I. INTRODUCTION

The number of computer security incidents and the resulting costs of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, early detection and mitigation of security incidents can reduce the risk and drive down the cost of security incidents.

II. PURPOSE & SCOPE

This policy describes the requirements for dealing with computer security incidents. Security incidents include, but are not limited to, virus, worm, and Trojan horse detection, unauthorized use of computer accounts and computer systems, as well as complaints of improper use of information resources and technology as outlined in the Email Policy (MAPP 04.06.10), the Internet Use Policy (MAPP 04.06.12), and the Computer Use Policy (MAPP 04.06.03). To the extent this policy conflicts with existing University policy, the existing policy is superseded by this policy. The Incident Management Policy applies equally to all individuals who use any University information resources and technology.

III. POLICY

A. University Computer Security Incident Response Team ("CSIRT") members have pre-defined roles and responsibilities which can take priority over normal duties.
B. Whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed, the appropriate Incident Management procedures must be followed.
C. The Information Security Officer ("ISO") is responsible for notifying the Information Resource Manager ("IRM") and the CSIRT, and initiating the appropriate incident management action including restoration as defined in the Incident Management Procedures. The Incident Management Procedures are determined by the Information Resource Manager.
D. The ISO is responsible for determining the physical and electronic evidence to be gathered as part of the incident investigation.
E. The appropriate technical resources from the CSIRT are responsible for monitoring to ensure that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
F. The ISO, working with the IRM, will determine if a widespread University communication is required, the content of the communication, and how best to distribute the communication.
G. The appropriate technical resources from the CSIRT are responsible for communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.
H. The ISO is responsible for initiating, completing, and documenting the incident investigation with assistance from the CSIRT.

I. The University ISO is responsible for reporting the incident to the:
   1. IRM,
   2. Department of Information Resources as outlined in Texas Administrative Code 202 and/or,
   3. Local, state or federal law officials as required by applicable statutes and/or regulations

J. The ISO is responsible for collaborating with the Office of Communications through the CSIRT in coordinating communications with outside organizations and law enforcement when a security incident occurs. In the case where law enforcement is not involved, the ISO will consult with the Office of Human Resources regarding appropriate disciplinary action in accordance with University policy. In the case where law enforcement is involved, the ISO, in collaboration with the university police department, will act as the liaison between law enforcement and University.

IV. DISCIPLINARY ACTION

Violation of this policy may result in immediate Disciplinary Action pursuant to University policy (MAPP 02.05.03 — Discipline and Termination Policy).

V. APPLICABLE TSU SECURITY POLICY STANDARDS

All individuals with authorized access to any TSU information resource and technology, including staff, faculty, students, consultants, contractors and volunteers, must adhere to all provisions of this policy, as well as applicable security standards included in the Security Standards Policy — MAPP 04.06.22). Applicable security standards include, but are not limited to:

- Security Standard 3
- Security Standard 6
- Security Standard 7
- Security Standard 16
- Security Standard 21
- Security Standard 22