Information Security Program

Risk Assessment Report

The Government of British Columbia

# GROUP 3 CONTACTS

|  |  |  |
| --- | --- | --- |
| Name | Email | Project Role |
| Steffannie Egbuziem | Steffannie.egbuziem@dcmail.ca | Senior Auditor 100896975 |
| Ramini Thakur | Ramini.thakur@dcmail.ca | Senior Auditor 100899034 |
| Pratik | Pratikkumar.patel@dcmail.ca | Strategic Consultant 100896880 |
| Maisha | Maisha.khatoon@dcmail.ca | Strategic Consultant 100899259 |

# CONFIDENTIALITY

This document contains proprietary and sensitive government information. And due to this reason, it

should be treated with the protection that a confidential document requires.

This document should only be sent to relevant people and should not be copied without

authorization. The contents of a security assessment are treated as company secret material by Group 3 and will not be disclosed to anybody without consent.

TABLE OF CONTENTS

[GROUP 3 CONTACTS 2](#_Toc142083880)

[CONFIDENTIALITY 2](#_Toc142083881)

[INTRODUCTION 4](#_Toc142083882)

[Organization Description 4](#_Toc142083883)

[METHODOLOGY AND APPROACH 5](#_Toc142083884)

[EXECUTIVE SUMMARY DASHBOARD 6](#_Toc142083885)

[DOMAIN ASSESSMENT 7](#_Toc142083886)

[KEYS 7](#_Toc142083887)

[DOMAIN PRIORITY ROADMAP 8](#_Toc142083888)

[RECOMMENDATIONS 13](#_Toc142083889)

[ASSESSMENT QUESTIONS AND RESULTS 14](#_Toc142083890)

[APPENDIX A 16](#_Toc142083891)

[INFORMATION SECURITY ROLES 16](#_Toc142083892)

[INFORMATION SECURITY POLICY DOCUMENTS 17](#_Toc142083893)

[APPENDIX B – Artifacts Reviewed 23](#_Toc142083894)

# INTRODUCTION

The Network devices, servers, and applications of the British Columbia government are evaluated seasonally for potential vulnerabilities in the system and a risk assessment report is generated. Computer networks are appealing targets for attacks and information and asset exploitation due to the growing storage and transmission of sensitive data on them.

Furthermore, as computer users become informed, there are greater risks of sensitive data kept on network servers being compromised or stolen. To reduce these potential risks, this report will expand on recommendations for proper risk management practices and identify potential threats as well as weaknesses.

Most times, security threats can come as insider threats from disgruntled employees or outsiders as well as from well-prepared intruders who could access BC’s information or prevent access to the systems. These threats are becoming more numerous and sophisticated every year which makes security risk assessment important in every organization, as it helps to measure their security posture. A security evaluation was carried out in these domains to show areas that require improvements.

* Security Policy
* Organization of Information Security
* Human Resource Security
* Asset Management
* Access Control
* Cryptography
* Physical and Environmental Security
* Operations Security
* Communication Security
* System Acquisition, Development and Maintenance
* Supplier Relationships
* Information and Security Incidence
* Information Security Aspects of Business Continuity
* Compliance

# Organization Description

The British Columbia's elected leaders and public servants are meant to serve the citizens of B.C. and they're held accountable for their actions and decisions that impact residents. The legislative parliament is made up of:

The Lieutenant Governor

he Lieutenant Governor of B.C. represents the King at the provincial level in Canada and is the legal head of state in British Columbia, which means he or she acts as chief public representative and has the highest-ranking position in the provincial government.

Office of The Premier

The Premier acts as the head of government for B.C. In other words, he or she is the first minister and chief officer of the executive branch.

Cabinet

The B.C. Executive Council, otherwise known as the Cabinet of British Columbia, is made up of the Lieutenant Governor in Council, the Premier and Cabinet Ministers, of whom are members of the Legislative Assembly and selected by the Lieutenant Governor and Premier.

The Legislative Assembly

The Legislature of British Columbia is composed of the Lieutenant Governor and 87 elected Members of the Legislative Assembly (MLAs). Together, members of the governing party, members of the opposition and independent members make up the B.C. Legislative Assembly.

Ministries and Organizations

The Government of B.C. is made up of ministries, agencies, and Crown corporations. Browse ministry, agency and Crown corporation websites for the latest news, service plans, publications and more.

Public Service

Members of the public service are the politically impartial government employees who are responsible for carrying out the day-to-day activities of government and for delivering public services to the citizens of B.C.

# METHODOLOGY AND APPROACH

Our assessment entails a combination of best practices, control standards, and frameworks that are specific to the sector and organizational design of British Columbia government.

The ISO/IEC 27001 standard was used for the purpose of this assessment, including but not limited to Information security, Cybersecurity, and Privacy protection. The report is broken down into four sections:

• An Executive Dashboard designed to give the board and senior executives a brief, high-level

report.

• A Priority Roadmap containing strategic recommendations for improvement, in tabular form, prioritized based on British Columbia’s internal resources and the environmental threat at this time. The roadmap documents the present situation which requires (an area for improvement), the risk, the recommended future situation, and residual risk.

• Specific questions and responses gathered during the weekly assessment with data owners.

• Guidance and best practices have also been included in this audit to help with developing areas that

require improvement.

# EXECUTIVE SUMMARY DASHBOARD

We have identified a few instances where elements of Information Security Policies were lacking in the policy documentation of British Columbia, which include inadequate controls, as well as a lack of enforcement of some of the current policies and the supporting procedures. Some crucial security measures were not applied as well. We have setup a dashboard to evaluate the matrix which provides an overview of the assessment carried out.

|  |
| --- |
| OVERALL SCORE |
| 85% |

# DOMAIN ASSESSMENT

|  |  |
| --- | --- |
| PROCESS | OVERALL EFFECTIVENESS |
| Security Policy |  |
| Organization of Information Security |  |
| Human Resource Security |  |
| Asset Management |  |
| Access Control |  |
| Cryptography |  |
| Physical and Environmental Security |  |
| Operations Security |  |
| Communication Security |  |
| System Acquisition, Development and Maintenance |  |
| Supplier Relationships |  |
| Information and Security Incidence |  |
| Information Security Aspects of Business Continuity |  |
| Compliance |  |

# KEYS

|  |  |
| --- | --- |
|  | This specifies that the control area is effectively and efficiently setup, and that technology solutions address pending needs. |
|  | This represents the need for improvement regarding efficiency and effectiveness of the system, and technology solutions address some, but not all pending needs. |
|  | This connotes a large section of Inefficiency or ineffectiveness observed, including People, Processes, and  Technology. Technology solutions do not address needs, or process, people may not be formalized. |

# DOMAIN PRIORITY ROADMAP

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| DOMAIN | CURRENT STATE | RISK | FUTURE STATE | RESIDUAL RISK |
| Security Policy | The organization has a defined security policy, approved by management before it is published, and communicated to employees and relevant external parties. The policies are also reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness. | LOW |  | LOW |
| Organization of Information Security | All security policies are defined, Conflicting duties and areas of responsibility are also segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets, but it lacks appropriate contact with relevant authorities, special interest groups, and it is not addressed in terms of project management. | HIGH |  | LOW |
| Human Resource Security | Background verification checks are carried out on all candidates for employment, in accordance with relevant laws, regulations and ethics and are proportional to the state’s requirements, the classification of the information to be accessed and the perceived risks. The employment and  termination contract  are drafted in  compliance with the organization’s security  policy. | LOW |  | LOW |
| Asset Management | All information assets  are identified,  classified, and  appropriately  protected at the time.  of audit. This includes,  asset inventory, asset  classification, risk  assessment, access  control, asset  protection, asset  disposal and asset  ownership. But the rules for acceptable use of assets are not properly documented and implemented. | Medium |  | LOW |
| Access Control | The organization used the Microsoft Azure Directory to restrict access and some users are only provided with access to the network and network services that they have been specifically authorized to use. | Medium | Recommend a NAC  solution to enforce policies on devices that  access networks. This will improve the security and visibility of  the network. | LOW |
| Cryptography | There are cryptographic controls for protection of information which have been implemented but the system can have better controls in place. AES-256 is  being used for data at  rest while TLSv1.2 is in use for data in transit. | High | Recommend AES-512  and TLSv1.3 for  additional security. | LOW |
| Physical and Environmental Security | The boundaries of  security are clearly established. This  includes using  workplaces and  spaces that have  access cards and  biometric fingerprint  readers.  Additionally, guests  are given visitor tags.  to aid in navigating the  organization. All  employees follow the clean desk policy at  the conclusion of each day to protect data. | Medium | Recommend more physical perimeter security to be implemented. | LOW |
| Operations Security | The Development, testing, and operational environments are not separated to reduce the risks of unauthorized access or changes to the operational environment. | High |  | LOW |
| Communications Security | The Networks is properly managed and controlled to protect information in  systems and applications. Firewalls are setup to control the traffic into the  network, and  the use of VPN for hybrid staff | High | Recommend the need to implement Multi factor authentication for an extra layer of security. | LOW |
| System Acquisition, Development and Maintenance | The use of Github for version control to ensure code management and track the progress as well. | MEDIUM | Recommend using CID tools to automate the software development and deployment process. | LOW |
| Supplier Relationships | The Information security requirements for mitigating risks associated with supplier’s access to assets are usually agreed on with the supplier and documented but they do not address risks associated with information communication technology. | Medium |  | LOW |
| Information and Security Incidence | There is an incident response team set up in the event of an incident with the documentation regularly updated depending on the severity of incidents that take place. | LOW |  | LOW |
| Information Security Aspects of Business Continuity | The IT department and Risk management team have ensured there is a continuity of business operations and disaster recovery plan and procedures put in place to mitigate risk and impact on the institution. | LOW |  | LOW |
| Compliance | The organization  complies with  regulatory bodies, and compliance audits are conducted regularly. | LOW |  | LOW |

# RECOMMENDATIONS

|  |  |
| --- | --- |
| RECOMMENDATIONS | JUSTIFICATION |
| The Use of Network Access Control | It allows institutions to enforce access controls and security policies across their network, ensuring that only authorized users and devices are granted access. By doing so, NAC helps prevent unauthorized access and can mitigate the risk of security breaches, data theft, and other cyber-attacks |
| Improve Cryptographic Controls | To improve the confidentiality, integrity, and availability of data, it is recommended to upgrade to AES-512 and TLSv1.3 for additional security. |
| The use of Multifactor Authentication on VPN’s in use. | For stronger authentication, we advise they adopt the use of multifactor authentication on their VPN to provide additional layers of authentication beyond the conventional username and password, making it more difficult for unauthorized users to gain access to the VPN.  Some authentications like the OTP code and biometric authentication, can be helpful. |
| Adopting the use of CI/CID Tools | By automating the software  delivery process, CI/CD systems enable better team productivity and efficiency.  The solution offers automated testing and  feedback methods, allowing developers to find  faults and errors early in the development  process which leads to better code quality and fewer production-related problems.  It also increases collaboration amongst teammates. |
| The implementation of more environmental control | To guarantee that the institution complies with specific environmental standards, environmental controls are frequently required by law or regulations. These criteria must be followed or the institution risk legal action, financial penalties, and reputational harm |

# ASSESSMENT QUESTIONS AND RESULTS

The responses to the ISO/IEC 27001 set of questions provided during the assessment are listed in

the following section, and they constitute the current implementation status.

|  |  |  |
| --- | --- | --- |
| Security Policy 1 | | |
| Question | Availability of Information Security Policy | YES |
| Comment | There is an information Security Policy documented for procedures, to be adhered | |

|  |  |  |
| --- | --- | --- |
| Security Policy 2 | | |
| Question | Information Security Policy Updated Periodically | NO |
| Comment | There policy is set to be adhered to bi-annually but should be periodically | |

|  |  |  |
| --- | --- | --- |
| Security Policy | | |
| Question | Communicating policy to all stakeholder and employees | YES |
| Comment | The Information Security policy is communicated to all stakeholders that are required | |

|  |  |  |
| --- | --- | --- |
| Asset Management 1 | | |
| Question | Information of assets are identified and tracked throughout their lifecycle | YES |
| Comment | Specific Identity and access management tools are used for assets in the organization. | |

|  |  |  |
| --- | --- | --- |
| Asset Management 2 | | |
| Question | Information assets are appropriately protected based on their value and criticality | YES |
| Comment | Regular assessments are carried out to ensure information assets are categorized based on the level of criticality. | |

|  |  |  |
| --- | --- | --- |
| Organization of Information Security | | |
| Question | Employees understand their roles and responsibilities regarding information security | YES |
| Comment | Custodians ensure all information required are available to the respective stakeholders. | |

|  |  |  |
| --- | --- | --- |
| Human Resource Security 1 | | |
| Question | performing background checks on employees and contractors | YES |
| Comment | Background checks are done in house due to the resources available to them. | |

|  |  |  |
| --- | --- | --- |
| Human Resource Security 2 | | |
| Question | Employees are aware of their responsibilities and obligations with regards to information security | YES |
| Comment | Regular information security seminars and periodic testing to ensure employees know they are the most important assets. | |

|  |  |  |
| --- | --- | --- |
| Access Control 1 | | |
| Question | Implementing access controls based on the principle of least privilege | YES |
| Comment | Microsoft Azure is used to grant access. | |

|  |  |  |
| --- | --- | --- |
| Access Control 2 | | |
| Question | Access controls are consistently applied across all information systems and applications | YES |
| Comment | Access is restricted to only what is required, and the principle of least privilege is implemented. | |

|  |  |  |
| --- | --- | --- |
| Cryptography 1 | | |
| Question | Appropriate cryptographic controls to protect sensitive information | YES |
| Comment | The standard encryption protocol is set to AES 256 | |

|  |  |  |
| --- | --- | --- |
| Physical and Environmental System 1 | | |
| Question | Implementing appropriate physical security controls to protect information assets | YES |
| Comment | security key cards on badges together with bars at entry points to eradicate tail gating. | |

|  |  |  |
| --- | --- | --- |
| System Acquisition, Development and Maintenance 1 | | |
| Question | conducting proper security assessments and testing during system development and maintenance | NO |
| Comment | This can be improved by setting up schedules to evaluate systems and maintenance. | |

# APPENDIX A

## INFORMATION SECURITY ROLES

1. Senior Information Security Official: Designated to direct and oversee information security activities, guaranteeing the creation, application, and management of security controls to protect data and services.

2. Setting priorities and communicating them: Senior management makes sure that stakeholders are aware of information security priorities while taking organizational demands into account.

3. Information Security Procedures: Ensures that information security procedures are clear, documented, and conveyed in a way that complies with specific organizational needs.

4. Program Governance and Oversight: The formal designating of a contact or group to oversee programs, evaluate and update security plans, ensure compliance, and assess risks on behalf of the organization.

5. Formulates, reviews, and approves information security policies, which serve as a foundation for putting controls in place and directing secure practices.

6. Assessment of efficacy: Conducts annual assessments to evaluate the information security policy's efficacy and pinpoint opportunities for development.

7. Support and Resources from Management: Provides security initiatives with a clear plan, visible backing, and the resources they need.

8. Establishes initiatives to keep stakeholders and employees informed about information security.

9. Assures that safeguards are in place to stop identity theft that targets clients, staff members, and other parties.

10. Coordination of Security measures: Ensures coordination of information security measures throughout the organization.

11. Information security experts: Choose and organize the engagement of internal or external security experts to deal with certain issues.

12. Determines and synchronizes information security strategy and goals with website requirements.

13. Programs for privacy, security, and risk management are formally reviewed and approved to be consistent with organizational goals.

14. Roles and Responsibilities Are Assigned: The organization's formal approval of the roles and responsibilities for information security.

15. Senior Security Official Professional Competency: The appointed official must provide documentation of their professional competence, such as credentials or related experience.

16. Process for managing recognized risks and deciding whether to accept or mitigate them, as documented in the Risk Acceptance Process.

17. Reviewing the security program periodically is necessary to make sure it is working properly (third parties may be involved).

## INFORMATION SECURITY POLICY DOCUMENTS

1. Information security rules for the organization are outlined in the policy introduction, together with information on the organization's purpose, vision, values, and essential infrastructure.

2. Information security is defined along with its goals, with the emphasis being placed on secure information sharing.

3. Information security is a priority for management, and this commitment is in accordance with corporate strategy.

4. Creates a framework for establishing control objectives and risk management strategies.

5. Information security is required, and it emphasizes how crucial strong security measures are for safeguarding stakeholders' assets.

6. It lists confidentiality, integrity, and availability as the main objectives of information security.

7. Compliance Scope: Clearly outlines compliance with legal requirements and contract clauses.

8. Ensures anonymous incident reporting while putting a strong emphasis on legal and ethical responsibilities.

9. Emphasizes the importance of adhering to industry best practices by addressing topics including education, incident response, and more.

10. Outlines basic and management responsibilities in the section on information security management.

11. Formal processes are set forth for putting security measures in place in the development and dissemination of procedures.

12. References to supplementary documentation that supports the policy are made in the documentation section.

13. Communication and Accessibility: Ensures that policies are communicated in a pertinent and clear manner.

14. Covers the rules and regulations for dealing with organizations that interact with third parties.

INFORMATION SECURITY STRATEGIC PLAN

By integrating risk management, performance management, and investment management, this approach synchronizes information security with corporate goals. Consistent procedures, proactive decision-making, and shortening the delivery time are stressed. A unified security environment that smoothly interacts with applications, data, processes, and workflows is the aim. The plan emphasizes resource planning, human capital management, and the use of a business case for resource requirements.

DRIVERS OF STRATEGY

1. Integration of performance, risk, and investment planning.

2. Integrated Methodologies That Are Consistent.

3. Detecting and solving problems proactively.

4. Time to Delivery is Reduced.

5. Architectures that can be modified and expanded.

6. Choosing Things Wisely.

7. redundancy is eliminated.

8. Planning and controlling human resource operations.

9. Integrated Security that works seamlessly.

10. Creating a business case and resource planning.

11. Resources for information security are readily available.

RISK MANAGEMENT FRAMEWORK

Risks involving third parties, compliance, and security are all regularly identified and managed by the RMF. It entails putting in place corrective controls, maintaining a constant watch, and informing key parties like the Board of Directors of progress.

Items in the risk management program:

1. Objectives, acceptable risk thresholds, strategy alignment, and mechanisms for documenting risk assessment are all outlined in a formally authorized risk management policy.

2. Risk assessments are conducted on a regular basis to find potential weaknesses.

3. Risk mitigation refers to the application of corrective actions to hazards and dangers that have been identified.

4. Thresholds for each risk category are established in the risk tolerance definition.

5. Operational Risk Plan Communication: The operational risk plan is shared with all relevant parties.

6. Re-evaluation on a regular basis: The effectiveness and accuracy of the policy are checked.

7. A system monitors risk assessments and the development of risk mitigation.

8. Risk Management Policy Updates: Changes are considered when the risk management policy is updated.

9. Monitoring on a continuous basis: Standard monitoring also involves change and incident response.

10. Dashboard for Risk Reporting: To provide stakeholders and the Board with ongoing risk information.

RMF's primary steps are:

1. Setting the context for managing security and privacy risk is the first step in preparation.

2. Create categories based on effect assessments for systems and information.

3. Baseline rules Selection: Using the results of a risk analysis, choose and modify the baseline security and privacy rules.

4. Implementing the controls will involve securing the environment and system and implementing privacy and security controls.

5. Assessment of Controls: Examine the efficiency and correctness of the controls' implementation.

6. Authorizing the system: Based on risk assessments, authorize the system or common controls.

7. Monitoring That Never Stops: Reporting and evaluating the efficiency of controls are both part of ongoing monitoring.

Protecting information assets and vital infrastructure is ensured by the RMF. Effective risk mitigation techniques are made possible by it. The RMF ensures risk acceptance prior to system operation and is customizable to organizational demands.

ELECTRONIC RECORDS RETENTION

To dispose of data securely when it is no longer required for legal, regulatory, or business purposes, the organization must create a formal record retention program. This program must cover the secure disposal of data, including data on disposed assets. Additionally, this program incorporates the categorization-based disposal of personally identifiable information. Furthermore, a programmatic review procedure, either automatic or manual, shall be in place on a quarterly basis to identify and delete personally identifiable information that does not comply with the data retention policy's standards.

Record access, retention, destruction, and storage must all be done according to specific protocols. It must include the following safety measures:

1. Schedule for Retention: A schedule for retention must be made, outlining the sorts of important records to keep and how long they must be kept.

2. Inventory of Information Sources: To ensure proper administration of records, an inventory of sources that provide important information must be kept.

3. Security in the Handling of Cryptographic Keys: Any relevant cryptographic keys must be safely held and only made available when required.

4. Storage of Cryptographic Keying Material and Programs: For the duration of a record's retention period, cryptographic keying material and programs connected to encrypted archives or digital signatures must also be kept on hand to facilitate decryption.

IDENTITY AND ACCESS MANAGEMENT

1. Secure VPN solutions are utilized for remote user authentication, which uses challenge/response protocols, hardware tokens, or cryptographic-based mechanisms. Also possible for authentication is the use of dedicated private lines. The management of access control points is used to regulate access.

2. Periodic inspections: Checking regularly makes sure that equipment does not possess unforeseen dial-up capabilities. It is necessary for authorized connections to call back and re-authenticate.

3. Vendor login: To access the network, vendors are required to provide their User IDs and passwords. Annual reviews, logging, and authorization of access are performed.

4. Node authentication: In VPN-based solutions, node authentication using cryptographic methods such machine certificates are possible for groups of remote users connecting to a shared computer facility.

5. All dial-up and VPN remote login access must use two-factor authentication to ensure secure access to internal systems and sensitive data.

The organization guarantees secure remote access, reduces risks, and safeguards sensitive information by putting in place strong Identity & Access Management practices.

Secure Logon Procedures

The operating system's logon method is made to give unauthorized users as little access to the system as possible to minimize unauthorized access.

The following are the logon procedures:

Restricting Ineffective Logon Attempts

• Just three (3) unsuccessful logon attempts are permitted.

• Whenever an attempt fails, the data link connection is terminated.

• Once the allotted logon attempts have been used up, an alarm message is broadcast to the system console.

• Depending on the password length and system settings, the number of password retries is restricted.

Setting Time restrictions

• If the maximum or minimum time restrictions for the logon procedure are exceeded, the system ends the logon process.

Authenticated Credential Transmission

• The network does not send plain text containing usernames and passwords.

Identification Display Under Control

• Only after a successful logon are system or application identifiers shown.

Limiting help messages:

• During the logon process, no assistance messages are given to help unauthorized users.

Checking the information from a logon:

• Only complete input data is used to confirm logon information, and even then, the wrong data is not identified.

Added Critical Systems

User Account Lockout

• The user account is automatically locked out by the system after three unsuccessful logon attempts within one hour.

• A minimum of three (3) hours had passed since the lockout began.

Techniques for Reporting and Training:

• Authorized users are responsible for reporting attempted and unauthorized logons; reporting methods are covered in training.

Concurrent Sessions:

• All account categories are subject to the organization's concurrent session limit.

By following these Secure Logon Procedures, the organization strengthens the security of the logon process and protects against unauthorized access.

ASSET MANAGEMENT

The company executes a thorough asset management program, identifying, cataloguing, and recording all assets and services, including Personally Identifiable Information (PII), whether encrypted or not, across numerous locations, including third-party websites. The inventory specifically identifies the designated record sets that include PII.

The asset inventory, which contains crucial data for disaster recovery such as asset type, format, location, backup details, licenses, and business worth, also includes approved Bring Your Own Device (BYOD) equipment. Assets are recorded for ownership, custodianship, and information classification. Based on the importance of the asset, the value of the business, and the security classification, the level of protection and sustainment is chosen. The keeping of records for organizational property (capital and non-capital) given to employees and contractors is governed by certain policies. To ensure returns upon termination or transfer, procedures are created for issuing and inventorying property assigned to employees.

Procedures for allocating and observing property use are contained in the contract for contractors who are given organization-owned property. Before transferring, exchanging, or discarding or surplusage property, secure data erasure from hard drives is a process that is documented. According to the lifespan of the organization, the same procedures must be followed when transferring, exchanging, or disposing of IT-related assets.

The asset inventory includes all systems and gadgets that are network-connected, and it keeps track of crucial data such network addresses, machine names, system functions, asset owners, and related departments. The inventory contains information about all networked devices with an Internet Protocol (IP) address, such as desktops, laptops, servers, network devices, printers, Voice Over IP phones, and more.

The asset inventory lists all mobile and personal data processing and storage devices, regardless of network connectivity. The asset inventory includes all systems and gadgets that are network-connected, and it keeps track of crucial data such network addresses, machine names, system functions, asset owners, and related departments. The inventory contains information about all networked devices with an Internet Protocol (IP) address, such as desktops, laptops, servers, network devices, printers, Voice Over IP phones, and more. The asset inventory lists all mobile and personal data processing and storage devices, regardless of network connectivity.

THREAT AND VULNERABILITY MANAGEMENT

For technological vulnerability management, the organization specifies roles and duties for monitoring, evaluating, patching, tracking assets, and coordinating. To identify pertinent vulnerabilities, information resources are frequently updated. Including network- and application-layer testing, quarterly vulnerability evaluations of sensitive information systems and networked settings are carried out. Technologies for virtualization are supported by vulnerability assessment tools. The application of patches is done in accordance with change control processes, including backup controls in case patches are delayed or unavailable. For fresh security flaws, a risk ranking procedure is set up. System hardening guidelines are followed when configuring systems.

On specified systems, annual internal and external penetration testing is done to look for weaknesses and attack methods. Frequently, independent agents or teams undertake vulnerability screening and testing. Audit logs from the past are checked for vulnerabilities that have been exploited.

In conclusion, implementing these procedures enables the British Columbian Government Policy to protect itself more effectively by proactively identifying and reducing security risks.

# APPENDIX B – Artifacts Reviewed

The following list of artifacts were reviewed as a part of the Information Security Program Risk Assessment.

|  |  |
| --- | --- |
| S/N | Document Name |
| 1 | C-CERT Response Plan |
| 2 | Employee Onboarding /Offboarding Document |
| 3 | Backup Policy 2023 |
| 4 | BC Business Continuity Plan |
| 5 | BC Information Security Policy |
| 6 | BC Asset Management |