

# Seattle Pacific University Computer and Information Systems Policies, Procedures, Plans and Standards

## Security Incidents: Management and Reporting

Effective: January 19, 2007  
Updated and Approved by CIS: February 6, 2009

Contents:

### **1.0 Introduction/Purpose**

### **2.0 Definitions**

- A. Internal Security Violations (University Employees, Students, Agents)
- B. External Security Violations
- C. What Constitutes an Incident

### **3.0 Incident Notification (Internal)**

### **4.0 Incident Response**

- A. Alerting/Discovery
- B. Data Breach Incident
- C. Credential disclosure or compromise (including phishing scams and other disclosure)
- D. General Response Procedures
- E. Authority
- F. Response Coordination, Planning

### **5.0 Incident Reporting: Internal Violations**

- A. Incident Response – Preservation/Suspension of Confidentiality
- B. Incident Control and Reporting Procedures (Internal Target)
- C. Incident Control and Reporting Procedures (External Target)

### **6.0 Incident Reporting: External Violations**

- A. Initial Response - Preservation of Confidentiality
  - B. Incident Control and Reporting Procedures
  - C. Incident Reporting (External Agency)
  - D. Incident Report Details
- 

### **1.0 Introduction/Purpose**

This policy serves as a guideline for CIS response and reporting procedures involving security incidents affecting the availability of University computer and information system resources, or the confidentiality or integrity of the information stored or transported across these resources. As a guideline, this document represents a best practices strategy for incident response and reporting. Ultimate authority for the actions and methods conducted in the event of a security violation rests with the university CIO or official designee.

### **2.0 Definitions**

- A. "Internal Security Violations" are those in which the offender is a known employee, student, or agent of the university, and as such, subject to the provisions set forth in the Acceptable Use Policy (AUP).
- B. "External Security Violations" are those coming from outside the campus network, and/or from sources that are unidentifiable or unaffiliated with Seattle Pacific University.
- C. An incident is considered a security violation if it meets one or more of the following criteria:
  - Attempts to gain unauthorized access to a system or its data;
  - An accidental or deliberate disclosure of SPU account or email credentials;
  - Deliberate disruptions or attempted disruptions associated with a denial of service;
  - Unauthorized attempts to modify protected system access or data;
  - Presence (confirmed or suspected) of actively-propagating malicious code, including but not limited to viruses, spyware, root kits, bots, etc.;
  - Theft or compromise of account access credentials;
  - Physical security compromise of a CIS secure and restricted space (server room, PBX, MDF, etc.);
  - Accidental or deliberate data breach involving the release, disclosure or loss of student or employee sensitive personal information or confidential records;
  - Confirmed or suspected violations of regulatory statutes of law, including but not limited to FERPA, PCI, HIPAA, GLB, SOX, etc.;
  - Threats involving bodily injury or property damage to students, employees, guests, or the institution made or propagated via network, computer or electronic resources
  - Other activities deemed malicious in nature or in violation of the university AUP.

### 3.0 Incident Notification (Internal)

In the event that a CIS employee becomes aware of a security violation (confirmed or suspected), that staff member will immediately notify the CIS management team in-person or via direct telephone conversation (not voicemail), beginning with the CIO and continuing through the CIS reporting hierarchy until a CIS team manager is contacted *in-person*. The employee will also send an urgent-flagged message to the CIS full staff email distribution group with the details of the suspected violation. In matters involving immediate physical threat to a member of the campus community, Campus Security will also be notified of the incident in-person or via direct telephone conversation

### 4.0 Incident Response

#### A. Alerting/Discovery

In the event that the incident response occurs during normal CIS operating hours, the full SysAdmin team – or subset of that team (see “Coordination and Planning” below) – will be assembled at the discretion of the CIO or senior CIS staff member coordinating incident response.

#### B. Data Breach Incident

Due to the high level of financial, legal, and institutional impact/exposure, incidents involving suspected or actual data breaches require a more specific response and process.

- 1) In the event of a suspected or actual data leak, or data breach, immediate notification of CIS senior leadership and also the VP of Business and Planning is required.
- 2) Was “sensitive personal information (SPI)” breached? There are several overlapping regulations, both federal and state, that define sensitive information.
  - a. Washington State disclosure laws - for purposes of this regulation, SPI means an individual's name, with any of the following data elements: social security number, driver's license number or other Washington ID card, credit or debit card number in combination with PIN or password.
  - b. Other personal records and data:
    - i. Academic records – FERPA defines several types of records that must be protected including grades, transcripts, academic history, placement records, financial aid, student payroll, campus security records, and disciplinary files.
    - ii. Health Care - means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.
    - iii. Medical information – any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional.
    - iv. Financial/Credit Reports – any information regarding an individual's bank records, credit history, tax records, employment records and payment history, credit scores, or financial investments.
    - v. Usernames and email addresses by themselves are simple directory elements, but when combined with access codes, passwords, or PIN's they would permit access to systems and databases that store other SPI.
    - vi. Date and place of birth by itself might not appear as sensitive, but when used in combination with other information could be used for identity theft or system access.
    - vii. Your mother's maiden name is also a frequent verification element and should be kept private as well
- 3) Directory Information – the University has defined specific data elements as directory information that may be released unless the student requests in writing that the information be made confidential. Directory information includes: student's name, mailing address and telephone number, email address, photograph, date and place of birth, major field of study, date of attendance, full-time or part-time status, degrees, awards, and honors received, dates degrees conferred, class standing, high school attended, most recent previous educational institution attended by the student, participation in officially recognized activities and sports; and weight and height of athletic team members.
- 4) Notification of data breach – in the event of a discovery or notification that SPI data was, or is reasonably believed to have been, released or acquired by an unauthorized person, a notification to the person or business is required. The notification shall be made in the most expedient time possible, consistent with the legitimate needs of law enforcement and measures necessary to determine the scope and integrity of the data system.
- 5) Campus use of Social Security Number's – limiting access to and use of SSN's is one significant tool to reduce the risk and impact of a SPI data breach. SPU moved away from using SSN's as an ID number many years ago, but there are still many areas that must collect and use the number for legitimate purposes. The following guidelines should be followed:
  - a. Limit access to records that contain SSN's to only those employees who require access in the performance of campus duties.
  - b. Require the SPU ID number and not the SSN as a form of identification.
  - c. Remove SSN from forms and documents where it is not required.
  - d. Documents that require SSN's must be stored, handled, and disposed of in a secure manner.
  - e. Remove SSN from printed reports.
  - f. Electronic records containing SSN must only be stored on central servers (not desktops, laptops, floppy disks, CD/DVD's, etc..)
  - g. Do not transmit SSN's through insecure communication mediums (email, ftp, etc...).
  - h. Use encryption on all data stores, and transmissions containing SSN's

#### C. Credential disclosure or compromise (including phishing scams and other disclosure)

Due to the significant increase in the frequency of disclosing SPU account credentials through phishing email scams, and other social engineering techniques, the following incident response is in place, effective January 2009.

- 1) As soon as CIS is aware, or has been made aware, of the disclosure of SPU account credentials the account will be locked from access.
- 2) To prevent the sending of spam or phishing messages, outbound email messaging will be disabled.
- 3) CIS will attempt contact with the account holder through email, or other means if possible, to notify regarding the account action.
- 4) The account holder must change their password and notify CIS of that action, prior to having the account unlocked.
- 5) If the disclosure of account credentials was intentional to allow someone else to use that credential, the account will be locked, and it shall be treated as a willful security breach and disciplinary action.

#### D. General Response Procedures

Pursuant to the guidelines set forth in the Federal Communications Commission's Computer Security Incident Response Guide, CIS response will involve the following activities:

- 1) Identification of the threat
- 2) Notification of appropriate university authorities as outlined in sections 5 and 6 of this document.
- 3) Containment

- 4) Preservation of Evidence
- 5) Eradication
- 6) Determination of Cause
- 7) Recovery/Restoration
- 8) Follow-up
- 9) User notification as required

#### E. Authority

Unless otherwise noted, the specific methods associated with incident response will be determined and directed by the CIO or his designee, and coordinated and executed by the CIS SysAdmin team or incident response designee. At times, this activity will be done in coordination with university legal counsel or other university officials, as outlined in the "Incident Reporting" sections below.

#### F. Response Coordination and Planning

Computer security incident response is a CIS team effort. Effective response strategies are procedural and highly technical. Efforts to deal with emerging threats and statutory requirements demand structure, coordination and expertise across all areas of team discipline, yet must also be flexible and adaptable to each unique threat. The purpose of the outline below is not to prescribe strict response activities, but to ensure that incident response activities are conducted in a coordinated and effective manner.

The following activities constitute a minimal framework for the formation of an effective incident response capability:

##### Incident Response Leadership (CIO and CIS Team Managers):

- Coordination of team efforts as described herein
- Development of CIS incident response plans, procedures, policies
- Training in best practices regarding Incident Command Structure (ICS)
- Coordination of team drills, table top exercises and communication processes
- Development of CIS security awareness and incident response resources, including but not limited to advanced forensic capabilities and internal communications and tracking systems
- Coordination of campus-wide information security training and resources

##### Applications Systems Team:

- Establishment of campus-wide data and information classification system within established CIS policy and procedure framework
- Identification and classification of SPI data sources
- Development of procedures and policies governing the maintenance of SPI data at rest and in motion
- Establishment of penetration testing procedures and processes focusing on specific data stores
- Development of internal controls to monitor, detect, and respond to potential and confirmed data breaches
- Interdepartmental cross training in the procedures and processes outlined herein, and advocacy of security awareness and training within C5 and other users of central application data and systems

##### Central Systems Team:

- Design/development of internal server DMZ architecture
- Establishment of internal controls and structure for the segmentation of protected server resources
- Development of DMZ/server/host intrusion detection, firewall, and associated forensic capabilities
- Establishment of penetration testing procedures and processes focusing on specific DMZ and servers
- Establishment of 'best practices' and associated requirements for non-CIS systems within the core server network
- Development of internal controls to monitor, detect, and respond to potential and confirmed server/host compromises
- Design and develop an email data storage strategy (private, secure, accessible, protected)

##### HelpDesk Team:

- Development and design internal Help Desk reporting/monitoring system for tracking reported incidents
- Criteria for initiation of incident response escalation
- Development of internal controls to monitor, detect, respond to, and escalate potential and confirmed personal desktop and laptop system compromises
- Training and awareness of all team student employees in regards to the security provisions set forth herein
- Establish (in the context of CIS reporting and notification procedures) a strategy to communicate evolving threats and incidents to the campus community at large

##### Micro Systems Team:

- Development and design of local desktop/laptop security policies
- Execution of local policies via Group Policy, SMS or other control mechanism
- Establishment of penetration testing procedures and processes for local systems
- Development of internal controls to monitor, detect, and respond to potential and confirmed local system compromises
- Design and develop a desktop/laptop data storage strategy (Datasync- private, secure, accessible, protected)
- Training and awareness of all team student employees in regards to the security provisions set forth herein
- Development of tools to monitor and control data stored on desktop/laptop systems

##### Network-Telecommunications Team:

- Design/development of campus network security architecture
- Establishment of internal controls for the segmentation of wired and wireless network resources
- Development and cross training on procedures and resources for network intrusion detection
- Development of campus gateway security infrastructure and VPN architecture
- Establishment of penetration testing and forensic procedures and processes focusing on network pathways and active electronics
- Monitoring/enforcing compliance on personal devices connecting to the campus network
- Training and awareness of all team student employees in regards to the security provisions set forth herein
- Development of internal controls to monitor, detect, and respond to potential and confirmed network compromises

## **5.0 Incident Reporting: Internal Violations**

### **A. Initial Response – Preservation/Suspension of Confidentiality**

- 1) In the event that confidential or protected university resources or assets are being eminently threatened, CIS will take immediate and appropriate action to contain the threat prior to notification of the individuals/departments noted in 5.B. Such actions constitute a “suspension of confidentiality” on the part of an individual’s access credentials, and may involve immediate denial of university privileges (credentials) and resource access.
- 2) In the event that no immediate threat to availability, integrity of confidentiality exists CIS will execute the procedures for reporting and notification as outline below and in advance of any account-limitation activity.

### **B. Incident Control and Reporting Procedures (Internal Target)**

- 1) CIS will notify the director of Residence Life/ Student Life for security violations by students. In the event that no eminent threat to university resources exists, CIS SysAdmin shall take direction from Residence Life as to the appropriate disciplinary course of action.
- 2) CIS will notify the director of Human Resources for security violations by employees. In the event that no eminent threat to university resources exists, CIS SysAdmin shall take direction from Human Resources as to the appropriate disciplinary course of action.
- 3) In instances where the incident goes beyond simple nuisance violations associated with the university AUP, when there is evidence or suspicion of legal or monetary compromises to university resources, the VP-OBP will be notified. At this point, authority for and coordination of incident response (section 4.B) shall fall to the direction of the university counsel or cabinet, or as otherwise directed by the CIO or VP-OBP.

### **C. Incident Control and Reporting Procedures (External Target)**

- 1) In the event that the security violation involves threats or activities beyond the control of the university (ie., denial of service attacks against the Internet, conducted by individuals affiliated with the university), procedures for external reporting shall occur as detailed in section 6.C ( below), in addition to those set forth above (5.A).

## **6.0 Incident Reporting: External Violations**

### **A. Initial Response**

- 1) In the event that confidential or protected university resources or assets are being eminently threatened, or where there is evidence that a high-risk exposure to system or resource compromise exists, CIS will take immediate and appropriate action to contain or mitigate the threat.

### **B. Incident Control and Reporting Procedures (Internal)**

- 1) In instances where the incident involves no known compromise to confidential university information, where the threat is minimal and easily contained, response authority shall rest with the CIO and CIS SysAdmin team. At the discretion of the CIO, incident details may be provided to the VP-OBP or president’s cabinet.
- 2) In instances where the external violation goes beyond simple nuisance violations, when there is evidence or suspicion of legal or monetary compromises to university resources, the VP-OBP will be notified and authority and coordination of incident response shall move to university counsel or cabinet, or other designee as directed by the CIO or VP-OBP.

### **C. Incident Reporting (External Agency)**

Pursuant to recommendations set forth by CERT, the FBI, and/or the US Secret Service, notification of security incidents to external agencies and authorities should occur under the following circumstances and as directed by the CIO, VP-OBP, university cabinet or counsel:

- 1) Incidents involving compromises to US assets by a foreign agency are to be reported to the United States Secret Service field office: [http://www.secretservice.gov/field\\_offices.shtml](http://www.secretservice.gov/field_offices.shtml)
- 2) Incidents involving compromises to United States Department of Defense assets are to be reported to the DoD Criminal Investigative Service: <http://www.dodig.osd.mil/INV/DCIS/programs.htm>
- 3) Incidents involving child pornography are to be reported immediately to the FBI and local authorities. Incidents involving other law enforcement violations should also be reported to the FBI and/or local authorities: <http://www.fbi.gov/contact/fo/fo.htm>
- 4) Security incidents should be reported to CERT Coordination Center ([cert@cert.org](mailto:cert@cert.org)) under the following conditions:
  - The incident involved a life threatening activity
  - The incident constituted an attack on the Internet infrastructure
  - The incident involved widespread automated attacks
  - The incident is indicative of a new attack or vulnerability (zero day)
  - When technical assistance beyond the capabilities of the affected organization is needed to arrest the threat
- 5) Incidents involving external agents should always be reported to the upstream Internet site point of contact. Methods and procedures for site point contact reporting are set forth by CERT at [http://www.cert.org/tech\\_tips/finding\\_site\\_contacts.html](http://www.cert.org/tech_tips/finding_site_contacts.html).

### **D. Incident Report Details**

Incident reporting to external agencies should include the following information, as directed by university counsel or other university designee:

- 1) An incident reference number (internally generated or provided by CERT)
- 2) Local university contact information
- 3) Report of disclosure or non-disclosure (whether SPU wants details of the incident to be made public)
- 4) Summary of hosts involved (source and target)
- 5) Description activity and sampling of evidentiary logs
- 6) Date, time, location and time zone in which the incident occurred
- 7) Clarification of the course of action desired by the university

End of Document