# Table of Contents

## OVERVIEW

Information Security Policy Framework ................................................................. 6
Information Security Policy Availability and Maintenance ................................. 8
Regulations Addressed ......................................................................................... 8
Security Policy Exceptions .................................................................................... 8
Security Policy Violations ..................................................................................... 8
1.1 Security Policy Summary ................................................................................ 9
1.2 Intent ............................................................................................................... 9
1.3 Scope ............................................................................................................. 9
1.4 Regulations Addressed ................................................................................... 9
1.5 Enforcement .................................................................................................. 9
1.6 Guidance ...................................................................................................... 9

## AUTHENTICATION & AUTHORIZATION

2.1 Security Policy Summary .............................................................................. 11
2.2 Intent ........................................................................................................... 11
2.3 Scope .......................................................................................................... 11
2.4 Regulations Addressed ................................................................................ 11
2.5 Enforcement ................................................................................................ 11
2.6 Guidance ..................................................................................................... 11

## PASSWORD MANAGEMENT

3.1 Security Policy Summary .............................................................................. 15
3.2 Intent ........................................................................................................... 15
3.3 Scope .......................................................................................................... 15
3.4 Regulations Addressed ................................................................................ 15
3.5 Enforcement ................................................................................................ 15
3.6 Guidance ..................................................................................................... 15

## CONFIDENTIALITY & NON-REPUDIATION

4.1 Security Policy Summary .............................................................................. 17
4.2 Intent ........................................................................................................... 17
4.3 Scope .......................................................................................................... 17
4.4 Regulations Addressed ................................................................................ 17
4.5 Enforcement ................................................................................................ 17
4.6 Guidance ..................................................................................................... 17

## EXTERNAL THIRD-PARTY ACCESS

5.1 Security Policy Summary .............................................................................. 18
5.2 Intent ........................................................................................................... 18
5.3 Scope .......................................................................................................... 18
5.4 Regulations Addressed ................................................................................ 18
5.5 Enforcement ................................................................................................ 18
5.6 Guidance ..................................................................................................... 18
6 FAULT TOLERANCE, BACKUP & RECOVERY ................................................................. 20
   6.1 SECURITY POLICY SUMMARY ........................................................................... 20
   6.2 INTENT ............................................................................................................. 20
   6.3 SCOPE .............................................................................................................. 20
   6.4 REGULATIONS ADDRESSED ........................................................................... 20
   6.5 ENFORCEMENT ............................................................................................... 20
   6.6 GUIDANCE ....................................................................................................... 20

7 INCIDENT RESPONSE & REPORTING ................................................................. 22
   7.1 SECURITY POLICY SUMMARY ........................................................................ 22
   7.2 INTENT ............................................................................................................. 22
   7.3 SCOPE .............................................................................................................. 22
   7.4 REGULATIONS ADDRESSED ........................................................................... 22
   7.5 ENFORCEMENT ............................................................................................... 22
   7.6 GUIDANCE ....................................................................................................... 22

8 MAINTENANCE & OPERATIONS ........................................................................ 23
   8.1 SECURITY POLICY SUMMARY ........................................................................ 23
   8.2 INTENT ............................................................................................................. 23
   8.3 SCOPE .............................................................................................................. 23
   8.4 REGULATIONS ADDRESSED ........................................................................... 23
   8.5 ENFORCEMENT ............................................................................................... 23
   8.6 GUIDANCE ....................................................................................................... 23

9 NETWORK & REMOTE ACCESS .......................................................................... 24
   9.1 SECURITY POLICY SUMMARY ........................................................................ 24
   9.2 INTENT ............................................................................................................. 24
   9.3 SCOPE .............................................................................................................. 24
   9.4 REGULATIONS ADDRESSED ........................................................................... 24
   9.5 ENFORCEMENT ............................................................................................... 24
   9.6 GUIDANCE ....................................................................................................... 24

10 PHYSICAL ACCESS ............................................................................................. 26
   10.1 SECURITY POLICY SUMMARY ....................................................................... 26
   10.2 INTENT ............................................................................................................ 26
   10.3 SCOPE ............................................................................................................. 26
   10.4 REGULATIONS ADDRESSED ......................................................................... 26
   10.5 ENFORCEMENT ............................................................................................. 26
   10.6 GUIDANCE ..................................................................................................... 26

11 ANTI-VIRUS PROTECTION .................................................................................. 27
   11.1 SUMMARY ...................................................................................................... 27
   11.2 INTENT ............................................................................................................ 27
   11.3 SCOPE ............................................................................................................. 27
   11.4 REGULATIONS ADDRESSED ......................................................................... 27
   11.5 ENFORCEMENT ............................................................................................. 27
   11.6 GUIDANCE ..................................................................................................... 27
<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1</td>
<td>SECURITY POLICY SUMMARY</td>
<td>28</td>
</tr>
<tr>
<td>12.2</td>
<td>INTENT</td>
<td>28</td>
</tr>
<tr>
<td>12.3</td>
<td>SCOPE</td>
<td>28</td>
</tr>
<tr>
<td>12.4</td>
<td>REGULATIONS ADDRESSED</td>
<td>28</td>
</tr>
<tr>
<td>12.5</td>
<td>ENFORCEMENT</td>
<td>28</td>
</tr>
<tr>
<td>12.6</td>
<td>GUIDANCE</td>
<td>28</td>
</tr>
<tr>
<td>13.1</td>
<td>SECURITY POLICY SUMMARY</td>
<td>30</td>
</tr>
<tr>
<td>13.2</td>
<td>INTENT</td>
<td>30</td>
</tr>
<tr>
<td>13.3</td>
<td>SCOPE</td>
<td>30</td>
</tr>
<tr>
<td>13.4</td>
<td>REGULATIONS ADDRESSED</td>
<td>30</td>
</tr>
<tr>
<td>13.5</td>
<td>ENFORCEMENT</td>
<td>30</td>
</tr>
<tr>
<td>13.6</td>
<td>GUIDANCE</td>
<td>30</td>
</tr>
<tr>
<td>14.0</td>
<td>APPROPRIATE USAGE</td>
<td>32</td>
</tr>
<tr>
<td>15.0</td>
<td>LEGISLATIVE AND REGULATORY COMPLIANCE</td>
<td>34</td>
</tr>
<tr>
<td>16.0</td>
<td>BUSINESS REQUIREMENTS</td>
<td>35</td>
</tr>
<tr>
<td>17.0</td>
<td>BUSINESS CONTINUITY PLANNING</td>
<td>36</td>
</tr>
<tr>
<td>18.0</td>
<td>APPENDIX I</td>
<td>37</td>
</tr>
<tr>
<td>19.0</td>
<td>APPENDIX II</td>
<td>38</td>
</tr>
<tr>
<td>20.0</td>
<td>APPENDIX III</td>
<td>41</td>
</tr>
<tr>
<td>21.0</td>
<td>APPENDIX IV</td>
<td>42</td>
</tr>
<tr>
<td>22.0</td>
<td>APPENDIX V</td>
<td>43</td>
</tr>
</tbody>
</table>
## IT Security Policy Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Description</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/28/10</td>
<td>0.1</td>
<td>Initial Review</td>
<td>D. Berger</td>
</tr>
<tr>
<td>11/06/10</td>
<td>1.0</td>
<td>Structural Review by CSSD Security</td>
<td>J. Hudson</td>
</tr>
<tr>
<td>11/10/10</td>
<td>1.1</td>
<td>Document re-work, edit, alignment</td>
<td>B. Vidic</td>
</tr>
<tr>
<td>12/17/10</td>
<td>1.2</td>
<td>Document edit completion</td>
<td>B. Vidic</td>
</tr>
<tr>
<td>02/01/11</td>
<td>1.3</td>
<td>Document re-work, edit, alignment</td>
<td>B. Vidic</td>
</tr>
<tr>
<td>03/24/11</td>
<td>1.4</td>
<td>Document review and editing</td>
<td>B. Vidic</td>
</tr>
<tr>
<td>01/18/12</td>
<td>1.5</td>
<td>Final review</td>
<td>B. Vidic</td>
</tr>
<tr>
<td>11/7/13</td>
<td>1.6</td>
<td>Edits based on 2013 Audit</td>
<td>B. Vidic</td>
</tr>
<tr>
<td>12/19/13</td>
<td>1.7</td>
<td>Edits based on 2013 Audit</td>
<td>B. Vidic</td>
</tr>
<tr>
<td>01/08/14</td>
<td>1.8</td>
<td>Edits based on 2013 Audit</td>
<td>B. Vidic</td>
</tr>
<tr>
<td>03/17/14</td>
<td>1.9</td>
<td>Edits based on 2013 Audit</td>
<td>B. Vidic</td>
</tr>
<tr>
<td>05/06/14</td>
<td>2.0</td>
<td>Edits based on 2013 Audit</td>
<td>B. Vidic</td>
</tr>
<tr>
<td>6/10/14</td>
<td>2.1</td>
<td>Edits based on 2013 Audit</td>
<td>B. Vidic</td>
</tr>
<tr>
<td>7/27/15</td>
<td>2.2</td>
<td>Edits based on review of best practices</td>
<td>B. Vidic</td>
</tr>
<tr>
<td>3/10/16</td>
<td>2.3</td>
<td>Edits based on NIST CSF exercise</td>
<td>B. Vidic</td>
</tr>
</tbody>
</table>
Overview

The Swanson School of Engineering (hereafter SSoE) recognizes that information and information systems are critical and important assets. SSoE will take appropriate steps to properly protect information and information systems from a variety of risks and threats such as error, fraud, sabotage, privacy violation, regulatory non-compliance and service interruption.

This IT security policies document provides direction for the consistent implementation of controls across platforms and applications to protect information and information systems. This Information Security Policy describes how IT security policies will be created, adopted, maintained and enforced.

All SSoE employees, as well as contractors and third parties with access to SSoE IT resources, are expected to understand and comply with the IT security policies presented in this document. SSoE also complies with University level security policy, managed and enforced by the University’s Computing Services & Systems Development group (hereafter CSSD).

Information Security Policy Framework

To ensure that security risks of all types are addressed, the Swanson School of Engineering Information Security Policies has been written to align with the control objectives of both the Committee of Sponsoring Organizations of the Treadway Commission (COSO), and National Institute of Standards and Technology (NIST) SP 800-53A. These both represent acceptable control frameworks that can be used to demonstrate compliance with Sarbanes-Oxley and FISMA regulatory requirements and includes the following control objectives:

1. Auditing, Logging, & Monitoring
   Controls within this category represent tools and processes that enhance the identification of potential security incidents and tracking of subsequent actions. Logging and monitoring controls help to identify and report key security information to responsible personnel. Other items covered by this category include, auditing, denial of service defense, hacking, host based intrusion detection, logging, network intrusion detection and active content monitoring.

2. Authentication & Authorization
   Controls within this category represent tools and processes that positively identify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

3. Password Management
   Controls within this category represent standards and processes that govern the use of passwords within the SSoE computing environment.

4. Confidentiality & Non-Repudiation
   Controls within this category represent tools and processes that use various forms of cryptography to disguise information providing for data integrity, confidentiality and authenticity. The types of technologies involved include encryption, digital certificates, digital signatures, etc.

5. External Third-Party Access
   Controls within this category represent tools and processes that govern access to SSoE-owned computing resources and data by external, non-SSoE users (e.g., business partners/alliances) including security requirements and audit clauses within business partner and vendor contracts.
6. Fault Tolerance, Back-up & Recovery  Controls within this category represent tools and processes that provide for the assurance of systems and data availability.

7. Incident Response & Reporting  Controls within this category represent tools and processes that facilitate SSoE’s response to malicious technical threats and incidents. Included are the roles and responsibilities of key incident response personnel. This area includes anti-virus software, intrusion detection systems and other security threat monitoring tools.

8. Maintenance & Operations  Controls within this category represent tools and processes that provide for the proper handling and protection of system documentation, storage devices and back-up media and other miscellaneous security maintenance and operational risks.

9. Network & Remote Access  Controls within this category represent tools and processes that provide for the protection of networks and their services from unauthorized modification, destruction, or disclosure and provision of assurance that the network performs its critical functions correctly and there are no harmful side-effects. This area includes wireless networks, firewalls and other network technology and controls.

10. Physical Access  Controls within this category represent tools and processes that address the threats, vulnerabilities and countermeasures that can be utilized to physically protect SSoE facilities and physical assets.

11. Anti Virus  Controls within this category represent tools and processes that provide for the protection of SSoE’s computing environment from malicious code.

12. System Configuration  Controls within this category represent tools and processes that govern technology configurations and standards, default user permissions and configurations and the protection of systems and data from malicious code (e.g. viruses, Trojans, worms, etc.).

13. Systems Development & Change Control  Controls within this category represent tools and processes that provide assurances for areas such as systems development process and life cycle, application controls, change controls, data warehousing, data mining, knowledge-based systems, program interfaces and concepts used to ensure data and application integrity, security and availability.

14. Appropriate Usage  Controls within this category include items that should be presented to new employees as part of an orientation prior to granting system access.
Information Security Policy Availability and Maintenance

The most recent version of the Swanson School of Engineering Information Security Policies can be obtained from the SSoE Technology Group.

The Swanson School of Engineering Information Security Policies will be maintained by the SSoE Technology Director and SSoE Dean’s Committee (including Dean, Associate Deans, Assistant Deans, Department Chairmen, and Executive Administrator). The Information Security Policy will be updated periodically based on industry standards with input from SSoE’s departments.

Regulations Addressed

SSoE recognizes the importance of complying with applicable state, federal and international regulations governing security controls for the IT environment. As a result, the Swanson School of Engineering Information Security Policies encompasses control requirements for Sarbanes-Oxley and FISMA.

The policies in this document also encompass control frameworks used to demonstrate compliance with federal regulations; for example, the COSO and COBIT control frameworks used to demonstrate compliance with Sarbanes-Oxley and FISMA for protecting the integrity and availability of critical financial reporting data.

Security Policy Exceptions

SSoE acknowledges that there will be exceptions to the Swanson School of Engineering Security Guidelines. These exceptions will require a documented risk assessment by the SSoE Director of technology and if deemed apropro, by the SSoE Dean’s Committee. Decisions regarding risk of a security breach versus the cost of protecting the information and information systems will be settled by the SSoE Dean’s Committee, along with the SSoE subsidiary management or their designated alternate. Certain systems will not permit implementation of indicated control activities without replacement of entire system (e.g. expiring passwords). These exceptions are also required to be brought to the attention of the SSoE Dean’s Committee.

Exception note – SSoE Technology Director must log granted exceptions from policy. Indicate if exception is granted because of system limitations or existence of mitigating controls.

Security Policy Violations

Control objectives are to be implemented and followed. Violations of policies stated in this document will require a review of the incident. Violations will be reviewed with respect to the severity of the violation. Severity of the violation and the resulting course of action will be determined by taking into consideration the intent, potential damage, actual damage and legal guidelines.
1 Auditing, Logging & Monitoring

1.1 Security Policy Summary

- Computer systems may be reviewed as necessary to ensure compliance with SSoE policies and procedures.
- Each SSoE Technology Group Department Lead will monitor and may audit systems as necessary to detect potentially inappropriate or unauthorized activities.
- Only authorized SSoE Technology Group personnel may use auditing, logging and monitoring tools on University networks and SSoE computer systems in cooperation with CSSD.
- SSoE systems handling Sarbanes-Oxley regulated data must securely log/retain all security relevant events for a minimum of 15 months.

1.2 Intent

The purpose of this policy is to provide authority for members of the SSoE Dean’s Committee to monitor, as reported by or directed through the SSoE Technology Director, IT resources as well as conduct security audits on any computer systems at SSoE and to define their activities.

1.3 Scope

This policy covers all computer and communication devices owned or operated by SSoE. This policy also covers any computer and communications device that are present on SSoE premises, but which may not be owned or operated by SSoE.

1.4 Regulations Addressed

- Sarbanes-Oxley and FISMA

1.5 Enforcement

SSoE Faculty and staff will be strongly encouraged to support and uphold this policy; failure to do so may contribute to or cause negative impact to SSoE and the University. Impact of negative actions will be dealt with on a case-by-case basis directly with the faculty member, staff member, and their respective supervisors. SSoE Director of Technology will leverage in place committees including Monthly Dean/Chair meeting, Quarterly Administrator Forum, Per Semester Engineering Circle, and Bi-Weekly Technology Group meetings to perform regular communication updates on the ISP.

1.6 Guidance

1.6.1 Auditing, logging and monitoring activities may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources.
- Investigate possible security incidents to ensure conformance to SSoE security policies.
- Monitor user or system activity where appropriate.
Auditing Guidance

1.6.2 Computer systems may be audited as necessary to ensure compliance with SSoE policies and procedures.

1.6.3 When requested, and for the purpose of performing an audit, any access needed will be provided to members of the SSoE Technology Group. This access may include:

- User level and/or system level access to any computing or communications device.
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on SSoE equipment or premises.
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on SSoE networks.

1.6.4 Audits that can be performed include:

- Password strength.
- Unauthorized network devices.
- Unsecured sharing of devices.
- Operating System and Software License.

1.6.5 On an annual basis SSoE Director of Technology will perform a review of the ISP with two committees comprised of department leadership and technology staff. Changes will be reviewed and considered for addition or amendment to ISP.

Logging Guidance

1.6.6 All computer systems handling regulated information must securely log and retain all security relevant events for fifteen months or as mandated by regulation.

1.6.7 Procedures and controls must be designed and implemented for logs to:

- Be able to identify the user who created or modified a document or record;
- Be secure from unauthorized modification;
- Be computer-generated;
- Be time-stamped and date-stamped.

1.6.8 The following logs should be captured and used to check for signs of wrongdoings and vulnerability exploitation as needed by authorized SSoE Technology Group personnel:

- CSSD generated firewall and network scanning logs.
- User account logs.
- System error logs.
- Application logs.

Monitoring Guidance

1.6.9 Mission critical servers must be protected by controls that detect and alert on security events.

1.6.10 Safeguards must be implemented to:

- Detect any attempt at unauthorized use of identification codes and/or passwords.
- A formal review will be performed every 60 days to review and act on: results from 1.6.8, reported security incidents, firewall exception requests, reports from intrusive scans of public facing resources, vulnerability scans. Results will be regularly documented and reviewed annually to review security state in SSoE.

1.6.11 Information owners must review system and application privileges on a periodic basis.
2 Authentication & Authorization

2.1 Security Policy Summary

- All employees, contractors, visitors and third parties must adhere to University Human Resources policy and agreements prior to accessing any SSoE IT resources.
- Privileges of all users and systems will be restricted based on the business need and role of requestor.
- Human Resources Department and Department Heads are authorized to inform a Department IT Lead or designated alternate to disable or re-enable security for a user.
- User IDs may not be shared.
- Anonymous login accounts (such as “guest”) are not permitted.
- Any User ID that has not been accessed within 90 days will be disabled.
- After no activity on a terminal or workstation for a certain period of time, the system must disconnect the current session or lock the workstation.

2.2 Intent

The purpose of this policy is to define standards of authority in accessing SSoE systems, networks and facilities and to establish accountability for use of SSoE IT resources.

2.3 Scope

This policy applies to all individuals in any type of employment relationship with SSoE, as well as contractors, consultants and any other users of SSoE computer systems. This policy applies to all computer and data communication systems owned, leased and/or administered by SSoE.

2.4 Regulations Addressed

- Sarbanes-Oxley and FISMA

2.5 Enforcement

SSoE Faculty and staff will be strongly encouraged to support and uphold this policy; failure to do so can and may contribute to or directly cause negative impact to SSoE and the University. Impact of negative actions will be dealt with on a case-by-case basis directly with the faculty member, staff member, and their respective supervisors.

2.6 Guidance

2.6.1 All Third Parties (person or entity) such as consultants, contractors and temporaries will be required to sign a Swanson School of Engineering Third Party Security & Access Control Agreement prior to accessing any SSoE resources. It is the responsibility of the Department IT Lead or designated alternate to ensure that a signed original copy of the security agreement is obtained and filed in the Third Party’s contract file.
2.6.2 Privileges of all users and systems will be restricted based on the business need. This means that privileges will not be extended unless a legitimate business-oriented need for such privileges exists. A Department Director should promptly report all significant changes in a user(s) duties or employment status to a Department IT Lead or designated alternate. The Department IT Lead or designated alternate should promptly revoke all privileges no longer needed by users.

2.6.3 Requests for new User IDs and changed privileges will be presented in writing and approved by the responsible Department Director before a Department IT Lead or designated alternate completes these requests. This will ensure the validity of the request and provide an audit trail of all changes to access. Change requests should be filed in a designated area.

2.6.4 The Human Resources Department and Department Directors are authorized to inform a Department IT Lead or designated alternate to disable or re-enable security for a user. A Department Director/Manager or designated alternate will be responsible for reviewing and distributing a terminated user’s system files.

2.6.5 Annually, in May of every calendar year, comprehensive user account reviews will be performed based on business and academic need on all University issued primary and sponsored accounts of SSoE faculty, students and staff. Additionally, sponsored accounts issued 3rd party entities will be reviewed for validity and continuation. University issued accounts will be reviewed annually as well for business or academic need to access SSoE-focused applications. Finally, any locally created/issued/managed accounts accessing SSoE-focused applications that are not LDAP integrated will be reviewed annually at this time as well. Logs and results of these reviews will be housed securely on the SSoE Technology Group SharePoint site.

User Identification

2.6.6 For the purpose of user authentication, demographic information will be captured and used to validate the identity of persons utilizing SSoE resources. This includes, but is not limited to: first name, last name, middle initial and other personal information provided by the user. Other measures may also be used to authenticate a user whose identity is in question.

User ID

2.6.7 Generic User IDs will be limited. (Examples of a business need to utilize generic User IDs are: user training, software installations or to minimize the user login steps to launch an application.) Privileges of these generic User IDs will be severely restricted. This means that extra measures will be taken to limit privileges such as, the time of day the id can be used, restriction of the User ID to a specific workstation, as well as a login expiration date.

2.6.8 Users will be restricted from logging into any SSoE system or network anonymously (for example, by using “guest”, “administrator” or “root” User IDs). They will initially log in using a User ID that clearly indicates their identity. Whatever the operating system, logs must record all such changes of the current User ID where the system allows for such logging. Exceptions may be made for servers retaining only public information.

2.6.9 On UNIX/Linux servers, administrator users will be assigned a User ID with security equivalence of the root User ID. When possible, the sudo utility should be installed and used to grant and/or limit the type of root privileges assigned to a non-administrator user while logging all commands and arguments. If the sudo utility is not compatible, then the preferred alternate method for granting root access will be to assign a non-administrative and an administrative equivalent User ID. The user will initially log in as the non-administrative account, then use the /bin/su command to gain root access. All administrative network access to the UNIX/Linux servers must connect using a Secure Shell (SSH) terminal program.

2.6.10 On Windows, users will not be assigned a User ID with security equivalence of the Admin or Administrator User ID.

2.6.11 All “System default Administrator” User IDs and passwords will be immediately documented and secured upon assignment by the Department IT Lead or designated alternate. These passwords will be stored in a secure location, safe from fire, water and other types of damaging influences. Offsite storage is preferred. A process will exist for authorized personnel to acquire these passwords in a “true emergency” situation. These passwords will be immediately changed following their use for system upgrades, “true emergency” situations or if they have become known to any unauthorized person.
2.6.12 Any User ID that has not been accessed within 90 days will be disabled. Re-enabling of these accounts will require proof of identification.

**Auto Logoff/Locking**

2.6.13 After no activity on a terminal or workstation for a certain period of time, the system will disconnect the current session or lock the workstation. Re-establishment will occur after the user has provided a valid password. The recommended period of time is 15 minutes.

**Concurrent Sessions**

2.6.14 Concurrent session connections should be limited. This means that the number of sessions a user can initiate simultaneously will be controlled.

- A maximum of four (4) will be allowed.

2.6.15 Requests for additional concurrent sessions may be submitted to an Department IT Lead or designated alternate.

**Access Control**

2.6.16 System access must be limited to authorized individuals on a need to do and/or know basis. At minimum:

- Maintain a record of specific access granted to users.
- Expire temporary accounts (e.g., for contractors) on a predetermined schedule.
- Disable and/or revoke user account access after 90 days of inactivity.
- Limit privileged (e.g., command line, root, etc.) access to only those people who require it for their job function.

2.6.17 Network and application access controls must provide adequate security functionality (e.g. ability to create, edit, display) so that access is granted to users on a need to know/do basis.

2.6.18 Network and application access levels must be reassessed for appropriateness when job functions change (e.g. transfers) or during organizational changes (e.g., creation or merger of units, departments, etc.).

2.6.19 User IDs must uniquely identify users. Other User ID and password guidelines include:

- User IDs must not be shared by users. User IDs used as server-level service accounts are exempt from this control; however, reasonable compensating controls (e.g., such as strong passwords) should be implemented.
- Social Security numbers or other non-SSoE personal identification should not be used as User IDs.

2.6.20 Client-based automated processes (e.g., an automated logon script containing user id and password) that by-pass user manual access control mechanisms should not exist.

2.6.21 System documentation must provide a logical process flow of the overall authentication process and must document control testing.

- Network access accounts must be disabled after 5 login failures. Disabled accounts must be reset manually.
- Application user accounts must be disabled after 5 login failures where the system allows this to be enforced. Disabled accounts must be reset manually.

2.6.22 User accounts must be disabled upon termination/suspension of the user and disposition of user files must be determined within 90 days.

2.6.23 Portable computers (including laptops and PDAs) should use power-on and/or hard drive passwords and, if available, inactivity timeouts (e.g., screen saver) of 15 minutes or less.

2.6.24 Automated access to global email address directories must be controlled to prevent the spread of viruses and malicious code.
2.6.25 Operating system accounts (e.g., Windows or UNIX/Linux user ids) established as "service accounts" are permitted if other more secure implementation scenarios are not available, with the following qualifications:

- Specific accountability and ownership for such accounts must be documented and retained for audit and control purposes. Account owners must ensure that regulatory and/or local statutes permit the use of such generic accounts for the type of application being implemented.
- The scope of control/access for such accounts must be restricted to only the server(s) and/or applications required.
- Service account owners must perform annual and/or periodic reviews of account use and access to determine that the account is still required and that access continues to be properly restricted.
- Where technically possible service accounts should not permit interactive (console) login from the Operating System command line, (e.g. In UNIX/Linux, users should be forced to login to a unique named personal account on a given computer and then may "switch-user" to a general or service type account).
3 Password Management

3.1 Security Policy Summary

- Access to any SSoE system must require a password.
- Passwords cannot be shared between users.
- Passwords must not be an easily guessable word or name.
- Passwords should be a minimum of 8 characters in length and contain alphanumeric characters.
- Passwords stored within an application or existing within a file must be encrypted.
- Non-encrypted passwords must not be stored in readable form where unauthorized persons might discover them.

3.2 Intent

The purpose of the Password Management policy is to establish guidelines for implementing and maintaining passwords in a manner that will prevent them from being easily compromised.

3.3 Scope

This policy applies to all individuals in any type of employment relationship with SSoE, as well as contractors, consultants and any other users of SSoE’ IT resources. This policy applies to all computer and data communication systems owned, leased and/or administered by SSoE.

3.4 Regulations Addressed

- Sarbanes-Oxley and FISMA

3.5 Enforcement

SSoE Faculty and staff will be strongly encouraged to support and uphold this policy; failure to do so can and may contribute to or directly cause negative impact to SSoE and the University. Impact of negative actions will be dealt with on a case-by-case basis directly with the faculty member, staff member, and their respective supervisors.

3.6 Guidance

3.6.1 Passwords are important to ensure user authentication and integrity of SSoE systems and data. The University’s Human Resources group and CSSD centrally manage accounts, and issue default passwords.

3.6.2 Since currently CSSD-managed passwords are non-expiring, strong passwords must be implemented, including use of special characters, upper and lower case and length of 8 to 15 characters.

3.6.3 Vendor/Business partner sponsored account passwords will be changed immediately upon or prior to production use.

3.6.4 Per CSSD policy and procedure, newly issued or reissued passwords will only be valid for the user’s first session. At that time, the user will be forced to choose another password.
3.6.5 Per CSSD policy and procedure, a different unique password will be required when the existing password has been newly issued, reissued, or expires. This will prevent the same password from being used over and over.

3.6.6 Passwords must be of sufficient length and strength to deflect brute-force cracking attempts. At a minimum:

- Passwords must have a minimum length of 8 characters and of sufficient complexity to prevent compromise. Applications that can accept network authentication can do so (e.g., single sign-on).

- Applications and operating systems that cannot interface with network authentication must meet the standards above. Those that cannot be configured to meet the above should use the maximum possible length and character complexity allowed by the Operating System or the application.

3.6.7 Passwords stored within an application, batch files, automatic log-in scripts, software macros, terminal function keys or in other locations where unauthorized persons might discover them or existing within a file must be encrypted.

Incidental Discovery of Passwords

3.6.8 Data acquired through CSSD by network traffic analyzing utilities or tools, system or application dumps and reports from printers may contain sensitive information. During the course of investigating system or network problems, personnel may accidentally discover a user’s system or application User ID and password. If this occurs, this discovery will immediately be reported to the Department IT Lead. The Department IT Lead will then contact the user immediately to have the password changed.

3.6.9 All passwords must be immediately changed if they are suspected of being disclosed or known to have been disclosed to anyone besides the authorized user.
4 Confidentiality & Non-Repudiation

4.1 Security Policy Summary

- Data considered to be high risk must be encrypted.
- The encryption standard used must be considered strong in accordance with prevailing standards at the time.
- When encryption is used, keys shall be maintained by two different individuals, with additional copies of the keys stored in two different secure locations.

4.2 Intent

The purpose of the Confidentiality & Non-Repudiation policy is to establish guidelines for the use of encryption when deemed necessary.

4.3 Scope

This policy applies to all individuals in any type of employment relationship with SSoE, as well as contractors, consultants and any other users of SSoE’ IT resources. This policy applies to all computer and data communication systems owned, leased and/or administered by SSoE.

4.4 Regulations Addressed

- Swanson School of Engineering Information Security Policies

4.5 Enforcement

SSoE Faculty and staff will be strongly encouraged to support and uphold this policy; failure to do so can and may contribute to or directly cause negative impact to SSoE and the University. Impact of negative actions will be dealt with on a case-by-case basis directly with the faculty member, staff member, and their respective supervisors.

4.6 Guidance

4.6.1 SSoE data which is considered high risk should be encrypted. This could include data that by its nature is high risk, i.e., proprietary and of significant value, or data that is placed in a high risk situation, such as on a laptop or flash drive. Until such time as a formal data classification policy is adopted, responsibility is placed upon each division to assess the risk of data on a case by case basis and apply the appropriate level of protection accordingly.

4.6.2 Regardless of encryption methodology used, each methodology requires the appointment of two key holders. Additional copies of the keys should also be stored at an off site secure location.

4.6.3 When encryption is used, it must be of such strength as to be considered strong in accordance with prevailing standards at that time. For example, at the time of this writing (version 1.2), WPA 128-bit is the minimum strength considered to be strong.
5 External Third-Party Access

5.1 Security Policy Summary

- Each SSoE Department IT Lead must approve all network connections to the University and SSoE network environment from third parties with authorization by the SSoE Director of Technology.
- If Wide Area Network (WAN) connections are established between SSoE and other parties, the SSoE Director of Technology, CSSD Security and CSSD Network Engineering must approve all network connections from third parties.
- CSSD managed firewalls must be implemented for any external network connection, including internet and third-party network connections.
- Third-party connections must be restricted to specific hosts, applications and files.

5.2 Intent

The purpose of this policy is to establish how access to SSoE-owned computing resources and data by external, non-SSoE users (business partners, vendors and other third-parties) including security requirements and audit clauses within business partner and vendor contracts is granted, monitored and controlled.

5.3 Scope

This policy applies to all individuals in any type of employment relationship with SSoE as well as contractors, consultants and any other users of SSoE’s IT resources. This policy applies to all computer and data communication systems owned, leased and/or administered by SSoE.

5.4 Regulations Addressed

- Sarbanes-Oxley and FISMA

5.5 Enforcement

SSoE Faculty and staff will be strongly encouraged to support and uphold this policy; failure to do so can and may contribute to or directly cause negative impact to SSoE and the University. Impact of negative actions will be dealt with on a case-by-case basis directly with the faculty member, staff member, and their respective supervisors.

5.6 Guidance

5.6.1 Precautions must be taken whenever it is necessary to connect the University network to the network of a non-University owned company or the Internet. This is necessary so that only authorized network traffic passes through such a connection and our information assets are appropriately protected against outside threats. This will be accomplished by the use of a firewall or by using secure filtering on the network router.

5.6.2 SSoE Director of Technology will be notified well in advance of such new connections so risk can be assessed and proper precautions put in place.
5.6.3 Only devices approved by the SSoE Technology Group can be used on the network.

5.6.4 Where required by University General Counsel, SSoE temporary employees, consultants and vendors must sign a confidentiality and non-disclosure agreement which, at minimum, requires them to safeguard SSoE confidential and proprietary information and trade secrets.

5.6.5 Data confidentiality, integrity and availability controls will be specifically defined in contracts with third parties. Controls will cover all appropriate physical, personnel and logical information protection risks based on information protection risk levels. In addition, controls will take into account all prevailing statutory and regulatory requirements.

5.6.6 Contractual agreements will grant SSoE the right to audit the relevant systems within third parties and/or the third parties will commit to having independent, periodic audits performed which SSoE will have the right to review.

5.6.7 Third-party agreements must include a provision for adherence to appropriate SSoE policies and any other policies per University General Counsel.

5.6.8 Third parties should notify SSoE of all personnel changes affecting SSoE accounts.

5.6.9 Third-party controls must specify roles and responsibilities for destruction or disposal of SSoE data in accordance with SSoE policy and risk of loss.

5.6.10 All SSoE network connections to networks or systems operated by non-SSoE entities will implement a SSoE-side firewall design approved by the SSoE Technology Group, CSSD Security, and CSSD Network Engineering.

5.6.11 All unique or "one off" SSoE-external connections must be checked for vulnerabilities prior to production launch to ensure that the connections are secure. Connections made through pre-architected firewalls are exempt. The SSoE Technology Group will periodically conduct or commission appropriate vulnerability studies of such standardized connections.

5.6.12 External third parties must have a defined process to issue and respond to intrusion alerts. Provision must be made for notification to SSoE for high-risk intrusions/alerts.

5.6.13 All SSoE-external connections – CSSD will be requested to implement network monitoring systems to monitor changes to critical system files and to provide detection and alerts of unauthorized file changes.

5.6.14 Third-party connections must be restricted to specific hosts, applications and files.

- Controls must ensure that a failure of logical security or any component of a third-party site/connection does not permit external users to gain access to unauthorized University network resources.
- A documented information protection plan assessment must be conducted by the project/system/data owner with respect to the system and data being accessed to determine the level of protection required.
- SSoE Technology Group or other authorized provider will only enable third-party connections upon receipt of the completed information protection plan assessment and authorization from the data owner.
6 Fault Tolerance, Backup & Recovery

6.1 Security Policy Summary
   - Data records are to be protected from loss, destruction and falsification.
   - Backup copies of data and software associated with critical electronic information resources must be sufficient to satisfy data backup and disaster recovery requirements.
   - Backup copies of critical data for disaster recovery purposes must be stored at a secure, commercial site that provides standard protection or at an off-site facility providing equivalent protection.
   - Backups must be maintained to meet SSoE’s data retention requirements.

6.2 Intent
The purpose of this policy is to define processes that provide for the assurance of systems and data availability.

6.3 Scope
This policy applies to all individuals in any type of employment relationship with SSoE, as well as contractors, consultants and any other users of SSoE’s IT resources. This policy applies to all computer and data communication systems owned, leased and/or administered by SSoE.

6.4 Regulations Addressed
   - Sarbanes-Oxley and FISMA

6.5 Enforcement
SSoE Faculty and staff will be strongly encouraged to support and uphold this policy; failure to do so can and may contribute to or directly cause negative impact to SSoE and the University. Impact of negative actions will be dealt with on a case-by-case basis directly with the faculty member, staff member, and their respective supervisors.

6.6 Guidance

Organization Records

6.6.1 Backup copies of critical data for disaster recovery purposes must be stored at Business Records Management (BRM). These backup requirements extend to critical data stored on shared servers. Software must be readily available to permit timely restoration.

6.6.2 Information Owners must ensure that all information related to their functional area is backed up and recoverable in accordance with regulatory requirements and SSoE corporate policies, guidelines and procedures.

6.6.3 Information must be backed-up and stored in a manner that will limit loss exposure to 5 days or less.
6.6.4 Backup procedures and data recovery procedures must be documented, reviewed, practiced and updated on a periodic basis including annual testing of off-site storage tapes with the results thereof documented.

6.6.5 Physical media (tapes, disks, etc.) must be properly labeled to ensure restoration of proper data.

6.6.6 Users must understand the need for and methods of backing up files under their control (e.g. files kept on their hard drive) on a scheduled basis and be knowledgeable concerning the methods of backing up files.
7 Incident Response & Reporting

7.1 Security Policy Summary

- Security incidents involving a breach of security shall be reported.

7.2 Intent

The purpose of the Incident Response & Reporting policy is to establish guidelines for the reporting of security incidents when deemed necessary.

7.3 Scope

This policy applies to all individuals in any type of employment relationship with SSoE, as well as contractors, consultants and any other users of SSoE’s IT resources. This policy applies to all computer and data communication systems owned, leased and/or administered by SSoE.

7.4 Regulations Addressed

- Swanson School of Engineering Information Security Policies

7.5 Enforcement

SSoE Faculty and staff will be strongly encouraged to support and uphold this policy; failure to do so can and may contribute to or directly cause negative impact to SSoE and the University. Impact of negative actions will be dealt with on a case-by-case basis directly with the faculty member, staff member, and their respective supervisors.

7.6 Guidance

7.6.1 If a breach of security occurs, it must be reported to the SSoE Executive Administrator and the SSoE Director of Technology; those persons will be responsible for the determination of whether or not to bring the incident to the attention of CSSD Security and/or the SSoE Dean’s Committee or any other persons deemed necessary.
8 Maintenance & Operations

8.1 Security Policy Summary

- The SSoE Technology Group is responsible for protecting SSoE’s IT assets, and reports its activities to the SSoE Dean’s Committee.
- Operational procedures and controls must be documented and maintained.

8.2 Intent
The Maintenance & Operations Policy provides guidance for the proper handling and protection of systems, system documentation, storage devices, back-up media and other security maintenance and operational risks. It establishes security governance for SSoE and defines the role security professionals will play.

8.3 Scope
This policy applies to all individuals in any type of employment relationship with SSoE, as well as contractors, consultants and any other users of SSoE’s IT resources. This policy applies to all computer and data communication systems owned, leased and/or administered by SSoE.

8.4 Regulations Addressed

- Sarbanes-Oxley and FISMA

8.5 Enforcement
SSoE Faculty and staff will be strongly encouraged to support and uphold this policy; failure to do so can and may contribute to or directly cause negative impact to SSoE and the University. Impact of negative actions will be dealt with on a case-by-case basis directly with the faculty member, staff member, and their respective supervisors.

8.6 Guidance

8.6.1 Procedures on “how to . . .” execute the specific guidance (e.g. how to backup a system) are documented and maintained by the SSoE Technology Group. Documentation is updated when changes occur or reviewed at least annually for continued applicability. Revised procedures are reviewed with the affected users.
9 Network & Remote Access

9.1 Security Policy Summary

- All University-managed wireless networks must be protected with encryption that is considered strong in accordance with prevailing standards at the time.
- Remote access must be controlled through network solutions approved by CSSD and the SSoE Technology Group.
- Remote access methods must have authorization as well as network encryption controls; SSLVPN is the recommended solution for remote access to all networks.

9.2 Intent

The purpose of the Remote Access policy is to define standards for protecting and connecting to the University’s network from any host. These standards are designed to minimize the potential exposure to SSoE/University from damages that may result from unauthorized use of SSoE IT resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical SSoE internal systems, etc.

9.3 Scope

This policy applies to all individuals in any type of employment relationship with SSoE, as well as contractors, consultants and any other users of SSoE’s computer system. This policy applies to all computer and data communication systems owned, leased and/or administered by SSoE.

This policy also applies to remote access connections used to do work on behalf of SSoE, including reading or sending electronic mail and viewing intranet web resources.

9.4 Regulations Addressed

- Sarbanes-Oxley and FISMA

9.5 Enforcement

SSoE Faculty and staff will be strongly encouraged to support and uphold this policy; failure to do so can and may contribute to or directly cause negative impact to SSoE and the University. Impact of negative actions will be dealt with on a case-by-case basis directly with the faculty member, staff member, and their respective supervisors.

9.6 Guidance

9.6.1 Policies and procedures regarding remote access must exist to safeguard SSoE’s IT assets and the integrity of its financial data.

9.6.2 All University networks with external access must be protected by firewalls
9.6.3 All communications over University-managed wireless LANs must be protected by encryption that is considered strong.

9.6.4 SSLVPN access should be granted on an as-needed basis.

9.6.5 SSLVPN accounts must follow all of University and SSoE’s policies regarding Authentication & Authorization (Section 2) and Passwords (Section 3).

9.6.6 An annual review of users with SSLVPN access should be performed, and the list of users “reauthorized” via approval by the list reviewer.
10 Physical Access

10.1 Security Policy Summary

- Access to Co-Location IDF rooms and the University’s Network Operations Center (NOC) will be restricted to only authorized SSoE Technology Group personnel.

10.2 Intent

The intent of this policy is to address the threats, vulnerabilities and countermeasures that could compromise University or SSoE facilities, physical assets and computer systems.

10.3 Scope

The scope of this policy is applicable to all SSoE facilities worldwide. This policy applies to all individuals in any type of employment relationship with SSoE, as well as contractors, consultants and any other users of SSoE’s IT resources. This policy applies to all computer and data communication systems owned, leased and/or administered by SSoE.

10.4 Regulations Addressed

- Sarbanes-Oxley

10.5 Enforcement

SSoE Faculty and staff will be strongly encouraged to support and uphold this policy; failure to do so can and may contribute to or directly cause negative impact to SSoE and the University. Impact of negative actions will be dealt with on a case-by-case basis directly with the faculty member, staff member, and their respective supervisors.

10.6 Guidance

10.6.1 Physical access to all SSoE facilities must be controlled with appropriate responsibility assigned for periodic inspection and review of security policies.

10.6.2 Access to computer rooms, computing classrooms, Co-Location IDF rooms, and other restricted areas must be strictly controlled, monitored and logged.

10.6.3 Annually, SSoE will review/audit all employees granted access to Co-Location IDF rooms. Action will be taken based on continuing need or removed due to lack of access justification.
11 Anti-Virus Protection

11.1 Summary

- All SSoE workstations and servers will comply with University policy and have anti-virus software installed.
- Anti-virus software should be updated on a periodic basis.

11.2 Intent

The purpose of this policy is to define standards and expectations for protecting the University network and SSoE resources from malicious code. These guidelines are designed to minimize the potential exposure to SSoE from damages that may result from unauthorized entry into SSoE’s resources for the intent to spread infection through malicious code.

11.3 Scope

This policy applies to all individuals in any type of employment relationship with SSoE, and will be validated through SSLVPN “health checks.” This policy applies to all computers and systems owned, leased and/or administered by SSoE.

11.4 Regulations Addressed

- Swanson School of Engineering Information Security Policies

11.5 Enforcement

SSoE Faculty and staff will be strongly encouraged to support and uphold this policy; failure to do so can and may contribute to or directly cause negative impact to SSoE and the University. Impact of negative actions will be dealt with on a case-by-case basis directly with the faculty member, staff member, and their respective supervisors.

11.6 Guidance

11.6.1 Anti-virus software resides on the Internet gateway, exchange servers and desktops/laptops, and updates for each are run every 24 hours at a minimum.

11.6.2 The SSoE Technology Group will aid employees’ efforts to prevent virus problems by making persons aware of the risks to SSoE's systems and information; the Group will foster employee awareness, and promote employee vigilance.

11.6.3 Regular Symantec console reports will be secured from University CSSD addressing all SSoE-based virus notification and removal activities. These procedures will be integrated into 1.1.5 and 1.6.10.
12 System Configuration & Software Usage

12.1 Security Policy Summary

- SSoE workstation operating system configurations should be restricted from alteration where possible.
- SSoE workstations and servers should be supported by a patch management solution.
- Only approved software may be installed and used on all workstations and servers. Installation of unauthorized software is prohibited and technically enforced where possible.

12.2 Intent

The purpose of this policy is to address issues relevant to software installation and deployment on SSoE’s IT resources. This policy is designed to let SSoE employees achieve their business objectives. Any aberrations from this strategy will require the SSoE Technology Group to re-deploy software solutions. The purpose of this policy is also to ensure that equipment is always safeguarded appropriately, especially when left unattended.

12.3 Scope

This policy applies to all individuals in any type of employment relationship with SSoE, as well as contractors, consultants and any other users of SSoE’s computer system. This policy applies to all computer and data communication systems owned, leased and/or administered by SSoE.

12.4 Regulations Addressed

- Swanson School of Engineering Information Security Policies

12.5 Enforcement

SSoE Faculty and staff will be strongly encouraged to support and uphold this policy; failure to do so can and may contribute to or directly cause negative impact to SSoE and the University. Impact of negative actions will be dealt with on a case-by-case basis directly with the faculty member, staff member, and their respective supervisors.

12.6 Guidance

Software Installation

12.6.1 One of the SSoE Technology Group’s objectives is to enable its employees to perform their tasks with technology that is in good operating condition while appropriately addressing business needs. The SSoE Technology Group is exclusively responsible for installing and supporting all software on School computers including: office desktop computers, University-owned laptop computers, computer classroom computers, and business/home computers that are provided by SSoE to faculty and select staff.

Software Licensing
12.6.2 To comply with legislation and to ensure ongoing vendor support, the terms and conditions of all End User License Agreements are reviewed by University General Counsel, and are to be strictly adhered to.

12.6.3 It is the goal of the SSoE Technology Group to keep licensing accurate and up to date. To address this, the SSoE Technology Group is responsible for validating the licensing compliance of all software packages installed on all computing devices.

12.6.4 All SSoE employees are to ensure compliance with the specific legislation governing intellectual property rights and software licensing. These guidelines look at copyright and software licensing issues from a legal perspective.

12.6.5 Unless SSoE has a license from the owner of the software to copy and distribute computer software, copying is illegal.

12.6.6 SSoE Technology Group members will adhere to the Group’s Software Management Standards and Procurement Process.

12.6.7 Where a legitimate license has been purchased, the maximum number of permitted users cannot be exceeded. A single excess copy places SSoE at risk from prosecution under copyright laws.

12.6.8 Resale of old or redundant computer equipment can result in an infringement of the copyright law, as software license agreements may not be transferable, therefore all resale of computer equipment should first be processed through the SSoE Technology Group for thorough cleaning.

**Notebook/Laptop Configuration and Usage**

12.6.9 Users will take every precaution and available steps to avoid saving sensitive University information on the internal hard drive, SD card or other onboard storage device.

12.6.10 Default operating system and application settings must be reviewed for security exposures and steps must be taken to ensure identified vulnerabilities are addressed appropriately. Unnecessary features, functions, services, etc., must be removed or disabled if possible, restrictive access control to sensitive privileges must be implemented and trust relationships between systems must be restricted and supported by documented business requirements.

12.6.11 Standardized time synchronization with CSSD managed time servers or network time sync should occur across all systems.
13 System Development & Change Control

13.1 Security Policy Summary

- Changes to production IT systems must undergo a change control approval process.

13.2 Intent

The intent of this policy is to provide assurances for areas such as systems development process and life cycle, application controls, change controls, data warehousing, data mining, knowledge-based systems, program interfaces and concepts used to ensure data and application integrity, security and availability.

13.3 Scope

This policy applies to all individuals in any type of employment relationship with SSoE, as well as contractors, consultants and any other users of SSoE’ IT resources. This policy applies to all devices owned, leased and/or administered by SSoE.

13.4 Regulations Addressed

- Sarbanes-Oxley and FISMA

13.5 Enforcement

SSoE Faculty and staff will be strongly encouraged to support and uphold this policy; failure to do so can and may contribute to or directly cause negative impact to SSoE and the University. Impact of negative actions will be dealt with on a case-by-case basis directly with the faculty member, staff member, and their respective supervisors.

13.6 Guidance

13.6.1 If any changes made to hardware or software are identified as having regulatory impact, then it should be further verified that systems (hardware, software and applications) continue to meet the regulatory validation guidelines.

13.6.2 SSoE and vendor application development projects must define security requirements in the planning phase of system design.

13.6.3 Change requests must be adequately documented via a change request process.

13.6.4 Version control procedures must be documented and provide for an audit trail of changes to application software, hardware, network and the environment. A minimum of three versions of previous production code shall be retained.

13.6.5 Separate logical environments must exist for development (source and executables), and production (source and executables).

13.6.6 Access to source code must be restricted to authorized programmers and their supervisors within the context of the change management process.
13.6.7 Other than secondary storage backup (e.g. tape, disc, diskette, etc.) only one live copy of source code should exist in the development environment to represent the production system or application.

13.6.8 All modifications, major enhancements and new systems must be integration tested prior to installation of the software in production and receive implementation approval from the defined application and/or system owner.

13.6.9 SSoE’s patch and update installations follow SSoE’s Change Management procedures and schedule.
14 Appropriate Usage

The following are considered to be guidelines for content in the development of a user security awareness and training document.

Do not use the same password for SSoE accounts as for other non-SSoE access (e.g., personal accounts, option trading, benefits, etc.).

Regardless of the circumstances and per University policy, do not share SSoE passwords with anyone. All passwords are to be treated as highly sensitive, Confidential University information.

Here is a list of the most commonly exploited "don’ts":

- Don't reveal a password over the phone to ANYONE.
- Don't reveal a password in an email message.
- Don't reveal a password to your supervisor or other manager.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (e.g., "my family name").
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members.
- Don't reveal a password to co-workers while on vacation.
- Don’t use the "Remember Password" feature of applications.

If someone demands a password, or if an account or password is compromised, report the incident to your SSoE Technology Group Department IT Lead or your supervisor.

Strong passwords have the following characteristics:

1. Are case sensitive, contain lower case characters (e.g., a-z).
2. Have numerical characters as well as letters (e.g., 0-9).
3. Are at least eight alphanumeric characters in length.
4. Are not found in any language, slang, dialect, jargon, etc.
5. Are not based on personal information, names of family, birth date, pet name, etc.
6. Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember Your Password" and the password could be tmb1w2ryp.

Poor, weak passwords have the following characteristics:

- The password contains less than six characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- The words "Swanson School of Engineering" or any deviation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

The following is expected of all SSoE’s’ employees accessing the University network to protect it from virus problems:
- Always run the University standard, supported anti-virus software provided by the SSoE Technology Group and CSSD’s Software Licensing Services team.
- Never open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Delete Spam, chain, and other junk email without forwarding, in accordance with the University’s Internet and Email Security Policy and Procedures.
- There will be no unauthorized downloading of any information or files.
- Avoid direct disk sharing with read/write access unless there is an absolute business requirement to do so and the process has prior approval from the SSoE Technology Group.
- Always scan a removable storage device from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.

If an employee is suspect to a possible virus or other malicious code infection in an SSoE computer, it is the employee’s responsibility to contact the SSoE Technology Group immediately. Employees are to take no action on their own behalf against the suspected malicious code.

Notebook/Laptops must not be checked in to airline luggage systems or left in vulnerable situations where it might be stolen.

Missing Notebook/Laptops will be reported to your SSoE Technology Group Department IT Lead or designated alternate immediately, so that appropriate passwords can be revoked.

Employees should not have an expectation of privacy in anything they create, store, send or receive on the computer systems.

Questions about the confidentiality / sensitivity of a specific piece of information should be addressed to the employee’s manager. Questions about these guidelines should be addressed to the SSoE Technology Group or the SSoE Director of Technology.

All messages sent over University of Pittsburgh internal computer and communications systems are the property of University of Pittsburgh.
15 Legislative and Regulatory Compliance
16 Business Requirements
17 Business Continuity Planning
2.2 STRATEGY FOR CONDUCTING SECURITY CONTROL ASSESSMENTS

Organizations are encouraged to develop a broad-based, organization-wide strategy for conducting security assessments, facilitating more cost-effective and consistent assessments across the inventory of information systems. An organization-wide strategy begins by applying the initial steps of the Risk Management Framework to all information systems within the organization, with an organizational view of the security categorization process and the security control selection process (including the identification of common controls). Categorizing information systems as an organization-wide activity taking into consideration the enterprise architecture and the information security architecture helps to ensure that the individual systems are categorized based on the mission and business objectives of the organization. Maximizing the number of common controls employed within an organization: (i) significantly reduces the cost of development, implementation, and assessment of security controls; (ii) allows organizations to centralize security control assessments and to amortize the cost of those assessments across all information systems organization-wide; and (iii) increases overall security control consistency.

An organization-wide approach to identifying common controls early in the application of the RMF facilitates a more global strategy for assessing those controls and sharing essential assessment results with information system owners and authorizing officials. The sharing of assessment results among key organizational officials across information system boundaries has many important benefits including:

- Providing the capability to review assessment results for all information systems and to make organization-wide, mission/business-related decisions on risk mitigation activities according to organizational priorities, the security categorization of the information systems supporting the organization, and risk assessments;
- Providing a more global view of systemic weaknesses and deficiencies occurring in information systems across the organization;
- Providing an opportunity to develop organization-wide solutions to information security problems; and
- Increasing the organization’s knowledge base regarding threats, vulnerabilities, and strategies for more cost-effective solutions to common information security problems.

Organizations can also promote a more focused and cost-effective assessment process by: (i) developing more specific assessment procedures that are tailored for their specific organizational environments of operation and requirements (instead of relegating these tasks to each security control assessor or assessment team); and (ii) providing organization-wide tools, templates, and techniques to support more consistent assessments throughout the organization.

While the conduct of security control assessments is the primary responsibility of information system owners and common control providers with oversight by their respective authorizing officials, there is also significant involvement in the assessment process by other parties within the organization who have a vested interest in the outcome of assessments. Other interested parties include, for example, mission/business owners, information owners/stewards (when those roles are filled by someone other than the information system owner), information security officials, and the risk executive (function). It is imperative that information system owners and common control providers coordinate with the other parties in the organization having an interest in security control assessments to help ensure that the organization’s core missions and business functions are adequately addressed in the selection of security controls to be assessed.
19 APPENDIX II

19.1.1 Servers Housed at Benedum Hall

19.1.2 2013 Schneider Downs Audit, Finding 22, Control F.5
(As of July 2015)

SERVER NAME: conmael2.ee.pitt.edu
IP ADDRESS: 136.142.70.165
PHYSICAL LOCATION: B08 BEH
STAFF RESPONSIBLE FOR DEVICE: McGahey/Lyle
RESPONSIBLE STAFF DIRECT REPORT: Brian Vidic
CATEGORIES OF DATA HOUSED: University-Public Sensitivity
RETENTION SCHEDULE FOR DATA HOUSED: Two months
BACKUP SCHEDULE: Full backup on 1st day of month and incremental on the remaining days of the month
OFF SITE LOCATION OF BACKUP MEDIA: None

SERVER NAME: dc001.engr.pitt.edu
IP ADDRESS: 136.142.82.183
PHYSICAL LOCATION: B08 BEH
STAFF RESPONSIBLE FOR DEVICE: McGahey/Lyle
RESPONSIBLE STAFF DIRECT REPORT: Brian Vidic
CATEGORIES OF DATA HOUSED: University-Public Sensitivity (This server is strictly a user authentication server and does not house ECE user data)
RETENTION SCHEDULE FOR DATA HOUSED: Six months
BACKUP SCHEDULE: Full backup at beginning of six month cycle and incremental for remainder of period
OFF SITE LOCATION OF BACKUP MEDIA: None

SERVER NAME: dc002.engr.pitt.edu
IP ADDRESS: 136.142.82.183
PHYSICAL LOCATION: B08 BEH
STAFF RESPONSIBLE FOR DEVICE: McGahey/Lyle
RESPONSIBLE STAFF DIRECT REPORT: Brian Vidic
CATEGORIES OF DATA HOUSED: University-Public Sensitivity (This server is strictly a user authentication server and does not house ECE user data)
RETENTION SCHEDULE FOR DATA HOUSED: Six months
BACKUP SCHEDULE: Full backup at beginning of six month cycle and incremental for remainder of period
OFF SITE LOCATION OF BACKUP MEDIA: None

SERVER NAME: dc003.engr.pitt.edu
IP ADDRESS: 136.142.82.190
PHYSICAL LOCATION: B08 BEH
STAFF RESPONSIBLE FOR DEVICE: McGahey/Lyle
RESPONSIBLE STAFF DIRECT REPORT: Brian Vidic
CATEGORIES OF DATA HOUSED: University-Public Sensitivity (This server is strictly a user authentication server and does not house ECE user data)
RETENTION SCHEDULE FOR DATA HOUSED: Six months
BACKUP SCHEDULE: Full backup at beginning of six month cycle and incremental for remainder of period
OFF SITE LOCATION OF BACKUP MEDIA: None
SERVER NAME: licsrv-ece.ee.pitt.edu  
IP ADDRESS: 150.212.166.178  
PHYSICAL LOCATION: B08 BEH  
STAFF RESPONSIBLE FOR DEVICE: McGahey/Lyle  
RESPONSIBLE STAFF DIRECT REPORT: Brian Vidic  
CATEGORIES OF DATA HOUSED: University-Public Sensitivity (This server is strictly used for licensing and houses no ECE user data)  
RETENTION SCHEDULE FOR DATA HOUSED: Six months  
BACKUP SCHEDULE: Full backup at beginning of six month cycle and incremental for remainder of period  
OFF SITE LOCATION OF BACKUP MEDIA: None

SERVER NAME: ttc1.ee.pitt.edu  
IP ADDRESS: 150.212.166.157  
PHYSICAL LOCATION: B08 BEH  
STAFF RESPONSIBLE FOR DEVICE: McGahey/Lyle  
RESPONSIBLE STAFF DIRECT REPORT: Brian Vidic  
CATEGORIES OF DATA HOUSED: University-Public Sensitivity (This server houses both user ECE course data and research data)  
RETENTION SCHEDULE FOR DATA HOUSED: Two weeks  
BACKUP SCHEDULE: Full backup at beginning of week and incremental for remainder of the week.  
OFF SITE LOCATION OF BACKUP MEDIA: None

SERVER NAME: iess01.ie.pitt.edu  
IP ADDRESS: 150.212.188.71  
PHYSICAL LOCATION: 216 IDF  
STAFF RESPONSIBLE FOR DEVICE: Jim Segneff  
RESPONSIBLE STAFF DIRECT REPORT: Brian Vidic  
CATEGORIES OF DATA HOUSED: public internal  
RETENTION SCHEDULE FOR DATA HOUSED: as disk space permits  
BACKUP SCHEDULE: Monthly  
OFF SITE LOCATION OF BACKUP MEDIA: none

SERVER NAME: iess02.ie.pitt.edu  
IP ADDRESS: 150.212.188.72  
PHYSICAL LOCATION: 216 IDF  
STAFF RESPONSIBLE FOR DEVICE: Jim Segneff  
RESPONSIBLE STAFF DIRECT REPORT: Brian Vidic  
CATEGORIES OF DATA HOUSED: public internal  
RETENTION SCHEDULE FOR DATA HOUSED: as disk space permits  
BACKUP SCHEDULE: Monthly  
OFF SITE LOCATION OF BACKUP MEDIA: none

SERVER NAME: iess04.ie.pitt.edu  
IP ADDRESS: 150.212.188.74  
PHYSICAL LOCATION: 216 IDF  
STAFF RESPONSIBLE FOR DEVICE: Jim Segneff  
RESPONSIBLE STAFF DIRECT REPORT: Brian Vidic  
CATEGORIES OF DATA HOUSED: public internal  
RETENTION SCHEDULE FOR DATA HOUSED: as disk space permits  
BACKUP SCHEDULE: Monthly  
OFF SITE LOCATION OF BACKUP MEDIA: none

SERVER NAME: iess05.ie.pitt.edu  
IP ADDRESS: 150.212.188.75  
PHYSICAL LOCATION: 216 IDF  
STAFF RESPONSIBLE FOR DEVICE: Jim Segneff  
RESPONSIBLE STAFF DIRECT REPORT: Brian Vidic  
CATEGORIES OF DATA HOUSED: public internal  
RETENTION SCHEDULE FOR DATA HOUSED: as disk space permits  
BACKUP SCHEDULE: Monthly
OFF SITE LOCATION OF BACKUP MEDIA: none

SERVER NAME: cemorfs1.ie.pitt.edu
IP ADDRESS: 150.212.188.82
PHYSICAL LOCATION: 216 IDF
STAFF RESPONSIBLE FOR DEVICE: Jim Segneff
RESPONSIBLE STAFF DIRECT REPORT: Brian Vidic
CATEGORIES OF DATA HOUSED: public internal
RETENTION SCHEDULE FOR DATA HOUSED: as disk space permits
BACKUP SCHEDULE: none
OFF SITE LOCATION OF BACKUP MEDIA: none

SERVER NAME: cemorfs2.ie.pitt.
IP ADDRESS: 150.212.188.83
PHYSICAL LOCATION: 216 IDF
STAFF RESPONSIBLE FOR DEVICE: Jim Segneff
RESPONSIBLE STAFF DIRECT REPORT: Brian Vidic
CATEGORIES OF DATA HOUSED: public internal
RETENTION SCHEDULE FOR DATA HOUSED: as disk space permits
BACKUP SCHEDULE: none
OFF SITE LOCATION OF BACKUP MEDIA: none

SERVER NAME: iess03.ie.pitt.edu
IP ADDRESS: 150.212.188.73
PHYSICAL LOCATION: 216 IDF
STAFF RESPONSIBLE FOR DEVICE: Jim Segneff
RESPONSIBLE STAFF DIRECT REPORT: Brian Vidic
CATEGORIES OF DATA HOUSED: none
RETENTION SCHEDULE FOR DATA HOUSED: none
BACKUP SCHEDULE: none
OFF SITE LOCATION OF BACKUP MEDIA: none
APPENDIX III
CERT 2012 CIRCULAR – RISKS OF USING PORTABLE DEVICES

Recommended Practices for Portable Storage Media
SSoE Faculty and Staff will:

- Install anti-virus software that will scan any device that connects to your PC via a peripheral port (such as USB).
- Never connect a found jump drive or media device to a PC. Give any unknown storage device to security or IT personnel near where you found it.
- Disable the Autorun and Autoplay features for all removable media devices. These features automatically open removable media when it’s plugged into your USB port or inserted into a drive.
- Keep your personal and business data separate. Don’t plug your personal audio player into your work PC or your work jump drive into your home PC.
- Secure all sensitive data stored on jump drives, CDs, and DVDs using strong encryption, such as AES 128/256 bit.

Recommended Practices for Portable Smart Devices
SSoE Faculty and Staff will:

- Password protect device using strong password or PIN, and change periodically.
- Before downloading applications and games, discern what they will have access to on device. Most applications provide that information; avoid downloading any that don’t.
- Download applications, games, and music only from trusted sources. For example, only download well-known games from reputable and verified vendors or from the commercial store backed by your device manufacturer or provider.
- Run anti-malware software on the device and take the appropriate action when it identifies suspicious applications. Also, scan the entire device periodically for malware.
- When possible, set up a local firewall on the device to filter inbound and outbound traffic and block malicious software.
- Set an idle timeout that will automatically lock the device when you’re not using it.
- Do not “jailbreak” the device. Jailbreaking is removing the limitations imposed on a device by the manufacturer, often through the installation of custom operating-system components or other third-party software.
- If your device supports location tracking, activate global positioning system (GPS) functionality so you can track the location of your device if you misplace it.
- Disable Bluetooth, Wi-Fi, and other services when you’re not using them.
- When using Wi-Fi, be sure to encrypt your home network, use a VPN connection, or otherwise ensure that traffic is encrypted when you’re in a semi-trusted environment (for example, when you may trust the wireless access point but not necessarily the other users on the network).
- When using Bluetooth, set it to “non-discoverable” mode to make the device invisible to unauthenticated devices.
- Secure all the data stored on tablets using AES 128/256-bit encryption. Also be sure to have a backup copy of the data stored in a secure location.
- If available, enable a remote-wiping feature to erase all data on device if misplaced.
## 21 APPENDIX IV


<table>
<thead>
<tr>
<th>SUNDAY</th>
<th>MONDAY</th>
<th>TUESDAY</th>
<th>WEDNESDAY</th>
<th>THURSDAY</th>
<th>FRIDAY</th>
<th>SATURDAY</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEEK 1</td>
<td>NETCOOL - MONTHLY APPLICATION PERFORMANCE RUN: 1/2 APPS: USR, CMI, GATS, SHAREPOINT TEAM TIME: 10:00AM OWNER: KRATZ</td>
<td>APPLICATIONS - MONTHLY TENABLE VULNERABILITY REPORTS. APPS: USR, CMI, GATS, SHAREPOINT TEAM DETAILS: CSSD, TBD OWNER: KRATZ</td>
<td>NETCOOL – CAPACITY PLANNING REPORT. ALL SSOE NOC CO-LO. TIME: 01:00PM OWNER: DENNIS</td>
<td>SCCM – SCHOOL WIDE INVENTORY REPORT for MONTH PREVIOUS for LAST PATCH DATE + ADMIN GROUP CONTENTS OWNER: DENNIS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WEEK 2</td>
<td></td>
<td>SCCM – MONTHLY PATCH REVIEW. OWNER: DENNIS</td>
<td>SYMANTEC A/V – MONTHLY SERVER REVIEW OWNER: DENNIS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WEEK 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WEEK 4</td>
<td></td>
<td></td>
<td>NETCOOL - MONTHLY APPLICATION PERFORMANCE RUN: 2/2 APPS: USR, CMI, GATS, SHAREPOINT T/SITE TIME: 10:00AM OWNER: KRATZ</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WEEK 5</td>
<td></td>
<td>APPLICATIONS – EVENT LOG REVIEW. PROJECT MEETING. APPS: USR, CMI, GATS, SHAREPOINT TEAM OWNER: KRATZ</td>
<td>BACKUP &amp; RECOVERY – DELETE &amp; RECOVER FILES. NETCOOL (TBD) OWNER: DENNIS</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Pursuant to University of Pittsburgh policies 10-02-06 and 10-02-08, the Swanson School of Engineering endeavours to further define how the School will classify and control access to differing levels of sensitive information, and how systems the School manages will be defined with relation to levels of criticality. These definitions will be a component of the overall IT Governance model across the Swanson School of Engineering.
Information/Data Sensitivity

Sensitivity classification of data is the need to help protect data from unauthorized disclosure, fraud, waste, or abuse. Information may be physical or digital. System Owners/Managers must determine the appropriate system security level based on (1) confidentiality, integrity and availability objectives of the information, and (2) data sensitivity and its criticality to the SSoE and University missions. This is the basis for assessing the risks to operations and assets and in selecting appropriate security controls and techniques.

Unrestricted-Public Sensitivity
Requirements a minimal amount of protection. This level includes information that is considered to be in the public domain, or does not fit into the other levels, such as employee campus contact files, some of which are already available on the public web. At this level, we can conclude that any disclosures could be reasonably expected to not have an adverse effect while acknowledging that unintentional alteration or destruction is the primary concern for this sensitivity information.

University-Confidential Sensitivity
Includes internal information at SSoE, and requires strong security safeguards at the user level and therefore must be protected against acts that are considered to be malicious and destructive. This level data could include: Computerized correspondence and documents that are regarded as highly sensitive and/or critical to SSoE, where release or distribution outside the University and/or outside SSoE needs to be controlled; Proprietary information that has inherent informational value, such as formulas and early research findings; Financial data that is used to authorize or make payments to individuals or organizations; Grant application and related data; Academic or department information that pertains to teaching, workload, staffing, general correspondence and memoranda, and other document files. Data that must be protected from unauthorized alteration and/or disclosure.

Restricted Sensitivity
Includes the most sensitive information at SSoE and requires the greatest security safeguards at the user level. This level data could include: Proprietary information that has inherent informational value, such as formulas, trade secrets, and early research findings; Clinical trial data; Automated systems or records subject to the federal or state regulations for which unauthorized disclosure would constitute a clearly unwarranted invasion of personal privacy or contribute to a possible identity theft issue; Technical information concerning the internal operation, protection, and security methods of the SSoE or the University’s networks and systems;

Data that must be protected from unauthorized disclosure by mandate of law or regulation.
Criticality Levels

Operational criticality of systems is the assessment of “what if the processing capabilities were interrupted for a period of time or subject to fraud or abuse.” “Criticality Level 1” applies to capabilities with the least amount of criticality and “Criticality Level 3” applies to automated capabilities with the greatest amount of criticality. These criticality levels are used to help determine the appropriate level of protection for automated information capabilities.

System Owners/Managers and System Support/Developers must ensure that their information collections or databases and the processing capabilities of their systems are accessed only by authorized users who fully use the required security level safeguards.

**Criticality Level 1**
Refers to an automated information system that users only need to take minimal precautions to protect. Noticeable impact on an agency’s missions, functions, image, or reputation. A breach of this security level would result in a negative outcome; or would result in damage, requiring repairs, to an asset or resource. In the event of an alteration or failure, the loss of this system would affect the organization minimally, and/or this information could be replaced with minimum staff time and expense.

**Criticality Level 2**
Identifies an automated information system that is considered important, but not imperative, to SSoE's internal management. Severe impairment to an agency’s missions, functions, image, and reputation. The impact would place SSoE at a significant disadvantage; or would result in major damage, requiring extensive repairs to assets or resources.

**Criticality Level 3**
Refers to an automated information system essential to the organization. At this level, if the system is unable to function for even a short period of time, it would have a severe impact on the organization.
# Information Security Level Standard

The Security Level designation will be used to determine the minimum-security safeguards required to protect sensitive data and to ensure the operational continuity of critical data processing capabilities.

<table>
<thead>
<tr>
<th>Information Category</th>
<th>Category Explanation and Examples</th>
<th>System Security Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigation and security information</td>
<td>Information related to investigations for law enforcement or security purposes that cannot be classified, but is subject to confidentiality and extra security controls. Includes security plans, contingency plans, emergency operations plans, incident reports, reports of investigations, risk or vulnerability assessments certification reports; does not include general plans, policies, or requirements.</td>
<td>High</td>
</tr>
<tr>
<td>Business-critical information</td>
<td>Information designated as critical to a department's mission, includes vital information for emergency operations.</td>
<td>High</td>
</tr>
<tr>
<td>Life-critical information</td>
<td>Information critical to life-support systems (i.e., information where inaccuracy, loss, or alteration could result in loss of life).</td>
<td>High</td>
</tr>
<tr>
<td>Information about persons</td>
<td>Information related to personnel, medical, and similar data. Includes all information covered by the Privacy Act of 1974 (e.g., salary data, social security information, passwords, user identifiers (IDs), EEO, personnel profile (including home address and phone number), medical history, employment history (general and security clearance information), and arrest/criminal investigation history), FERPA, etc.</td>
<td>High</td>
</tr>
<tr>
<td>Financial, budgetary, commercial, proprietary and trade secret information</td>
<td>Information related to financial information and applications, commercial information received in confidence, or trade secrets (i.e., proprietary, contract bidding information, sensitive information about patents, and information protected by agreement. Also included is information about payroll, automated decision making, procurement, inventory, other financially-related systems, and site operating and security expenditures.</td>
<td>Moderate</td>
</tr>
<tr>
<td>Internal administration</td>
<td>Information related to the internal administration of an agency. Includes personnel rules, bargaining positions, and advance information concerning procurement actions.</td>
<td>Moderate</td>
</tr>
<tr>
<td>Operational information</td>
<td>Information that requires protection during operations; usually time-critical information.</td>
<td>Moderate</td>
</tr>
<tr>
<td>Public information</td>
<td>Any information that is declared for public consumption by official authorities. This includes information contained in press releases approved by the Office of Public Affairs or other official sources. It also includes information placed on public access world-wide-web (WWW) servers.</td>
<td>Low</td>
</tr>
<tr>
<td>Other sensitive information</td>
<td>Any information for which there is a management concern about its adequate protection, but which does not logically fall into any of the above categories. Use of this category should be rare.</td>
<td>Low</td>
</tr>
</tbody>
</table>