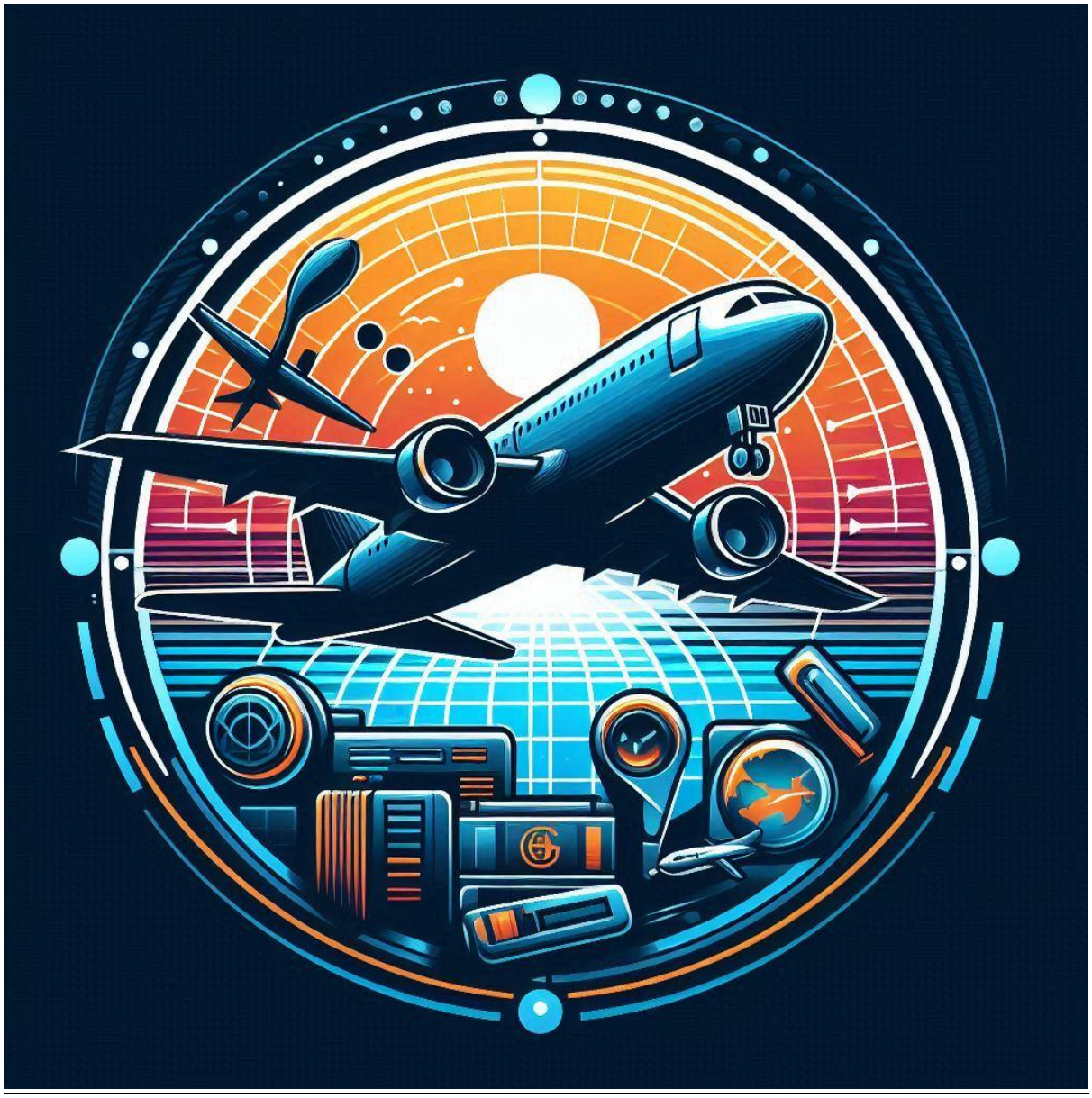

Aviata Airlines

Computer Incident Response Team (CIRT) Manual

Version: 1.0

Last Updated: 10/09/2022

Approved By: John Smith

Prepared By: Paul Jones

Table of Contents

6. Tools and Resources

   - Tools for Detection and Analysis

   - Resources and External Parties

7. Appendices

   - Incident Reporting Form

   - Incident Classification Matrix

   - System Logs

1. Introduction

Purpose

The purpose of this manual is to provide a structured framework for the Computer Incident Response Team (CIRT) to handle security incidents effectively. This document outlines the procedures for identifying, responding to, mitigating, and recovering from cybersecurity incidents.

Scope

This manual applies to all employees, contractors, and third-party vendors involved in the organisation's network, systems, or services. It covers incidents ranging from minor cybersecurity breaches to major incidents affecting critical infrastructure.

Objectives

- Detect and respond to cybersecurity incidents quickly and efficiently.
- Minimise damage to organisational assets and operations.
- Ensure compliance with legal and regulatory requirements.
- Document and learn from security incidents to prevent recurrence.

Definitions & Terminology

- Incident: Any event that may compromise the confidentiality, integrity, or availability of information systems.
- Breach: Unauthorised access to sensitive data or systems.
- CIRT: Computer Incident Response Team, tasked with handling cybersecurity incidents.

2. Incident Response Team (CIRT)

Roles and Responsibilities

Role	Responsibilities
CIRT Manager	Oversees incident response efforts and coordinates the team.
Incident Handler	Leads the technical investigation and directs containment efforts
Communications Lead	Manages communication between internal and external stakeholders.
Legal/Compliance	Ensures the response aligns with legal obligations.
Forensic Analyst	Collects and analyses evidence for investigation purposes.

Reporting Structure

CIRT reports directly to the Chief Information Security Officer (CISO) and works in conjunction with IT, Legal, and HR teams during incident handling.

3. Incident Response Lifecycle

The incident response process is divided into six phases:

3.1 Preparation

- Develop incident response policies and procedures.
- Implement tools for detecting, logging, and monitoring systems for anomalies.
- Train personnel and test incident response plans through tabletop exercises and simulations.

3.2 Identification

- Objective: Detect incidents and determine their nature and severity.
  - Use monitoring tools (e.g., IDS, SIEM) to identify suspicious activity.
  - Confirm whether an event qualifies as an incident.
  - Record essential details such as the time of detection, type of attack, affected systems, and potential damage.

3.3 Containment

- Objective: Prevent the spread of the incident and minimise impact.
  - Short-term containment: Isolate affected systems.
  - Long-term containment: Apply patches or reroute traffic to reduce future risks.
  - Create backups of affected systems for later analysis.

3.4 Eradication

- Objective: Remove the root cause of the incident.
  - Identify and eliminate all malicious components (e.g., malware, unauthorized access points).
  - Update security measures (e.g., patch vulnerabilities, remove malicious files).

3.5 Recovery

- Objective: Restore systems to normal operations.
  - Restore systems from clean backups.
  - Monitor for signs of recurring malicious activity.

- Verify that all systems are secure and functioning as intended.

3.6 Lessons Learned

- Objective: Review the incident for future improvements.

- Conduct a post-incident review to analyse the root cause, the effectiveness of the response, and what improvements can be made.

- Update policies, procedures, and incident response strategies.

4. Incident Handling Procedures

4.1 Incident Classification

Category	Description	Severity
Low	Minor incidents that do not compromise data integrity	Low
Medium	Incidents that could potentially harm systems or data	Moderate
High	Major incidents affecting business-critical operations	High

4.2 Incident Categories and Severity Levels

- Malware Infection: Viruses, worms, ransomware.
- Unauthorized Access: Compromised credentials, privilege escalation.
- Denial of Service (DoS): Disruptions to normal operations.
- Data Breach: Unauthorized access to sensitive data.

4.3 Initial Response

- Log all actions taken and record timestamps.
- Analyse initial information from detection tools.
- Notify CIRT members according to escalation procedures.

4.4 Communication Plan

- Notify affected stakeholders (management, employees, vendors, customers) promptly.
- Use secure channels for internal communication.
- Ensure legal and compliance teams are informed for regulatory reporting.

4.5 Escalation Procedures

- Low/Medium Severity: Handled by IT/CIRT, no immediate executive involvement.
- High Severity: Immediate notification to executive leadership and potential engagement of external forensics/legal experts.

5. Post-Incident Procedures

5.1 Documentation and Reporting

- Record all details about the incident, including logs, emails, and screenshots.
- Prepare a final report for management and regulatory bodies if required.

5.2 Post-Incident Review

- Conduct a meeting with all relevant stakeholders to review the incident.
- Identify weaknesses in the response process and recommend improvements.
- Update the response manual, security controls, or training if necessary.

5.3 Legal and Regulatory Compliance

- Ensure adherence to data breach notification laws (e.g., GDPR, HIPAA).
- Engage legal counsel to assess liabilities.

6. Tools and Resources

6.1 Tools for Detection and Analysis

- Intrusion Detection Systems (IDS): Snort

- Security Information and Event Management (SIEM): Exabeam Fusion

- Forensics Tools: Autopsy

6.2 Resources and External Parties

- Managed Security Service Provider (MSSP): **SecurityHQ** – help@securityhq.com

- Incident Response Retainers: **Rapid7** - analysts@rapid7.com

- Law Enforcement: **City of London Police** – cyber@cityoflondon.police.uk

7. Appendices

Appendix A: Incident Reporting Form

Field	Description
Date/Time Detected	[Insert Date/Time]
Incident Type	[Insert Type]
Affected Systems	[Insert Systems]
Actions Taken	[Insert Actions]
Incident Status	[Open/Closed]

Appendix B: Incident Classification Matrix

Severity	Impact	Response Time
Low	Minimal business impact	24 hours
Moderate	Moderate impact on operations	8 hours
High	Critical business services impacted	1 hour

Appendix C: System Logs

Upon analysis of network traffic, the following information has been established by the Network Security Monitoring (NSM) team at the MSSP:

“There has been typical network communication between airline check-in desks using 3 IP addresses which are 192.168.1.1, 10.0.0.5, 172.16.0.2; however there seems to be an unknown device connecting in externally from 203.0.113.5 which we are unable to trace. We have therefore placed this IP address on the rogue device blacklist until we can establish its origins.”

Some of the log files generated by the system are encoded using Base64, but this can easily be decoded using the following online tool:
https://www.base64decode.org/

The NSM team have also taken the following action to protect the system:

“As part of our initial actions we have locked down ports 21 (FTP) and 22 (SSH) to prevent external access. As a precaution we also closed ports 80 and 8080 as we were seeing a lot of data exfiltration on these.”