Policy Name:	CUNET Domain Membership and Access Policy
Originating/Responsible Department:	Information Technology Services (ITS)
Approval Authority:	Chief Information Officer (CIO)
Date of Original Policy:	July 2013
Last Updated:	April 2018
Mandatory Revision Date:	April 2023
Contact:	Director, Information Security, ITS

1 Policy

CUNET is the primary network logon and computer management domain for faculty, staff and students. This policy establishes the standards, guidelines and processes relating to the configuration and management of the CUNET domain and its member systems to ensure that the domain is operated in a consistent and secure fashion.

2 Purpose

This Policy describes the CUNET domain membership requirements for workstations and servers and the requirements for access to CUNET resources.

3 Scope

This Policy applies to individuals and systems that use, access, or otherwise interact with the CUNET domain

4 Procedures

4.1 CUNET Access

All computer or computing devices connecting to and accessing the CUNET domain for resource access must have a vendor supported operating system and be appropriately patched according to the vendors release cycle.

In the case where domain resources must be accessed by systems that are not member objects of the CUNET domain, the following security requirements exist:

- Maintain current patch level for all software installed. Critical patches that address a severe vulnerability (ex: Common Vulnerability Scoring System score greater than 4) must be validated and applied within 30 days or sooner.

- Where available, operating systems must be protected by an up-to-date industry recognised endpoint security product.
- Support vulnerability assessments to ensure the security of the system.

4.2 Domain Membership for Computer Objects

All systems that are connected to the domain exist as a computer object. These are the minimum set of requirements for any computer object that is connected to the CUNET domain.

ITS monitors the wellbeing and health of the CUNET domain and may need to remove or limit membership to the CUNET domain, or potentially remove a computer object from the CUNET domain, to maintain the security of the environment.

Member computers must meet minimum security standards to be permitted domain membership – computers that do not meet these requirements may be removed from the domain until these requirements have been met.

All domain member computers must:

- Support centralized management for the delivery of OS and software upgrade, updates, and security patches.
- Have an OS image provided by ITS, or have an OS installation that meets these requirements.
- Be protected by the Carleton University approved Anti-Virus and Malware protection agent or agents and accept delivery of regular updates to anti-virus definitions or update software.
- Be centrally managed by a host based firewall.
- Be securely configured according to ITS or industry standards.
- Allow Domain Administrators access for CUNET management purposes.
- Be running operating systems in a vendor supported state.
- Be running software in a vendor supported state.
- Not be tampered or modified in such a way to affect the security of the operating system and/or the security of the system software.
- Have regular vulnerability assessments performed by ITS.
- Have their vulnerability assessment findings remediated.

4.3 Domain Membership for Workstations

Workstations that are members of the CUNET domain are provided with enhanced access to domain services. Administrative workstations that do not communicate with the domain controller for 90 days or greater are subject to removal from the domain.

4.4 Domain Membership for Servers

Servers that are members of the CUNET domain are provided with enhanced access to domain services.

Servers must meet additional security requirements to join the CUNET domain. These additional security requirements include:

- Member Servers must be securely configured in accordance with standards (Member Server Baseline Security Standard and specific Server-Role standards)

- Servers must employ firewalls and be zoned appropriately (e.g. PCI-DSS systems are properly segmented).
- All CUNET servers will be physically secured in an ITS approved data centre.
- Ingress and egress firewall rules must prohibit all unsolicited network traffic, including internet access.

4.5 Domain Controllers

Domain Controllers are responsible for the authentication requests within the CUNET domain. These authentication servers require additional safeguards to preserve their confidentiality, integrity and availability.

The following are the additional requirements for Domain Controllers on the CUNET domain:

- Domain controllers for the CUNET domain will be securely configured in accordance with applicable Carleton University standards for Windows servers and Active Directory configuration and hardening.
- All CUNET domain controllers will be physically secured in the Robertson Hall data center or Library data center.

4.6 Domain and/or Forest Trust Relationships

Trust relationships between domains establish a trusted communication path through which a computer in one domain can communicate with a computer in the other domain. Trust relationships allow users in the trusted domain to access resources in the trusting domain.

Carleton University does not permit any form of Domain or Forest Trust with CUNET, and therefore the creation of domain or forest trusts is prohibited.

5 Roles and Responsibilities

When managing CUNET or utilizing resources from CUNET the following roles and responsibilities apply.

ITS is responsible for:

- Ensuring the computer meets the membership requirements for the CUNET Active Directory domain, and where necessary, zoned correctly.
- Ensuring the host based firewall rules are enforced where necessary, and any appropriate outbound whitelisting is defined.
- The removal of the computer object from the domain if it no longer meets the membership requirements of the CUNET domain.
- Ensuring the computer is actively managed including software delivery, configuration settings and firewall management.
- Ensuring that operating system updates and software updates are applied.
- Ensuring all software that is installed is licensed and has vendor support for security and update patching.
- Ensuring the computer has the required protections in place.
- Ensuring servers are inventoried and identify the system and process owner(s).

- Ensuring that servers are physically secured.
- Ensuring that no domain or forest trusts are formed or created.
- Ensuring that all member computer objects are part of the ITS vulnerability management program.
- Remediation of vulnerability assessment findings.
- Patching of server components supported by ITS.

Computer Support Units are responsible for:

- Installing operating systems that are vendor supported and are patched with security and stability updates.
- Ensuring that computer objects that are joined to the domain follow standard naming conventions.
- Ensuring all software that is installed is licensed and is at current vendor support levels.
- Ensuring designated domain accounts are provided local administrator rights for computer management.
- Ensuring that all member servers are part of the vulnerability management program.
- Remediation of vulnerability assessment findings.

Faculty, staff and students are responsible for:

- Ensuring that the computer system is not altered in any way to prevent the management and security of the domain joined computer object.
- Ensuring that only approved, licensed software is installed on a member computer.
- Ensuring that the computer is not altered in any way that would remove its eligibility for being a CUNET member computer.
- Having a industry recognised anti-virus and malware protection installed and running.
- Ensuring that their personal computers have the latest security updates for the OS and software installed.
- Remediation of vulnerability assessment findings.

6 Compliance

Non-compliance with this policy may result in disciplinary action, and/or the removal of domain use privileges.

7 Contacts

Director, Information Security, ITS

8 Links to Related Policies

Related Carleton University polices are located here: https://carleton.ca/secretariat/policies/

- Information Security
- Information Technology (IT) Security
- Mobile Technology Security
- Password Policy for Information Systems
- Remote Network Access

The Carleton ITS specific polices are located here: https://carleton.ca/its/about-its/policies/

- Vulnerability Management Policy