Millersville University **Governance & Policies**

Effective: February 21, 2017

Information Technology Policy
INCIDENT RESPONSE

Approved: February 21, 2017
President's Cabinet

Introduction

Millersville University computing resources and Information Technology assets have been developed to encourage widespread access and distribution of data and information for the purpose of accomplishing the University's educational mission. Millersville University seeks to protect the University's data, as well as its Information Technology assets from any incidents that originate from within the Millersville University network or from an outside entity.

Purpose

The purpose of this policy is to establish guidelines ensuring that security incidents are promptly reported to the appropriate Millersville University officials, that incidents are consistently and expertly responded to, and that serious incidents are appropriately monitored.

Definitions

Information Technology Asset – Any University owned, or operated, system, hardware device, or software; including any and all data on such assets. Such assets include, but are not limited to: desktop computers, laptops, servers, printers, telephones, firewalls, E-mail and web based services.

University Community – Includes all faculty, staff, students, contractors, vendors, or visitors associated with Millersville University.

Policy

Reporting

1. The University community must immediately report any actual, or suspected security incident that involves:

   A. Unauthorized access to electronic systems owned or operated by Millersville University.
   B. Malicious alteration, or destruction of data, information, or communications.

C. Unauthorized interception or monitoring of communications.
D. Any deliberate and unauthorized destruction or damage of Information Technology assets.

2. All actual or suspected incidents should be reported to the CIO.

Response

1. Once an incident has been reported, the University IT department will investigate, assess, and respond to threats to Millersville University resources.

   A. 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.
   B. Any University Information Technology assets, or personally owned technologies, that pose a security threat may be disconnected from the Millersville University network.
   C. Security incidents may be reported to the appropriate law enforcement, PASSHE, or University officials if necessary.
   D. All communications with the media regarding an incident will be coordinated through University Communications.