1. PURPOSE

Vulnerability scans are conducted to identify potential risks to networks, software, systems, and data. Proactively scanning government information systems allows security teams to identify potential exploits that can be mitigated; thereby securing government information systems from known vulnerabilities.

2. DESCRIPTION

This standard establishes a common understanding of the roles and responsibilities for vulnerability scanning. The intent is to manage security risks associated with known vulnerabilities.

The Office of the Chief Information Officer will monitor the effectiveness of this standard and provide notification where and when appropriate

3. AUTHORITY

Information Security Policy (ISP)

4. APPLICATION / SCOPE

This standard applies to all government organizations (ministries, agencies, boards and commissions) that use government information technology services.

Effective Date: This standard is effective as of February 26, 2021.

Non-compliance: Non-compliance to this standard could lead to appropriate security measures not being established for data, information, applications, hardware, associated documentation or computer facilities. This could lead to security incidents or breaches causing harm to the province and its stakeholders.

5. REQUIREMENTS

1. Roles and Responsibilities

1.1 Government Organizations are responsible for and must:

- Maintain a current asset inventory which can support vulnerability scanning;
- Scan for vulnerabilities in information systems and applications which they manage themselves and/or through contracts and outsourcing agreements that are new, changed or upgraded, and otherwise at a regular interval (minimum yearly for critical systems);
- Prepare risk-based response plans for vulnerabilities;

- Remediate and address risks in accordance with response plans. System owners and system administrators are responsible to implement the remediation/response plan;
- Ensure that critical and high validated vulnerabilities are addressed within timeframes communicated by the OCIO; an exemption or remediation plan may be required when a critical or high vulnerability can not be remediated; this plan will be approved by the Ministry Information Security Officer (MISO), or designate;
- Notify OCIO Change Management through a Request for Special Processing (RSPs) in advance of vulnerability scanning activities. The MISO, or designate, should provide oversight, be notified about scans and receive scan findings/reports; and,
- Ensure that any related contracts and/or outsourcing agreements address vulnerability scanning requirements as defined by the OCIO.

1.2 OCIO Information Security Branch (ISB) is responsible for and must:

- Scan for vulnerabilities in information systems and applications which OCIO manages themselves, and/or through contracts and outsourcing agreements, that are new, significantly changed or upgraded, and otherwise at a regular interval (minimum yearly for critical systems); Communicate timeframes expected for vulnerability remediations;
- Provide guidance, expert advice, and recommendations on vulnerability scanning and mitigation; and,
- Ensure vulnerability scanning services exist and are provided to government organizations; conduct regular background vulnerability scans of the government network and information systems; and communicate potential vulnerabilities to government organizations.

6. SUPPORTING DOCUMENTS

List Links to International and/or Government Policy
Core Policy and Procedures Manual (CPPM)
Information Security Policy (ISP)
Information Security Standard (ISS)
OCIO Patch Guidelines
Security Threat and Risk Assessment Standard

7. DEFINITIONS/GLOSSARY

- **Information Owner** is defined in the Province's Information Security Standard (ISS).
- **Must** is defined as an absolute requirement of the specification.
- **Should** means that there may be valid reasons in particular circumstances to use alternate methods, but the full implications must be understood and carefully weighed before choosing a

different course. The use of an alternate method requires the approval of the Assistant Deputy Minister (ADM) of the Information Owner.

- **Vulnerability** is a weakness of an asset, including systems and software, or a control, including procedures and processes, that can be exploited by one or more threats.

8. REVISION HISTORY

Date	Author	Version	Change Reference
February 26, 2021	Brian Horncastle, Gary Merrick	1.0	Approved by GCIO
December 22, 2020	Brian Horncastle, Gary Merrick	DRAFT 1.0	Final DRAFT endorsed by ASRB
September 10, 2020	Brian Horncastle, Gary Merrick	DRAFT 1.0	Initial draft presented to ASRB

9. CONTACTS

Enquiries and update/change notifications about this standard can be directed to:

Office of the Chief Information Officer
Information Security Branch
Ministry of Citizens' Services
Email: InfoSecAdvisoryServices@gov.bc.ca