

Information Security Incident Response

- Authority** This Guide Memo was approved by the Vice President for Business Affairs and Chief Financial Officer.
- Summary** This Guide Memo describes the procedures to be followed when a computer security incident is discovered to have occurred involving an Academic or Administrative Computing System operated by Stanford University, its faculty, students, employees, consultants, vendors or others operating such systems on behalf of Stanford. It also describes the procedures to be followed when Prohibited or Restricted Information residing on any computing or information storage device is, or may have been, inappropriately accessed, whether or not such device is owned by Stanford. This policy outlines the procedures for decision-making regarding emergency actions taken for the protection of Stanford's information resources from accidental or intentional unauthorized access, disclosure or damage.
- Applicability** This policy is applicable to all University students, faculty, staff, and to all others granted use or custodianship of Stanford University information resources ("University Community"). Section headings are:
1. PURPOSE
 2. DEFINITIONS
 3. NOTIFICATION
 4. INVESTIGATION
 5. INFORMATION SECURITY INCIDENT RESPONSE TEAM
 6. REPORT PREPARATION
 7. ADDITIONAL INFORMATION

1. PURPOSE

The purpose of information security incident response is to:

- a. mitigate the effects caused by such an incident,
- b. protect the information resources of the University from future unauthorized access, use or damage, and
- c. ensure that Stanford fulfills all of its obligations under University policy, and federal and state laws and regulations with respect to such incident.

Stanford recognizes the need to follow established procedures to address situations that could indicate the security of the University's information assets may have been compromised. Such procedures include ensuring the appropriate level of University management becomes involved in the determination of actions implemented in response to an information technology security incident.

A standard University-wide approach to information security is important in order to protect the security of Stanford's intellectual capital and to ensure that Information Security Incidents are handled properly, effectively and in a manner that minimizes the adverse impact to the University. Every user of any of Stanford's information resources has responsibility toward the protection of the University's information assets; certain offices and individuals have very specific responsibilities.

2. DEFINITIONS

- a. **Academic Computing System** – Any application, or information system, that directly or indirectly deals with or supports the University's primary mission of teaching, learning and research.
- b. **Administrative Computing System** – Any application, or information system, that directly or indirectly deals with or supports financial, administrative, or other information that is an integral part of running the business of the University (as defined in Administrative Guide Memo 61, Administrative Computing Systems, <http://adminguide.stanford.edu/61.pdf>).
- c. **Electronic Information Security Incident** – An Electronic Information Security Incident is defined as any real or suspected adverse event in relation to the security of computer systems, computer networks, electronic Prohibited information or electronic Restricted Information. Examples of incidents include:
 - Attempts (either failed or successful) to gain unauthorized access to a system or its data.
 - Theft or other loss of a laptop, desktop, PDA, or other device that contains Prohibited or Restricted Information, whether or not such device is owned by Stanford.
 - Unwanted disruption or denial of service.
 - The unauthorized use of a system for the processing or storage of data.
 - Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.
- d. **Information Security Incident** – An Electronic Information Security Incident or a Non-electronic Information Security Incident.
- e. **Non-electronic Information Security Incident** – Real or suspected theft, loss or other inappropriate access of physical content, such as printed documents and files.
- f. **Prohibited Information** – Information defined as Prohibited at http://www.stanford.edu/group/security/securecomputing/dataclass_chart.html
- g. **Restricted Information** – Information defined as Restricted at http://www.stanford.edu/group/security/securecomputing/dataclass_chart.html

3. NOTIFICATION

A member of the University Community who becomes aware of an Information Security Incident should immediately:

- a. Disconnect the compromised system and equipment from Stanford's network.
- b. Avoid making any updates or other modifications to software, data, or equipment involved or suspected of involvement with an Information Security Incident until after the Information Security Office has completed its investigation and authorizes such activity.
- c. Contact the University's Information Security Office at (650) 723-2911 security@stanford.edu.

4. INVESTIGATION

When an Information Security Incident is reported, the University's Chief Information Security Officer (CISO) will do the following:

- a. The CISO will investigate the Information Security Incident. In order to minimize the impact of the Information Security Incident on the University and in order to complete a proper investigation, the CISO has the authority to restrict information system access or operations to protect against unauthorized information disclosures. In order to complete the investigation, the CISO may convene a preliminary fact-finding working group comprised of relevant business and technical personnel.
- b. If the CISO concludes that applicable federal or state laws or regulations may have been violated, the CISO will notify the Office of the General Counsel, which will, in turn, notify law enforcement agencies if appropriate.
- c. If the CISO concludes that there is a possibility of unauthorized access to Restricted or Prohibited Information, or other sensitive information, the CISO will notify the University Privacy Officer, who will convene an Information Security Incident Response Team.
- d. If appropriate, the CISO will notify offices of the Deans, Vice Provosts and Vice Presidents with responsibility for areas affected by the Information Security Incident.
- e. If the CISO determines that an employee may not have carried out their assigned tasks as instructed or in accordance with University rules and policies, the CISO will notify the employee's manager and the Vice President for Business Affairs and CFO. If the University opens an investigation into the situation, the CISO will cooperate with the employee's manager and/or Stanford's Human Resources Group in its investigation of the incident to determine appropriate corrective or disciplinary action, if any. The office conducting the investigation and making the recommendation will complete and submit to the appropriate parties all supporting documentation related to the investigation and recommended action.

5. INFORMATION SECURITY INCIDENT RESPONSE TEAM

Based on information provided by the CISO and in consultation with the Office of the General Counsel, the University's Privacy Officer will convene an Information Security Incident Response Team (ISIRT) to develop an appropriate Information Security Incident Response Plan (Plan). Depending on the circumstances of each situation, the Privacy Officer shall include in the ISIRT representatives of some or all of the following offices:

- Information Security Office
- Office of the General Counsel
- Internal Audit and Institutional Compliance Department
- Office of the Vice President for Public Affairs
- Administrative Systems
- IT Services
- Departments or schools directly affected by the Information Security Incident (including both the appropriate business and technical personnel)
- Other constituencies, as appropriate.

The ISIRT, led by the University Privacy Officer, will develop and execute communication and other action plans to ensure:

- a. Appropriate action is taken in a timely manner, including reporting, notification and other communication of the Information Security Incident, as required by law or otherwise deemed appropriate.
- b. Appropriate progress reports are made on the Information Security Incident and execution of the Plan, including to:
 - Office of the President and Provost
 - Board of Trustees
 - Alumni Association
 - Office of Student Affairs
 - Office of Development
 - Other impacted constituencies, as warranted by the situation

In carrying out this responsibility, the ISIRT will ensure that important operational decisions are elevated to the appropriate levels to protect the fundamental interests of the University and others impacted by the incident.

The University Privacy Officer will also be responsible for documenting the deliberations and decisions of the ISIRT as well as all actions taken pursuant to ISIRT deliberations.

6. REPORT PREPARATION

The Information Security Office, jointly with the Internal Audit Department, will be responsible for writing a final report on the incident and the ensuing investigation (Report), which summarizes findings regarding the Information Security Incident and, if appropriate, makes recommendations for improvement of related information security practices and controls. The Report will be distributed to the Vice President for Business Affairs and CFO, and other appropriate University office(s), if any.

7. ADDITIONAL INFORMATION

Specific guidelines, procedures, standards, and best practices for secure computing can be found at <http://securecomputing.stanford.edu>.

Additional information can be found at:

- Administrative Guide Memo 61, Administrative Computing Systems <http://adminguide.stanford.edu/61.pdf>
- Administrative Guide Memo 62, Computer and Network Usage Policy, <http://adminguide.stanford.edu/62.pdf>
- Administrative Guide Memo 63, Information Security, <http://adminguide.stanford.edu/63.pdf>
- Information Security Office website, <http://security.stanford.edu>