I. Title

A. Name: Information Systems Security Incident Response Policy

B. Number: 20070103-secincidentresp

C. Author(s):
David Millar (ISC Information Security) and Lauren Steinfeld (Chief Privacy Officer)

D. Status: [ ] proposed [ ] under review [X] approved [ ] rejected [ ] obsolete

E. Date Proposed: 2005-10-24

F. Date Revised:

G. Date Approved: 2007-01-03

H. Effective Date: 2007-01-16

II. Authority and Responsibility

Information Systems and Computing is responsible for the operation of Penn's data networks (PennNet) as well as the establishment of information security policies, guidelines, and standards. The Office of Audit, Compliance and Privacy has authority to develop and oversee policies and procedures regarding the privacy of personal information. These offices therefore have the authority and responsibility to specify security incident response requirements to protect those networks as well as University data contained on those networks.

III. Executive Summary

This policy defines the response to computer security incidents.

IV. Purpose

This policy defines the steps that personnel must use to ensure that security incidents are identified, contained, investigated, and remedied. It also provides a process for documentation, appropriate reporting internally and externally, and communication so that organizational learning occurs. Finally, it establishes responsibility and accountability for all steps in the process of addressing computer security incidents.

V. Risk of Non-compliance

Without an effective incident response process, corrective action may be delayed and harmful effects unnecessarily exacerbated. Further, proper communication allows the University key learning opportunities to improve the security of data and networks. Individuals who fail to comply are subject to sanctions as appropriate under Penn policies.

VI. Definitions

Confidential University Data includes:

* **Sensitive Personally Identifiable Information** – Information relating to an individual that reasonably identifies the individual and, if compromised, could cause significant harm to that individual or to Penn. Examples may include, but are not limited to: Social Security numbers, credit card numbers, bank account information, student grades or disciplinary information, salary or employee performance information, donations, patient health information, information Penn has promised to keep confidential, and account passwords or encryption keys used to protect access to Confidential University Data.

* **Proprietary Information** – Data, information, or intellectual property in which the University has an exclusive legal interest or ownership right, which, if compromised could cause significant harm to Penn. Examples may include, but are not limited to, business planning, financial information, trade secret, copyrighted material, and software or comparable material from a third party when the University has agreed to keep such information confidential.

* Any other data the disclosure of which could cause significant harm to Penn or its constituents.

Security Incident. There are two types of Security Incidents: Computer Security Incidents and Confidential Data Security Incidents.

* A **Computer Security Incident** is any event that threatens the confidentiality, integrity, or availability of University systems, applications, data, or networks. University systems include, but are not limited to: servers, desktops, laptops, workstations, PDAs, network servers/processors, or any other electronic data storage or transmission device.

* A **Confidential Data Security Incident** is a subset of Computer Security Incidents that specifically threatens the security or privacy of Confidential University Data.

User. A Penn user is any faculty, staff, consultant, contractor, student, or agent of any of the above.

VII. Scope

This policy applies to all Users. It applies to any computing devices owned or leased by the University of Pennsylvania that experience a Computer Security Incident. It also applies to any computing device regardless of ownership, which either is used to store Confidential University Data, or which, if lost, stolen, or compromised, and based on its privileged access, could lead to the unauthorized disclosure of Confidential University Data. Examples of systems in scope include, but are not limited to, a User's personally owned home computer that is used to store Confidential University Data, or that contains passwords that would give access to Confidential University Data.

This policy does not cover incidents involving the University of Pennsylvania Health System (UPHS) information systems, which has a separate incident response policy. ISC Information Security will coordinate with UPHS as appropriate when UPHS computing devices, data, or personnel are involved.

VIII. Statement of Policy

A. Overview of Penn's Incident Response Program

i. All Computer Security Incidents must be reported to ISC Information Security promptly. See Section B below.

ii. All Confidential Data Security Incidents must:

a. Generate the creation of an Immediate Response Team, as designated by the Information Security Officer (ISO), on a per incident basis. See Section C below.

b. Follow appropriate Incident Handling procedures. See Sections C and D below.

iii. ISC Information Security, under the direction of the Vice President for Information Systems and Computing (VP-ISC) is responsible for logging, investigating, and reporting on security incidents. See Sections D and E below.

B. Identifying and Reporting Computer Security Incidents

i. Users and Local Support Providers (LSPs). In the event that a User or an LSP detects a suspected or confirmed Computer Security Incident, the User must report it to his or her Local Security Officer or IT Director for issues including but not limited to viruses, worms, local attacks, denial of service attacks, or possible disclosure of Confidential University Data.

ii. Local IT Management. Local IT Management must notify ISC Information Security of all Computer Security Incidents, except for categories of incidents that ISC Information Security may designate in Appendix I of this policy.

iii. ISC Information Security. ISC Information Security shall notify appropriate systems administrators and other personnel of all emergency and attack incidents, as well as all suspicious activity incidents when it believes that an administrator's system is at risk. The system's administrators will then work with ISC Information Security to properly address the incident and minimize the risk of future occurrences.

C. Immediate Response Team

i. Purpose. The purpose of each Immediate Response Team is to supplement Penn's information security infrastructure and minimize the threat of damage resulting from Computer Security Incidents.

ii. Per Incident Basis. An Immediate Response Team shall be created for Confidential Data Security Incidents.

iii. Membership. Membership on the Immediate Response Team shall be as designated by the ISO. In most cases, members shall include a representative from ISC Information Security and from the affected School or Center's technical and management staff.

iv. Responsibilities. Responsibilities of the Immediate Response Team are to assess the incident and follow incident handling procedures, appropriate to the incident as determined by the ISO.

v. Confidentiality. Immediate Response Team members will share information about security incidents beyond the Immediate Response Team only on a need-to-know basis, and only after consultation with all other team members.

D.Incident Handling. For incidents requiring the formation of an Immediate Response Team, the following is a list of response priorities that should be reviewed and followed as recommended by the ISO. The most important items are listed first

i. Safety and Human Issues. If an information system involved in an incident affects human life and safety, responding to any incident involving any life-critical or safety-related system is the most important priority.

ii. Address Urgent Concerns. Schools and Centers may have urgent concerns about the availability or integrity of critical systems or data that must be addressed promptly. ISC Information Security shall be available for consultation in such cases.

iii. Establish Scope of Incident. The Immediate Response Team shall promptly work to establish the scope of the incident and to identify the extent of systems and data affected. If it appears that personally identifiable information may have been compromised, the Immediate Response Team shall immediately inform the VP-ISC and the Chief Privacy Officer (CPO).

iv. Containment. Once life-critical and safety issues have been resolved, the Immediate Response Team shall identify and implement actions to be taken to reduce the potential for the spread of an incident or its consequences across additional systems and networks. Such steps may include requiring that the system be disconnected from the network.

v. Develop Plan for Preservation of Evidence. The Immediate Response Team shall develop a plan promptly upon learning about an incident for identifying and implementing appropriate steps to preserve evidence, consistent with needs to restore availability. Preservation plans may include preserving relevant logs and screen captures. The affected system may not be rebuilt until the Immediate Response Team determines that appropriate evidence has been preserved. Preservation will be addressed as quickly as possible to restore availability that is critical to maintain business operations.

vi. Investigate the Incident. The Immediate Response Team shall investigate the causes of the incident and future preventative actions. During the investigation phase, members of the incident response team will attempt to determine exactly what happened during the incident, especially the vulnerability that made the incident possible. In short, investigators will attempt to answer the following questions: Who? What? Where? When? How?

vii. Incident-Specific Risk Mitigation. The Immediate Response Team shall identify and recommend strategies to mitigate risk of harm arising from the incident, including but not limited to reducing, segregating, or better protecting personal, proprietary, or mission critical data.

viii. Restore Availability. Once the above steps have been taken, and upon authorization by the Immediate Response Team, the availability of affected devices or networks may be restored

ix. Penn-Wide Learning. The Immediate Response Team shall develop and arrange for implementation of a communications plan to spread learning from the security incident throughout Penn to individuals best able to reduce risk of recurrence of such incident.

E. Senior Response Team (SRT). If the ISO or CPO in their judgment believe that the incident reasonably may cause significant harm to the subjects of the data or to Penn, each may recommend to the VP-ISC or Associate Vice President for Audit, Compliance and Privacy (AVP-OACP) that a Senior Response Team be established. The Senior

Response Team shall be comprised of senior-level officials as designated by the VP-ISC or AVP-OACP. The Senior Response Team shall:

i. Establish whether additional executive management should be briefed and the plan for such briefing.

ii. Determine, with final approval by the General Counsel, whether Penn shall make best efforts to notify individuals whose personal identifiable information may have been at risk. In making this determination, the following factors shall be considered:

a) legal duty to notify
b) length of compromise
c) human involvement
d) sensitivity of data
e) existence of evidence that data was accessed and acquired
f) concerns about personnel with access to the data
g) existence of evidence that machine was compromised for reasons other than accessing and acquiring data
h) additional factors recommended for consideration by members of the Immediate Response Team or the Senior Response Team.

iii. Review and approve any external communication regarding the incident.

F. <u>Documentation</u>

i. Log of security incidents. ISC Information Security shall maintain a log of all reportable security incidents recording the date, School or Center affected, whether or not the affected machine was registered as a critical host, the type of Confidential University Data affected (if any), number of subjects (if applicable), and a summary of the reason for the intrusion, and the corrective measure taken.

ii. Critical Incident Report. ISC Information Security shall issue a Critical Incident Report for every reportable security incident affecting machines qualifying as Critical Hosts, or other priority incidents in the judgment of ISC Information Security describing in detail the circumstances that led to the incident, and a plan to eliminate the risk.

iii. Annual Summary Report. ISC Information Security shall provide annually for the VP-ISC and AVP-OACP a report providing statistics and summary-level information about all significant incidents reported, and providing recommendations and plans to mitigate known risks.

IX. Best Practices

A. Preserving Evidence: It is essential to consult Penn Information Security when handling Computer Security Incidents. However, if Information Security is not available for emergency consultation, the following practices are recommended:

i. Generally, if it is necessary to copy computer data to preserve evidence for an incident, it is a good idea to use bit-wise file-system copy utilities that will produce an exact image, (e.g.UNIX dd) rather than to use file level utilities which can alter some file meta-data.

ii. When making forensic backups, always take a cryptographic hash (such as an SHA-1 hash) of both the original object and of the copied object to verify the authenticity of the copy. Consult your System Administrator if you have questions.

iii. Assigning Members to an Immediate Response Team: In cases where an incident involves an investigation into misconduct, the School or Center should consider carefully whom to assign to the Immediate Response Team. For example, one may not wish to assign an IT professional who works closely with the individual(s) being investigated.

X. Compliance

A. Verification: ISC Information Security and the Office of Audit, Compliance and Privacy will verify any known computing security incidents as having been reported and documented as defined by this policy.

B. Notification: Violations of this policy will be reported by ISC Security and the Office of Audit, Compliance and Privacy to the Senior Management of the Business Unit affected.

C. Remedy: The incident will be recorded by ISC Information Security and any required action to mitigate the harmful affects of the attack will be initiated in cooperation with the Business Unit Security Officer/Liaison.

D. Financial Implications: The owner of the system shall bear the costs associated with ensuring compliance with this policy.

E. Responsibility: Responsibility for compliance with this policy lies with the system administrator, system owner, and Business Unit's Senior Manager.

F. Time Frame: All incidents involving critical hosts systems and networks must be reported immediately. All other incidents should be reported within one business day of determining something has occurred.

G. Enforcement: Compliance with this policy will be enforced by disconnecting any machines that may compromise the University network, or other machines with Confidential University Data. Workforce members not adhering to the policy may be subject to sanctions as appropriate under Penn policies.

H. Appeals: Appeals are decided by the Vice President for Information Systems and Computing

XI. References

1. PennNet Computer Security Policy at http://www.net.isc.upenn.edu/policy/approved/20040524-hostsecurity.html

2. Critical PennNet Host Security Policy at http://www.net.isc.upenn.edu/policy/approved/20000530-hostsecurity.html

3. Policy on Computer Disconnection from PennNet at http://www.upenn.edu/computing/policy/disconnect.html

4. Adherence To University Policy at http://www.hr.upenn.edu/policy/policies/001.asp

5. Policy on Security of Electronic Protected Health Information (ePHI) at http://www.upenn.edu/computing/security/policy/ePHI_Policy.html

Appendix I

The following category of incidents need not be reported to Penn Information Security:

* Unsuccessful network scans