# Rove Incident Response Plan (IRP)

### Company Overview

- **Company Name**: Rove
- **Industry**: Commercial Flight
- **Size**: Medium Enterprise with 450 employees
- **Key Departments**: IT, HR, Legal, Sales, Customer Support
- **Stakeholders**: CEO, CFO, CTO, All IT staff, All HR staff

---

## 1. IRP Overview

The Incident Response Plan (IRP) for Rove is designed to ensure a swift and effective response to security incidents, minimizing impact and safeguarding company assets. The plan outlines the procedures for detecting, analyzing, containing, eradicating, and recovering from incidents, as well as the process for continuous improvement.

### 1.1 Objectives

- Minimize damage from security incidents.
- Restore normal operations as quickly as possible.
- Learn from incidents to prevent future occurrences.

### 1.2 Scope

The IRP covers all systems, networks, and data within Rove's operations. It applies to all employees and stakeholders involved in the incident response process.

---

## 2. Incident Response Team (IRT)

- **Roles and Responsibilities**: The IRT consists of key stakeholders and IT staff who are responsible for managing and executing the IRP. Roles include Incident Coordinator, Security Analyst, Forensic Analyst, Communications Officer, and Legal Advisor.
- **Contact Information**: The contact list includes phone numbers, email addresses, and emergency contact details for key stakeholders. This list is stored in both printed form and a secure cloud location.

# 3. Incident Handling Steps

## 3.1 Detection and Analysis

- **Detection**: Incidents are detected using Splunk, which monitors and detects security threats.
- **Analysis**: When an incident is detected, it is automatically escalated to the security team. The team analyzes the incident to determine its source, cause, and scope of affected systems.
- **Incident Classification**: Incidents are classified by severity:
    - **Low Severity**: Minor incidents with little to no impact.
    - **Medium Severity**: Incidents with moderate impact, contained quickly.
    - **High Severity**: Significant incidents affecting multiple systems.
    - **Critical Severity**: Major incidents causing widespread disruption.

## 3.2 Containment

- **Isolation**: Affected systems are removed from the network to isolate the threat.

## 3.3 Eradication

- **Malware**: Removed from the affected systems.
- **Vulnerabilities**: Patched to close security gaps.

## 3.4 Recovery

- **Malware**: Systems restored from the last known incremental backup.
- **Vulnerabilities**: New backups created after patching.

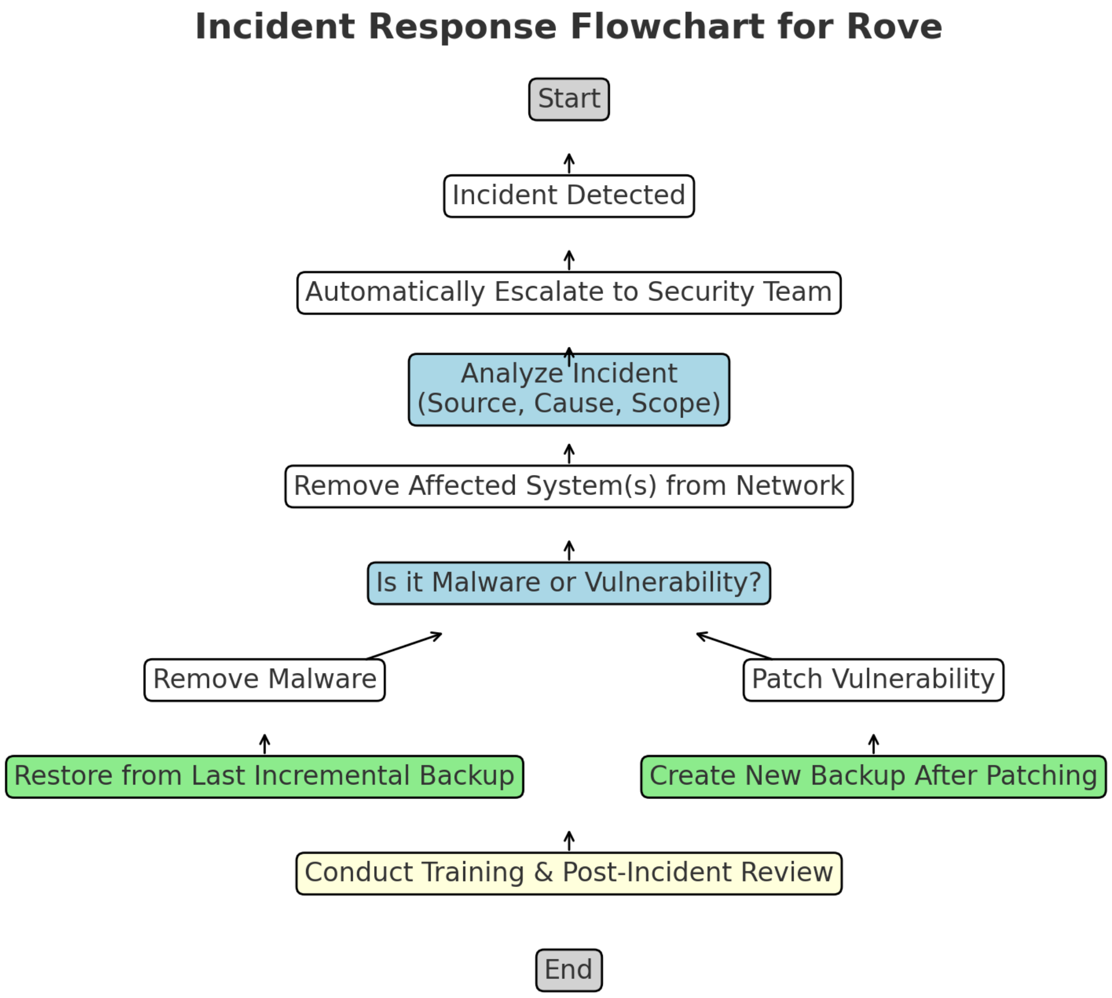
## 3.5 Post-Incident Activity

- **Training and Reviews**: Lessons learned are incorporated through training sessions and post-incident reviews.

# 4. Supporting Documentation

## 4.1 Incident Response Flowchart

A visual representation of the incident handling process, detailing each step from detection to post-incident activity.


Incident Response Flowchart for Rove
Start
Incident Detected
Automatically Escalate to Security Team
Analyze Incident (Source, Cause, Scope)
Remove Affected System(s) from Network
Is it Malware or Vulnerability?
Remove Malware
Patch Vulnerability
Restore from Last Incremental Backup
Create New Backup After Patching
Conduct Training & Post-Incident Review
End

## 4.2 Checklists

Checklists are provided for each phase of the incident response process:

### 1. Detection and Analysis Checklist

- ☐ **Receive Incident Alert**: Ensure the incident is automatically escalated to the security team.
- ☐ **Analyze Logs in Splunk**: Review relevant logs and alerts in Splunk to identify the source, cause, and scope of the incident.
- ☐ **Determine Incident Severity**: Classify the incident according to its severity (Low, Medium, High, Critical).

- □ **Document Initial Findings**: Record the initial analysis, including the systems affected and the nature of the threat.
- □ **Notify Stakeholders**: Inform key stakeholders (e.g., CTO, IT team) about the incident, its classification, and the next steps.

## 2. Containment Checklist

- □ **Isolate Affected Systems**: Remove the compromised systems from the network to prevent the spread of the incident.
- □ **Block Malicious IPs**: If applicable, block any identified malicious IP addresses at the firewall level.
- □ **Quarantine Infected Devices**: Move infected devices to a secure, isolated environment for further analysis.
- □ **Restrict Access**: Limit access to the affected systems to authorized personnel only.
- □ **Document Containment Actions**: Record all actions taken to contain the incident, including timestamps and personnel involved.

## 3. Eradication Checklist

- □ **Identify Root Cause**: Confirm whether the incident is caused by malware or a vulnerability.
- □ **Remove Malware**: If malware is detected, use appropriate tools to completely remove it from affected systems.
- □ **Patch Vulnerabilities**: If a vulnerability is identified, apply necessary patches to close the security gap.
- □ **Verify Eradication**: Run scans to ensure that the threat has been completely eradicated and no traces remain.
- □ **Document Eradication Process**: Record the steps taken to eradicate the threat, including tools used and verification results.

## 4. Recovery Checklist

- □ **Restore from Backup**: For incidents involving malware, restore systems from the last known incremental backup.
- □ **Create New Backup**: For incidents involving vulnerabilities, create a new backup after the patching process to avoid reintroducing the vulnerability.
- □ **Test Systems**: Ensure that restored or patched systems are functioning correctly and securely.
- □ **Reintegrate Systems**: Gradually reintegrate affected systems back into the network, monitoring for any signs of recurring issues.
- □ **Document Recovery Actions**: Record all recovery actions, including the date and time of restoration or patching and system verification results.

## 5. Post-Incident Activity Checklist

- ☐ **Conduct a Post-Incident Review**: Hold a meeting with the incident response team and key stakeholders to review what happened and how it was handled.
- ☐ **Identify Lessons Learned**: Discuss what went well and what could be improved in the response process.
- ☐ **Update Incident Response Plan**: Make any necessary updates to the Incident Response Plan based on lessons learned.
- ☐ **Provide Training**: Offer additional training to staff based on gaps identified during the incident.
- ☐ **Archive Incident Documentation**: Ensure all documentation related to the incident is securely stored for future reference and compliance purposes.

## 4.3 Incident Report Template

The incident report template includes the following sections:

## Incident Report Template

---

**Incident Report: [Incident Name]**

**Date of Report:** [Date]

**Reported By:** [Name]

---

## 1. Incident Summary

- **Date and Time of Incident:** [Date and Time]
- **Incident Type:** [e.g., Malware, Phishing, Unauthorized Access]
- **Incident Description:** Provide a brief description of the incident, including how it was discovered and by whom.

## 2. Timeline

- **Detection:**
  - **Date and Time:** [Date and Time]
  - **Details:** When and how was the incident detected?
- **Containment:**
  - **Date and Time:** [Date and Time]

    - **Details:** What actions were taken to contain the incident?
- **Eradication:**
    - **Date and Time:** [Date and Time]
    - **Details:** How was the threat removed?
- **Recovery:**
    - **Date and Time:** [Date and Time]
    - **Details:** When were systems restored to normal operation?
- **Post-Incident Review:**
    - **Date and Time:** [Date and Time]
    - **Details:** Summary of the post-incident review meeting.

## 3. Impact Assessment

- **Affected Systems:** List the systems, applications, or data that were impacted.
- **Business Impact:** Describe the operational impact of the incident, including any downtime, data loss, or financial cost.
- **Stakeholder Impact:** Identify any stakeholders affected by the incident and how they were impacted.

## 4. Actions Taken

- **Detection and Analysis:**
    - **Summary:** Detail the analysis process and findings.
- **Containment:**
    - **Summary:** Describe the actions taken to isolate the incident.
- **Eradication:**
    - **Summary:** Provide a detailed account of the steps taken to remove the threat.
- **Recovery:**
    - **Summary:** Describe the recovery process, including any system restorations or patches applied.

## 5. Lessons Learned

- **Successes:** What aspects of the response went well?
- **Challenges:** What challenges were faced during the response?
- **Recommendations:** What improvements or changes should be made to the Incident Response Plan?
- **Training Needs:** Identify any training or skill gaps that were revealed.

## Attachments

- **Supporting Documents:** Attach logs, screenshots, or other relevant documents that support the report.

# 5. Common Threats and Incident Scenarios

## 5.1 Common Threats

- Phishing Attacks
- Ransomware
- Insider Threats
- DDoS Attacks
- Data Breaches
- Advanced Persistent Threats (APTs)

## 5.2 Incident Scenarios

## 1. Phishing Attack Scenario

- **Scenario**: An employee at Rove receives an email that appears to be from a trusted vendor, asking them to click a link and update their account details. The link leads to a fake login page where the employee unknowingly enters their credentials, which are then stolen by attackers.
- **Response Steps**:
    1. **Detection**: The security team receives an alert from Splunk about unusual login attempts from the employee's account.
    2. **Containment**: The employee’s account is immediately disabled, and the security team resets the credentials.
    3. **Eradication**: The phishing email is analyzed, and similar emails are identified and removed from the company’s email system.
    4. **Recovery**: Affected systems are scanned for further compromise, and any unauthorized access is logged and reviewed.
    5. **Post-Incident**: Conduct phishing awareness training and review email security filters.

## 2. Ransomware Attack Scenario

- **Scenario**: Rove’s customer booking system is compromised by ransomware that encrypts critical customer data and system files. The attackers demand a ransom payment in cryptocurrency to decrypt the data.
- **Response Steps**:
    1. **Detection**: An alert is generated by Splunk when multiple files on the booking system are encrypted.

2. **Containment**: The affected system is removed from the network, and backups are verified to ensure they are not compromised.
3. **Eradication**: The ransomware is removed, and the origin of the infection is traced and closed (e.g., unpatched vulnerability or phishing).
4. **Recovery**: The booking system is restored from the last known clean backup, and normal operations are resumed.
5. **Post-Incident**: Review and update backup and patch management procedures to prevent future incidents.

## 3. Insider Threat Scenario

- **Scenario**: A disgruntled employee with elevated privileges intentionally deletes critical customer data before leaving the company.
- **Response Steps**:
  1. **Detection**: The security team detects unauthorized data deletion through Splunk's monitoring of unusual data access patterns.
  2. **Containment**: The employee's access is immediately revoked, and the data deletion process is stopped.
  3. **Eradication**: A forensic analysis is conducted to recover deleted data and identify any additional malicious activities by the insider.
  4. **Recovery**: Deleted data is restored from backups, and the employee's actions are documented for legal proceedings.
  5. **Post-Incident**: Review and strengthen access controls and monitoring for privileged accounts.

## 4. DDoS Attack Scenario

- **Scenario**: Rove's online booking system experiences a distributed denial-of-service (DDoS) attack, overwhelming the servers and making the website unavailable to customers.
- **Response Steps**:
  1. **Detection**: The IT team receives an alert from the monitoring system about an unusual spike in traffic targeting the booking system.
  2. **Containment**: Traffic filtering and rate-limiting measures are implemented to mitigate the attack.
  3. **Eradication**: The source of the attack is identified, and malicious IP addresses are blocked at the firewall.
  4. **Recovery**: The booking system is stabilized, and normal service is restored.
  5. **Post-Incident**: Review and enhance DDoS protection measures, including load balancing and traffic filtering strategies.

## 5. Data Breach Scenario

- **Scenario**: An attacker gains unauthorized access to Rove's customer database, exfiltrating sensitive customer information, including names, contact details, and payment information.

- **Response Steps**:
    1. **Detection**: An alert is generated by Splunk when unusual data export activity is detected.
    2. **Containment**: Access to the customer database is immediately restricted, and the affected account is disabled.
    3. **Eradication**: The vulnerability used to access the database is identified and patched, and any malicious code is removed.
    4. **Recovery**: Customer data is reviewed for integrity, and security measures are enhanced.
    5. **Post-Incident**: Notify affected customers and regulators, if required, and review database security protocols.

### 6. Advanced Persistent Threat (APT) Scenario

- **Scenario**: Rove is targeted by an APT group aiming to steal sensitive flight operation data and disrupt operations. The attackers use sophisticated tactics, including spear-phishing and zero-day exploits.
- **Response Steps**:
    1. **Detection**: Splunk detects a pattern of unusual behavior, including lateral movement between systems and attempts to exfiltrate data.
    2. **Containment**: The affected systems are isolated from the network, and a broader investigation is launched to assess the full extent of the compromise.
    3. **Eradication**: The security team coordinates with external experts to remove the APT, patch vulnerabilities, and enhance security measures.
    4. **Recovery**: Systems are restored, and additional monitoring is implemented to detect any lingering threats.
    5. **Post-Incident**: Conduct a thorough review of the attack, update incident response procedures, and improve threat intelligence and detection capabilities.

---

# 6. Testing and Training

## 6.1 Distribution

- **Access**: Only stakeholders and the IRP team have access to the full IRP. Employees receive a digital copy of the necessary steps to avoid incidents and handle compromises.
- **Acknowledgment**: Recipients must sign an acknowledgment in person to confirm understanding.
- **Review and Update**: The IRP is reviewed and updated quarterly, with additional updates triggered by significant incidents, changes in the threat landscape, or organizational changes. Senior management approves updates, and stakeholders are notified via email.

### 6.2 Training

- **Frequency**: Training is conducted every three months.
- **Format**: In-person sessions for stakeholders and the IRP team, online modules, and workshops for employees.

### 6.3 Testing

- **Methods**: Quarterly tabletop exercises and live simulations are conducted.
- **Scope**: Comprehensive testing of the entire IRP.
- **Post-Test Review**: Each test is followed by a review to evaluate the response, gather feedback, and document results.

---

## 7. Continuous Improvement

### 7.1 Post-Incident Reviews

- **Process**: Reviews include a timeline review, action analysis, and identification of gaps and successes. The review is conducted with the IRP team and stakeholders.
- **Reporting**: A formal report is created to document findings, followed by follow-up tests and analytics to ensure improvements are implemented.

### 7.2 Regular Updates

- **Frequency**: The IRP is reviewed and updated quarterly.
- **Triggers**: Updates are also triggered by significant incidents, changes in the threat landscape, and organizational changes.
- **Approval**: Senior management is responsible for approving updates.
- **Communication**: Updates are communicated to relevant teams and stakeholders via email.