SECURITY POLICIES

Presented by: Prinson D'silva

Note: This project was created for educational purposes only and is not affiliated with BC Ferries by any means.

WHY DO WE NEED POLICIES?

Protect

To protect company and customer data from Cyber attacks

Compliance

To align with government regulations such as PIPEDA

Respond

To ensure effective operation and swift recovery of sensitive data

THREE MAIN POLICIES

MALWARE DETECTION RESPONSE

Rapid containment, eradication, and recovery from ransomware attacks

DATA BREACH MANAGEMENT

Timely identification and notification of stakeholders during compromise of Personally Identifiable Information (PII)

LOG RETENTION

Guidelines for retaining logs upto 12 months, weekly reviews, and immediate forensic analysis

CORE MEMBERS INVOLVED

Incident Response

Monitoring the organization’s networks and systems for suspicious activity and identifying security incidents as they occur.

IT/ Networking

Managing and maintaining the organization’s networks, configuring security controls and monitoring network traffic.

Legal/ Compliance

Reviewing regulatory and legal obligations, handling notifications to authorities and overseeing compliance with data protection laws.

Communications Experts

Messengers for ensuring internal/external stakeholders, customers, and the public are informed in a timely and compliant fashion.

CONCLUSION

01 Policies ensure quick action and protect company as well as individuals from facing non-compliance disciplinary actions.

02 Protect sensitive data which could otherwise result in legal and reputational damage of the organization.

03 Promote teamwork resulting in minimal disruptions, secure operations and trust.