Information Security Practices Recommended by New York State
Appendix G, *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 in 2006 to add value to the practices promulgated in New York State policy.[1] It gives 294 self-sufficient, practice-style statements drawn from that policy. The statements carefully preserve the policy's key ideas, phrases, order, and categories. Program managers can use this document and its related spreadsheet (Appendix H) in a wide variety of managerial and operational processes, including creation of audience-specific policy (Standard B2), assessing campus practices and protections (Standard D1), and selecting appropriate projects (Standards E1,E2,E3).

Since its origin five years ago (April 2003), the policy has been the guiding text for the information security programs of state agencies. The policy itself asserts that it "shall serve as best practices for the State University of New York and the City University of New York campuses" but is not required to be followed by the universities' campuses. The policy's value is also greatly augmented by its being freely available online[2] and free of copyright restrictions. In contrast, the international standard on which it is based, ISO 27002 (previously, ISO 17799), costs over US$100 per copy and may not be quoted or distributed—even internally.

Even a free and widely available policy, however, will not simply soak into daily practice. It cannot on its own affect procedure, operations, training, or even management without significant locally applied intelligence and action. Often, that work involves carefully selecting portions of the policy for differing audiences and purposes. To do that, it is helpful to have the policy's ideas cast as individual, stand-alone statements that retain their meaning when separated. This helps managers select statements for differing audiences and purposes, such as awareness campaigns, training, job expectations, and staff meetings. The practice statements can be placed into spreadsheets like Appendix H and databases and used to record and monitor status and growth. For example, the Appendix H spreadsheet was used to select the content used in Appendix F, *Confidentiality Practices and Protections in NYS Policy*.

[1] New York State's *Information Security Policy*, P03-002, V3.0, Office of Cyber Security & Critical Infrastructure Coordination. Original, April 2003.
[2] http://www.cscic.state.ny.us/lib/policies/Cyber-Security-Policy-P03-002-V3.0.pdf

Information Security Practices Recommended by New York State

Version August 14, 2007
Ted.Phelps@suny.edu

Derived from Cyber Security Policy P03-002
(updated to Policy V3.0
Information Security Policy
New York State
Office of Cyber Security & Critical Infrastructure Coordination
30 South Pearl Street, Floor P2
Albany, N.Y. 12207-3425

The purpose of the CSCIC policy is to define a set of minimum security requirements that state entities (SE) must meet. As regards SUNY, it states, "This policy shall serve as best practices for the State University of New York and the City University of New York campuses. Any SE may, based on its individual business needs and specific legal requirements such as Health Insurance Portability and Accountability Act (HIPAA), exceed the security requirements put forth in this document, but must, at a minimum, achieve the security levels required by this policy."

To assist SUNY in using the policy in a variety of ways, and especially to do so as a set of best practices, we have recast the statements of the policy, preserving as much of the words as possible. The items are sequentially numbered. The statements are cast as instructions (imperative), such as "Establish a framework.." Almost all items are addressed to an undetermined person (role) and this is because the policy has not stated a clear responsibility for the practice. Where the role is made explicit in the policy, it is included in one of several ways in the recasting of the text. One such way is naming the role in square brackets (e.g. [ISO]). Each statement has stand-alone meaning so that it can be fairly well interpreted without knowing the section it falls in. This allows a simple and unambiguous reference to the practices, allowing them to be handed out, printed, inserted in job requirements and performance reviews, put on posters, and sorted (see spreadsheet details, next). Where the policy gives information rather than a directive, we preserve the text as a comment inserted at the top of the section in which it appeared in the policy.

To assist the wide and penetrating distribution of these ideas in an organization, the practices are also represented in an associated spreadsheet of the same name. The spreadsheet leaves out the comments. This spreadsheet is in database format, which allows the text to be used directly in a wide variety of management tasks. One can create columns of associated data for each item, such as responsibility, priority, degree of completion. For example, all items that apply to the general workforce or to a specific programming unit can be quickly marked, sorted, and pasted into a document. The context of each item is retained in three columns.

Most items are kept in their original order and location within the New York state policy, and the headings and subheadings are retained, not only to assist in the reading of this document, but also to assist in cross-references to the state policy. Fidelity to the original order is lower in the beginning sections, where much redundancy exists in the policy. The section Cyber Security Citizens' Notification Policy is removed as it is a representation of a NYS law, not a best practice. The Compliance section is also removed.

The policy states that it is "a statement of the minimum requirements, ethics, responsibilities and accepted behaviors required to establish and maintain a secure environment, and achieve the state's information security objectives. It sets the direction, gives broad guidance and defines requirements for information security-related processes and actions. This policy documents many of the security practices already in place in some SE's."

The Policy's stated primary objectives are to:

- effectively manage the risk of security exposure or compromise within SE systems;
- communicate the responsibilities for the protection of SE information;

- establish a secure processing base and a stable processing environment;
- reduce to the extent reasonably possible the opportunity for errors to be entered into an electronic system supporting SE business processes;
- preserve management's options in the event of an information asset misuse, loss or unauthorized disclosure;
- promote and increase the awareness of information security in all SEs.

The policy “encompasses all systems, automated and manual, for which the state has administrative responsibility, including systems managed or hosted by third parties on behalf of the SE. It addresses all information, regardless of the form or format, which is created or used in support of business activities of state entities. This policy is to be communicated to all staff and all others who have access to or manage SE information.”

1.Organizational and Functional Responsibilities

-The Information Security Function

1. Establish a framework to initiate and control the implementation of information security within the state entity (SE).

2. Ensure [head of the SE] that an organization structure is in place for:
    a. the implementation of information security policies and standards;
    b. assigning information security responsibilities;
    c. the implementation of a security awareness program;
    d. monitoring significant changes in the exposure of information assets to major threats, legal or regulatory requirements;
    e. responding to security incidents;
    f. the approval of major initiatives to enhance information security;
    g. the development of a process to measure compliance with this policy;
    h. the approval of new applications and services.

3. Maintain an Information Security Function that develops, deploys and maintains an information security architecture that provides security policies, mechanisms, processes, standards and procedures that meet current and future business needs of the SE.

4. Maintain an Information Security Function that provides information security consulting to the SE regarding security threats that could affect the SE computing and business operations, and makes recommendations to mitigate the risks associated with these threats.

5. Maintain an Information Security Function that assists management in the implementation of security measures that meet the business needs of the individual SE.

6. Maintain an Information Security Function that develops and implements security training and awareness programs that educate SE employees, contractors and vendors with regard to the SE's information security requirements.

7. Maintain an Information Security Function that investigates and reports to management breaches of security controls and implements additional compensating controls when necessary to help ensure security safeguards are maintained.

8. Maintain an Information Security Function that participates in the development, implementation and maintenance of disaster recovery processes and techniques to ensure the continuity of the SE's business and the security controls in the event of an extended period of computing resource unavailability.

9. Designate staff to be responsible for the implementation of information security policies and the compliance of employees.

10. Maintain control of the security of SE information even where information security roles & responsibilities are outsourced to third parties.

-The Role of the Information Security Officer

11. Appoint an Information Security Officer (ISO).

12. Have the ISO report to a high level person in the organization or directly to the Chief Information Officer (CIO), but not an Information Technology (IT) director, to balance security with technological and programmatic issues. If the CIO is an IT director, the ISO reports to another equivalent-level position.

13. Give the ISO responsibility and authority for providing consultation to the SE management with regard to all information security.

14. Give the ISO responsibility and authority for ensuring the implementation, enhancement, monitoring, and enforcement of the information security policies and standards; and coordinating and overseeing security program activities and reporting processes in support of policy and other security initiatives.

15. Give the ISO responsibility and authority for evaluating new security threats and counter measures that could affect the SE, making appropriate recommendations to the SE's CIO and other management to mitigate the risks.

16. Give the ISO responsibility and authority for providing direction and leadership to the SE through the recommendation of security policies, standards, processes and education and awareness programs to ensure that appropriate safeguards are implemented and to facilitate compliance with those policies, standards and processes.

17. Give the ISO responsibility and authority for coordinating the development and implementation of information security policies, standards, procedures, and other control processes that meet the business needs of the SE.

18. Give the ISO responsibility and authority for coordinating information security awareness and education to all SE employees, and where appropriate third party persons.

19. Give the ISO responsibility and authority for
    a. investigating all alleged information security violations according to SE procedures for referring the investigation to other investigatory entities, including law enforcement;
    b. investigating and reporting to appropriate internal management and CSCIC according to the CSCIC Incident Reporting Policy P03-001;
    c. ensuring appropriate follow-up to security violations.

20. Require that the ISO
    a. know the laws and regulations that could affect the security controls and classification requirements of the SE's information;
    b. consult with the various SE computing platforms;
    c. work closely with security administration or those serving in that function to ensure security measures are implemented to meet policy requirements;
    d. review and approve all external network connections to the SE's network.

- Role of Information owners

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.

22. Give the information owners responsibility and authority to maintain appropriate security measures such as assigning and maintaining asset classification and controls, managing user access to their resources, and even where responsibility for implementing security measures has been delegated, maintain the identified owner of the asset accountable.

23. Give the information owners responsibility and authority to determine who should have access to protected resources within their jurisdiction and what those access privileges should be (read, update, etc.), based on the user's job responsibilities.

24. Give the information owners responsibility and authority to communicate to the ISO the legal requirements for access and disclosure of their data.

- Role of Security Administrators

25. Establish procedures and practices such that Security Administrators work closely with the ISO and support staff.

26. Give the Security Administrators responsibility and authority for administering security tools, reviewing security practices, identifying and analyzing security threats and solutions, and responding to security violations.

27. Give the Security Administrators administrative responsibility over all user-IDs and passwords and the associated processes for reviewing, logging, implementing access rights, emergency privileges, exception handling, and reporting requirements.

-Role of Information Technology

28. Establish procedures and practices such that IT Management supports the Information Security Policy and provides resources needed to enhance and maintain a level of information security control consistent with the SE's Information Security Policy.

29. Give IT Management responsibility and authority to identify and implement processes, policies, and requirements relative to security requirements defined by the SE's business.

30. Give IT Management responsibility and authority to implement the proper technical controls of information, controls for which the SE's business have assigned ownership responsibility, based on the SE's classification designations.

31. Require that IT Management ensure the participation of the ISO with its technical staff in identifying and selecting appropriate and cost-effective technical security controls and procedures, and in protecting information assets.

32. Give IT Management responsibility and authority to define appropriate security requirements for user access to automated information for files, databases, and physical devices assigned to their areas of responsibility.

33. Require that IT management ensure that critical data and recovery plans are backed up and kept at a secured off-site storage facility and that recovery of backed-up media will work if and when needed.

-Other Roles in Information Security

34. Protect SE information and resources, including passwords. [all employees]

35. Report suspected security incidents to the appropriate manager and the ISO. [all employees]

36. Place under the control of SE's information security policies all persons who work under agreements with the SE such as contractors, consultants, vendors, volunteers and other persons in similar positions, to the extent of their present or past access to SE information.

2. Information

37. Develop and implement standards and procedures to ensure uniformity of information protection and security management across the different technologies deployed within the SE.

38. Establish a process to determine information sensitivity, based on best practices, state directives, and legal and regulatory requirements to determine the appropriate levels of protection for that information.

39. Classify and protect information based on its importance to business activities, risks, and security best practices.

40. Use only for SE business all information, regardless of the form or format, which is created, acquired or used in support of SE's business activities.

41. Protect SE information from its creation, through its useful life, and to its authorized disposal and maintain it in a secure, accurate, and reliable manner such that it is always readily available for authorized use.

-Individual Accountability for Information

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.

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.

44. Require that persons who use SE computers only access SE information assets to which they are authorized.

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.

46. Treat passwords, tokens, or similar technology as confidential information and do not disclose them.

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

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.

-Confidentiality / Integrity / Availability

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.

50. Define in the SE recovery plan and implement processes for the reasonable and timely recovery of all SE information, applications, systems and security regardless of computing platform, should they become corrupted, destroyed, or unavailable for a defined period.

3. Asset Classification and Control

Comment: As with other assets, different types of information have different uses and value and therefore require different levels of protection.

51. Classify and manage information based on its need for confidentiality, integrity, and availability.

52. Perform periodic high-level business impact analyses on SE information to determine its relative value, risk of compromise, etc. and based on that analysis place the information into an SE-standardized class.

53. Assign to each SE-standardized class a set or range of controls designed to provide a level of protection for the information and its associated application software that is commensurate with the value of the information in that class.

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

4. Personnel

-Including Security in Job Responsibilities

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.

-User Training

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.

-Security Incidents or Malfunctions Management Process

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.

63. Track the types and volumes of security incidents and malfunctions'

64. Identify recurring or high impact incidents.

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.

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.

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.

68. Document approaches to incident management.

69. Follow these procedures once an incident has been identified:
    a. report the action to CSCIC according to the CSCIC Incident Reporting Policy P03-001;
    b. identify the underlying cause of the incident;
    c. identify procedures the SE will employ to resolve the problem;
    d. identify procedures the SE will employ to prevent the same or similar incident from occurring;
    e. track the response procedure from initial report through follow-up for review and audit purposes; and,
    f. provide adequate follow-up to ensure that persons involved or affected by the incident understand what took place and how the incident was resolved.

70. Inform employees and contractors that they must not attempt to prove a suspected weakness unless authorized by the ISO to do so.

5. Physical and Environmental

Comment: Physical protection measures protect the facility from unauthorized access, damage and interference.

71. Perform periodic threat and risk analysis to determine where additional physical security measures are necessary.

72. Implement measures to mitigate the risks identified in physical security risk and threat assessments.

-Physical Security Perimeter

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.

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.

75. Perform a threat and risk assessment to determine the various physical perimeters creating barriers around assets and the types of controls necessary to mitigate the identified risks.

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.

-Equipment Security

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

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.

-Secure Disposal or Re-use of Storage Media and Equipment

79. Establish formal processes to minimize the risk of disclosure of sensitive information through careless disposal or re-use of equipment.

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.

-Clear Screen

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.

6. Communications and Network Management

82. Implement appropriate security controls to ensure the integrity of the data flowing across SE networks.

83. If there is a business need, implement additional measures for data flowing across SE networks to ensure the confidentiality of the data.

84. Ensure that measures are in place to mitigate any new security risks created by connecting the SE networks to a third party network. [ISO]

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]

86. Authorize [network managers] and review [ISO] all connections to the SE networks.

87. Review and approve through the SE change management process all additions and changes to network configurations.

-Sharing Information Outside State Entity

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.

89. Establish a process for information to be released outside an SE or shared between SEs.

90. Identify the responsibilities of each party for protecting SE information to be released or shared with another SE.

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.

-Network Management

96. Implement a range of network controls to maintain security in the SE's trusted, internal network and defend against unauthorized access and use of the SE private network.

97. Use network controls to protect services and networks.

98. Separate operational responsibility for networks from computer operations.

99. Establish responsibilities and procedures for remote use.

100. Implement controls to safeguard integrity and confidentiality of data passing over public networks, especially the Internet.

-Vulnerability Scanning

101. Prohibit vulnerability scans on SE systems by anyone not authorized by the ISO or by CSCIC.

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.

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]

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

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

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

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

-Penetration & Intrusion Testing

110. Prohibit penetration testing on SE systems by anyone not authorized by the SE.

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).

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

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

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

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

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

-Internet and Electronic Mail Acceptable Use

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.

118. Prohibit the employees from using the Internet and electronic mail to:

a. to represent oneself as someone else (i.e., “spoofing”);
b. for spamming;
c. for unauthorized attempts to break into any computing system whether SE’s or another organization’s (i.e., cracking or hacking);
d. for theft or unauthorized copying of electronic files;
e. for posting sensitive SE information without authorization from SE;
f. for any activity which creates a denial of service, such as “chain letters”;
g. for “sniffing” (i.e., monitoring network traffic), except for those authorized to do so as part of their job responsibilities.

-External Connections

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.

122. Obtain written approval of the ISO for all connections from the SE network to external networks.

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.

124. Perform a risk analysis to ensure that a proposed connection to an external network will not compromise the SE's private network

125. Assess and implement as appropriate additional controls, such as firewalls and a DMZ (demilitarized zone) between the third party and the SE.

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.

127. Make all external connections to the SE network in a secure manner that preserves the integrity of the SE network, data transmitted over that network, and the availability of the network.

128. Individually assess the security requirements for each external connection to the SE network.

129. Drive the security requirements for each external connection by the business needs of the parties involved.

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.

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

132. Document the business case, developed by an internal SE sponsor, for each third party network and/or workstation connection to the SE network.

133. Obtain the written approval of the ISO before making any third party network and/or workstation connection to the SE network.

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.

135. For third party network and/or workstation connections to the SE network, 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.

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

-Security of Electronic Mail

137. Use the SE email systems in a legal, professional and responsible manner.

138. Do not connect to commercial email systems, such as AOL and Yahoo, from the SE's systems or workstations without prior management approval.

-Portable Devices

139. Secure all portable computing resources and information media to prevent compromise of confidentiality or integrity.

140. Do not use any computer device to store or transmit non-public information without suitable protective measures that are approved by the ISO.

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.

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.

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.

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

145. Provide access to quick and easy back up of information on mobile devices.

146. Protect back-ups of mobile devices from theft and loss of information.

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.

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.

-Telephones and Fax Equipment

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.

151. Do not leave sensitive or confidential messages on voicemail systems.

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

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.

-Wireless Networks

Comments: Advances in wireless technology and pervasive devices create opportunities for new and innovative business solutions. However security risks, if not addressed correctly, could expose SE information systems to a loss of service or compromise of sensitive information. Wireless is a shared medium. Everything that is transmitted over the radio waves can be intercepted if the interceptor is within the coverage area of the radio transmitters. This represents a potential security issue in the wireless Local Area Networks (LANs). The security exposure is more evident if the wireless LANs are deployed or used in public areas, such as airports, hotels or conference centers.

155. Perform a risk assessment and obtain the written approval of the ISO before installing wireless network or wireless access points.

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.

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.

-Modem Usage

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.

-Public Websites Content Approval Process

Comments: The World Wide Web provides an opportunity for SEs both to disseminate information and to provide interactive government services quickly and cost effectively. Because anything posted on a public web server is globally available and each web presence is a potential connection path to SE networks, care must be exercised in the deployment of publicly accessible servers. There is also potential for an insecure server to be used or exploited to assist in an unauthorized or illegal activity, such as an attack on another web site.

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.

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.

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.

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
i. in transit over public and SE networks,
ii. in storage
iii. while being processed.

-Electronic Signatures

Comment: New York State's Electronic Signatures and Records Act (ESRA) 9 NYCRR Part 540 provides that the use of an electronic signature that meets the requirements established by ESRA shall have the same validity and affect as a signature affixed by hand.

168. Comply with New York State's Electronic Signatures and Records Act (ESRA) and any associated rules and regulations.

-Public Key Infrastructure

Comment: The establishment of Public Key Infrastructure (PKI) based security architecture is a significant undertaking that requires the establishment of the required business processes to support the PKI and the implementation of technology to support the resulting business processes.

169. Where Public Key Infrastructure (PKI) security architecture is used, define an appropriate trust model 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.

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.

7. Operational Management

171. Define the roles and responsibilities of persons who operate or use SE information processing facilities.

172. For SE information processing facilities, document operating instructions, management processes, and formal incident management procedures related to information security matters.

173. Alter computing hardware, software or system configurations provided by SE only under documented, written policy, procedures or specific written approval of SE management.

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

-Segregation of Security Duties

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

176. Separate duties or areas of responsibility, where practical, to reduce the risk of accidental or deliberate system misuse, and where not practical, implement other compensatory controls such as monitoring of activities, audit trails and management supervision.

-Separation of Development, Test, and Production Environments

177. Logically or physically separate development, test, and production environments.

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

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.

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

181. Use distinct logon procedures and environmental identification for production, testing, and development.

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.

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

-System Planning and Acceptance

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

185. Monitor storage and memory capacity demands and project future capacity requirements to ensure adequate processing and storage capability is available when needed and thereby to avoid potential bottlenecks that might threaten system security or user services.

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.

-Protection against Malicious Code

Comments: The introduction of malicious code such as a computer virus, network worm program and Trojan horse can cause serious damage to networks, workstations and business data.

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.

193. Inform users of the dangers of unauthorized or malicious code.

-Software Maintenance

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.

196. Log maintenance of SE-developed software to ensure changes are authorized, tested, and accepted by SE management.

-Information Back-up

197. Determine the criticality of business systems and the time frame required for recovery based on a threat and risk assessment.

198. Develop plans that can meet the IT backup and recovery requirements of the SE.

199. Perform back-ups of critical SE data and software regularly.

-Assessment

200. Maintain an assessment of the criticality of the services provided and the sensitivity of the information held on all hosts and servers, including all installed software and operating system versions, firewalls, switches, routers and other communication equipment operating systems.

-System Security Checking

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.

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.

8. Access Control

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.

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.

-User Registration and Management

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).

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.

-Logon Banner

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.

-Privileged Accounts Management

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.

211. Change passwords on multi-user system privileged accounts more often than normal user accounts.

-User Password Management

212. Develop and implement password standards to ensure all authorized persons accessing SE resources follow proven password management practices.

213. Whenever possible, mandate password rules by automated system controls.

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.

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

221. To ensure good password management, wherever technically feasible, implement password controls through the use of established standards.

-Network Access Control

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.

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.

-User Authentication for External Connections (Remote Access Control)

Comment: For the purposes of this policy, "remote access" is defined as any access coming into the SE's network from off the SE's private, trusted network. This includes, but is not limited to: dialing in from another location over public lines by an employee or other authorized individual for the purpose of telecommuting or working from home; connecting a third party network via dial or other temporary access technology to the SE network; Any access coming into the SE's network from off the SE's private, trusted network must be done in a secure manner.

224. Maintain individual accountability for all access, including during remote access.

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.

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

227. Assess and document the scope, method, risks, and required controls (contractual, process, and technical) required for any remote access,.

228. Use stronger passwords or other comparable methods for remotely connecting to the SE network.

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

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.

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

Comment: Using this type of entry system to access a SE computer provides many benefits, including simplified and cost effective security, maintenance, and support.

232. Require individual accountability for vendors to access SE computers or software.

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.

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.

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.

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.

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.

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.

-Segregation of Networks

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.

-Operating System Access Control

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.

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.

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.

245. Rename, remove, or disable, wherever feasible, default administrator accounts.

246. Change the default passwords on administrator accounts.

-Application Access Control

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

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.

-Monitoring System Access and Use

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.

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.

9. Systems Development and Maintenance

Comment: Software applications are developed or acquired to provide efficient solutions to SE business problems. These applications generally store, manipulate, retrieve and display information used to conduct SE business. The SE business units become dependent on these applications, and it is essential the data processed by these applications be accurate. It is also critical that the software that performs these activities be protected from unauthorized access or tampering. Controls in systems and applications can be placed in many places and serve a variety of purposes.

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.

253. Involve the ISO in all phases of the System Development Lifecycle from the requirements definition phase through implementation and eventual application retirement.

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.

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.

256. For each SE-built application, have the information owners address the business risks and develop a profile of the data.

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

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.

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.

264. Implement security measures on SE-built applications and systems that are based on cost/benefit analysis and the information owners' threat and risk assessments of the information being processed.

-Input Data Validation

265. Validate (in SE-built applications) input data, ensuring it is correct and appropriate and detecting data input errors. Clearly identify personnel to perform these functions.

266. Perform (in SE-built applications) the same data integrity checks at the server that are performed on the client.

267. Perform data integrity checks (in SE-built applications) on the input of business transactions, static data (names, addresses, employee numbers, etc.) and parameter tables.

268. Set up a process (in SE-built applications) to verify and correct fields, characters, completeness of data, and range/volume limits.

-Control of Internal Processing

Comment: Data that has been entered correctly can be corrupted by processing errors or through deliberate acts.

269. Incorporate checks and balances into SE-built applications and systems to prevent or stop an incorrect program from running.

270. In application designs for SE-built applications, implement controls to minimize the risk of processing failures leading to a loss of data or system integrity. Consider using correction programs to recover from failures and access to add and delete functions to make changes to application data and to ensure the correct processing of data.

-Message Integrity

Comment: Message integrity will not protect against unauthorized disclosure.

271. Establish a method in SE-built applications to detect unauthorized changes to the content of a transmitted electronic message.

272. Perform an assessment of threats and risks in SE-built applications to determine whether message integrity is required and to identify the most appropriate method of implementation. Consider message integrity especially for applications such as electronic funds transfer and EDI transactions.

-Cryptographic Controls

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

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.

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.

-Key Management

Comment: Loss of confidentiality of a cryptographic key would cause all information encrypted with that key to be considered compromised.

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.

-Protection of System Test Data

Comment: Test data is intended to test the expected behavior of software, systems and applications. Test data is developed to test a comprehensive set of conditions and outcomes, including exception processing and error conditions to demonstrate accurate processing and handling of information and the stability of the software, system or application. Its protection is essential to ensuring a valid and controlled simulation with predictable outcomes.

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

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.

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.

-Change Control Procedures

280. Use strict and formal change control procedures for changes to SE business applications and systems software used to maintain operating systems, network software, hardware changes, etc. ensuring that
    a. security and control procedures are not compromised;
    b. support programmers are given access only to those parts of a system necessary to perform their jobs;
    c. formal agreement and approval processes for changes are implemented.

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.

10. Compliance

-Monitoring

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.

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.

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

-Compliance

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.

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.

287. Establish a post, such as Information Security Officer, to monitor compliance with information security laws, regulations, and policies.

288. Implement a process [head of SE] to determine the level of SE compliance with information security laws, regulations, and policies and to document areas of non compliance. Review such compliance at least annually and develop plans to address areas of non compliance. {SUNY interpretation}

289. Set and keep an annual date, such as the start of Fiscal Year, by which SE Executive Management will have read and certified a formal report of the SE's current level of compliance with information security laws, regulations, and policies. {SUNY interpretation}

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}

291. Ensure [SE managers and supervisors] that workers within supervisory areas of responsibility follow security processes and procedures.

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.

-Enforcement and Violation Handling

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. authorization for user accounts involved in a compromise may be suspended during an investigation.

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.

INDEX