Incident Response Policy

ITS security staff should be notified immediately of any suspected or confirmed Security Incident involving a Baylor Information Technology Asset.

These are policies and procedures for Baylor University faculty, staff and students to report any potential security incidents. The policy will also outline the anticipated response by ITS security staff.

**Topic Listing:**
- Definitions
- Reporting a Security Incident
- Response

**Related Polices and Legislation:**
Technology Systems Usage Policy BU-PP 025

**Contact:**
ITS Security 710-2711

**Sanction:**
Sanctions may include but are not limited to suspension of technology privileges, termination of employment, referral to Student Judicial Services, and/or criminal prosecution. For additional information, please reference Technology Systems Usage Policy BU-PP 025.

**Date created/ updated:**
Updated – September 17, 2007

**Definitions:**
*Information Technology Asset* – A system or systems comprised of computer hardware, software, networking equipment, and any data on these systems. Such assets include but are not necessarily limited to desktop computers, servers, printers, telephones, network lines, E-mail and web based services.

*Security Incident* – an incident meeting one or more of the following conditions:
- Any potential violation of Federal law, Texas law or Baylor University Policy involving a Baylor Information Technology Asset.
A breach, attempted breach or other Unauthorized Access of a Baylor University Information Technology Asset. The incident may originate from the Baylor University network or an outside entity.

- Any Internet worms or viruses.
- Any conduct using in whole or in part a Baylor Information Technology Asset which could be construed as harassing, or in violation of Baylor University Policies.

Unauthorized Access - Any action or attempt to utilize, alter or degrade a Baylor owned or operated Information Technology Resource in a manner inconsistent with university policies.

Reporting a Security Incident:
ITS security staff should be notified immediately of any suspected or confirmed Security Incident involving a Baylor Information Technology Asset. If it is unclear as to whether a situation should be considered a Security Incident, ITS security staff should be contacted to evaluate the situation.

With the exception of steps outlined below, it is imperative that any investigative or corrective action be taken only by ITS Security personnel. When faced with a potential situation, faculty and staff should do the following:

- If the incident involves a compromised computer system,
  - Do not alter the state of the computer system. The computer system should remain on, and all currently running computer programs should be left as is. Do not shutdown the computer or restart the computer.
  - Immediately disconnect the computer from the network by removing the network cable from the back of the computer.

- Report the security incident.
  - Contact Details

Security Incidents involving possible violation of Federal or state law should be immediately reported to the Baylor University Police. Baylor Police will work with ITS Security staff and other law enforcement agencies as necessary to help resolve the incident.

Phone - 710-2222.

Any other Security Incident should be immediately reported to Baylor University ITS security staff. ITS security staff will then determine the appropriate response.

Primary Contact
Jon Allen - 709-5699

Secondary Contact
Bob Hartland - 744-0212

- Document any information you know while waiting for Baylor University Police or ITS security staff to respond to the incident. This may include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.

Response
ITS security staff will first determine if the Security Incident justifies a formal incident response. In cases where a Security Incident does not require an incident response, the situation will be forwarded to the appropriate area of ITS to ensure that all technology support services required are rendered.

An incident response may range from getting a critical system back online, gathering evidence, taking appropriate
legal action against individual(s), or in some cases notifying appropriate ISP’s or other third parties of inappropriate activity originating from their network.