

Incident response plan, playbook, and policies

Lighthouse Labs



August 24, 2002

By: Curtis Crawford

Contents

[BC Ferries Information Security Policies 2](#_Toc173489668)

[Network Monitoring Policy 2](#_Toc173489669)

[TLP Communication Policy 3](#_Toc173489670)

[Data Retention and Destruction Policies 4](#_Toc173489671)

[Log Retention Policy 5](#_Toc173489672)

[NIST RMF Integration Policy 6](#_Toc173489673)

[Incident Response Plan & Playbook 7](#_Toc173489674)

[NIST Incident Response Phases 9](#_Toc173489675)

[Supporting Policies 10](#_Toc173489676)

[**Communication and Training** 10](#_Toc173489677)

[Resources and Implementation 11](#_Toc173489678)

[Risks and Impact Assessment 11](#_Toc173489679)

[Legal and Regulatory Compliance 11](#_Toc173489680)

[Contact Information 11](#_Toc173489681)

[Incident Scenarios and Response Procedures 12](#_Toc173489682)

[Cybersecurity Breach 12](#_Toc173489683)

[Operational Failure 13](#_Toc173489684)

[Natural Disasters 14](#_Toc173489685)

[Terrorist Threats 15](#_Toc173489686)

[Marine Accidents 16](#_Toc173489687)

[Incident Reporting and Documentation 17](#_Toc173489688)

[Review and Continuous Improvement 17](#_Toc173489689)

[Conclusion 18](#_Toc173489690)

[References 19](#_Toc173489691)

# BC Ferries Information Security Policies

## Network Monitoring Policy

**Effective Date: Review:**

August 1, 2024 Annually

**Policy Owner: Approved by:**

IT Security Department Chief Information Officer

**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:** Utilize advanced network monitoring tools to oversee network traffic and identify anomalies.
2. **24/7 Monitoring:** Establish a Security Operations Center (SOC) that operates 24/7 to manage network monitoring.
3. **Alerts and Notifications:** Set up automatic alerts for suspicious activities and ensure timely notifications to the security team.
4. **Regular Audits:** Conduct regular audits of network monitoring processes to ensure effectiveness and compliance with regulatory standards.

## TLP Communication Policy

**Effective Date: Review:**

August 1, 2024 Annually

**Policy Owner: Approved by:**

IT Security Department Chief Information Officer

**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:** Label all communications involving sensitive information with appropriate TLP codes.
2. **Communication Channels:** Use secure communication channels for TLP

and TLP information.

1. **Training:** Provide regular training to staff on the use and importance of TLP in communications.
2. **Compliance:** Ensure compliance with TLP guidelines in all internal and external communications.

## Data Retention and Destruction Policies

**Effective Date: Review:**

August 1, 2024 Annually

**Policy Owner: Approved by:**

IT Security Department Chief Information Officer

**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 and maintain a data retention schedule that specifies retention periods for different types of data.
2. **Secure Storage:** Store data securely throughout its lifecycle to prevent unauthorized access.
3. **Destruction Methods:** Use approved methods for data destruction, including shredding, degaussing, and secure deletion.
4. **Documentation:** Maintain records of data retention and destruction activities.

## Log Retention Policy

**Effective Date: Review:**

August 1, 2024 Annually

**Policy Owner: Approved by:**

IT Security Department Chief Information Officer

**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:** Retain logs related to system access, network traffic, application usage, and security events.
2. **Retention Period:** Define retention periods for different log types based on legal, regulatory, and business requirements.
3. **Secure Storage:** Ensure logs are stored securely and protected from tampering.
4. **Access Controls:** Restrict access to logs to authorized personnel only.

## NIST RMF Integration Policy

**Effective Date: Review:**

August 1, 2024 Annually

**Policy Owner: Approved by:**

IT Security Department Chief Information Officer

**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 foundation for risk management practices.
2. **Assessment and Authorization:** Conduct regular security assessments and obtain authorizations to operate (ATO) for information systems.
3. **Continuous Monitoring:** Implement continuous monitoring processes to track security controls and risk levels.
4. **Training and Awareness:** Provide training on the NIST RMF to relevant personnel.

# Incident Response Plan & Playbook

**Effective Date: Review:**

August 1, 2024 Annually

**Policy Owner: Approved by:**

IT Security Department Chief Information Officer

**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

**Preparation**

Conduct regular risk assessments.

Develop and maintain an incident response plan.

Train staff on incident response procedures.

**Identification**

Monitor systems continuously using automated tools.

Report potential incidents to the IRT immediately.

**Containment**

Implement short-term containment measures to limit the impact.

Develop long-term containment strategies to prevent further damage.

**Eradication**

Investigate the root cause of the incident.

Remove threats from the environment.

**Recovery**

Restore affected systems to normal operations.

Validate system functionality and ensure no threats remain.

**Post-Incident Activity**

Conduct a post-incident review

Update the incident response plan based on lessons learned.

## Supporting Policies

**Data Protection Policy**

Ensure the protection of PII and sensitive data through encryption and secure handling practices.

**Access Control Policy**

Restrict access to critical systems and data to authorized personnel only.

**Communication Policy**

Communicate effectively and on time to stakeholders, including staff, customers and, where relevant, regulators.

## **Communication and Training**

**Internal Communication**

Communicate the incident response policy through memos, intranet postings, and departmental meetings.

**Training**

Conduct quarterly training sessions for employees on incident response procedures.

## Resources and Implementation

**Training**

The IT Security Department will conduct regular training sessions for all relevant personnel.

**Technology**

Employ IDS, IPS and incident response tools to handle and mitigate incidents.

**Personnel**

Engage a cybersecurity company or hire qualified staff to support the IRT.

## Risks and Impact Assessment

**Risks**

Increased workload on IT staff.

Potential resistance from employees to new procedures.

**Impact**

Improved security posture.

Better regulatory compliance.

Increased trust from stakeholders.

## Legal and Regulatory Compliance

This policy is compliant with the following standards and regulations: PCI DSS, PIPEDA, ISO/IEC 27001:2013, Coastal Ferry Services Contract.

## Contact Information

For questions or further information, contact the IT Security Department at [itsecurity@bcferries.com](mailto:itsecurity@bcferries.com).

# Incident Scenarios and Response Procedures

## Cybersecurity Breach

**Response Procedures:**

**Identification:**

Monitor network traffic for unusual activity.

Detect and report the breach to the IRT.

**Containment:**

Isolate affected systems.

Disable compromised accounts.

**Eradication:**

Remove malware or unauthorized software.

Patch vulnerabilities.

**Recovery:**

Restore data from backups.

Test systems for integrity.

**Post-Incident Activity:**

Conduct a forensic analysis.

Update security measures.

## Operational Failure

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

**Response Procedures:**

**Identification:**

Monitor operational systems and schedules.

Detect and report operational issues to the IRT.

**Containment:**

Reallocate resources to manage immediate service demands.

Communicate delays to customers and stakeholders.

**Eradication:**

Repair or replace faulty equipment.

Address staffing issues through reassignments or hiring.

**Recovery:**

Resume normal ferry operations.

Ensure all systems are functioning properly.

**Post-Incident Activity:**

Review incident for operational improvements.

Update procedures to prevent recurrence.

## Natural Disasters

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

**Response Procedures:**

**Identification:**

Monitor weather alerts and geological activity.

Detect and report incidents to the IRT.

**Containment:**

Evacuate and secure affected areas.

Redirect ferries and passengers to safe locations.

**Eradication:**

Assess and repair infrastructure damage.

Coordinate with emergency services.

**Recovery:**

Restore ferry routes and schedules.

Ensure passenger and crew safety.

**Post-Incident Activity:**

Conduct a damage assessment.

Update emergency response plans.

## Terrorist Threats

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

**Response Procedures:**

**Identification:**

Monitor for suspicious activities or threats.

Report threats to the IRT and law enforcement.

**Containment:**

Secure ferry terminals and vessels.

Implement lockdown procedures if necessary.

**Eradication:**

Neutralize threats with law enforcement assistance.

Conduct thorough security sweeps.

**Recovery:**

Restore ferry services with heightened security.

Communicate safety measures to passengers.

**Post-Incident Activity:**

Review security protocols.

Update threat response strategies.

## Marine Accidents

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

**Response Procedures:**

**Identification:**

Monitor vessel operations and emergency signals.

Report incidents to the IRT and maritime authorities.

**Containment:**

Evacuate passengers and crew as needed.

Contain and control the situation onboard.

**Eradication:**

Address and mitigate the cause of the accident.

Conduct repairs or salvage operations.

**Recovery:**

Resume safe ferry operations.

Provide support to affected passengers and crew.

**Post-Incident Activity:**

Conduct a thorough investigation.

Implement safety improvements.

## 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.

# Conclusion

In summary, BC Ferries' Network domains establish and enforces information security policies that ensure the protection of its network infrastructure, sensitive data, and operational integrity through information sharing and operational procedures. Specifically, this entails Network Monitoring, Capture and Forwarding, PII Access and Dissemination, TLP Communication, Data Retention and Destruction, Log Retention, NIST RMF Integration and Incident Response policies in relation to the BC Ferries' network.

Network traffic is constantly monitored, access controls on Personally Identifiable Information are stringent, and the communications protocol is standardised, for example. Rules pertaining to data retention and destruction and log management practices serve both compliance with regulatory requirements and aid in conducting investigations into security breaches.

All three standards have now been incorporated into the NIST Risk Management Framework (RMF), which is a standardised process for risk management that enables organisations to implement an effective approach to identify, assess and treat risks. The organisation also has in place an effective Incident Response Plan and Playbook to respond to security incidents, minimise their impact and restore normal operations as soon as possible.

Through these policies, we create a culture of security awareness among our staff and make sure that we’re constantly reviewing the policies and engaging in continual improvement. We regularly audit them for both our security group and the business units, and train internal and some external users. Audits are now included in contracts and engagements with our suppliers. We get them to go through audits with us to make sure their systems are secure and meet our requirements so that it can be integrated into ours. It’s a continual grasp of a moving target in the cybersecurity world.

*Taken together, these efforts build credibility with BC Ferries’ stakeholders to safely and reliably operate ferry service along the coast.*

# 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>

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. <https://www.cisecurity.org/controls/>

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

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