Curtis Crawford

Lighthouse labs

BC Ferries incident response playbook

**Incident Response Policy**

**Effective Date: Review:**

August 1, 2024 Annually

**Policy Owner: Approved by:**

IT Security Department Chief Information Officer

**1.1 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.

**1.2 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.

**1.3 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.

**2. Roles and Responsibilities**

**2.1 Policy Owner**

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

**2.2 Employees**

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

**2.3 Incident Response Team (IRT)**

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

**3. Incident Response Phases**

**3.1 Preparation**

Conduct regular risk assessments.

Develop and maintain an incident response plan.

Train staff on incident response procedures.

**3.2 Identification**

Monitor systems continuously using automated tools.

Report potential incidents to the IRT immediately.

**3.3 Containment**

Implement short-term containment measures to limit the impact.

Develop long-term containment strategies to prevent further damage.

**3.4 Eradication**

Investigate the root cause of the incident.

Remove threats from the environment.

**3.5 Recovery**

Restore affected systems to normal operations.

Validate system functionality and ensure no threats remain.

**3.6 Post-Incident Activity**

Conduct a post-incident review

Update the incident response plan based on lessons learned.

**4. Supporting Policies**

**4.1 Data Protection Policy**

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

**4.2 Access Control Policy**

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

**4.3 Communication Policy**

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

**5. Communication and Training**

**5.1 Internal Communication**

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

**5.2 Training**

Conduct quarterly training sessions for employees on incident response procedures.

**6. Resources and Implementation**

6.1 Training

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

6.2 Technology

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

6.3 Personnel

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

**7. Risks and Impact Assessment**

7.1 Risks

Increased workload on IT staff.

Potential resistance from employees to new procedures.

7.2 Impact

Improved security posture.

Better regulatory compliance.

Increased trust from stakeholders.

8. 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.

9. Contact Information

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

**10. Incident Scenarios and Response Procedures**

**10.1 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.

**10.2 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.

**10.3 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.

**10.4 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.

**10.5 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.

**11. Incident Reporting and Documentation**

11.1 Reporting

All incidents must be reported to the IRT immediately.

Use the incident report form to document details.

11.2 Documentation

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

Store incident reports securely for future reference and compliance audits.

**12. Review and Continuous Improvement**

12.1 Regular Reviews

Conduct annual reviews of the incident response playbook.

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

12.2 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>

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/>