# Incident Response Plan for Spendology Solutions

***Purpose & Scope***

To provide a structured approach for detecting, responding, and recovering from security incidents at Spendology Solutions.

***Authority***

Approved by senior management for company-wide enforcement.

***Definitions***

- **Ransomware:** Malicious software that encrypts data and demands a ransom.
- **Sensitive Data Leak:** Unauthorized exposure of confidential data.
- **Malware:** Software designed to disrupt, damage, or gain unauthorized access.

***How To Recognize A Cyber Incident***

- Sudden system slowdowns, inaccessible data, or unusual activity.

***Cyber Security Incident Response Team (CSIRT)***

Key members include:

- **CISO**: Incident commander.
- **IT Security**: Responsible for containment and recovery.
- **Legal/Compliance**: Manage legal obligations and communications.

## Incident Types

1. **Ransomware**
2. **Sensitive Data Leaks**
3. **Malware**

## Incident Severity Matrix

| Severity | Impact | Response Time |
|---|---|---|

| | | |
|---|---|---|
| **High** | Data breaches affecting clients | Immediate |
| **Medium** | Isolated system issues | Within 1 hour |
| **Low** | Minor issues with no significant impact | Within 24 hours |

## Incident Handling Process

1. **Detection**
    - Monitor logs and alerts for suspicious activities.
2. **Assessment**
    - Determine the type and severity.
3. **Containment**
    - Isolate affected systems to prevent the spread.
4. **Eradication**
    - Remove malware, patch vulnerabilities.
5. **Recovery**
    - Restore affected systems from backups.
6. **Lessons Learned**
    - Review the incident and update policies as needed.

## Incident-Specific Handling Processes

***Ransomware***

1. **Isolate affected systems** immediately.
2. **Inform key stakeholders** using pre-defined communication protocols.
3. **Evaluate backups** and perform recovery steps without paying the ransom.
4. **Communicate with law enforcement**, if necessary.
5. **Review logs and systems** for vulnerabilities exploited.

***Sensitive Data Leaks***

1. **Detect** the leak through monitoring tools.
2. **Assess the scope**, determining the type of data and the potential impact.
3. **Notify affected parties** (internal and external) as per legal requirements.
4. **Seal the breach** and implement measures to prevent further leaks.
5. **Coordinate with legal and PR** for external communications.

***Malware***

1. **Identify the infected system** through endpoint detection.
2. **Contain the malware** by disconnecting the infected machine from the network.
3. **Run anti-malware scans** to identify and remove the malware.
4. **Patch vulnerabilities** to prevent re-infection.
5. **Notify relevant stakeholders** and update the incident log.

## Testing & Review Cycle

- **Quarterly drills** simulating ransomware, data leaks, and malware infections.
- **Annual review** of the IR plan to incorporate new threats.

## References


- **AWS Security Best Practices**
- **NIST Cybersecurity Framework**