The University of JMTSJ Information Security Response Policy

Responsible Official: Chief Information Security Officer at JTMSJ University

Authors: Jon Whitehurst (Information Security Deputy), Joshua Zenker (Director of Compliance), Mushima Ngalande (Information Assurance Analyst), Shain Amzovski (Director of IS Internal Audit), Tamer Tayea (Senior Security Analyst)

Effective Date: October 9, 2015

Policy Sections

I. Purpose
II. Scope
III. Risk of Non-Compliance
IV. Policy
V. Roles and Responsibilities
VI. Definitions and Terms
VII. Policy Compliance
VIII. Revision History

I. Purpose:

The University of JMTSJ is formalizing the Information Security Response policy to provide assurance that security incidents will be handled in an effective and consistent manner. This policy provides a framework to ensure that security incidents are reported, identified, prioritized, investigated, and remediated in a timely and consistent manner. It establishes the incident communication procedure and governance framework for every step of incident management. It also identifies those responsible and accountable in the process of addressing security incidents.

This policy will apply to the entire University community which includes students, staff, faculty, third party vendors, consultants, and anyone affiliated to the university as it applies to any computing device connected to JMTSJNet either owned or leased by the University. It also applies to any device that holds University confidential data that if lost, or stolen, or compromised could lead to unauthorized access to data such as personal information, financial data, or intellectual property.

The goal of this policy is to ensure immediate response and mitigation of security incidents. This policy authorizes the office of the Chief Information Security Officer (CISO) to secure university resources that are actively threatened, however the office of the CISO will abide by this standard and the security response policy to mitigate the threat.

II. Scope:

The scope of the policy applies to all those using the University Information Technology resources or data. It applies to any electronic computing device and its data whether the device is used for testing, User Acceptance (UA), or for production. This will apply to any device regardless of who owns it. At a minimum, each IT department must have its own security response plan which complies with this policy.

III. Risk of Non-Compliance:

With the absence of an effective response strategy, corrective measures would inevitably be hindered and systems and people would be negatively impacted. Proper communication and documentation will provide key learning points in improving systems and data security. Those found to be non-compliant would be subject to penalties as outlined in the JMTSJ University policies.

IV. Policy:

A. Reporting

1. All users will be responsible for reporting security related events to the Help Desk. All university employees are expected to report any suspicious activities and/or unavailability of computer services like the University web portal to their immediate supervisor as soon as detected.

2. All Computer Services staff are expected to report any suspicious activities on University systems, networks, applications, IDS, or regular monitoring software to their immediate supervisor as soon as detected.

3. The Office of the CISO is responsible for reporting the event to upper management and law enforcement agencies as appropriate.

B. Triage and Classification

1. The Office of the CISO will perform the initial investigation of the reported event, analyze all facts collected at the time, and evaluate it regardless of whether it has caused damage to system/network or not. During the evaluation process, the Office will examine the event's impact, the potential for a data leakage, and the nature of the data compromised. The Office of the CISO will perform qualitative and quantitative risk assessment to damage reported by the event. It will consult with other relevant entities within the University as needed to complete the evaluation.

2. The Office of the CISO will classify the event as either an incident or not. If the event is classified as an incident, the Office will assign a severity rating (i.e. high, medium, or low) based on the incident type, the data leaked, and the extent of the breach.

3. The goal of triage is to categorize and prioritize the incident. During the triage stage, all data collected about the incident will be assessed, and the severity of the incident will be examined in a timely manner.

C. Communication

1. The Office of the CISO will determine how the Information Security team will respond and whom to contact about the incident. See example diagram for type of severity.

2. In the case of incidents that involve personal or financial information, the Help Desk will immediately notify the Office of the CISO, who will inform the President of the University. The Help Desk will be overseen by an executive team. For all incidents determined to have high impact, the Help Desk will notify the Office of the CISO and the Senior Director, who will handle them accordingly. For incidents determined to have medium impact, the Senior Director will be notified and handle them accordingly.

3. In the case of incidents determined to have low impact, the Manager-on-Duty will be notified and will handle them accordingly. All individuals involved in the incident will maintain confidentiality until the CISO allows disclosure of the details of the incident.

4. Incident updates will be periodically posted on the JMTSJNet portal under the "System Status" section (http://www.jmtsjuniv.edu/systemupdate.html). These updates are intended to keep the University community informed.

5. The CISO will keep log reported incidents including date, area(s) impacted by incident, severity rating of incident, and any other relevant information.

D. Incident Management

Once the triage stage concludes, an incident response plan will be created to address specific threats discovered during triage review. The incident response plan may vary from one incident to another based on specifics of the incident. The remediation plan timeline and actions will also vary depending on the nature of incident, the rate at which the investigation is progressing, and the type of IT asset at risk of being compromised.

1. Containment

The goal of containment is to limit exposure of systems/networks/data and isolate the problem. The extent of containment and defense posture activities will depend on the Office of the CISO's incident severity rating and the facts known about the incident at the time. The Incident Response Team (IRT) is authorized, under this policy, to disconnect any affected device from the network to assess or contain the vulnerability. The circumstances of incident detection will be documented, and evidence collected will be preserved for further incident investigation.

2. Eradication

IRT will develop an eradication action plan to remove the attacker's access to the environment and to mitigate the vulnerabilities the attacker used to gain and maintain unauthorized access to systems and/or data.

3. **Recovery**

   Information Security staff will return systems and networks to normal operations by using the established procedure for the systems' high availability setup and/or by restoring from verified backups.

4. **Postmortem**

   The Incident Response Team will develop comprehensive report of the incident, including analysis of what happened and when. The report may include suggested modifications to other IT policies that may help to avoid future incidents. It may include communication to University community with recommendations to avoid similar incidents. The postmortem review will include suggestions for incident response process improvement.

V. Roles and Responsibilities:

A. Incident Manager

Responsible for managing the response to a security incident in accordance with how the incident is classified in the Incident Severity Rating below. **I**ncident Manager is nominated by the Office of the CISO.

B. Incident Response Team

The IRT will oversee the management of security incidents involving confidential information. The team includes the members listed below:

IRT members may include the following:

- Incident manager (point of contact)
- Representative from IT Security office.
- Representative from Computer Services Systems and networks team.
- Representative from other technical teams to help with specifics like DBA/App Developer.
- Representative from Police/facilities
- Representative from Human Resource
- Representative from Communications team
- Representative from Legal Counsel.

Incident Severity Rating

The level of severity is determined by the impact to operations of the university and its data. It prioritizes the handling and management and response time to the associated incident.

A. High

This includes business-critical systems where an incident, such as a compromise can result with a critical service, privacy, financial, or reputation impact. These are threats that have adverse impact on a large number of systems and may also pose a threat to people's safety and security. The high impact threat can potentially replicate throughout systems causing on and off campus disruptions. Incidents with this severity level require immediate response.

Examples of incidents rated **High**:

- Security breach of financial data, research materials, and NPI on university, students, or employees.
- Active denial of service attack, total disruption of network connectivity
- Active virus spreading throughout compute environment with no known signature.
- Financial loss resulting in $1 million or greater.
- Unavailability of a critical University systems.

B. Medium.

This includes incidents with moderate service, privacy, financial, or reputation impact. Threatens to have an adverse impact on a modest number of systems and people. Limited to departments, buildings, individual systems. There is a moderate possibility of replication to other systems and disruptions on and off campus. Incidents with this severity level require a response time that is within two hours.

Examples of incidents rated as **Medium**:

- Computer/Server Vulnerability.
- Virus Alert
- Unable to provide core services to a select number of users, or able to provide core services but secondary services are unavailable
- Exposure of data from 100 to 1,000 users, such as names and addresses
- Financial loss or impact from incident is between $100k and $1 million
- Negative media attention results from incident, or negative view of department from Board of Trustees

C. Low.

This includes incidents with minor service, privacy, financial, or reputation impact. Threatens to have an adverse impact on a small number of systems and people. Has very little probability of replicating to other systems and causing disruptions on and off campus. Incidents with this severity level require a response time that is within four hours.

Examples of incidents rated as **Low**:

- Computer infected with a non-spreading virus, or is not on network
- No effect on the University's ability to provide core services to users
- Exposure of personal data is limited to less than 100 users.

- Financial loss or impact due to incident is less than $20k
- Reputation loss to a specific department within the university, but does not have any public exposure
- Unauthorized access to a system not containing NPI

VI. Definitions and terms:

- **Security inciden**t: Any event that may cause disruption to a system, process or data availability in the day to day operations of the university. Any violation of computer security policies, acceptable user policies, or standard computer security practices is an incident.

These are subdivided into: Computer Security Incidence and Confidential Data Incidents

- **Computer Security Incident** is an event that threatens the integrity of university systems, applications data or network. These may include but not limited to computers infected with malware including a worm or virus, web attack including running malicious code, widespread unavailability of data, systems, networks due to natural events like power outages.
- **Confidential Data Incident** is an event that threaten the integrity and privacy of confidential university data. This may include unauthorized access to data including leakage of Personally identifiable information, loss of data confidentiality or integrity

- **University Systems**: Electronic Device: Tablet, workstation, laptop, servers, printers, telephones, pagers, radios, network lines, personal digital assistants, E-mail and Web-based services

- **Personal Identifiable information** - This information includes names, address and social security number to name a few. This does not include information that is made available to the general public

- **User Acceptance (AU)** - These are rules and guidelines set forth by JMTSJ University on the way University systems may be used.

- **NPI**: Any nonpublic personal information like SSN.

- **User**: Any JMTSJ University student, faculty, staff, contractor, consultant or an agent of any the mentioned.

- **JMTSJNet** : JMTSJ University Data and Systems network.

- **IDS:** Intrusion Detection System.

- **IT Asset**: a system or systems comprised of computer hardware, software, networking equipment, as well as any data on those systems. Includes University systems.

- **Information Security Team**: Includes management level and technical staff assigned by the CISO to perform initial assessment of an abuse incident and to determine whether the incident requires a formal response.

- **IRT** : Incident Response Team
- **Security Breach**: The unauthorized access of computerized data that compromises the security, confidentiality or integrity of personal identifiable information.

VII. Policy Compliance

The policy will be reviewed every six months and updated accordingly. A revision record will be recorded when reviewed and if any changes were made.

VIII. Revision History

Version	date	Authors	Description
1	10/03/2015	InfoSec Team	Initial Document
1.5	10/05/2015	InfoSec Team	Refined Policy Statements and add incident ratings
2	10/08/2015	InfoSec Team	Final revision approved by CISO.