Cybersecurity Incident Response Plan

1. Introduction

This Cybersecurity Incident Response Plan (CSIRP) outlines the procedures and responsibilities for responding to cybersecurity incidents within the library. The goal is to minimize damage, restore services, and protect sensitive information. Our patron information is maintained by OSL (Ocean State Libraries). Working in collaboration with OSL, staff are required to undergo cybersecurity training. OSL also provides technical support for unusual incidents.

2. Incident Response Team

The Incident Response Team (IRT) is responsible for managing cybersecurity incidents.

Role	Responsibility	Contact
IRT Lead	Overall incident management and decision-making	Director of the Library
IT Manager	Technical lead, system recovery, and forensic analysis	Head of Youth Services
Communications Officer	Internal and external communications	Director and Department Heads
Legal Counsel	Legal guidance and compliance	Vacant
Public Relations	Media relations and public statements	Department Heads

3. Incident Classification

Cybersecurity incidents will be classified based on their severity and potential impact.

- **Low Severity:** Minor service disruptions, unauthorized access attempts without data compromise.

- **Medium Severity:** Moderate service disruptions, potential data compromise, or unauthorized access to non-critical systems.
- **High Severity:** Significant service outages, confirmed data breaches involving sensitive information, or compromise of critical infrastructure.
- **Critical Severity:** Catastrophic service failure, widespread data loss, or compromise of multiple critical systems with high public impact.

4. Incident Response Phases

4.1. Preparation

- **Training:** Regular cybersecurity awareness training for all staff is provided by OSL
- **Tools and Resources:** Ensure necessary tools for incident detection, analysis, and recovery are available.
- **Documentation:** Maintain up-to-date documentation of systems, networks, and data.
- **Backups:** Regular backups of critical data and systems.
- **Contact List:** Maintain an up-to-date contact list for the IRT and external stakeholders.

4.2. Detection and Analysis

1. **Identify Incident:** Staff or automated systems detect unusual activity.
2. **Initial Assessment:** The Director and Department Heads along with support from OSL conducts an initial assessment to determine the nature and scope of the incident.
3. **Log Analysis:** Review system logs, network traffic, and security alerts to gather information.
4. **Verification:** Confirm the incident and classify its severity.

4.3. Containment, Eradication, and Recovery

1. **Containment:** Take immediate steps to limit the spread of the incident. This may include isolating affected systems or networks.
2. **Eradication:** Remove the cause of the incident (e.g., malware, vulnerabilities).
3. **Recovery:** Restore affected systems and data from backups. Verify full functionality and security.

4.4. Post-Incident Activities

1. **Lessons Learned:** Conduct a post-incident review meeting with the IRT to discuss what went well and what could be improved.

2. **Reporting:** Document the incident, the response, and the lessons learned in an incident report. This report should be submitted to OLIS and OSL
3. **Policy Updates:** Update security policies and procedures based on the lessons learned.

5. Communication Plan

Effective communication is crucial during an incident.

- **Internal Communication:**
    - Inform relevant staff members about the incident's status and impact.
    - Regular updates provided by the Director
- **External Communication:**
    - **Patrons:** If patron data is affected, notify them as required by law. OSL will manage public statements.
    - **Law Enforcement:** Notify law enforcement if required by law or if the incident involves criminal activity.
    - **Vendors:** Coordinate with third-party vendors if their systems are involved or affected.