Data Security Incident Reporting Procedures

Purpose:

University Policy requires all Faculty, staff, students, and affiliates who work with University information assets or information assets in the University's care *to immediately report* all suspected information security incidents to their supervisors and to the Information Security Office for investigation. Such incidents include, but are not limited to, workstation viruses, spyware infections, data system or storage theft, or other unauthorized interactions with or removal of University Information Systems or data. These procedures provide guidance for this reporting.

Immediate Actions and Reporting Procedures:

1. Immediately report all incidents of equipment theft (computers and/or media) to your supervisor, University Police (336-334-5963), and Information Security Office (through 6-TECH, 336-256-8324).

2. Report all other potential incidents (such as workstation viruses, spyware infections or unauthorized interactions with or removal of University Information Systems or data) to your supervisor and the Information Security Office (through 6-TECH, 336-256-8324).

3. Supervisors should report incidents as appropriate within their units.

4. Immediately disconnect potentially compromised computers or devices from the network (whether wirelessly connected or connected via a physical cable). Do not power them off. Ensure the device(s) remain(s) charged. DO NOT ATTEMPT TO RECTIFY A POTENTIAL COMPROMISE ON YOUR OWN! ITS will provide remediation assistance upon your report!

Investigative Procedures:

1. The Information Security Office will investigate all reports and provide results, and the ITS Help Desk team will assist with returning the potentially compromised computer or device to productive service.

2. During investigation, Information Security will ask about personally identifiable information stored on the computer, and types of data accessible while using the computer. This information will help guide the investigation and determine level of risk to data that might have been compromised.

3. Based on answers to Information Security questions, Information Security may run a utility designed to isolate and identify the scope sensitive data.

4. The Information Security Office will report relevant results to the Vice Chancellor for Information Technology Services, to the reporter of the incident and to the reporter's supervisor.

5. Any further reporting or internal and external notifications will take place per the requirements and process outlined in the University's Information Security Incident Reporting and Notification Policy.

Updated February, 2021