McMaster University

University Information Security Standard

Complete Policy Title: **CLIENT COMPUTING DEVICES SECURITY STANDARD**	Policy Number (if applicable): **IS-14-CLN**
Approved by: **Chief Information Officer**	Date of Most Recent Approval: (annual review)
Date of Original Approval(s):	Supersedes/Amends Policy dated: **n/a**
Responsible Executive: **Chief Information Officer**	Enquiries: **IT Security (c-it-security@mcmaster.ca)**

DISCLAIMER: *If there is a discrepancy between this electronic policy and the written copy held by the policy owner, the written copy prevails.*

TABLE OF CONTENTS

CLIENT COMPUTING DEVICES SECURITY STANDARD

INTRODUCTION

Client computing devices are critical tools in the McMaster environment. Proper management of these devices provides an essential layer of defense in securing University assets from loss, unauthorized access or unauthorized use.

It is the responsibility of all University constituents to exercise appropriate care and discretion in the management of their computing devices, and to protect the information that may be accessed by or stored on these devices as outlined by this standard.

Failure to securely configure client computing devices may lead to unauthorized access to personally identifiable information, disclosure of intellectual property, unauthorized disclosure of McMaster University information, reputational damage and monetary loss.

Purpose

1. This standard provides direction for the secure configuration of client computing devices in support of the objectives defined by the ***Information Security Policy***. This standard endeavours to provide client computing device configuration strategies that will mitigate risks related to the protection of personal privacy, intellectual property and copyrighted materials, and safeguarding the reputation of the University.

Scope

2. This standard applies to any computing device which is used to access internal, confidential or restricted University information regardless of ownership or physical location of the device. It should be adhered to when installing, configuring, using or disposing of any such computing device.

Definitions

3. A **client computing device** is used by a Constituent to access University information technology services, computing resources, or information. This may include, but is not limited to, desktop computers, laptop computers, netbooks, tablets, smartphones, PDAs and other specialized equipment.

4. **Portable storage devices** are ***any*** device or media which is easily transportable, upon which information can be stored. This definition is ***not restricted*** to purpose built storage devices such as CD/DVDs, removable hard drives, and USB flash drives, but also may include laptop computers, tablets, smart phones, PDAs, and any other portable computing device

5. The **primary user** of a client computing device is the owner of the device, or the person to whom the client computing device has been assigned for use.

6. **Authentication** is the process by which a service, server, system, or computing device verifies the identity of a customer. **Authentication controls** are the mechanisms used to perform the verification. Examples of authentication controls include, but are not limited to, passwords, passphrases, personal identification numbers, swipe patterns, fingerprint recognition, and one time passwords.

7. Accounts with **elevated privilege** are those that are used to configure service and resource settings, and the access privileges of other users. Such accounts include, but are not limited to, *administrator*, *root,* and service principal accounts. In most cases an account with elevated privilege is a named account to which administrative privilege or role(s) have been granted.

8. **Internal** information requires some controls against unauthorized disclosure and modification, however the sensitivity and impact of disclosure is less than that for confidential information. Internal information is mostly routine business communication and documentation.

9. **Confidential** information requires strong controls against unauthorized disclosure, loss, and modification. Disclosure, loss, or unauthorized modification of confidential information may result in reputational damage, disruption to business, with high potential for financial consequence and legal liability. Confidential information should only be disclosed to authorized persons. Examples of Confidential information may include Personally Identifiable Information (PII), Personal Health Information (PHI) and credit card information (PCI).

10. **Restricted** information requires very strong controls against unauthorized disclosure, loss, and modification. Disclosure, loss, or unauthorized modification of restricted information may result in significant reputational damage, significant disruption to business, as well as very serious financial consequence and legal liability. Restricted information must only be disclosed to authorized persons. Examples of restricted information include strategic organizational plans and financial

information, and in-camera senate and board meetings. See the ***Information Classification Matrix*** for information handling guidance.

11. A complete glossary of definitions can be found in the ***Information Security Glossary.***

CLIENT COMPUTING DEVICES SECURITY

Device Protection

12. The primary user is responsible for ensuring that their client computing device is appropriately protected according to the device protection and integrity controls herein, and the classification of information stored on or accessed by the device. Where the technology does not support the device protection and integrity controls described herein, compensating controls must be implemented.

Device Protection and Integrity Controls

13. Client computing devices must be physically secured.

14. Client computing devices must be protected by an authentication control, and must be configured to automatically lock within a reasonable amount of time if left unattended.

15. Client computing devices must be configured to prevent the execution of unauthorized software and the modification of system files.

    a) Endpoint protection software, such as antivirus and browser security software, must be used to prevent the execution of malicious software, and malicious outbound network connections.

    b) Client computing devices should be accessed with the privilege necessary for user activities, such as accessing email, internet browsing, and general office functions; local and domain user accounts should not be configured to have elevated local privilege. Access to local accounts with elevated privilege, such as administrator or root, must be restricted.

16. Client computing devices must be configured to refuse unauthorized, unnecessary or malicious inbound network connection attempts.

17. Unsupported software and operating systems should not be used. Applications and operating systems must be regularly updated with vendor provided security patches and updates. Software

that is not in use or not required should be removed from the client computing device. Unused communications protocols should be disabled.

18. Confidential and restricted information stored on portable client computing devices and / or portable storage devices must be encrypted. Confidential and restricted information stored on client computing devices should be encrypted.