprotected areas outside of the agency's premises, they must use appropriate protection, such as using cryptographic techniques, firewalls, and updated virus protection shall be in place to avoid the unauthorized access to or disclosure of the agency information stored and processed by these devices.

**E.** Agency users shall be instructed that when such portable devices or removable media are used in public places care shall be taken to avoid the risk of unauthorized persons viewing on-screen sensitive or protected information.

**F.** Procedures protecting portable devices or removable media containing sensitive information against malicious software shall be developed, implemented, and be kept up-to-date.

**G.** Portable devices and removable media containing sensitive or protected information shall be attended at all times and shall be secured e.g. do not leave devices unattended in public places.

**H.** Agency shall provide training to all staff using portable devices and removable media to raise their awareness with respect to risks resulting from the use of portable devices and removable media and what controls are in place by the agency to protect state data and equipment.

**I.** Employees in the possession of portable devices and removable media shall not check such items in airline luggage systems or leave in unlocked vehicles. Such devices shall remain in the possession of the employee as carry-on luggage unless other arrangements are required by federal or state authorities.

**J.** In the event that a state-owned portable device or removable media is lost or stolen, it is the responsibility of the user of that device to immediately report the loss following procedures in 1.12.20.34 NMAC.
[1.12.20.27 NMAC - N/E, 04/14/2010]

**1.12.20.28 TELEPHONES AND FAX EQUIPMENT:**

**A.** Users are prohibited from sending documents containing sensitive and confidential information via fax unless allowed by law.

**B.** Users are prohibited from using fax services to send or receive sensitive and confidential information.

**C.** Users are prohibited from using third-party fax services to send or receive sensitive and confidential information.

**D.** Users are prohibited from sending documents containing sensitive and private information via wireless fax devices.

**E.** Users are prohibited from sending teleconference call-in numbers and pass codes to a pager when sensitive and confidential information shall be discussed during the conference.

**F.** Teleconference chair people shall confirm that all teleconference participants are authorized participants, if sensitive or confidential information shall be discussed.

[1.12.20.28 NMAC - N/E, 04/14/2010]

**1.12.20.29 MODEM USAGE:** Connecting any dial-up modem to any computer systems which are also connected to the agency's local area network, to the state network, or to another internal communication network shall first be approved in writing by the agency CIO.

[1.12.20.29 NMAC - N/E, 04/14/2010]

**1.12.20.30 PUBLIC WEBSITES CONTENT APPROVAL PROCESS:**

**A.** Sensitive and confidential information shall not be available through a server accessible to a public network without appropriate safeguards in place as approved in writing by the agency CIO in consultation with the agency legal counsel. The agency ISO shall implement safeguards to ensure user authentication, data confidentiality and integrity, access control, data protection and logging mechanisms.

**B.** The design of any proposed web service shall be first reviewed and approved in writing by the agency CIO in coordination with DoIT to ensure that the security of the web server, protection of agency networks, performance of the site, integrity, and availability considerations are adequately addressed.

**C.** Agency websites and agency websites hosted outside the state network shall be tested for security vulnerabilities prior to being put into production by DoIT or a DoIT approved contractor.

**D.** Agency website content shall first be reviewed by the agency information owner and approved by the agency CIO to ensure that the collection and processing of information meets state security and privacy requirements. Such review shall ensure that the information is adequately protected in transit over public and state networks, in storage, and while being processed.

[1.12.20.30 NMAC - N/E, 04/14/2010]

**1.12.20.31 BUSINESS CONTINUITY:** This section is limited to the IT infrastructure and the data and applications of the local agency environment.

**A.** A threat and risk assessment shall be performed by the agency to determine the criticality of business systems and the time frame required for recovery in the event of disaster.

**B.** To minimize interruptions to normal agency business operations and critical agency business applications and to ensure they are protected from the effects of any major failures, each agency business unit or each agency ISO, under the direct guidance of the agency CIO, shall develop plans to meet the IT backup and recovery requirements of the agency and approved by DoIT.

**C.** Back-ups of critical agency data and software shall be performed daily.

[1.12.20.31 NMAC - N/E, 04/14/2010]

**1.12.20.32 LOG-ON BANNER:**

**A.** Log-on banners shall be implemented on all state IT systems to inform all users that agency systems are only for agency business and other approved uses consistent with agency policy, to inform that users their activities may be monitored, and to inform the user that they have no expectation of privacy.

**B.** Logon banners shall be displayed on computer screens during the authentication process.

[1.12.20.32 NMAC - N/E, 04/14/2010]

**1.12.20.33 MONITORING SYSTEM ACCESS AND USE: NO EXPECTATION OF PRIVACY:**

**A.** Consistent with applicable law, the agency reserves the right to monitor, inspect, and search at any time, all agency information systems and equipment used by agency users. Since agency computers and networks are provided for state business purposes, agency staff and any contractor(s) specifically allowed limited use of state systems or equipment shall have no expectation of privacy with regard to the information stored in or sent through

the state information systems. Agency management may remove from its information systems any material unauthorized by the agency or by state statute.

**B.** Systems and applications shall be monitored and analyzed by agency ISO or agency designated IT staff to detect deviation from the state access control policy.

**C.** Events shall be recorded to provide evidence of misuse and to reconstruct lost or damaged data by the agency system administrator.

**D.** Audit logs shall be used to record user activities and other security-relevant events.

**E.** Audit log reports shall be produced to agency CIO and ISO and kept consistent with agency record retention schedules.

[1.12.20.33 NMAC - N/E, 04/14/2010]

**1.12.20.34 LOST OR STOLEN IT ASSET:** In the event of a lost or stolen IT asset, the user shall:

**A.** immediately report the incident to the user's supervisor;

**B.** immediately report the incident to the DoIT help desk at (505)827-2121 or EnterpriseSupportDesk@state.nm.us; a state IT asset incident form must be completed and signed by the agency CIO and returned to the DoIT help desk; the asset incident form can be found on the DoIT security web site at: http://www.doit.state.nm.us/securityoffice.html;

**C.** if stolen, user must contact the local law enforcement agency to report the theft and receive a crime report case number;

**D.** upon loss of or in the event of loss of an IT asset by theft, the agency CIO shall work with the DoIT ISO to identify the nature of the data exposed; the loss of confidential or sensitive data shall be reported to the agency executive management for direction.

[1.12.20.34 NMAC - N/E, 04/14/2010]

**HISTORY OF 1.12.20 NMAC:** [RESERVED]