Augsburg University Incident Response Policy

I. Overview

An information system security or data security incident is one that threatens or compromises confidentiality, integrity or availability of University Information Systems. While such incidents may vary in severity and scope, the handling and response to such incidents must be managed appropriately in order to best preserve the University's reputation as well as all personal or institutional information assets that reside under the University's control.

II. Purpose

This policy defines the steps that personnel must use to ensure that security incidents are identified, contained, investigated, and remedied. It also provides a process for documentation, appropriate reporting internally and externally, and communication so that organizational learning occurs. Finally, it establishes responsibility and accountability for all steps in the process of addressing computer security incidents. This policy works with the Disaster Recovery Plan to handle routine incidents.

III. Scope

This policy applies to all individuals or entities using any University Information Systems. This includes personal electronic devices containing confidential University data or that contain passwords that would give access to University Information Systems.

This policy governs the University's general response, documentation and reporting of incidents affecting computerized and electronic communication information resources, such as theft, intrusion, misuse of data, other activities contrary to the University's Acceptable Use Policy, denial of service, corruption of software, computer- and electronic communication-based HIPAA violations, and incidents reported to the University by other institutions and business entities. This policy does not include damage to personal computers owned by students, unless their computers contribute to the Incident defined by the parameters in Definitions, below.

IV. Definitions

Security Incident: any event that threatens the confidentiality, integrity, or availability of University systems, applications, data, or networks.

User: any University faculty, staff, student, or consultant that has been granted access to University Information Systems.

University Information Systems: any University computer system, network, or data.

Regulated Data: defined in the Data Classification Policy.

V. Procedures

A. Reporting and Assessment

Any member of the University community who identifies an information Security Incident or potential concern should report it promptly through one of the following channels:

- Student TechDesk at (612) 330-1400 (business hours)
- Contact a Liaison for Computing (business hours)
- Submit an IT Systems Issue Reporting Form (after business hours) http://inside.augsburg.edu/it/contact
- IT staff should contact their supervisor or the CIO.

B. Response

1. **Determination of the nature and scope of a security incident**
    - identification of the person reporting the security incident (name, contact info, etc.)
    - record of the location, timeframe, and apparent source of the security incident
    - preliminary identification of regulated data that may be at risk
2. **Communication**
    - chief information officer
    - president and senior officers (depending on sensitivity and scope of data exposed)
    - legal counsel (depending on sensitivity and scope of data exposed)
    - federal student aid office within 24 hours of confirmed or unconfirmed security incident discovery
    - law enforcement (depending on the nature/scope of theft)
    - EIIA (company retained by Augsburg to assist with security incident notification)
    - director of marketing (depending on sensitivity and scope of data exposed)
    - if credit card data is involved notify bankcard holder within 24 hours of confirmed security incident discovery
3. **Investigation**
    - identify ongoing vulnerability of data to exposure from security incident source (take immediate steps to address)
    - conduct preliminary forensic analysis (retain outside assistance as needed)
    - prepare inventory of data at risk
    - determine if exposed data were encrypted
    - identify security measures that were defeated (and by what means)
4. **Assessment of breach**
    - identify affected individuals at risk of identity theft or other harm
    - assess financial, legal, regulatory, operational, reputational and other potential institutional risks
5. **Remediation**
    - implement password changes and other security measures to prevent further data exposure
    - determine if exposed/corrupted data can be restored from backups; take appropriate steps
    - determine if value of exposed data can be neutralized by changing account access, ID information, or other measures
6. **Notification**

Based on regulatory requirements (e.g., Minnesota statutes 325E.61, 325E.64) and other factors, Senior Officers, CIO, and Director of Marketing (in consultation with legal counsel as appropriate) determine whether notifications are indicated for:

- government agencies
- affected individuals
- Augsburg community
- business partners
- public
- other

If Senior Officers, CIO, and Director of Public Affairs determine that notifications are needed:

- the CIO will notify EIIA who will coordinate notifications to affected individuals. Unless directed otherwise by law enforcement, such notifications will be made without delay.
- the Chief Financial Officer and/or CIO will notify government agencies and business partners.
- the Director of Marketing will coordinate notifications to the Augsburg community, the public, and others as necessary.

Communications will address the following points:

- nature and scope of security incident
- general circumstances of the security incident (e.g., stolen laptop, hacked database etc.)
- approximate timeline (e.g., date of security incident discovery)
- steps the university has taken to investigate and assess the security incident
- any involvement of law enforcement or other third parties
- appraisal of any misuse of the missing data
- university-provided *credit-watch* service for affected individuals
- EIIA steps on behalf of affected individuals
- steps that the university is taking to prevent future breaches of this nature

Post-Incident Follow-Up

In the wake of a data security incident, Augsburg will:

- take steps to ensure that missing data cannot be used to access further information or cause harm in other ways to Augsburg's electronic or other resources;
- pursue with law enforcement all reasonable means to recover lost data and equipment;
- review and modify as needed all procedures governing systems administration, software management, database protections, access to hardware, etc., to prevent future data breaches of a similar nature;
- take appropriate actions if staff negligence or other's behavior contributed to the incident.
- modify procedures, software, equipment, etc., as needed to prevent future data security incidents of a similar nature;
- take appropriate actions if personnel negligence caused or contributed to the incident.

C. Documentation

The University Information Technology will employ an internal tracking system to facilitate and archive communication, including the preceding elements, surrounding an incident. Any outages of University Information Systems associated with an incident will be tracked.

Revision History

Revision	Change	Date
1.0	Initial Policy	4/9/2012
1.1	Response update	1/9/2018
1.2	Response update	5/3/2019