DIRECTIVE – VIRTUAL MACHINES MANAGEMENT

Directive (Definition): Information Protection and Security (IP&S) directives derive from the **Information Management and Protection Policy, TBM 2018-111** (replaces TBM 2009-335) approved by Treasury Board. IP&S directives are mandatory for users to follow. Directives are supported by standards and guidelines, where applicable.

Issuing Branch	**Operations and Security Branch** *Information Protection Division*
Target Audience	All Government departments and public bodies supported by the OCIO
Approval Date	December 19, 2018
Review Period	Every 3 Years
Last Review Date	N/A
Next Review Date	September 2021
Related Standards	Not Applicable
Related Guidelines	Not Applicable

APPROVAL AND SIGN OFF

OCIO Senior Leadership Team (SLT)	*Approver of IP&S Directives*
OCIO Security Council	*Approver of IP&S Standards and Guidelines*

VERSION 1.0

TABLE OF CONTENTS

VIRTUAL MACHINES MANAGEMENT

DIRECTIVE

1. Overview

Virtual Machines (VM) are a common way and a valuable tool for application testers and developers to test enhancements and modifications to applications across multiple versions of operating systems and software. They allow for fast, easy and comprehensive testing and development capabilities. However, the same security challenges and risks exist with Virtual Machines as with a workstation.

Adherence to appropriate Virtual Machine Management processes will help maintain the confidentiality, integrity and availability of Government of Newfoundland and Labrador Network (hereafter referred to as 'the Network') and Electronic Information Assets; and reduce the risk of inappropriate access to and use of Electronic Information Assets.

2. Purpose and Scope

This Directive identifies expectations and establishes rules for creating, maintaining, securing and decommissioning Virtual Machines, created for Windows-based desktop operating systems, on enterprise virtualization infrastructure owned and supported by the Office of the Chief Information Officer (OCIO).

Adherence to the requirements in this Directive is mandatory for all Government departments and public bodies supported by the OCIO.

3. Directive Statements

a) Virtual Machines shall not be created on government workstations.

b) Virtual Machines shall be created on enterprise virtualization infrastructure that is owned and supported by the Operations and Security (O&S) Branch of the Office of the Chief Information Officer (OCIO).

c) Virtual Machines shall be maintained (i.e., configured, patched, etc.) and secured in the same manner as workstations.

d) Virtual Machines, like workstations, shall not be subject to backup procedures. As such, government information shall not be stored on Virtual Machines.

e) Virtual Machines shall have administrator rights for users disabled by default. A second administrator account (i.e., not a regular domain account) shall only be enabled when approval to grant elevated permissions has been obtained via the OCIO's desktop administrative rights process.

f) Virtual Machines shall be created with minimal access unless business justification is provided as to why access should be expanded (e.g., Virtual Machines will not have internet access unless business justification is provided and approved).

g) Virtual Machines shall be created for a period not exceeding one year.

h) The Virtual Machine Request Form[1] shall be completed and submitted to the OCIO Service Desk for appropriate review and action for creation and/or extension of Virtual Machines.

i) The Operations and Security Branch, of the OCIO, shall follow the workflow outlined in the Virtual Machine Requests Procedural document.

j) Virtual Machines creation, extension and exemption (e.g., creation of non-Windows-based operating systems VM) shall be approved by the OCIO's Director of Networks, Security and Information Protection.

4. Roles and Responsibilities

Operations and Security Branch (Information Protection Division)

- Development, implementation and maintenance of this Directive
- Education and awareness of this Directive across Government
- Issuance of Exemptions related to this Directive
- Oversight of the IP&S Policy Framework

Operations and Security Branch (Enterprise Application Division)

- Development, implementation and maintenance of any related standards and guidelines
- Education and awareness of any related standards and guidelines across OCIO

Employees

- Understanding of responsibilities as outlined in this Directive
- Adherence to this Directive and any related standards and guidelines

Deputy Ministers (or Equivalent)

- Enforce this Directive across their Department or Public Body

5. Compliance and Enforcement

Mandatory Compliance
Adherence to this Directive is mandatory for all employees.

Enforcement
Enforcement of this Directive is the responsibility of the Deputy Minister or equivalent of each department or public body, as per the *Management of Information Act*, and the *Information*

[1] Employees with a pre-existing Virtual Machine, created prior to the issuance of this Directive, must submit the Virtual Machine Request Form to obtain the required approvals and to ensure the Virtual Machine is created, maintained, secured and decommissioned in compliance with this Directive.

Management and Protection Policy as approved by Treasury Board, under which it is issued. Where necessary, enforcement will be undertaken by the OCIO in accordance with requirements to secure the Network and Government-issued and owned IT assets.

Penalty for failure to comply
Willful non-compliance with this Directive, including contravention through negligence, may result in disciplinary action by the Employer, up to and including termination of employment, in accordance with Government's human resource policies.

6. Monitoring and Review

The OCIO's O&S Branch (IP Division) is responsible for monitoring and reviewing this Directive, in accordance with processes set forth under the IP&S Policy Framework. For clarification of this Directive, contact the IP Division by emailing OCIOInfoProtection@gov.nl.ca.

7. Definitions

Availability – Ensuring timely and reliable access to and use of information (e.g., emergency communications or health services, financial systems, benefits systems); Availability means being accessible and useable upon demand by an authorized entity (source ISO/IEC 27000:2018). It is the ability of a component or service to perform its required function at a stated instant or over a stated period of time. Availability is usually expressed as the availability ratio, i.e. the proportion of time that the service is actually available for use by the customers within the agreed service hours (source: ITIL).

Confidentiality – Ensuring information is not made available or disclosed to unauthorized individuals, entities, or processes (source ISO/IEC 27000:2018); Upholding required restrictions against unauthorized access or disclosure of information (e.g., personal information, Cabinet confidences, trade secrets).

Electronic Information Asset – Information within a Government of Newfoundland and Labrador application or information system and/or device that has value to the organization.

Employee - For the purpose of this Directive, 'Employee' refers to employees of departments and public bodies supported by the OCIO; it does not include contractors, external consultants, partners, vendors or other third parties entrusted to access or use the Network on behalf of the Government of Newfoundland and Labrador.

Government – in the context of this Directive, 'Government' refers to departments and public bodies supported by the OCIO.

Information Protection (IP) – Information protection is an area of practice focused on the protection of information from inappropriate access or use, using a variety of means as required; including, but not limited to, policy and standards; physical and electronic security measures; and compliance monitoring and reporting. Information Protection represents the point at which the management of information converges with security policy and measures. In the Government of Newfoundland and Labrador, public bodies are required to protect information as part of their accountability under Section 6 of the *Management of Information Act SNL2005 c.M-1.01.*

Information Protection and Security (IP&S) Program – The comprehensive, organized collection of documented policies, directives, standards, guidelines and processes that are used to continuously deliver information protection and security across the OCIO (Source: Deloitte).This program is managed by the Information Management Branch and is focused on governance, policy and standards; planning and strategy; education and awareness; information risk management; monitoring and compliance; and executive incident response.

Information Protection and Security (IP&S) Policy Framework – Outlines the roles, responsibilities and processes for Information Security policies, directives, standards and guidelines within the OCIO. It also provides the overall model and the supporting method and responsibilities for making the OCIO policies, directives, standards and guidelines a vital element in the overall Information Security Program. The framework depends upon communication and coordination between the various stakeholders to ensure that overall risk is well managed.

Integrity – Maintaining the authenticity and preventing unauthorized modification or destruction of information (e.g., food or water testing, health care, law enforcement). Maintaining integrity consists of safeguarding the accuracy and completeness of assets. Integrity demonstrates that the record is complete and has been unaltered. (Source: ISO/IEC 27000:2018).

Operating System – A collection of software that manages computer hardware resources and provides common services for computer programs (Source: NIST SP 800-152).

Virtual Machine – A simulated environment created by virtualization (Source: NIST SP 800-125); software that allows a single host to run one or more guest operating systems (Source: NIST SP 800-115).

Workstation – A computer (e.g., desktop, laptop, tablet devices, etc.) used for tasks such as programming, engineering and design (Source: NIST SP 800-82 Rev. 2).

8. References

Management of Information Act – http://assembly.nl.ca/Legislation/sr/statutes/m01-01.htm

Human Resource Policies – http://www.exec.gov.nl.ca/exec/hrs/working_with_us/policies.html

9. Revision History

December 19, 2018 Version 1.0