| | |
|---|---|
| Policy Name | Information Security Incident Response Plan (IRP) |
| Policy Number | 50000.013 |
| Effective Date | March 29, 2019 |
| Administrative Division | Division of Academic Affairs |
| Unit | Department of Information Technology |
| Revised Date | March 29, 2019 |

1.0 Policy Statement

This plan outlines the steps to follow in the event secure data is compromised and identifies and describes the roles and responsibilities of the Incident Response Team ("IRT"). The Incident Response Team is in charge of activating this plan in the event a data breach occurs.

2.0 Purpose

The purpose of this policy is to establish the requirement that all business units supported by the IRT develop and maintain a security response plan. This ensures that the security incident management team and IRT has all the necessary information to formulate a successful response should a security incident occur.

3.0 Definitions

Incident Response Team ("IRT") - The Incident Response Team's mission is to prevent a serious loss of profits, public confidence or information assets by providing an immediate, effective and skillful response to any unexpected event involving computer information systems, networks or databases. The Incident Response Team is authorized to take appropriate steps deemed necessary to contain, mitigate or resolve a computer security incident.

Intellectual Property ("IP") – refers to the creation of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce.

National Incident Management System ("NIMS") – provides a consistent nationwide template to enable partners across the Nation to work together to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity.

Security Incident - is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; interference with information technology operations; or significant violation of responsible/acceptable use policy.

Personally Identifiable Information ("PII") - is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

Protected Health Information ("PHI") - is any information about health status, provision of health care, or payment for health care that is created or collected by Jackson State University ("JSU" or "University") (or a Business Associate of Jackson State University), and can be linked to a specific individual.

Data Breach - is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve PHI, PII, trade secrets or intellectual property.

Sensitive Data - data that is encrypted or in plain text and contains PII or PHI data.

Trade Secrets – any confidential business information which provides and enterprise a competitive edge.

4.0 Employee Adherence

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle PII or PHI of Jackson State University including any agreements with vendors.

5.0 Policy

The Chief Information Officer (CIO) will chair the Incident Response Team to handle the breach or exposure.

As soon as a theft, data breach exposure of Jackson State University's protected/sensitive data is confirmed, the CIO will be notified of the theft, breach or exposure. IT, along with the designated forensic team, will analyze the breach or exposure to determine the root cause.

The Incident Response Team includes members from:

- IT Infrastructure - Networking
- IT Information Security
- Finance (if applicable)
- Legal
- University Communications
- Alumni Relations (if applicable)
- Human Resources
- The affected unit/department that uses the involved system whose data may have been breached or exposed
- Additional departments based on the data type involved, additional individuals as deemed necessary by the CIO.

**Work with Forensic Investigators**

Jackson State University's insurer will be provided access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

**Develop a communication plan.**

IT will work with University Communications, the Division of General Counsel and Human Resources to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

**Ownership and Responsibilities**

Roles & Responsibilities:

- **Sponsors** are those members of the Jackson State community that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any Jackson State Executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.

- **Information Security Administrator** is that member of the Jackson State community, designated by the CIO, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.

- **Users** include virtually all members of the Jackson State community to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees and volunteers.
- **The Incident Response Team** shall be chaired by The CIO and shall include, but will not be limited to, the following departments or their representatives: IT-Network, IT-Information Security; University Communications; Legal; Management; Financial Services; Human Resources.

6.0 Policy Compliance

Any Jackson State University personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third party partner company found in violation may have their network connection terminated/contract cancelled and subject to prosecution to the fullest extent of the law.

7.0 Related Standards, Policies, and Processes

- Acceptable Use Policy, 50000.002
- Business Continuity Plan, 50000.005
- Data Security Policy, 50000.008
- Disaster Recovery Plan, 50000.015
- IHL Policies and Bylaws, Section 711.08 Incident Preparedness Plan (November 15, 2018)
- JSU Faculty Handbook, Campus Safety (December 1, 2011)
- JSU Faculty Handbook, Responsibilities during Campus Emergencies (December 1, 2011)

8.0 Revision History

- Created: November 15, 2016
- Revised: February 13, 2018
- Revised: March 29, 2019