Standard for Internet-Facing Systems and Services

Parent Policy:	*Use of Information Technology Resources*		
Standard Sponsor:	College Information Officer		
Standard Contact:	Manager, IT Security		
Stakeholders:	Okanagan College Application Owners		
Approved by:	College Information Officer		
Effective Date:	29-April-2024		
Last reviewed:	29-April-2024	Scheduled review date:	29-April-2025

1. Purpose

1.1 College systems and services that are Internet-facing (i.e. visible or accessible from the Internet) are prime targets for exploitation. Without adequate security, these systems and services provide an avenue for malicious activity such as theft of College electronic information or the denial of service to College resources.

1.2 This document defines minimum standards to be followed by College IT staff for the security architecture, protected network protocols, hardening/patching and monitoring/logging of College's Internet-facing systems and services to ensure they are adequately protected. This standard focusses on web servers because these are primary targets for exploitation and therefore pose the highest risk to the College. Servers that are not Internet-facing, such as intranet servers, should also follow this standard, wherever feasible.

2. Security Architecture Requirements

2.1 Web applications must be protected with the following compensating controls:

a) web application (layer 7) firewall;

b) file integrity monitoring;

c) Intrusion Detection Systems/Intrusion Prevention Systems; and server endpoint monitoring (XDR/MDR)

d) log monitoring (e.g. SIEM).

2.2 Ideally, web application and database functions should be hosted on separate servers;

2.3 When web, application and database functions are hosted on separate servers, web servers are permitted to communicate with application servers but not with database servers.

2.4 All Internet-facing servers must be placed in a Demilitarized Zone (DMZ) configured as follows:

a) the DMZ must contain all web servers;

b) the DMZ may only contain application servers if they are combined with web servers;

c) the DMZ must not contain database servers that store or process high or very high risk information;

d) a firewall must be in place between the DMZ and the Internet as well as between the DMZ and the College internal network;

e) wherever possible the DMZ should be protected from the Internet by web application firewalls, as they are better equipped to protect web applications from threats;

f) firewalls must use ingress filtering at a minimum, and must also use egress filtering if the firewall is used to protect high or very high risk information; and

g) firewalls must use access rules that restrict traffic to only the minimum necessary to conduct College business; access rules must not be wide-open allowing any source to connect to any destination, as this defeats the security of the firewall.

2.5 Access to all medium, high and very high risk information on servers must be authorized and limited based on the user’s role, following the principle of least privilege.

3. Network Protocol Requirements

3.1 Secure transmission of medium, high or very high risk information must comply with the following requirements:

a) any form, application or service that requires some type of authentication, or that is used to collect or transmit information from user to server or between servers, must be encrypted using HTTPS with TLS version 1.2 at a minimum (or the equivalent, for non-web-based applications);

b) information transmitted via SSH must be encrypted using a minimum of AES-256-bit encryption with mutual authentication between the server and user; and

c) known weak network protocols (e.g. all versions of SSL, and TLS versions prior to 1.2) should be disabled.

3.2 Secure transmission to/from Web applications is required to be encrypted using HTTPS with TLS version 1.2 at a minimum.

3.3 It is required that all HTTP requests are re-directed to HTTPS.

3.4 Users frequently access desktops, laptops and servers remotely. Remote access covers a broad range of technologies, protocols and solutions (e.g. RDP, SSH, VNC, VDI, terminal services, etc.). Remote access must comply with the following requirements, where possible:

a) Multi Factor Authentication (MFA) must be used;

b) Remote access servers (e.g. terminal server, VDI, Remote Access Gateways, etc.) must be located in the DMZ and use strong encryption for server-to-user transmissions, e.g. RDP with network level authentication, SSH with AES-256-bit encryption, etc.;

c) host desktops, laptops or servers not located in the DMZ must be remotely accessed via a remote access gateway, VPN or SSH; and

d) VPN connections must be encrypted and restricted at both ends to the minimum number of systems necessary. To support this:

i) DNS or service-based split tunneling (e.g. Dynamic Split Tunneling) may be used with authorization of specific services by IT Services;

ii) IP or subnet-based split tunneling must not be enabled; and

iii) Local LAN access may be enabled with authorization by IT Services.

3.5 Servers running other Internet-facing protocols must be located in the DMZ and must encrypt transmissions of medium, high or very high risk information.

4. Additional Requirements for Merchant Systems

4.1 College IT staff must configure remote access technologies, used in Merchant Systems, to automatically disconnect user sessions after a specific period of inactivity. 30 minutes is recommended.

5. Hardening and Patching Requirements

5.1 Servers must be hardened, patched, and scanned in accordance with the Vulnerability Management standard.

History / Revisions

Date	Action
2024-04-29	*New Standard Approved by: College Information Officer*