JACKSONVILLE STATE UNIVERSITY

Manual of Policies and Procedures

POLICY NO.: VII:06 **DATE: April 2021**

REVIEW/REVISION DATES: TBD

SUBJECT: Incident Response

APPROVED: Dr. Don C. Killingsworth, Jr., President

PURPOSE

This policy provides Jacksonville State University (JSU) with processes and procedures to properly identify and handle incidents that may affect the safety and/or security of any system.
'Security incident' refers to any incident (accidental, intentional, or deliberate) relating to JSU communications or information processing systems. The attacker could be a malicious stranger, a competitor, or a disgruntled employee, and their intention might be to steal information or money, or just to damage JSU.

POLICY

Indications and Symptoms

Employees of JSU will be expected to report to the University's Information Security Officer for any security-related issues. The use of audit logs, as well as complaints about systems could be symptoms of an attack could be used to identify incidents. Look for any of these symptoms:

- System crashes.
- New user accounts (for example, the account RUMPELSTILTSKIN has been unexpectedly created), or high activity on a previously low usage account.
- New files, usually with novel or strange file names, such as data.xx or k or .xx.
- Accounting discrepancies.
- Changes in file lengths or dates (a user should be suspicious if .EXE files have unexplainably grown by over 1800 bytes).
- Attempts to write to the system.
- Data modification or deletion (files start to disappear).
- Denial of service.
- Unexplained, poor system performance.
- Anomalies ("GOTCHA" is displayed on the screen, or there are frequent unexplained "beeps").
- Suspicious browsing.
- Inability of a user to log in due to modifications of his/her account.
- Unauthorized software

Response

JSU's Security Incident Response plan is as follows:
1. Each department must report a security incident to the Office of Information Security.

2. The member of the team receiving the report will advise the Response Team of the incident.
3. The Information Security Response Team will investigate the incident and assist the potentially compromised department in limiting the exposure of data and in mitigating the risks associated with the incident.
4. The Information Security Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties. This can include credit card associations, credit card processors, etc,. as in a case involving PCI data.
5. The Information Security Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future and whether additional safeguards are required in the environment where the incident occurred or for the institution.
6. A department that reasonably believes it may have an account breach or a breach of cardholder information for of systems related to the PCI environment in genera, must inform the Information Security Response Team. After being notified of a compromise, the Information Security Response Team, along with other designated staff, will implement the Information Security Incident Response Plan.

In response to a system compromise, the Information Security Response Team will:
1. Ensure isolation of the compromised system(s) on/from the network.
2. Gather, review, and analyze the logs and related information from various central and local safeguards and security controls.
3. Conduct appropriate forensic analysis of compromised system.
4. Contact internal and external departments and entities as appropriate.
5. Make forensic and log analysis available to appropriate law enforcement or card industry security personnel, as required.
6. Assist law enforcement and card industry security personnel in investigative processes, including in prosecutions.

JSU Security Incident Response Team

- Chief Information Officer
- Information Security Officer
- Communications Director
- Compliance Officer
- University Counsel

- Other Business Services

Incident Response Notification

Escalation Members

- Escalation – First Level
    - Information Security Officer
    - University Counsel
    - Risk Manager
    - Director of JSU Communications

- Escalation – Second Level
    - JSU President
    - President's Cabinet
    - Internal Audit
    - Auxiliary members (as needed)

- External Contacts (as needed or in case of PCI incident)
    - Merchant Provider
    - Card Brands
    - Internet Service Provider (if applicable)
    - Internet Service Provider of Intruder (if applicable)
    - Communication Carriers (local and long distance)
    - Business Partners
    - Insurance Carrier
    - External Response Team as applicable (CERT Coordination Center 1, etc.)
    - Law Enforcement Agencies as applicable inn local jurisdiction

The Incident Response Plan must be tested annually. Copies of the Incident Response Plan will be made available to all relevant staff members and the JSU Security Response Team will take steps to ensure that all relevant staff members understand the plan and what is expected of them in the event of a security incident.

RESPONSIBILITY

The Vice President for Information Technology is responsible for this policy.

EVALUATION

This policy will be reviewed at least every five (5) years by the Vice President for Information Technology.