IT Incident Handling

Effective Date: September 2009

Approval: December 17, 2015

Maintenance of Policy: Chief Information Officer

PURPOSE: The purpose of this policy is to provide guidance regarding notification and investigation of IT security incidents involving the University of Dayton.

SCOPE: This policy applies to all computer, communications, infrastructure, services and storage devices used by UD faculty, staff, contractors, consultants, and student employees in the course of their work and to systems hosting UD proprietary data off campus.

POLICY:

The University of Dayton maintains a sophisticated computing environment in support of its diverse operations. To that end, UD hosts large quantities of data, some confidential, across a large assortment of diverse systems. We have a requirement to detect, contain, eradicate, recover, and report on IT security incidents. An IT security incident will be defined as "any adverse event which compromises some aspect of computer or network security." [RFC 2350] UD's response to an IT security incident depends largely on the nature of the potentially compromised data or service. In general, any suspected IT incident should be reported immediately to the IT Risk Management Officer (IRMO), who will coordinate the appropriate parties and activities to develop and implement a response. IT security incidents include, but are not limited to, denial of service, malicious software infection, loss/theft of equipment, and unauthorized access to data.

Incidents are categorized by the nature and scope of the data they hold the potential to expose (as defined in UD's Electronic Use of Confidential Data policy):

REFERENCE DOCUMENTS:

1. ISO 27002 2013 Sec. #16

APPLICABLE REGULATIONS:

Including, but not limited to:

1. Family Educational Rights and Privacy Act (FERPA)
2. Health Insurance Portability and Accountability Act of 1996 (HIPAA)
3. Payment Card Industry Data Security Standards (PCI DSS)
4. DFAR 252.204-7012, Safeguarding of Unclassified Controlled Technical Data
5. National Industrial Program Operating Manual (NISPOM)

POLICY HISTORY:

Approved in its Original Form:
September 2009

Approved as Amended:
April 2015

POLICY (continued):

Level 1: IT security incident involving a personal computing or communications device or media on which the user maintains or accesses his/her own personal information.

Level 2: IT security incident involving a non-critical service or a server or associated media that is not a part of a system identified as hosting any of the confidential data types listed in UD's Electronic Use of Confidential Data policy.

Level 3: IT security incident involving a personal computing or communications device or media hosting the confidential data of others or through which unauthorized individuals might access the confidential data of others.

Level 4: IT security incident involving a business critical service or a server or associated media identified as part of a system hosting any of the confidential data types listed in UD's Electronic Use of Confidential Data policy. IT security incidents involving network infrastructure, security systems and identity management components will also be addressed at this level.

Responsibilities are outlined below:

Chief Information Officer: The CIO will be notified of all but Level 1 IT security incidents.

Data Owner: Data owners will be notified immediately of incidents involving their confidential data type.

Facility Security Officer: The FSO will be notified of **any** IT security incidents involving data, systems or services regulated/classified under the referenced DFARS and NISPOM guidelines or by UDRI contract. He/she will coordinate internally with UDRI's Information Systems Security Manager (ISSM) and contracting officers as well as externally with the Defense Security Service, FBI and others, as required.

IT Risk Management Officer: The IRMO will be notified of **any** IT security incidents. He/she will coordinate activities, provide Legal and PIO with information, work with data and system owners and managers to investigate and to document the internal investigation.

Legal: Legal will be notified of all but Level 1 IT security incidents and will make final determination, with respect to best practice, industry regulation and federal and state law, on UD's course of action. In the case the University of Dayton is first notified of an IT security incident through Legal, that office will notify the IRMO immediately. If the Legal Office determines criminal investigation is warranted, Public Safety will be engaged. The Legal Office will provide guidance on evidence requirements.

Public Information Office: The PIO will be notified of all but Level 1 IT security incidents and will be responsible for external communications.

Public Safety: Public Safety will be notified in the event criminal investigation is required. In the case the University of Dayton is first notified of an IT security incident through Public Safety, that office will notify the IRMO immediately. Public Safety will provide guidance on the collection and preservation of evidence.

System Owner: The System Owner will be notified of IT security incidents involving their system or notify the IRMO immediately if he/she first determines an IT security incident has occurred. He/she will work with the IRMO to coordinate UD's investigation and response. The System Owner will be required to ensure accurate and current information is maintained in UD's server inventory database with respect to software, authentication, update status, data, etc.

System Administrator/Manager: System Managers will notify the System Owner and the IRMO immediately in the case an IT security incident occurs. Systems Managers, under the direction of the IRMO and the System Owner, will work with the assembled response team to investigate the incident.

Policy [continued]:

Technology Support Services: TSS will notify the IRMO immediately as IT security incidents are identified. All incidents determined to be Level 1 will be addressed by TSS with reporting handled through that office and existing service desk reporting facilities.

UD Risk Management: UD Risk Management will be notified of all but Level 1 IT security incidents. In the event a device is reported as lost or stolen for insurance purposes, the office will notify the IRMO to determine if further investigation is necessary.

Various: Departments including, but not limited to, Facilities, the Bursar, Human Resources, the Registrar, and Student Development shall be engaged as necessary as dynamic members of the incident handling team.

Training will be provided to staff with security breach investigation and response responsibilities. Exercise of this policy and associated procedures will be conducted annually.

With respect to enforcement, parties found to have violated this policy may be subject to disciplinary action.