FAU

FLORIDA ATLANTIC UNIVERSITY

Security Incident Procedures Policy

September 12, 2016

SCOPE

This policy applies to Florida Atlantic University's Covered Components and those working on behalf of the Covered Components (collectively "FAU") for purposes of complying with the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

POLICY

It is FAU's policy to rapidly identify and appropriately respond to all security incidents, regardless of their severity. FAU shall fully document all security incidents and its responses thereto.

REASON FOR POLICY

To establish procedures for reporting security incidents.

DEFINITIONS- Refer to Glossary and Terms

PROCEDURE

Incident Response Plan

FAU will adhere to its Security Incident Response Plan when dealing with suspected security incidents. A "Security Incident," in the context of this policy, is an attempt to gain unauthorized access to a system or data, unwanted denial of service to university resources, the unauthorized use of a system that processes or stores sensitive information, or an unauthorized disclosure or compromise of sensitive University data.

A Security Incident may involve any or all of the following (this list is illustrative only and does not include all possible Security Incidents):

- Unauthorized computer, device, network, systems, or data access;
- Presence of a malicious application, such as a virus or malware;
- Presence of unexpected/unusual programs;
- A denial of service condition against data, network, computer, or device;
- Physical or logical damage to systems;
- Theft, loss, or misplacement of a laptop or other device;
- Theft of sensitive electronic information;
- Cyber-extortion attempts; and
- Emergency disaster recovery operations that may have comprised security controls.

An Incident Response Plan ("IRP") is a set of written instructions for adequately identifying, containing, remediating, and reporting an information security incident, or an event that may be an attack or threat to FAU's data security.

FAU's IRP incorporates the following elements to handle Security Incidents:

(1) Preparation;
(2) Identification;
(3) Containment;
(4) Remediation;
(5) Recovery; and
(6) Process Improvement.

1. FAU will assess and respond to Security Incidents. All Security Incidents should be immediately reported to the University Information Security Officer who shall take appropriate action and notify the University Chief Compliance Officer and Chief Information Officer. If the University Information Security Officer is not available, the suspected incident should be reported to the Chief Information Officer or the Chief Technology Officer.

2. In accordance with OIT Security Incident Response Procedures and applicable laws, regulations and policies, breaches involving sensitive information will be reported by the Chief Information Officer and the Chief Compliance Officer in consultation with the University General Counsel's Office.

3. In addition, persons learning of a potential security incident should notify the Office of Information Technology at 561-297-3440 and report basic details of the security incident and leave contact information. The University Information Security Officer will maintain a log of security incidents ("Security Incidents Log"). The University Information Security Officer will investigate and resolve the issue in conjunction with the OIT and consult with the Chief Compliance Officer and the General Counsel's Office as appropriate based on the incident. The Security Officer will document the incident follow-up and resolution in the Security Incidents Log, including the remediation to resolve the issue. The University Information Security Officer will meet and report on major security incidents, if any, to the Chief Compliance Officer within 30 days of remediation in order to review and ensure timely resolution of Security Incidents taking into account the six (6) elements of the IRP listed above.

4. Appropriate responses to security incidents may include, but are not limited to:

   - Rapidly identifying and classifying the severity of security incidents.
   - Determining the actual risk to individually identifiable health information, and the subject(s) thereof.
   - Repairing, patching, or otherwise correcting the condition or error that created the security incident.

- Retrieving or limiting the dissemination of individually identifiable health information, if possible.
- Mitigating any harmful effects of the security incident.
- Fully documenting security incidents, along with their causes and FAU’s responses.
- Expanding FAU’s knowledge of security incident prevention, through research, analyses of security incidents, and improved training and awareness programs for workforce members.