Confidentiality Practices and Protections in New York State Policy
Appendix F, *Information Security Guidelines, Part 1, Campus Programs & Preserving Confidentiality*, Document #6608.
Responsible Office: Administrative Services and Technology
February 1, 2008

This appendix presents a document created by the University to present the many practices promulgated in New York State policy[1] that help protect Confidentiality (intended use and disclosure), which is one of the two primary aims of the Procedure. Program managers can use this document when considering practices for their *Catalog of Practices and Protections* (Standard D1). This document was used in that way to assist the design of Appendix E, *Sample Entries for a Catalog of Practices & Protections.*

This appendix presents 212 practices, selected for relevance to Confidentiality. See Appendix G for the full set (294) of practices from which these were selected.

The 212 practices are presented as 132 paragraphs arranged by the 13 categories (A through M) described in Standard D2. The serial numbers of the University practices are retained (bold numbers) for cross reference. Many of these items serve more than one of the categories, but they are not repeated when that is the case.

The term "SE" used in the state policy to mean "State Entity" is preserved and may be read as "SUNY Entity" or "campus."

[1] New York State's *Information Security Policy*, P03-002, V3.0, Office of Cyber Security & Critical Infrastructure Coordination. Original, April 2003.

A. ARCHITECTURE, CONFIGURATION: practices that maintain industry-standard security architecture, principles, and configuration settings in the "Sensitive Systems," which are physical and digital containers of "Sensitive Information," especially the buildings, rooms, computers, networks, databases, and applications that process, store, and transmit "Sensitive Information;"

1. **37**: Develop and implement standards and procedures to ensure uniformity of information protection and security management across the different technologies deployed within an SE.
2. **173**: Alter computing hardware, software or system configurations provided by SE only under documented, written policy, procedures or specific written approval of SE management. **87**: Review and approve through the SE change management process all additions and changes to network configurations.
3. **98**: Separate operational responsibility for networks from computer operations.
4. **186**: Develop and document acceptance criteria for new information systems, upgrades, and new versions of existing systems. **187**: Clearly define, agree upon, document, and test the security requirements and criteria for acceptance of new information systems. **188**: Perform acceptance testing for new information systems to ensure security requirements are met prior to the system being migrated to the production environment.
5. **201**: Conduct technical security reviews of systems and services that process or store sensitive or confidential information or provide support for critical processes to ensure compliance with implementation standards. Conduct reviews annually for systems and services that are essential to supporting a critical SE function and do a representative sample of all other systems and services at least once every 24 months.
6. **166**: Review and approve in writing [ISO] the design of SE hosting services to ensure that the security of the web server, protection of SE networks, performance of the site, integrity, and availability have all been adequately addressed.
7. **167**: Review and approve [ISO] the implementation of any web site or software to ensure that a) the site meets the security standards for SE systems development and maintenance; b) the collection and processing of information meets SE security and privacy requirements; c) the information is adequately protected in transit over public and SE networks, in storage and while being processed.

B. NETWORK: protections that control information transmitted or received at the external boundaries and key internal boundaries of "Sensitive Systems;"

<u>Internet and External Networks</u>

8. **240**: Implement controls, such as firewalls and routers, to prevent unauthorized users on other connected networks from obtaining access to sensitive areas of the SE's private network, as when the SE network is connected to another network, or becomes a segment on a larger network.

Review & Approval Processes for All Connections

9. **123**: Allow connections from the SE network only with external networks that have been reviewed and found to have acceptable security controls and procedures, or appropriate security measures have been implemented by the SE to protect SE network resources. **86**: Authorize [network managers] and review [ISO] all connections to the SE networks. **128**: Individually assess the security requirements for each external connection to the SE network. **122**: Obtain written approval of the ISO for all connections from the SE network to external networks [and **133**:] before making any third party network and/or workstation connection to the SE network.
10. **129**: Drive the security requirements for each external connection by the business needs of the parties involved. **124**: Perform a risk analysis to ensure that a proposed connection to an external network will

not compromise the SE's private network. **132**: Document the business case, developed by an internal SE sponsor, for each third party network and/or workstation connection to the SE network.

11. **126**: Periodically review external connections to ensure a) the business case for the connection is still valid; b) the connection is still required; c) the security controls in place (filters, rules, access control lists, etc.) are current and functioning correctly.

12. **134**: For any third party network and/or workstation connection to the SE network, obtain a signed SE non-disclosure agreement by a duly appointed representative from the third party organization who is legally authorized to sign such an agreement [and, **135**] attempt to confirm that the third party's equipment conforms to the state's security policies and standards and obtain approval of the ISO for the connection of that equipment to the SE network. **125**: Assess and implement as appropriate additional controls, such as firewalls and a DMZ (demilitarized zone) between the third party and the SE.

Internet Use

13. **117**: Require that SE employees connecting to the Internet using SE Internet addresses or sending electronic mail using the SE designation do so for purposes authorized by SE management.

14. **119**: Prohibit access to the Internet from any device that is connected, whether wired or wireless, to any part of the SE network unless such access is specifically authorized by the ISO. **120**: Prohibit access to the Internet from accounts with third party Internet service providers. **121**: Prohibit use of the SE's Internet account to establish connections to third party services except where SE management authorizes it and the ISO has reviewed and approved the security of the connection. **138**: Do not connect to commercial email systems, such as AOL and Yahoo, from the SE's systems or workstations without prior management approval.

<u>Wireless Networks</u>

15. **158**: Except where appropriate and adequate measures, including authentication, authorization, access controls and logging have been implemented and approved by the ISO, prohibit access via a wireless network to systems that hold non-public information and prohibit the transmission of non-public or sensitive information via a wireless network.

16. **155**: Perform a risk assessment and obtain the written approval of the ISO before installing wireless network or wireless access points; [and **156**] implement controls on wireless networks and access points to defend against their being exploited to disrupt SE information services or to gain unauthorized access to SE information. Such controls may include Media Access Control (MAC) address restriction, authentication, and encryption. **157**: When selecting wireless technologies, be sure 802.11x wireless network security features on the equipment are available and implement these features from the beginning of the deployment.

<u>Remote Access & Modems</u>

17. **226**: Require advance approval of SE management and ISO for any remote access connection.

18. **238**: Consider the following controls when implementing remote access: a) the physical security of the remote location; b) the accessing mechanism given the sensitivity of SE's internal system and the sensitivity of and method of transmitting information; c) appropriate business continuity procedures, including backing up critical information

19. **239**: Consider and appropriately implement in remote access locations the following controls and wherever implemented, monitor and audit:

    a) a definition of the classification of the information and the systems and services that the remote user is authorized to access;

    b) documented procedures and necessary tools allowing for secure remote access, such as authentication tokens and/or passwords, including procedures for revocation of authorization and return of equipment;

c) hardware and software support and maintenance procedures including anti-virus software and maintenance of current signature files;

d) implementation of suitable network boundary controls to prevent unauthorized information exchange between SE networks connected to remote computers and externally connected networks, such as the Internet. Such measures include firewalls and intrusion detection techniques at the remote location;

e) encryption of sensitive information in transit and on the local computer workstation;

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

20. **159**: Except with written approval of the ISO following a risk assessment and appropriate mitigation of risks, prohibit connecting dial-up modems to computer systems which are also connected to SE's local area network or to another internal communication network.

21. **235**: Require that the ISO review any connection and process in which servers, storage devices or other computer equipment may automatically connect to a vendor to ensure these connections will not compromise the SE or other third party connections.

C. TRAINING: practices that engage the workforce in understanding, assessing, and addressing risk to "Sensitive Information;"

22. **286**: Establish in written SE policy and then inform and educate all staff members that: a. compliance with SE information security policy is mandatory; b. each user must understand his/her role and responsibilities regarding information security issues and protecting SE's information; c. a failure to comply with this or any other security policy that results in the compromise of SE information confidentiality, integrity, privacy, and/or availability may be subject to disciplinary or other appropriate action in accordance with law, rule, regulation, policy or negotiated agreement. **42**: Require all authorized users of SE information to preserve and protect SE information and the technologies and systems that support it in a consistent and reliable manner. **292**: Inform and educate supervisors that all business units within the SE may be subject to regular reviews of compliance with security policies and standards. **283**: Inform and educate all staff members that since SE's computers and networks are provided for business purposes, staff members should not have an expectation of privacy in the information stored in or sent through these information systems.

23. **57**: Develop, implement and maintain an information security awareness program that addresses the security education needs of all SE employees, is given to new employees at orientation and is reinforced at least annually. **58**: Provide for all persons with access to SE information security awareness training to ensure they are knowledgeable of security procedures, their roles and responsibilities regarding the protection of SE information, and the proper use of information processing facilities to minimize security risks. **59**: Educate SE employees with regard to information security issues. Explain the issues, why policies have been established, what role(s) persons have in safeguarding information, and explain consequences of non-compliance. **141**: Train workers who use mobile computing resources about the added risk associated with mobile devices and the special controls needed to mitigate that risk. **193**: Inform users of the dangers of unauthorized or malicious code.

D. SCREENING: practices that screen potential workers who would be in a position that handles "Sensitive Information" and "Sensitive Systems;"

24. **55**: Document security roles and responsibilities in job definitions. **56**: In job definitions for all SE employees, document the general responsibilities for protecting SE information; and in job definitions for specific SE employees, document specific responsibilities for protecting specific information and performing tasks related to security procedures or processes.

E. CONTRACTS: practices that monitor third parties that handle "Sensitive Information" and "Sensitive Systems" or contractually require them to adhere to standards of good practice;

25. **232**: Require individual accountability for vendors to access SE computers or software.
26. **233**: Disable or change the passwords on built-in vendor accounts used for periodic maintenance and activate them only when needed. **234**: Log the activity performed while a vendor user-ID is in use and monitor unauthorized use of these privileged accounts during periods of inactivity.

F. ACCESS, IDENTITY, AUTHORIZATION: practices and protections that limit only to authorized persons and processes the access to "Sensitive Information" and related systems and physical enclosures (buildings, rooms, files, etc.) and limit such access only to authorized transactions and functions.

27. **203**: Protect SE's information assets by logical and physical access control mechanisms commensurate with the value, sensitivity, consequences of loss or compromise, legal requirements and ease of recovery of these assets.
28. **73**: House critical or sensitive SE business information processing and storage facilities in secure areas protected by a defined security perimeter, with appropriate security barriers and some form of access controls.

Responsibility & Process

29. **44**: Require that persons who use SE computers only access SE information assets to which they are authorized.
30. **171**: Define the roles and responsibilities of persons who operate or use SE information processing facilities. **48**: Hold each authorized user responsible to reasonably protect against unauthorized activities performed under his or her user-ID including not sharing passwords or other tokens or mechanisms used to uniquely identify individuals.
31. **205**: Establish and document a user management process to outline and identify all functions of user management, to include the generation, distribution, modification and deletion of user accounts for access to resources, and including: a) requests by the appropriate information owner or other authorized officer for the registration and granting of access rights for employees; b) enrolling new users; c) removing user-IDs; d) granting "privileged accounts" to a user; e) removing "privileged accounts" from a user; f) periodic reviewing "privileged accounts" of users; g) periodic reviewing of users enrolled to any system; and h) assigning a new authentication token (e.g. password reset processing).
32. **21**: Establish for all information an information owner within the SE's lines of business who is responsible for assigning the initial information classification, and who makes all decisions regarding controls, access privileges of users, and daily decisions regarding information management. These may be individuals or groups to serve as or represent information owners for the data and tools they use. **49**: Have the information owner classify and secure information within the owner's jurisdiction based on the information's value, sensitivity to disclosure, consequences of loss or compromise, and ease of recovery.
33. **204**: Give Information Owners responsibility and authority to determine who, based on job responsibilities, should have access to protected resources within their jurisdiction and what those access privileges are, such as "read," "update," etc. **206**: Give Information Owners responsibility and authority to ensure that an appropriate user management process is implemented for applications that interact with persons not employed by the SE. The process sets standards for the registration of such external users, including the credentials that must be provided to prove the identity of the user requesting registration, validation of the request, and the scope of access that may be provided.

Physical Access Control

34. **74**: Create physical barriers around assets being protected such that the barrier establishes a security perimeter that requires a method of access control to gain entry, such as an entry point with card key access, a staffed reception area, a locked cabinet or office or other physical barrier.

35. **76**: Establish in the following sites a physical security perimeter to prevent unauthorized access or theft of information or information assets: a) environments where information or information assets are stored or operational; b) data centers; c) wiring closets for network and telephonic connections; d) printers where confidential or sensitive information may be printed; e) any other location where information may be in use or stored.

36. **77**: Physically protect computer equipment from security threats and environmental hazards.

37. **78**: Protect supporting facilities such as electrical supply and cabling infrastructure in data centers, wiring closets, server rooms, and storage facilities where computers and computer peripherals are stored.

38. **80**: Physically destroy or securely overwrite storage devices or paper containing sensitive information. Such devices include hard disk drives, tape, diskette, CDs, DVDs, cell phones, digital copiers or other devices that store information.

Technical Access Control

Accounts and IDs

39. **222**: Require all authorized users to authenticate themselves to the SE's trusted internal network through use of an individually assigned user-ID and an authentication mechanism, e.g., password, token, smart card. **43**: Provide access through individually assigned unique computer identifiers, known as user-IDs, or other technologies including biometrics, token cards, etc. wherever there is a business need for information integrity and accountability or for limited user access to SE computer, computer systems and networks. **45**: Associate each user-ID with an authentication token, such as a password, which is used to authenticate the person accessing the data, system, or network.

40. **243**: Use user-IDs that do not indicate or suggest a level of privilege, such as supervisor, manager, administrator. **244**: Do not use shared user-ID/passwords for a group of users or a specific job except where: a) there is a clear business requirement or system limitation; and b) the ISO and SE management have given documented approval; and c) additional compensatory controls ensure accountability.

41. **47**: Where technically feasible, use secure mechanisms for transmission of authentication information.

42. **81**: On any computer systems where authentication is required, implement automated techniques and controls that require authentication or re-authentication after a predetermined period of inactivity. These controls include such techniques as password-protected screen savers, automated logoff processes, or re-authentication after a set time out period.

43. **207**: Implement logon banners on all systems having that feature to inform users that: a) the system is for SE business or other approved use consistent with SE policy; b) user activities may be monitored; and c) the user should have no expectation of privacy.

44. **245**: Rename, remove, or disable, wherever feasible, default administrator accounts. **246**: Change the default passwords on administrator accounts.

45. **208**: Restrict and control the issuance and use of privileged accounts. **209**: Monitor use of privileged accounts. **210**: Promptly investigate any suspected misuse of privileged accounts.

46. **281**: Tightly control access to source code libraries for both SE business applications and operating systems, ensuring that only authorized persons have access to these libraries and that access is logged such that all activity can be monitored.

Passwords

47. **211**: Change passwords on multi-user system privileged accounts more often than normal user accounts. **212**: Develop and implement password standards to ensure all authorized persons accessing SE resources follow proven password management practices.

48. **214**: Do not store passwords in clear text. **215**: Use passwords that are hard to guess and not subject to disclosure through a dictionary attack. **216**: Keep passwords confidential and do not share individual passwords. **217**: Change passwords at regular intervals. **218**: Change temporary passwords at the first logon. **219**: As far as technology permits, use a mix of alphabetic, numeric, special, and upper/lower case characters in passwords.

49. **220**: Do not include passwords in any automated logon process, such as a macro or function key, web browser, or in application code.

50. **213**: Whenever possible, mandate password rules by automated system controls. **221**: To ensure good password management, wherever technically feasible, implement password controls through the use of established standards.

Remote Access

51. **225**: Implement security mechanisms to control access to SE systems and networks from fixed and mobile remote locations including laptops used at any location other than an employee's work station. **227**: For any remote access, assess and document the scope, method, risks, and required controls (contractual, process, and technical).

52. **236**: Require authorization by SE management for working from a remote location and ensure through written policy and procedure that the work environment at the remote location provides adequate security for SE data and computing resources.

53. **224**: Maintain individual accountability for all access, including during remote access. **228**: Use stronger passwords or other comparable methods for remotely connecting to the SE network.

54. **230**: When accessing the SE network remotely, perform identification and authentication of the entity requesting access in such a manner as to not disclose the password or other authentication information that could be intercepted and used by a third party.

55. **231**: Use a common remote access point such that all remote connections are made through managed, central points-of-entry.

G. MINIMUMS, NEED-TO-KNOW: practices that keep to a minimum, based on business need, the types and instances of "Sensitive Information" used in the business processes and the persons and processes authorized to access it

56. **247**: Give access to SE business and systems applications only to persons needing such access for the normal performance of their job responsibilities.

57. **223**: Develop and implement network controls to prevent authorized users from accessing more network resources and services than are necessary to perform assigned job responsibilities.

58. **182**: Give development staff who are correcting problems with production systems only a short-term access and give only as much access as is necessary.

59. **284**: Reserve the right [SE management] to remove from SE information systems any unauthorized material.

60. **248**: Give access to source code for applications and systems only to persons needing such access for the normal performance of their job responsibilities, restricting it to applications and systems they directly support. **241**: Give access to operating system code, services, and commands only to persons needing such access for the normal performance of their job responsibilities, such as systems programmers, database administrators, network and security administrators.

61. **290**: Maintain at the highest level of security any documentation and report of SE security and preparedness, including statements of compliance with information security laws, regulations, and policies. Disclose such information only to those external parties for which a documented need has been formally accepted by SE Executive Management and for which an appropriate and secure process has been established for using, sharing, and storing such information. {SUNY interpretation}

H. ACCIDENTS, INATTENTION: practices and protections that reduce the threat of accidental disclosure of "Sensitive Information" through authorized mechanisms, such as websites, computer terminals, paper printouts, remote access, electronic commerce, online transactions, portable storage devices (laptops, USB flash, PDA, cell phones, etc.,) and the disposal of storage media;

62. **140**: Do not use any computer device to store or transmit non-public information without suitable protective measures that are approved by the ISO.
63. **46**: Treat passwords, tokens, or similar technology as confidential information and do not disclose them.
64. **79**: Establish formal processes to minimize the risk of disclosure of sensitive information through careless disposal or re-use of equipment.
65. **99**: Establish responsibilities and procedures for remote use.

Portable Devices

66. **142**: On all portable computer devices, such as notebooks, palmtops, laptops and mobile phones, maintain SE requirements for physical protection, access controls, cryptographic techniques, back-ups, virus protection and observe the rules associated with connecting mobile facilities to networks and guidance on the use of these facilities in public places.
67. **146**: Protect back-ups of mobile devices from theft and loss of information.
68. **237**: Implement appropriate protection mechanisms in remote access locations commensurate with risk and exposure to protect against theft of SE equipment, unauthorized disclosure of SE information, misuse of SE equipment or unauthorized access to the SE internal network or other facilities by anyone, including family and friends.
69. **143**: When using mobile computing facilities in public places, meeting rooms and other unprotected areas outside of the SE's premises, take special care to prevent unauthorized persons from viewing information on-screen and use special protections, such as encryption, to avoid the unauthorized access to or disclosure of SE information.
70. **147**: Physically lock away or use other special physical locks for any mobile equipment not being personally attended to, especially devices that contain important, sensitive and/or critical business information.
71. **148**: When traveling with SE-owned portable, laptop, notebook, palmtop, and other transportable computers keep the equipment in personal possession as hand luggage, not as checked (airline, bus, train) luggage, unless other arrangements are required by Federal or State authorities.

Telephone & Fax

72. **149**: Take care not to be overheard when discussing sensitive or confidential matters on the telephone. **150**: Avoid the use of wireless or cellular phones when discussing sensitive or confidential information. **153**: If sensitive or confidential information will be discussed during a teleconference, do not send call-in numbers and passcodes to a pager. **154**: When chairing a sensitive or confidential teleconference, confirm that all participants are authorized to participate before starting any discussion. **151**: Do not leave sensitive or confidential messages on voicemail systems.

73. **152**: If sending sensitive or confidential documents via fax, a) verify the phone number of the destination fax; b) contact the recipient to ensure protection of the fax, either by having it picked up quickly or by ensuring that the fax output is in a secure area; c) do not use Internet fax services; d) do not use third party fax services; e) do not use wireless fax devices.

Web Sites

74. **160**: Review the content of each public web site according to a process that is defined and approved by the SE. **161**: Review and approve updates to publicly available web content using an established process that includes consideration of :a) copyright issues (both the potential publication of copyright material and the appropriate protection of SE copyright materials); b) the type of information being made available (confidentiality, privacy and sensitivity of the information); c) the accuracy of the information; d) potential legal implications of providing the information.

75. **162**: Do not make available on SE public websites any sensitive or confidential State information without appropriate safeguards approved by the ISO to ensure user authentication, data confidentiality and integrity, access control, data protection, and logging mechanisms. **163**: Do not make available on SE public websites any information such as inventory, depictions, photographs, locations of physical equipment, assets and infrastructure regarding structures, individuals, and services essential to the security, government, or economy of the State or critical Infrastructure Assets which are so vital that their infiltration, incapacitation, destruction or misuse would have a debilitating impact on health, welfare or economic security of the citizens and businesses of New York State. **164**: Do not make available on SE public websites any sensitive information about the following infrastructures: a) telecommunications (voice, data, Internet); b) electrical power; c) , gas and oil storage and transportation; d) banking and finance; e) transportation; f) water supply; g) specific structural, operational, or technical information, such as: maps, mechanical or architectural drawings, floor plans, operational plans or procedures, or other detailed information relating to electric, natural gas, steam, water supplies, nuclear or telecommunications systems or infrastructure, including associated facilities. **165**: Do not make available on SE public websites any sensitive information about the following services: a) emergency services (including medical, fire, and police services); b) the continuity of government operations; c) training and security procedures at sensitive facilities and locations; d) descriptions of technical processes and technical architecture; e) plans for disaster recovery and business continuity; f) reports, surveys, or audits that contain sensitive information; g) other subjects and areas of relevant concern as determined by the SE.

Development

76. **277**: Protect test data used in SE-built applications and control it for the life of the testing.

77. **278**: If test data that is used in SE-built applications is to be reused, then whenever modifications are made to the software, system or application, protect the test data and control it during its entire useful life.

I. MISCONDUCT: practices that reduce the threat of employees and contracted external parties illegally or improperly disclosing "Sensitive Information," especially to unauthorized persons seeking the information through fraudulent means;

78. **285**: Establish in written SE policy and then inform and educate all staff members that authorized parties, both within and external to the SE, may periodically review compliance to information security laws, regulations, and policies. Such reviews may include review of the technical and business analyses required to be developed pursuant to policy, and other project documentation, technologies or systems which are the subject of published policy or standards. **282**: Reserve the right [SE management] to monitor, inspect, and/or search at any time all SE information systems, consistent with applicable law, employee contracts, and SE policies.

79. **293**: Establish in written SE policy and then inform and educate all SE staff that regarding observed or suspected compromises of information security laws, regulations, and policies: a. workers must report

these to an appropriate manager and the SE ISO; b. managers must submit a report, in accordance with SE labor relations, indicating the risk level of the violation; c. access authorization for user accounts involved in a compromise may be suspended during an investigation.

80. **229**: Establish policy whereby all remote access sessions are subject to periodic and random monitoring.

81. **101**: Prohibit vulnerability scans on SE systems by anyone not authorized by the ISO or by CSCIC. **110**: Prohibit penetration testing on SE systems by anyone not authorized by the SE. **130**: Prohibit unauthorized and unqualified staff or third parties from using sniffers or similar technology on the network to monitor operational data and security events. **70**: Inform employees and contractors that they must not attempt to prove a suspected weakness unless authorized by the ISO to do so.

Release & Sharing

82. **54**: Ensure that third parties that store any SE classified information are contractually required to protect that information appropriately.

83. **88**: When releasing information outside an SE or sharing it between SEs, evaluate and document the sensitivity and confidentiality of the information and use that as the basis for applying security measures that are commensurate and appropriate for the information being released or shared.

84. **89**: Establish a process for information to be released outside an SE or shared between SEs. **91**: Define the minimum controls required to transmit and use the information to be released or shared with another SE. **92**: Record the measures that each party has in place to protect the information to be released or shared with another SE. **93**: Define a method for compliance measurement for the other SE when releasing or sharing with another SE. **94**: Provide a signoff procedure for each party to accept responsibilities for SE information to be released or shared with another SE. **95**: Establish a schedule and procedure for reviewing the controls for SE information to be released or shared with another SE.

85. **174**: When providing server, application or network services to another SE, coordinate operational and management responsibilities with the other SE.

86. **85**: Perform periodic security reviews to ensure the security and availability of the SE's information and applications for all outsourced environments in which the SE has outsourced servers or applications (such as web applications) to a third party service. [ISO]

87. **175**: Keep the audit of security independent and segregated from the security function.

Systems & Software Development

88. **184**: Establish, document, and test the security requirements of new systems prior to their acceptance and use.

89. **177**: Logically or physically separate development, test, and production environments. **179**: Maintain development software and tools on computer systems that are physically separate from the production environment or on systems separated by access-controlled domains or directories. **181**: Use distinct logon procedures and environmental identification for production, testing, and development.

90. **242**: Give each authorized person requiring access to operating system code, etc, a unique privileged account (user-ID) for his or her personal and sole use in conducting privileged activities and provide each such person a second user-ID for performing normal business activities.

91. **178**: Govern with documented processes the transfer of software from the development environment to the production platform.

92. **279**: Allow production data to be used for testing in SE-built applications only where the information owner approves in writing a documented business case and a) access controls, system configurations and logging requirements for the production data are applied to the test environment; or b) personal, sensitive or confidential data will be masked or overwritten with fictional information and the data will be deleted as soon as the testing in completed.

93. **180**: Unless required, remove from production systems access to compilers, editors, and other system utilities.

94. **183**: Use a stable quality assurance environment where user acceptance testing can be conducted and changes cannot be made to the programs being tested.

J. SYSTEM VULNERABILITY protections that reduce the threat of information theft through exploitation of vulnerabilities in computer systems and applications, especially in systems developed in-house and systems connected to the Internet;

Anti-Virus

95. **189**: Implement software and associated controls across SE systems to prevent and detect the introduction of malicious code to the SE environment. **190**: Define the types of controls and frequency of updating signature files based on the value and sensitivity of the information being protected. **191**: Update virus signature files weekly for most SE workstations. **192**: Update virus signature files daily for most host systems or servers, or when the virus software vendor's signature files are updated and published.

96. **144**: Maintain up-to-date protection from malicious software on SE mobile devices.

Patching & Updates

97. **194**: Maintain system software at a vendor-supported level to ensure software accuracy and integrity. **195**: Review, evaluate, and appropriately apply all known security patches in a timely manner.

Vulnerability Scans

98. **109**: When doing vulnerability scans follow a tested process that minimizes the possibility of disruption.

99. **102**: Perform scans for vulnerabilities and weaknesses at least annually on all systems that are essential to supporting a process that is critical to SE business. **103**: Perform scans for vulnerabilities and weaknesses on all SE-owned hosts that are or will be accessible from outside the SE network a) before systems are installed on the network; b) after changes in software, operating system, or configuration; c) after new network software or major configuration changes have been made; d) as specified by the ISO or the information owner(s) based on the criticality and sensitivity of the information on the system.

100. **104**: Forward reports of exposures to vulnerabilities to the ISO and other defined staff. **105**: Review the output of the scans in a timely manner. [ISO]

101. **106**: Evaluate and mitigate the risk of all vulnerabilities detected by SE-authorized vulnerability scans.

102. **107**: Periodically update the tools used to scan for vulnerabilities to ensure that recently discovered vulnerabilities are included in the scans.

103. **108**: Where the SE has outsourced a server, application, or network services to another SE, coordinate responsibility for vulnerability scanning with both SEs.

104. **115**: Where the SE has outsourced a server, application, or network services to another SE, coordinate responsibility for penetration testing with both SEs.

Penetration Analysis

105. **116**: For each penetration test, acquire the prior approval of the ISO and notify CSCIC 24 hours prior to testing.

106. **111**: Perform penetration analysis and intrusion testing on all SE computing systems that provide information through a public network, either directly or through another service that provides

information externally (such as the World Wide Web). Such analysis and testing is used to determine if: a) an individual can make an unauthorized change to an application; b) a user may access the application and cause it to perform unauthorized tasks; c) an unauthorized individual may access, destroy or change any data; or d) an unauthorized individual may access the application and cause it to take actions unintended by the application designer(s).

107. **112**: Review the output of the penetration testing and intrusion testing in a timely manner. [ISO]

108. **113**: Evaluate and mitigate the risk of all vulnerabilities detected by SE-authorized penetration analysis and intrusion testing.

109. **114**: Periodically update the tools used to perform the penetration testing to ensure that recently discovered vulnerabilities are included in the testing.

110. **202**: Immediately correct any deviations from expected or required results that are detected when conducting technical security reviews of systems and services that process or store sensitive or confidential information or provide support for critical processes; report these deviations to the ISO and the SE application owner and have the SE application owner initiate and investigation into these deviations, including the review of system activity log records if necessary.

111. **115**: Where the SE has outsourced a server, application, or network services to another SE, coordinate responsibility for penetration testing with both SEs.

Systems & Software Development

112. **257**: For each SE-built application, have the information owners identify security measures based on the application's risk profile and protection requirements.

113. **252**: During the requirements phase of a project to build an SE information system and as part of the overall business case for it, identify, justify, document, and agree to all security requirements, including the need for rollback arrangements.

114. **254**: In projects to build SE information systems, especially in Web and other online applications, identify information security requirements and build controls that reflect the business value of the information involved, and the potential business damage that might result from a failure or absence of security measures.

115. **255**: Have the information owners for SE-built applications and systems perform threat and risk assessments analyzing the security requirements and identifying controls to meet them. **274**: Identify the level of confidentiality protection required by SE-built applications based on a risk assessment that takes into account the type and quality of the available encryption algorithms and the length of cryptographic keys that would be used.

116. **258**: For each SE-built application, identify specific controls based on security requirements and technical architecture. **259**: For each SE-built application, propose methods to test the effectiveness of the security controls. **260**: For each SE-built application, identify processes and standards to support changes, ongoing management and to measure compliance. **261**: For each SE-built application, document the specific control mechanisms at the application level, in the SE's System Development Methodology, and in the SE's security standards documents.

117. **262**: Before implementation of SE-built applications and systems, require that the ISO review the information owners' threat and risk assessments and risk management plans for the applications and systems. **263**: Before implementation of SE-built applications and systems, require that the SE executive management give written approval for the information owners' threat and risk assessments and risk management plans for the applications and systems.

K. ENCRYPTION: protections that encrypt and otherwise mask electronic data containing "Sensitive Information;"

118. **136**: On any connection between SE firewalls over external networks, encrypt all traffic containing sensitive information.

119. **273**: Consider using encryption in SE-built applications to protect high-risk, sensitive or critical information when other controls do not provide adequate protection.

120. **169**: Where Public Key Infrastructure (PKI) security architecture is used, define an appropriate trust model to that applies to the stakeholders and users of SE systems and data and support the trust domain or multiple trust domains with certificate policies and certification practice statements.

121. **170**: Where Public Key Infrastructure (PKI) security architecture is used for digital signatures or encryption, ensure that it operates under and complies with the State Certificate Policy for Digital Signatures and Encryption issued by the Office for Technology and any associated rules and regulations.

122. **275**: To the extent possible, give consideration in SE-built applications to the regulations and national restrictions that may apply to the use of cryptographic techniques in different parts of the world and to controls that apply to the export and import of cryptographic technology.

123. **276**: Where cryptographic techniques are used in SE-built applications, protect the cryptographic keys used to encrypt and decrypt information in a secured environment where access to the keys is tightly controlled and given only to persons needing such access for the normal performance of their job responsibilities.

L. DETECTION: practices and protections that detect attacks and intrusions to "Sensitive Information" and "Sensitive Systems" and record and trace actions sufficiently to hold individual actors accountable;

124. (see 19.d). **250**: Create and protect audit logs. **251**: Produce audit logs that record exceptions and other security-relevant events and keep these consistent with record retention schedules developed in cooperation with the State Archives and Records Administration (SARA) and SE requirements to assist in future investigations and access control monitoring.

125. **131**: Regularly review audit trails and system logs of external network connections for abuses and anomalies. [ISO or designee]

126. **294**: Configure automated violation reports generated by security systems to be forwarded to the appropriate management and the SE Information Security Officer for timely resolution.

M. INCIDENTS practices that define roles, responsibilities, and responses to be taken when intrusions to "Sensitive Systems" and unauthorized disclosures or leaks of "Sensitive Information" occur.

127. **60**: Clearly identify procedures and define responsibilities for a prompt, effective, and organized response to security incidents, including procedures for information system failure, denial of service, disclosure of confidential information and compromised systems of software. **61**: Establish formal incident or malfunction reporting and response procedures that define the actions to be taken when an incident occurs. Such actions include: a) documenting the symptoms of the problem; b) documenting any messages displayed; c) isolating the computer where appropriate; d) stopping the computer until the problem has been identified and resolved; e) reporting the incident immediately to the appropriate SE manager and the ISO. **62**: Establish feedback mechanisms so that persons reporting incidents are notified of the results after the incident has been resolved and closed.

128. **67**: Require all SE staff and contractors to report any observed or suspected incidents to the appropriate manager and the SE ISO as quickly as possible. **35**: Report suspected security incidents to the appropriate manager and the ISO. [all employees]

129. **66**: Inform all users of SE systems of the procedure for reporting security incidents, threats or malfunctions that may have an impact on the security of SE information.

130. **63**: Track the types and volumes of security incidents and malfunctions. **64**: Identify recurring or high impact incidents.

131. **65**: After a security incident or malfunction, record lessons learned and consider what may indicate the need for 1) additional controls to limit the frequency, damage, and cost of future incidents, or 2) additional controls to be taken into account in the policy review process.

132. **249**: Monitor and analyze systems and applications to detect deviation from the access control policy and record events to provide evidence and to reconstruct lost or damaged data.