SUPERSEDES:NEW

CODE NO: [xxxx]

NOVA SOUTHEASTERN UNIVERSITY

SECTION: Security Procedures

I. SUBJECT: Information Security Incident Response Procedure

Purpose:

This procedure is intended to provide guidance on how to handle certain types of security related incidents. This procedure is intended for every employee, student employee, or consultant to the OIIT department.

Description of a Security Incident

An IT or Information Security Incident ("Incident" or "Security Incident") is any activity that harms or represents a serious threat to the whole or part of NSU's computer, telephone and network-based resources such that there is an absence of service; inhibition of functioning systems, including unauthorized changes to hardware, firmware, software or data; or a crime or natural disaster that destroys access to or control of these resources. An Incident is also any activity that threatens the confidentiality, integrity, or availability ("CIA") of NSU information systems resources. NSU personnel must immediately report an Incident if it meets one (1) or more of the following conditions:

- Any potential violation of Federal law, Florida law or NSU policy involving a NSU Information Technology Asset, including, but not limited to, incidents pertaining to financial information in violation of the Gramm-Leach-Bliley Act ("GLBA").
- A breach, attempted breach or other unauthorized access of NSU's Information Technology Asset(s). The Incident may originate from within the NSU network or from an outside entity.
- Any Internet worms or viruses.
- Any conduct using in whole or in part an NSU Information Technology Asset that could be construed as harassment or in violation of NSU policies.

Procedures for Incident Response

The NSU CISO is responsible for carrying out and enforcing this Procedure and for assisting other teams within OIIT in remediation efforts of computer and electronic communication-based resources affected by Security Incidents.

Upon receiving notification of a potential Security Incident, the Security Team shall first attempt to determine if the Security Incident justifies a formal incident response.

- In cases where a Security Incident does not require a formal incident response, the situation will be forwarded to the appropriate area of NSU OIIT to ensure that all technology support services required are rendered.
- An incident response may range from getting a critical system back online, gathering evidence, taking appropriate legal action against individual(s), or in some cases notifying appropriate ISP's or other third parties of inappropriate activity originating from their network.

A decision on the operational status of the compromised system itself will be made by the OIIT Security Team within OIIT. Whether this system should be 1) shut down entirely; 2) disconnected from the network; or 3) be allowed to continue to run in its normal operational status (so that any activity on the system can be monitored) will depend on the risk to NSU assets threatened by the Incident.

If the compromised system is suspected or found to have had any type of data loss that could expose NSU to regulatory or legal risk, the CISO shall immediately notify the CIO and COO of the matter.

In the case of a virus/malware/Trojan/rootkit Incident, the OIIT Security Team will move quickly to eradicate the security incident using all available resources. If the infection threatens systems or information of a sensitive or critical nature, the Security Team will require the machine be shut down and no attempts to alter or remove any contents (software and hardware) of the machine be made.

The OIIT Security Team may take actions that include, but are not limited to, forensic analysis and physical inspection of an infected machine to determine the extent and severity of the security incident. Personal information may not be preserved in this process, and no claim to maintain or restore personal data will be made.

The OIIT Security Team is responsible for keeping logs of what issue was found and what steps were taken to rid the system of the problem. These logs shall be stored on a secure storage area on the OIIT network for review by the CISO and others within OIIT as needed.

Changing Passwords

OIIT will require users and/or system administrators immediately change their passwords on all affected systems and/or applications upon report or confirmation of a Security Incident.

Remedies

Non-compliance with this Procedure may be cause for disciplinary action up to and including termination for cause. Depending on the circumstances, federal or state law may permit civil or criminal litigation and/or restitution, fines, and/or penalties for actions that would constitute a violation of this procedure

Timeline

Effective Date: Upon Implementation

Review Date: Annually

Approvals

APPROVED AS TO OPERATING FORM

Signature:

Name/Title: **Tom West**
Chief Information Officer

APPROVED AS TO BUSINESS CONTENT

Signature:

Name/Title: **John Christly**
Chief Information Security Officer

APPROVED AS TO BUSINESS CONTENT

Signature:

Name/Title: **Lial Knight**
Sr. Exec. Dir-Infra, Ntwks, Fld Sv

APPROVED AS TO BUSINESS CONTENT

Signature:

Name/Title: **Chris Harrison**
Chief Technology Officer