US Solutions Pvt Ltd. - Incident Response Policy

Document Control:

- **Version:** 1.0
- **Date Issued:** 2024-01-12
- **Author:** IT & Infosec Department - Michael Davies
- **Approved By:** Eleanor Vance, Chief Information Officer (CIO)
- **Effective Date:** 2024-02-08
- **Review Frequency:** Annually

1. Introduction

US Solutions Pvt Ltd. recognizes that security incidents are inevitable. This Incident Response Policy outlines the procedures for detecting, responding to, and recovering from security incidents to minimize their impact on our business operations and protect our information assets. All employees, contractors, and authorized users ("Users") are required to adhere to this policy.

2. Purpose

The purpose of this policy is to:

- Establish a structured approach to incident response.
- Minimize the impact of security incidents on business operations.
- Protect the confidentiality, integrity, and availability of Company data.
- Ensure compliance with applicable laws and regulations.
- Provide clear roles and responsibilities for incident handling.

3. Scope

This policy applies to all security incidents affecting Company systems, applications, and data, including but not limited to:

- Malware infections.
- Unauthorized access attempts.
- Data breaches.
- Denial-of-service attacks.
- Phishing attacks.
- Lost or stolen devices.
- Insider threats.

4. Incident Response Team (IRT)

- The Incident Response Team (IRT) is responsible for coordinating and managing incident response activities.
- The IRT comprises representatives from the IT & Infosec Department, Legal, Human Resources, and other relevant departments.
- The IRT will be led by the Incident Response Manager (currently Johnathan Rivers).
- The IRT will be available 24/7 for critical incidents.

5. Incident Response Phases

The incident response process consists of the following phases:

- **Preparation:**
  - Establishing incident response plans and procedures.
  - Developing communication protocols.
  - Providing security awareness training.
  - Maintaining up-to-date security tools and resources.
- **Detection and Analysis:**
  - Identifying and analyzing security incidents.
  - Gathering evidence and documenting findings.
  - Determining the scope and impact of the incident.
  - Utilizing security information and event management (SIEM) systems.
- **Containment:**
  - Isolating affected systems and networks.
  - Preventing the spread of malware or unauthorized access.
  - Implementing temporary security measures.
- **Eradication:**
  - Removing malware or other malicious code.
  - Patching vulnerabilities.
  - Restoring systems to a known good state.
- **Recovery:**
  - Restoring affected systems and data.
  - Verifying system functionality.
  - Returning to normal business operations.
- **Post-Incident Activity:**
  - Conducting a post-incident review.
  - Documenting lessons learned.
  - Updating incident response plans and procedures.
  - Implementing preventive measures.

6. Incident Reporting Procedures

- Users must immediately report any suspected security incidents to the IT department ([email address removed]) or the Incident Response Manager.
- Reports should include as much detail as possible, including the date, time, and nature of the incident.
- The IRT will acknowledge the report and initiate an investigation.

7. Incident Severity Levels

Incidents will be classified according to their severity:

- **Low:** Minor incidents with minimal impact on business operations.
- **Medium:** Incidents with a moderate impact on business operations.
- **High:** Critical incidents with a significant impact on business operations.
- **Critical:** Incidents that threaten the core business operations.

8. Communication Procedures

- The IRT will establish communication channels for internal and external stakeholders.
- Communication will be timely, accurate, and consistent.
- Public statements will be approved by the Legal and Communications departments.

9. Legal and Regulatory Compliance

- The IRT will ensure compliance with all applicable laws and regulations (e.g., GDPR, CCPA, PCI DSS).
- Data breaches will be reported to relevant authorities as required.
- Evidence will be preserved for legal proceedings.

10. Training and Awareness

- All Users will receive training on incident reporting procedures.
- Regular security awareness training will be provided to reinforce incident response best practices.
- The IRT will conduct regular drills and simulations.

11. Policy Review and Updates

- This policy will be reviewed and updated annually or as needed to reflect changes in technology, threats, and regulations.
- Any updates to this policy will be communicated to all Users.

12. Acknowledgement

- By accessing Company systems, applications, and data, Users acknowledge that they have read, understood, and agree to comply with this Incident Response Policy.

This Incident Response Policy is designed to ensure that US Solutions Pvt Ltd. can effectively respond to and recover from security incidents. By adhering to these guidelines, Users contribute to a secure and resilient work environment.