

Title: Procedure for Reporting and Handling Security and Privacy Incidents
Effective Date: November 21, 2011
Issuing Authority: Chief Information Security Officer

Information Security Reporting Procedures

The Computer Incident Reporting Procedure provides a series of channels through which incidents can be reported, investigated, tracked, and administratively reviewed to ensure Temple information assets and/or infrastructure are protected. The Information Security Department will be the primary responder to incidents. Other departments will assist as the need arises.

* AFTER NOTIFYING THE INFORMATION SECURITY OFFICE, IT IS ESSENTIAL TO FOLLOW THE INSTRUCTIONS OF THE RESPONSE TEAM. ALL TECHNOLOGY DEVICES MUST NOT BE USED, TURNED OFF OR ON, OR CHANGED IN ANY MANNER THAT MAY COMPROMISE EVIDENCE.

Examples of what type of incidents should be reported appear below:

- Any suspected hacking or intrusion attempts
- Suspicion of a password compromise
- Harassment by e-mail
- Violation of any computer policy

Critical Issues

- Critical issues should be reported **immediately** to your manager and the Information Security Department. You must have confirmation from your management **and** from Information Security Department. E-mail, text, voicemail, or Remedy tickets are not confirmation. Follow the contact list below for Information Security Department.
- Critical issues involving notification of an intrusion from our Intrusion Detection Systems or Network logging facilities should be brought to the attention of the Information Security Department immediately.

Information Security Department Contact Information

- Information Security Office – Seth Shestack 215-204-5884
Escalation Manager – Larry Brandolph, CISO 215-204-7088
- ciso@temple.edu (Information Security Office departmental e-mail)
- Escalation for all of Computer Services – Tim O’Rourke 215-204-7077
or orouket@temple.edu
-

Non-Critical Issues

- Non-critical issues should be reported to the following management personnel by telephone, e-mail, in person, or via [TUhelp](#) system:
 - Your immediate supervisor within assigned Department

- Help Desk ([TUhelp](#) / 215-204-8000)
- Information Security Office
- Human Resources (if University policy or codes have been broken)

- Technical issues
 - The Help Desk will refer the matter to the appropriate Computer Services personnel through the [TUhelp](#) System.
- Non-technical issues
 - The Help Desk will refer the matter to an Information Security Office person through the [TUhelp](#) system.

Handling Procedures Following Reporting of Security and Privacy incident

1. The Office of Chief Information Security Officer, as appropriate, shall activate and lead its Incident Response Team following the report of a suspected or actual breach.
2. After notifying the Information Security Office it is essential to follow the instructions of the response team. All technology devices must not be used, turned off or on, or changed in any manner that may compromise evidence.
3. The Incident Response Team shall proceed to assess the nature and scope of the incident and identify what personal information has been accessed or misused.
4. The Incident Response coordinator will contact the Privacy Officer to review if there needs to be a Breach Declaration, if event is solely privacy or a combination of both.
5. System owners, working in full cooperation with the Incident Response Team, shall provide the necessary resources to take appropriate steps in order to contain and control the incident, to prevent further unauthorized access such as monitoring or suspending access, and to preserve records and other evidence.
6. The Incident Response Team shall create an Incident Report that will document the facts surrounding the incident; the steps taken to mitigate any immediate threat, the steps taken to ascertain the scope and nature of the breach; the nature of the breach itself; the list of affected individuals and any other relevant information relating to the incident.
7. The Incident Response Team, as needed, shall include Temple University Police, and will indicate in the Incident Report whether delay in public notification is necessary for the purposes of investigation.
8. The Chief Information Security Officer shall consult with the Chief Information Officer to determine if this is a Security incident, Privacy incident, or both
9. The Breach Declaration Team shall evaluate the Incident Report and make the final determination as to whether a Breach of Personal Information has occurred, and if so, what the appropriate response and relief should be.

10. The Chief Information Security Officer, independent or as appropriate, to the outcome of the Breach Declaration Team, shall lead an effort to formulate a long range plan to prevent recurrence of the incident.