Carleton UNIVERSITY
Canada's Capital University

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

Policy:
CUNET is the primary network logon domain for students, faculty, and staff. Information Technology Services (ITS) owns and is the custodian of the CUNET domain. ITS reserves the right to set policy and standards relating to the configuration and management of the CUNET domain.

Purpose:
This Policy describes the requirements for workstations, servers and domains to connect to, or access the CUNET domain services and resources.

Scope:
This Policy applies to all IT systems that connect to, or access the CUNET domain services and resources.

Procedures:
Domain Controllers

- Domain controllers for the CUNET domain will be securely configured in accordance with applicable Carleton University standards for Windows servers and Active Directory configuration
- All CUNET domain controllers will be physically secured in the Robertson Hall data centre, Library data centre, or other facilities deemed suitable by ITS

Domain Membership for Workstations
Workstations that are members of the CUNET domain are provided with enhanced access to domain services:

- Workstations must meet minimum security requirements, as defined by ITS, to join the CUNET domain. These minimum security requirements include:
    - Windows workstations must use one of the approved and supported operating systems
    - Workstations must use the institution's selected virus scanning software that is automatically kept up to date with the latest virus definitions from centralized servers maintained by ITS

        - Workstations must maintain up-to-date operating systems security patches – Updates will be centrally pushed to Windows workstations by ITS using the Systems Center Configuration Manager (SCCM) solution
        - Use of workstation firewall to secure workstation communications with the network – the firewall must employ a centrally managed policy
        - Workstations must be securely configured in accordance with ITS standards
        - Workstations must be configured to support CUNET server security configurations
    - Workstations that need to access the MS Exchange service must use Outlook 2010 (or greater) email client software or rely on Outlook Web Access for email access
    - Workstation membership in CUNET requires the use of the standard ITS workstation images as a baseline
    - Workstations must allow Domain Administrators access for CUNET management purposes – in addition, the ITS Service Desk (on site) must have local administrator access
    - Workstations must meet minimum security standards to be permitted domain membership - those that do not meet security requirements will be removed from the domain until security issues have been rectified
    - Administrative workstations that do not communicate with the domain controller for 90 days will be subject to removal from the domain – ITS will periodically (e.g. once per month) run a process to perform this cleanup activity
    - To ensure availability of lab services, lab workstations will be cleaned up according to a different schedule

Domain Membership for Servers

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

- Servers must meet minimum security requirements, as defined by ITS to join the CUNET domain. These minimum security requirements include:
    - Member Servers must be securely configured in accordance with ITS standards (Member Server Baseline Security Standard and specific Server-Role standards)
    - Windows servers must use one of the approved and supported operating systems
    - Member servers must use virus scanning software that is automatically kept up to date with the latest virus definitions
    - Member servers must maintain up-to-date operating systems security patches
    - Updates will be managed by ITS using the System Center Configuration Manager client to ensure that undue risk is not posed to other servers in the CUNET domain
    - Servers must employ firewalls and/or IPSec (Internet Protocol Security) policies to secure communications with the network
    - Servers must be configured to support CUNET workstation security configurations
- Member servers must allow Domain Administrators access for CUNET management purposes
- Member servers must meet minimum security standards to be permitted domain membership – servers that do not meet security requirements will be removed from the domain until security issues have been rectified

Domain 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.

- As a general practice, trust relationships are not generally recommended and two-way trust relationships with external domains will not be established
- As custodians of the CUNET domain, ITS reserves the right to deny requests for establishing trust relationships between the CUNET domain and other domains on/off campus
- External domains may establish one-way trust relationships where CUNET is the trusted domain, and the external domain is the trusting domain – an initial review of intended needs and a threat-risk assessment will be conducted prior to allowing trust relationships

Access to CUNET resources from non-domain members

In the case where domain resources must be accessed by systems that do not belong to the CUNET domain, the following security requirements must be adhered to:

- Systems accessing domain resources must meet minimum security standards for workstation or server access to the CUNET
- Where necessary, ITS may allow non-domain systems to authenticate to specific resources in the domain, without providing logon access to the domain – an initial review of intended needs and a threat-risk assessment will be conducted prior to granting access

Compliance:

Non-compliance with this Policy may result in disciplinary action.

Contacts:

Director, Information Security, ITS

Links to Related Policies:

N/A