

Incident response plan, playbook, and policies

Lighthouse Labs



August 2, 2024

By: Curtis Crawford

Table of Contents

[BC Ferries Information Security Policies 2](#_Toc173524724)

[Network Monitoring Policy 2](#_Toc173524725)

[TLP Communication Policy 3](#_Toc173524726)

[Data Retention and Destruction Policies 4](#_Toc173524727)

[Log Retention Policy 5](#_Toc173524728)

[NIST RMF Integration Policy 6](#_Toc173524729)

[Incident Response Plan & Playbook 7](#_Toc173524730)

[NIST Incident Response Phases 8](#_Toc173524731)

[Incident Scenarios and Response Procedures 9](#_Toc173524732)

[Cybersecurity Breach 9](#_Toc173524733)

[Operational Failure 10](#_Toc173524734)

[Natural Disasters 11](#_Toc173524735)

[Terrorist Threats 12](#_Toc173524736)

[Marine Accidents 13](#_Toc173524737)

[Incident Reporting and Documentation 14](#_Toc173524738)

[Review and Continuous Improvement 14](#_Toc173524739)

[References 15](#_Toc173524740)

# BC Ferries Information Security Policies

## Network Monitoring Policy

**Objective:** To ensure continuous monitoring of BC Ferries’ network to detect and respond to potential security incidents promptly.

**Scope:** This policy applies to all network infrastructure and systems operated by BC Ferries, including servers, workstations, and network devices. It covers the continuous monitoring of network traffic, the use of monitoring tools, and the responsibilities of the Security Operations Center (SOC) personnel. The policy is designed to detect, analyze, and respond to security threats and ensure the integrity, availability, and confidentiality of BC Ferries’ information systems.

**Policy:**

1. **Monitoring Tools:**

Deploy advanced network monitoring tools like IDS (Intrusion Detection Systems) and SIEM (Security Information and Event Management) systems.

Ensure these tools are regularly updated and configured to detect the latest threats.

1. **24/7 Monitoring:**

Establish a Security Operations Center (SOC) that operates around the clock.

Staff the SOC with qualified security analysts and engineers.

1. **Alerts and Notifications:**

Configure automatic alerts for suspicious activities such as unusual login attempts, unexpected data transfers, and malware detection.

Ensure the alerts are sent to designated personnel for immediate action.

1. **Regular Audits:**

Schedule regular audits of the network monitoring processes to verify their effectiveness.

Ensure audits are conducted by both internal teams and external third-party auditors for impartial assessments.

## TLP Communication Policy

**Objective:** To standardize the communication of sensitive information using the Traffic Light Protocol (TLP).

**Scope:** This policy covers the use of the Traffic Light Protocol (TLP) for the communication of sensitive information within BC Ferries. It applies to all employees and contractors involved in the transmission, reception, and handling of information that requires confidentiality. The policy details the designation of TLP codes, secure communication channels, and training requirements to ensure the proper handling of sensitive information.

**Policy:**

1. **TLP Designation:**

Use TLP codes to classify information based on its sensitivity and intended audience.

Ensure that all sensitive communications are appropriately labeled with TLP codes.

1. **Communication Channels:**

Utilize secure communication channels, such as encrypted emails and secure messaging platforms, for transmitting TLP-designated information.

Ensure that TLP information is shared only with authorized personnel.

1. **Training:**

Conduct regular training sessions for staff to familiarize them with TLP codes and their proper usage.

Include scenarios and examples in training to illustrate correct and incorrect TLP usage.

1. **Compliance:**

Monitor communications to ensure compliance with TLP guidelines.

Enforce disciplinary actions for non-compliance and provide remedial training.

## Data Retention and Destruction Policies

**Objective:** To manage the retention and secure destruction of data in accordance with legal and regulatory requirements.

**Scope:** This policy applies to the retention and destruction of all types of data generated, collected, or stored by BC Ferries. It includes guidelines for establishing retention schedules, secure storage of data, approved destruction methods, and documentation of retention and destruction activities. The policy ensures compliance with legal and regulatory requirements and protects the organization from data breaches and loss.

**Policy:**

1. **Retention Schedule:**

Develop a data retention schedule specifying retention periods for different types of data (e.g., financial records, customer data, employee records).

Ensure the schedule complies with relevant legal, regulatory, and business requirements.

1. **Secure Storage:**

Store data securely using encryption and access controls to prevent unauthorized access.

Implement physical security measures for on-premises storage and use trusted cloud providers for remote storage.

1. **Destruction Methods:**

Use approved methods such as shredding, degaussing, and secure deletion tools to destroy data when it is no longer needed.

Ensure destruction methods are appropriate for the type of data and storage medium.

1. **Documentation:**

Maintain detailed records of data retention and destruction activities, including dates, methods used, and personnel involved.

Store these records securely for future reference and compliance audits.

## Log Retention Policy

**Objective:** To retain logs for a specified period to support security investigations and compliance requirements.

**Scope:** This policy covers the retention of logs related to system access, network traffic, application usage, and security events within BC Ferries. It applies to all systems and applications that generate logs and all personnel responsible for managing and accessing these logs. The policy defines retention periods, secure storage practices, and access controls to support security investigations and compliance requirements.

**Policy:**

1. **Log Types:**

Identify and categorize different types of logs, including system access logs, network traffic logs, application logs, and security event logs.

Ensure all relevant systems and applications are configured to generate these logs.

1. **Retention Period:**

Define retention periods for different log types based on legal, regulatory, and business requirements (e.g., retain security logs for 1 year, financial transaction logs for 7 years).

Regularly review and update retention periods to reflect changing requirements.

1. **Secure Storage:**

Store logs securely using encryption and access controls to prevent tampering and unauthorized access.

Implement redundant storage solutions to ensure log availability in case of hardware failure.

1. **Access Controls:**

Restrict access to logs to authorized personnel only, using role-based access controls (RBAC).

Monitor and audit access to logs to detect and respond to unauthorized attempts.

## NIST RMF Integration Policy

**Objective:** To integrate the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) into BC Ferries’ information security program.

**Scope:** This policy applies to the integration of the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) into BC Ferries’ information security program. It covers all information systems and personnel involved in risk management activities. The policy outlines the adoption of the NIST RMF, assessment and authorization processes, continuous monitoring, and training requirements to manage and mitigate risks effectively.

**Policy:**

1. **Framework Adoption:**

Adopt the NIST RMF as the foundational framework for risk management practices.

Ensure all risk management activities align with the NIST RMF.

1. **Assessment and Authorization:**

Conduct regular security assessments of information systems to identify and evaluate risks.

Obtain Authorization to Operate (ATO) for information systems, ensuring they meet security requirements.

1. **Continuous Monitoring:**

Implement continuous monitoring processes to track the effectiveness of security controls and identify changes in risk levels.

Use automated tools and techniques to support continuous monitoring activities.

1. **Training and Awareness:**

Provide comprehensive training on the NIST RMF to relevant personnel, including risk managers, security officers, and system administrators.

Foster a culture of risk awareness and proactive risk management across the organization.

# Incident Response Plan & Playbook

**Purpose and Objectives**

To establish a structured and systematic method of response to cybersecurity and operational incidents that minimise impact to services, protect data and maintain regulatory compliance.

**Scope**

Any employee, contractor, or third-party vendor of BC Ferries who engages in unethical, unlawful, or illegal behaviour while using BC Ferries’ information systems and operations will be held accountable.

**Definitions**

**Incident:** Any occurrence that compromises the confidentiality, integrity, or availability of information systems or operational services.

**Incident Response Team (IRT):** A group responsible for managing the response to security incidents.

**PII:** Personally Identifiable Information.

**Operational Failure:** Service failure due to technical breakdown, lack of crew or any other cause.

**Roles and Responsibilities**

**Policy Owner**

The IT Security Department is responsible for maintaining and updating this policy.

**Employees**

All employees must adhere to the policy and report any suspected incidents immediately.

**Incident Response Team (IRT)**

IRT executing IRT incident response procedures and coordinating with relevant departments to manage the incident.

## NIST Incident Response Phases

1. **Preparation:**

* Conduct regular risk assessments to identify potential threats and vulnerabilities.
* Develop and maintain an incident response plan detailing roles, responsibilities, and procedures.
* Train staff on incident response procedures through regular drills and simulations.

1. **Identification:**

* Continuously monitor systems using automated tools to detect potential security incidents.
* Ensure that all employees know how to recognize and report potential incidents to the Incident Response Team (IRT).

1. **Containment:**

* Implement short-term containment measures to limit the immediate impact of the incident, such as isolating affected systems.
* Develop and execute long-term containment strategies to prevent further damage and mitigate the risk of recurrence.

1. **Eradication:**

* Investigate the root cause of the incident to understand how it occurred.
* Remove threats from the environment, such as deleting malware, closing vulnerabilities, and applying security patches.

1. **Recovery:**

* Restore affected systems and services to normal operations, ensuring they are fully functional and secure.
* Validate system integrity and confirm that no threats remain in the environment.

1. **Post-Incident Activity:**

* Conduct a post-incident review to analyze the response and identify lessons learned.
* Update the incident response plan and related policies based on insights gained from the incident.
* Implement improvements to prevent similar incidents in the future.

# Incident Scenarios and Response Procedures

## Cybersecurity Breach

**Response Procedures:**

* 1. **Identification:**
* Monitor network traffic: Use IDS/IPS and SIEM tools to detect unusual activity such as abnormal data transfer rates, repeated failed login attempts, or unusual login times.
* Detect and report the breach: As soon as a potential breach is detected, SOC analysts must report it to the IRT immediately.
  1. **Containment:**
* Isolate affected systems: Disconnect compromised systems from the network to prevent the spread of malware or unauthorized access.
* Disable compromised accounts: Lock accounts that are suspected to be compromised to prevent further unauthorized access.
  1. **Eradication:**
* Remove malware or unauthorized software: Use antivirus and antimalware tools to scan and clean the affected systems.
* Patch vulnerabilities: Apply security patches and updates to eliminate vulnerabilities exploited during the breach.
  1. **Recovery:**
* Restore data from backups: Use clean and recent backups to restore any lost or corrupted data.
* Test systems for integrity: Ensure that systems are fully operational and free of malware before reconnecting them to the network.
  1. **Post-Incident Activity:**
* Conduct a forensic analysis: Analyze logs and other evidence to understand how the breach occurred and identify the attackers.
* Update security measures: Enhance security controls and policies based on the findings from the forensic analysis.

## Operational Failure

**Scenario:** Technical breakdowns or crew shortages causing disruption to ferry services.

**Response Procedures:**

* 1. **Identification:**
* Monitor operational systems and schedules: Use automated tools and manual checks to monitor ferry operations.
* Detect and report operational issues: Report any issues such as equipment failure or crew shortages to the IRT immediately.
  1. **Containment:**
* Reallocate resources: Use available resources to manage immediate service demands, such as reallocating crew members or using backup equipment.
* Communicate delays: Inform customers and stakeholders about service disruptions and expected delays through multiple channels.
  1. **Eradication:**
* Repair or replace faulty equipment: Conduct necessary repairs or replacements to restore operational capacity.
* Address staffing issues: Reassign staff or hire temporary crew to fill in shortages.
  1. **Recovery:**
* Resume normal operations: Ensure that ferry services are restored to their regular schedule.
* Ensure system functionality: Test all repaired or replaced equipment to ensure it is working correctly.
  1. **Post-Incident Activity:**
* Review incident: Analyze the operational failure to identify root causes and potential improvements.
* Update procedures: Modify operational procedures to prevent similar failures in the future.

## Natural Disasters

Scenario: Storms, earthquakes, or other natural events damaging infrastructure and disrupting operations.

**Response Procedures:**

* 1. **Identification:**
* Monitor weather alerts and geological activity: Use real-time monitoring tools and subscribe to alert services.
* Detect and report incidents: Report any natural disaster-related incidents to the IRT immediately.
  1. **Containment:**
* Evacuate and secure affected areas: Ensure the safety of passengers and crew by evacuating affected areas and securing ferry terminals.
* Redirect ferries: If necessary, reroute ferries to safer locations.
  1. **Eradication:**
* Assess and repair infrastructure damage: Coordinate with emergency services and repair teams to assess damage and begin repairs.
* Coordinate with emergency services: Work closely with local emergency services for additional support.
  1. **Recovery:**
* Restore ferry routes and schedules: Re-establish normal ferry routes and schedules as quickly as possible.
* Ensure safety: Conduct thorough safety checks to ensure the safety of passengers and crew.
  1. **Post-Incident Activity:**
* Conduct a damage assessment: Evaluate the extent of damage and the effectiveness of the response.
* Update emergency response plans: Revise emergency plans based on lessons learned from the incident.

## Terrorist Threats

Scenario: Threats or attacks targeting ferries due to high passenger volumes and profile.

**Response Procedures:**

* 1. **Identification:**
* Monitor for suspicious activities or threats: Use security surveillance and intelligence reports to identify potential threats.
* Report threats: Immediately report any threats to the IRT and law enforcement authorities.
  1. **Containment:**
* Secure ferry terminals and vessels: Implement security measures such as increased patrols, security checks, and restricted access.
* Implement lockdown procedures: If necessary, initiate lockdown procedures to protect passengers and crew.
  1. **Eradication:**
* Neutralize threats: Coordinate with law enforcement to neutralize the threat and ensure the safety of passengers and crew.
* Conduct security sweeps: Perform thorough security sweeps of all affected areas.
  1. **Recovery:**
* Restore ferry services: Resume normal ferry operations with heightened security measures in place.
* Communicate safety measures: Inform passengers about the safety measures taken and ensure their confidence in the security of the services.
  1. **Post-Incident Activity:**
* Review security protocols: Assess the effectiveness of current security protocols and identify areas for improvement.
* Update threat response strategies: Enhance strategies based on the incident review and latest threat intelligence.

## Marine Accidents

Scenario: Collisions, groundings, or onboard fires posing danger to passengers and crew.

**Response Procedures:**

* 1. **Identification:**
* Monitor vessel operations and emergency signals: Use real-time monitoring tools to detect operational anomalies.
* Report incidents: Report any marine accidents to the IRT and maritime authorities immediately.
  1. **Containment:**
* Evacuate passengers and crew: Follow emergency evacuation procedures to ensure the safety of everyone onboard.
* Contain and control the situation: Use onboard firefighting and emergency equipment to manage the situation.
  1. **Eradication:**
* Address the cause of the accident: Investigate and mitigate the root cause of the accident, whether it’s a collision, grounding, or onboard fire.
* Conduct repairs: Perform necessary repairs to ensure vessel safety and seaworthiness.
  1. **Recovery:**
* Resume safe ferry operations: Restore normal ferry operations after ensuring all safety measures are in place.
* Provide support: Offer assistance and support to affected passengers and crew, including medical care and counseling.
  1. **Post-Incident Activity:**
* Conduct a thorough investigation: Analyze the incident to understand what went wrong and how to prevent similar accidents.
* Implement safety improvements: Update safety procedures and protocols based on the findings from the investigation.

## Incident Reporting and Documentation

**Reporting**

All incidents must be reported to the IRT immediately.

Use the incident report form to document details.

**Documentation**

Maintain detailed records of each incident, including identification, containment, eradication, and recovery steps.

Store incident reports securely for future reference and compliance audits.

## Review and Continuous Improvement

**Regular Reviews**

Conduct annual reviews of the incident response playbook.

Update the playbook based on new threats, technologies, and lessons learned.

**Continuous Improvement**

Encourage feedback from employees and stakeholders.

Integrate feedback into incident response procedures to enhance effectiveness.

# References

(Compass | IR Plan, Playbook, and Policy). (n.d.). [PDF Document].

National Institute of Standards and Technology. NIST Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide. 2012. [www.nist.gov/csrc/publications/sp/800-61r2](http://www.nist.gov/csrc/publications/sp/800-61r2)

OWASP Foundation. (n.d.). OWASP Top Ten. Retrieved from <https://owasp.org/www-project-top-ten/>

SANS Institute. (2018). Incident Handler's Handbook. Retrieved from <https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>

GPT for Excel Word. (n.d.). Retrieved from <https://appsource.microsoft.com/en-sg/product/office/WA200005502?tab=Overview>

ISO/IEC 27035:2013 – Information technology – Security techniques – Information security incident management. International Organisation for Standardization (2013). Available at: <https://www.iso.org/standard/44379.html>

Information Systems Audit and Control Association (ISACA). 2012. Responding to Security Incidents. Online, available: <https://www.isaca.org/resources/isaca-journal/issues/2012/volume-3/responding-to-security-incidents>

Cisco Systems, Inc. (2015). Incident Response: Planning, Management, and Operations. Retrieved from <https://www.cisco.com/c/en/us/products/collateral/services/high-availability/white_paper_c11-732366.html>

Center for Internet Security. CIS Controls: A Guide for Securing Cyberspace. 2019. Retrieved from <https://www.cisecurity.org/controls/>

ChatGPT. (n.d.). Used at <https://chatgpt.com>

BC Ferries. (n.d.). Connecting the Coast. Retrieved from <https://www.bcferries.com/>

BC Ferry Authority. (n.d.). Retrieved from <https://www.bcferryauthority.com/>