CYBER-SECURITY INCIDENT MANAGEMENT POLICY

Type: University
Category: Information Technology
Administrators: Vice President for Finance and Administration
Manager: Director of Instructional and Information Technology

Purpose

To minimize the impact of security incidents by ensuring controls are in place for identification, management, and communication of security events and weaknesses through a formal process to ensure that Viterbo University information assets and information systems are protected.

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.

Scope

This policy applies to Viterbo University employees and students.

Definitions

a. Security Incident - any event that threatens the confidentiality, integrity, or availability of University systems, applications, data, or networks. Some examples include compromised credentials, miss handled data, or installation of malware.
b. User - any University faculty, staff, student, or consultant that has been granted access to University Information Systems.
c. University Information Systems - any University computer system, network, or data.
d. Confidential Data – data whose unauthorized disclosure may have moderate adverse effects on a university's reputation, resources, services, or individuals. This is typically the default classification for most organizations and requires a moderate level of security. Alt Def. Sensitive information used by the university, including PII, as defined in the Data Classification Categories Guide.
e. Sensitive Data - data whose unauthorized disclosure may have serious adverse effects on a university's reputation, resources, services, or individuals. Typically, this includes data protected under federal or state regulations, or data that carries with it proprietary, ethical, or privacy considerations. Sensitive data requires the highest level of security, as defined in the Data Classification Categories Guide.

f. Tier 2 Professional Staff - Desktop support, Infrastructure Support, Admin Systems Support team members.

Policy

A potential cyber-security incident can take many forms and range in criticality. It is a key responsibility of all Viterbo University defined users to assist in protection against misuse & to report all potential incidents to the IIT Helpdesk. Examples may include compromised university username/password, miss directed email with confidential/sensitive information, installation of malware, broader than intended share permissions of folders/files that contain confidential/sensitive data, etc.

Detection: All employees and students are responsible for report incidents such as: password breach, phishing attack compromise, confidential data leak, etc. Suspected Security incidents should be reported to the IIT helpdesk, as soon as suspected activity occurs. The IIT team will also inform the helpdesk if it should suspect a security incident has occurred due to standard monitoring of systems. (O365 reports, EDR systems notifications, etc.)

Analysis: All Security incident reports/documentation of response will be stored in the IIT ticketing system. Security incidents will be reviewed by IIT Tier 2 professionals to determine classification of impact and if further action needs to be taken. Tier 2 professionals may include the following IIT positions: desktop support, programmer/analysts, server administration, network administrator, associate director of IIT and director of IIT.

The Director of Instructional & Information Technology is responsible for all Security incident management. The Director of IIT should be notified as soon as possible if a security incident has crossed multiple university systems or accounts automatically and/or if institutional data is suspected to have been compromised.

Containment: Upon review, If an incident is considered high-impact the Director of IIT will in cooperation with Network and Server admins will determine what initial containment steps are required. Following initial containment actions, the Director of Instructional & Information Technology or designee will contact the VPFA to consult regarding impacts and if cyber-insurance forensics should be launched.

The Cyber-insurance forensics team along with the VPFA and Director of Instructional & Information Technology will be in regular contact. The VPFA will inform the University President, and the University President will determine if the Emergency Incident Response Team needs to be enacted.

Related Resources

- Cyber-Security Incident management plan
- RACI Chart
- Data Safeguarding and Use for Employees

- Data Classification Categories
- Appropriate Use of Technology Policy
- University Privacy Policy