USAO Incident Response Plan

1. Overview

The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to safeguard sensitive customer information and respond effectively to incidents involving unauthorized access to or use of this information. This Incident Response Plan (IRP) outlines the necessary procedures to detect, respond to, mitigate, and recover from security incidents, in accordance with GLBA requirements.

2. Objectives

- Ensure timely detection and appropriate responses to security incidents involving non-public customer information.
- Mitigate the impact of the incident and prevent further unauthorized access or damage.
- Notify affected parties and regulatory bodies in accordance with applicable laws and regulations.
- Document the incident and response efforts to comply with GLBA and ensure continuous improvement.

3. Scope

This IRP applies to all employees, contractors, and third-party service providers who handle or have access to non-public customer information. It addresses any incidents that could result in the unauthorized access, disclosure, misuse, modification, or destruction of sensitive data.

4. Definitions

- **Incident**: An event that poses a potential or actual threat to the confidentiality, integrity, or availability of non-public customer information.
- **Non-public Customer Information**: Personally identifiable financial information provided by a customer or obtained in connection with providing a financial service.
- **GLBA**: Gramm-Leach-Bliley Act, which mandates that financial institutions safeguard sensitive information.

5. Roles and Responsibilities

Incident Response Team (IRT)

The IRT is responsible for managing all aspects of the incident. The team consists of key personnel from IT, and relevant business units.

- **Incident Response Coordinator**: Leads the response efforts, coordinates communication, documents progress in real-time, and reports to senior management. This role is filled by the Director of IT.
- **IT Team**: Investigates the technical aspects, identifies vulnerabilities, and assists in containment and recovery efforts. Ensures business operations are maintained or restored quickly and effectively during an incident.
- **President's Leadership Team**: Coordinates notifications to affected parties and regulatory bodies.

6. Incident Classification

Incidents are classified into different categories based on the potential impact:

- **Low**: Minimal or no impact on the confidentiality, integrity, or availability of customer information.
- **Medium**: Moderate impact with a limited number of records exposed or systems affected.
- **High**: Significant impact, potentially involving large-scale exposure of sensitive data or a critical system compromise.

7. Incident Detection and Reporting

- **Monitoring**: Continuous monitoring of systems and networks for signs of suspicious activity, using automated tools such as intrusion detection systems (IDS), firewalls, and logs. Current software used for this on all campus computers (including servers) is **Huntress EDR**.
- **Employee Awareness**: All employees are trained to recognize and report potential security incidents to the IRT immediately.
- **Third-Party Reporting**: Any third-party service provider handling sensitive data must report any incidents involving unauthorized access to the IRT.

8. Incident Response Phases

Phase 1: Preparation

- **Security Awareness Training**: Regular training for employees on identifying phishing, social engineering, and other attack vectors.
- **Data Classification**: Ensure all sensitive data is identified, labeled, and protected according to its sensitivity.
- **Testing and Drills**: Periodic testing of the Incident Response Plan through simulations and tabletop exercises.

Phase 2: Identification

- **Assess Incident**: Determine whether an event qualifies as a security incident. If customer information has been accessed, used, or disclosed without authorization, it is classified as an incident under GLBA.
- **Escalation**: Based on severity, notify the IRT, senior management, and relevant regulatory bodies as necessary. Also open incident ticket and begin logging time and effort towards response and remediation.

Phase 3: Containment

- **Short-Term Containment**: Isolate affected systems to prevent further unauthorized access or damage. This would require contacting appropriate personnel at third-party vendor for affected systems.
- **Long-Term Containment**: Apply temporary fixes, such as blocking malicious IP addresses or disabling compromised accounts, to minimize damage while a full investigation occurs.

Phase 4: Eradication

- **Root Cause Analysis**: Identify the vulnerability or cause of the incident and remove the threat (e.g., patch systems, update security policies).
- **Remove Malicious Code**: If malware or unauthorized software was used, ensure it is removed from all affected systems.

Phase 5: Recovery

- **System Restoration**: Recover systems from clean backups and ensure they are fully operational and secure.
- **Monitor for Recurrence**: Ensure continued monitoring of affected systems for signs of further compromise.
- **Security Testing**: Perform vulnerability assessments or penetration testing to verify that the threat has been fully neutralized.

Phase 6: Notification

- **Customer Notification**: If customer information has been compromised, provide timely and clear communication to affected individuals, as required by GLBA.
- **Regulatory Notification**: Report the incident to federal or state regulatory bodies (e.g., the FTC) as required. Timelines for reporting will be based on current requirements for GLBA regulations.
- **Internal Notification**: Provide senior management with a comprehensive report on the incident and response efforts.

9. Post-Incident Activities

Incident Documentation

- **Record Keeping**: Maintain detailed records of the incident, including timeline, impact analysis, and response efforts. This documentation will assist in future investigations and compliance audits. The intent of this is to be done in real-time as appropriate.

After-Action Report

- **Incident Documentation**: A complete report documenting the disaster, the response actions, and the recovery process is created. This will include timelines, systems affected, customer data involved, and lessons learned.
- **Lessons Learned**: The DRT conducts a post-incident review to assess what went well and what could be improved. This includes reviewing recovery timelines, success of backup restoration, and compliance with GLBA.
- **Post Incident Review**: Steps for mitigation to prevent similar disaster in the future.

Audit and Compliance

- **GLBA Audits**: Conduct regular internal audits to ensure compliance with GLBA. Make any necessary adjustments based on findings.
- **Continuous Improvement**: Regularly update the IRP and train employees to ensure evolving threats and vulnerabilities are addressed.

10. Training and Awareness

- **Annual Training**: Ensure that all employees receive annual training on security practices, GLBA requirements, and incident response procedures.
- **Incident Simulations**: Periodically conduct incident simulations to test the readiness of the IRT and ensure the effectiveness of the IRP.

11. Review and Updates

This plan will be reviewed annually or after any major incident to ensure it remains up-to-date with GLBA requirements and industry best practices. Any changes will be approved by senior management and communicated to all relevant parties.

12. Contact Information

Incident Response Coordinator(s)

- **Primary:**
  Name: Adeel Siddiqui
  Email: asiddiqui@usao.edu
  Phone: 405-574-1319

- **Secondary:**
  Name: Tom Coker
  Email: tcoker@usao.edu
  Phone: 405-574-1359

Revision History:
Last updated – May, 2025