McMaster University

University Information Security Standard

Complete Policy Title:
SERVER SECURITY STANDARD

Policy Number (if applicable):
IS-14-SVR

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

SERVER SECURITY STANDARD 2
- Introduction 2
  - Purpose 2
  - Scope 2
  - Definitions 3
- Requirements 4
  - Physical Environment 4
  - Operating System 5
  - Applications 5
  - Server Integrity Controls 5
  - Server Administration 6
  - Authentication and Access Control 6
  - Vulnerability Management 7
  - Backup, Restore, and Disaster Recovery 7
  - Server Hardware Disposal 7
  - High Performance/Distributed Computing 7
  - Logging 7

SERVER SECURITY STANDARD

INTRODUCTION

Servers are critical tools in support of McMaster University. Proper management of these devices provide an essential layer of defense in securing the University assets from loss or unauthorized use, as well as assuring the confidentiality, integrity and availability of information.

It is the responsibility of server administrators to exercise appropriate care in the configuration, maintenance and management of the servers for which they are responsible, and to protect the information that is processed or stored on these devices as outlined by the standard herein.

This standard is guided by fundamental principles of information technology security and privacy, including but not limited to the principle of least privilege, privacy by default, and a preference for simplified designs.

Purpose

1. The purpose of this document is to provide direction to resource owners with respect to the best practical configuration strategies for securing servers, in support of the objectives defined by the ***Information Security Policy***, with the intention of mitigating information technology risks and providing the best and most secure possible computing experience to all customers.

Scope

2. Compliance to the standards within this document is required for all high risk servers, where either the likelihood or impact of an incident is elevated, including:

    a) Servers that are accessible from the public network (internet);

    b) Servers that collect credentials to authenticate people, and particularly those that leverage the centralized authentication services (single-sign-on);

    c) Servers that handle credit card transactions, or are considered to be in scope for PCI-DSS compliance;

d) Servers that are used to collect or handle personally identifiable information (PII), personal health information (PHI), or any other information classified as confidential or restricted according to the ***Information Classification Matrix***.

e) Servers that provide or support communication and collaboration services, including electronic mail.

3. Compliance to the standards within this document is recommended for all other servers that are connected directly to the University data and telephony networks, as well as all other computing resources owned by, operated by, or operated on behalf of the University.

Definitions

4. A **computing resource** is any type of computer that is connected to the University data or telephony network. This includes but is not limited to servers, workstations, laptops, mobile devices, network appliances, telecommunication and teleconferencing devices, printers, automation hardware, and industrial control systems. A **server** is a computing resource that is used to provide a service, or to provide a supporting component to a service.

5. A **service** is software, servers, systems, and / or business processes and policies that fulfill Constituents' computing needs. Examples of services may include email, business process management (i.e., Mosaic), internet connectivity, deskside support, file storage and backup. The **service owner** is the department head who is accountable for the service, and computing resources required to provide the service, within the organization. A **technical specialist** is an individual or team to whom the service owner has delegated the responsibility for configuring and maintaining the computing resources upon which the service is offered.

6. A **public facing** resource accepts anonymous connection requests from any public internet protocol address. An **externally accessible** resource accepts connection requests from a limited number of known external internet protocol addresses. Public facing and externally accessible resources have been included in the perimeter network access control list to allow these connections. An **internal** resource accepts connection requests only from other computers on the University network.

7. **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.

8. **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).

9. **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.

10. **Production** computing resources are those that are used for handling live data and customer requests; **test** computing resources are those that are used to test new configurations and implementations before they are moved into production; **development** computing resources are intended to be used to create new configurations and implementations.

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

REQUIREMENTS

12. Service owners, and their designated technical specialists, are responsible for ensuring that their services and servers are appropriately protected according to the monetary value of the device and / or the classification of information stored on or processed by the device. Where the technology does not support the requirements described by this Standard, compensating controls must be implemented. In such situations, access restrictions must be applied to prevent unnecessary access to the server, especially from the public network.

Physical Environment

13. Servers must be hosted in areas with restricted physical access. Physical access to servers must be controlled proportionally to the value of the server or to the data and information stored on or processed by the server.

14. Physical access security must be maintained throughout all phases of a server life-cycle, including but not limited to design, initial configuration, testing, quality assurance, production, post-production and retirement.

Operating System

15. Vendor or community support must be available for server operating systems. Server operating systems that have reached "end of support" or "end of life" must not be used on production servers that are used to process or store Internal, Confidential or Restricted information.

16. Critical operating system updates, including but not limited to patches and hotfixes, must be installed in a timely manner. Exceptions may be made when installation of an update significantly impacts the functionality of the server or service, and there exists no workaround that would allow for installation of update without such impact. In such situations compensating controls must be implemented.

Applications

17. Servers must be "purpose-built"; servers should be configured to support as few customer facing services as possible.

18. Vendor or community support must be available for application software. Applications that have reached "end of support" or "end of life" must not be used to provide customer facing service, or to process or store internal, confidential or restricted information.

19. Application updates, including but not limited to patches, hotfixes and upgrades, must be installed in a timely manner. Exceptions may be made when installation of an update significantly impacts the functionality of the server or service, and there exists no workaround that would allow for installation of update without such impact. In such situations compensating controls must be implemented.

Server Integrity Controls

20. Unused physical ports and interfaces must be disabled.

21. Servers must be configured to detect and / or prevent the execution of unauthorized, unnecessary or malicious software.

22. Servers must be configured to prevent unauthorized, unnecessary or malicious network connection attempts. Unused services must be disabled.

23. External sources for services that require unauthenticated information polling must be known and trusted. Trust relationships identified be identified and reviewed at appropriate intervals.

24. All non-removable storage media must use file systems with access control enabled.

Server Administration

25. Client computing devices that are used to administer servers must comply with all requirements of the Client Computing Devices Security Standard.

26. Secure protocols and tools must be used for accessing administrative and management interfaces. Access to administrative and management interfaces must be restricted.

Authentication and Access Control

27. Service owners, and their delegated technical specialists, must manage the passwords for accounts with elevated privilege for which they are responsible in a secure manner.

    a) Default manufacturer and /or vendor passwords must be changed before connecting new systems to the network.

    b) Passwords for accounts with elevated privilege must be change regularly.

28. Service owners, their delegated technical specialists, or individuals responsible for creating customer access accounts, including assigning roles and access entitlements,) must establish secure processes and procedures for managing customer passwords:

    a) Roles and access entitlements must always be assigned using the principle of least privilege.

    b) Create strong and unique temporary passwords, and distribute these to customers in a secure manner which assures the confidentiality and integrity of the password. A secure procedure must be used to verify the identity of a customer prior to issuing a password.

    c) Customer password complexity requirements and first logon password reset must be enforced on all systems where the technology permits.

    d) Passwords must be stored and transmitted in a secure manner.

    e) Generic or shared accounts allowing users interactive logins should be disabled.

Vulnerability Management

1. Service owners are accountable to the University for risk related to vulnerabilities on their computing resources. Responsibility for treating this risk may be delegated to technical specialists. Service owners, and their delegated technical specialists, are responsible for managing software vulnerabilities on their servers in accordance with the ***Vulnerability Management Standard***.

Backup, Restore, and Disaster Recovery

2. Servers with operationally critical data must be configured to back up their data at regular intervals. Backups must not be stored solely in the same physical location where the operationally critical data is located. Backups should be appropriately accessible.

3. Service owners, and their delegated technical specialists, must create secure procedures for the restoration of critical data and information, as well as application and operating system configurations, for any server with operationally critical data. Restoration procedures must be optimized to ensure the integrity of the data being restored, as well as to ensure their timely completion during a disaster recovery. Back-up and recovery procedures must be verified regularly.

Server Hardware Disposal

4. Server hardware must be disposed of securely. Storage media and devices that contain University information must be disposed of in a manner that renders the information and data unrecoverable.

High Performance/Distributed Computing

5. Servers participating in High Performance, Distributed, Grid or Cloud Computing configurations must employ appropriate and documented safeguards to protect the confidentiality and integrity of the information.

Logging

6. Server and application logging must be configured to enable effective incident response and problem support. In order to support the creation of an operational baseline for systems, and service activities, and to detect and document access control violations, servers must be configured with appropriate real-time OS/application logging enabled.

7. Where capabilities exist, logs of relevant OS/application information should be retained as appropriate. Logging should include the following elements:

    a) Log entries must be time and date stamped

    b) All authentication

    c) Privilege escalation

    d) User additions and deletions

    e) Access control changes

    f) Scheduled job start-up

    g) System integrity information

8. Service owners, and their delegated technical specialists, must review logging for effectiveness at regular intervals proportional to the value of the system.

9. Intentional logging of confidential information, including but not limited to passwords, is prohibited.