EDINBORO UNIVERSITY OF PENNSYLVANIA

SECURITY INCIDENT REPORTING AND RESPONSE POLICY
Policy No. C064

Recommended for Approval by _____
Mr. Guilbert Brown, Vice President Finance and Administration

Approved by _____ on 2/2/15
Dr. Julie Wollman, President

Review Date: As Required

INTRODUCTION

This policy serves to minimize the negative consequences of an Information Security incident (as defined below) and to improve the University's ability to promptly restore operations affected by such incidents. The University's goal is to assure that incidents are promptly reported to the appropriate University officials, that they are consistently and expertly responded to, and that serious incidents are properly monitored.

PURPOSE

The purpose of information security incident response is:

- To ensure that incidents are promptly reported to the appropriate University officials.
- To mitigate the effects caused by such an incident.
- To protect the information resources of the University from future unauthorized access, use or damage.
- Ensure that Edinboro University fulfills all of its obligations under University policy, and federal and state laws and regulations with respect to such incident.

POLICY

Who should report a security incident?

Any person (faculty, staff, and student) who knows or reasonably believes that a security incident involving an Edinboro University-owned technology asset has occurred. If it is unclear as to whether a situation should be considered a security incident, it should be reported so that University Technology & Communications can evaluate the situation.

How do you report a security incident?

Security incidents must be reported as soon as possible by calling the University Helpdesk at 814-732-2111. Please be as detailed as possible. Anyone who discovers a weakness or vulnerability in the information security measures used by Edinboro University must not discuss these matters with anyone other than the University IT department.

RESPONSE

Once reported, the University IT department will investigate, assess, and respond to threats to Edinboro University IT resources. In cases of lost or stolen University Information Technology (IT) Assets, Edinboro University - Guidelines on Breach Notification will be followed. Incidents may also be reported to the appropriate law enforcement, PASSHE, or University officials. The University IT department will handle these notifications.

Any University information technology assets or personally owned technologies that pose a security threat may be disconnected from the network. If a security breach is discovered in progress, the University IT department may take immediate actions to isolate and deny access to the user, data or information technology asset.

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 equipment, E-mail and web based services.

Security Incident – an incident meeting one or more of the following conditions:

- Any Internet worms or viruses.
- Disruption of information technology service levels.
- Theft or loss of a laptop, desktop, PDA or other electronic device that may contain confidential or sensitive data.
- Web site defacement.
- Compromised password(s).
- Unauthorized use of an individual's computing account.
- Any activity that harms or represents a serious threat to the whole or part of Edinboro University's computer, telephone, and network-based resources.
- A breach, attempted breach or other unauthorized access of an Edinboro University technology asset.

The incident may originate from the Edinboro University network or an outside entity.

CONTACT INFORMATION:

Vice President Finance and Administration
219 Meadville Street
Edinboro, PA 16444
814-732-2585