I. OVERVIEW

The purpose of the University’s Cyber Incident Response Plan is to provide guidance for members of the University community on the processes required to establish a coordinated, University-wide response to any potential information security threats.

The University’s Information Security Incident Response Plan governs all University campuses, schools, departments, and responsibility centers, and applies to all individuals who access, use or control University data, including but not limited to: administrators, faculty, staff, students, researchers, contractors, consultants, agents or any other individuals authorized to access information by affiliated institutions and organizations.

II. DEFINITIONS

A breach is a potential acquisition, access, use, or disclosure of information in a manner not permitted under existing law or University policy. A breach may have reporting requirements to government entities and/or individuals impacted.

An Information Security Incident is any actual or suspected adverse event in relation to the security or privacy of computer systems, computer networks, or University data.

An Information Security Incident may also include inadvertent or intentional violations or threatened violations of the University’s information security or acceptable use policies. For example, using University computing resources to gain or attempt to gain unauthorized access to computing resources either inside or outside the University.

The Pitt Cyber Incident Response Team includes the Chief Information Security Officer and members of Pitt Information Technology (Pitt IT) designated by the Chief Information Officer and/or Chief Information Security Officer, designated members of the Office of
University Counsel, the University's Privacy Officer, the Director of Internal Audit, the Executive Director of Enterprise Risk Management, and the Director of Public Safety.

III. REPORTING AN INCIDENT

The University’s Cyber Incident Response Plan establishes responsibilities for the entire University community in reporting any Information Security Incident potentially affecting the confidentiality, integrity, or availability of University data.

Any member of the University community who becomes aware of an information security incident should immediately contact the 24/7 IT Help Desk by calling (412) 624-HELP [4357] or emailing helpdesk@pitt.edu.

The Pitt Cyber Incident Response Team will follow the Computer Security Incident Handling Guide, NIST 800-61, which involves preparation; detection and analysis; containment, eradication and recovery; and post-incident activity.

IV. INCIDENT DETECTION AND INVESTIGATION

Upon activation, the Pitt Cyber Incident Response Team will:

1. Immediately provide an initial assessment of the incident, including potential loss, corruption, inappropriate disclosure, inappropriate exposure, or breach of information.
2. Immediately advise and assist in containing and limiting the loss, corruption, inappropriate disclosure, inappropriate exposure, or breach.
3. Ensure appropriate information and evidence are collected and logged.
4. Invoke incident response procedures commensurate with the situation.
5. Determine if outside forensic and/or legal expert(s) are necessary to assist with the situation.
6. Notify the University’s Office of Risk Management to assess whether notice to the University’s insurance carrier(s) is necessary.
7. Notify the University’s Office of Communications to assess whether preparation of publicly disseminated communications within the University and with the general public regarding the information security incident is appropriate.

8. The University’s Privacy Officer shall provide regularly reports to Senior Management about the status of the response and recovery efforts taken by the Pitt Cyber Incident Response Team.

9. Working through Pitt Public Safety and Office of University Counsel, contact law enforcement for assistance if needed or required by law.

10. Initiate steps to warn other Pitt IT departments or teams if the situation has the potential to affect other university information or information systems.

11. Confirm actual or probable events from investigatory information and facilitate decision-making by the Response Team.

12. Determine if notification to individuals and/or regulatory or governmental authorities is required. The University Privacy Officer will invoke breach notification procedures commensurate with the situation.

13. Document decisions and any notifications made to individuals or regulatory and government officials.

V. POST-INCIDENT ACTIVITIES

Once the Cyber Incident Response Team verifies that an incident has been adequately contained, and all notifications and other legal obligations have been met, the Response Team will be responsible for analyzing the cause and impact of any cyber incident based on information received from the Response Team and any outside forensic and/or legal expert(s). This will include all aspects of the IT environments connected to the incident, including technical, policy, and organization aspects. The review should include activities leading up to the incident as well as during the response.

The Response Team will also consider information received from affected individuals and other responsibility centers in analyzing the cause and impact of any incident for purposes
of improving policies and procedures governing the security of confidential, protected, and sensitive information.

The Response Team will review whether:

- Communication was effective and sufficient.
- Escalation was appropriate.
- Media and customer communications were handled adequately.
- The proper number of expert resources were available.

The Response Team will conduct a “lessons learned” meeting to document both the positive and problematic issues. This internal debriefing will allow the University to evaluate opportunities for improvement, both with respect to response efforts and security controls. The University’s Privacy Officer and Chief Information Security Officer will issue a detailed report of the incident and its response to University leadership, including findings and recommendations.

Finally, the Cyber Incident Response Team will meet on a bi-annual basis to discuss what awareness and training are necessary for the University community to prevent a similar information security incident in the future. The Response Team will also discuss any changes, updates, revisions, etc., that are necessary to this Plan.

VI. INCIDENT RESPONSE WORKFLOW (See next page)