



UCIT INFORMATION SECURITY STANDARDS

Network Security Zones Standard

Classification Information Management	Table of Contents Definitions 1 Rationale 2 Applicability 3 Standard 4 Exceptions 5 Related Standards 6 History 7
Standard # ISS-012	
Approval Authority Chief Information Officer	
Implementation Authority Information Security Officer	
Effective Date Sept 10, 2010	
Latest Revision Sept 10, 2010	

- Definitions 1**
- 1.1 Zone: a portion of the data network delimited by a firewall. It may include private addresses, whole or partial subnets or virtual local area networks (VLAN).
 - 1.2 Sub-Zone(s): A portion of a Zone which may or may not be limited by Firewall.
 - 1.3 Area: A group of network Zones that share a trust relationship.
 - 1.3.1 Trusted Area: An area where all communication occurs between managed devices.
 - 1.4 Firewall: Firewalls can be physical or logical appliances.
 - 1.5 Access to Service: A client is allowed access to a specific service through a specific port or range.
 - 1.6 Secondary firewalls: a firewall that resides on a separate physical appliance from the Edge firewall.
 - 1.7 Public Facing: Services that require direct client access from the internet.
 - 1.8 Managed Devices: Have the following criteria.
 - a. All computers must allow automatic antivirus updates where applicable.(software and signatures)
 - b. All computers must have an approved management client installed where applicable.
 - c. All computers must allow automatic updates to be pushed by a centralized

management system.

Rationale 2 To prevent unauthorized use of resources, protect confidential data, and protect the integrity of our network and devices. Network segmentation allows data traffic to be separated into groups and provides containment should security incidents occur. This standard documents Zone specifications, requirements, and device placement.

Applicability 3 This standard applies to all devices connected to University of Calgary data networks.

Standard 4

4. All Network Security Zones

The following requirements apply to all Network Zones:

- a. All Zones must be protected by the Edge firewall.
- b. Logical or physical network segmentation is accepted for all Zones.
- c. In the Trusted and Semi-Trusted Areas, individual Zones may contain servers or clients, but not both
- d. Devices are not allowed to reside in multiple Zones, with the exception of firewalls and VPNs and devices with interfaces on the management network and the storage network.
- e. Sub-Zones are accepted but must comply with the corresponding Zone requirement.
- f. All public-facing services must reside in the Demilitarized Zone (DMZ) or in the Unmanaged Research Zone (approval required).
- g. Only the DMZ and the Unmanaged Research Zone can be accessed from the Internet without VPN access.
- h. All configuration and management of devices requires VPN access.
- i. No physical server will host virtual servers in multiple network zones.

4.1 Untrusted Area

Devices residing in this network area are not expected to be secure. High availability and critical systems, or systems containing confidential or highly confidential data will not reside in this area. Network service may be denied in case of security incidents and traffic will be constantly monitored.

4.1.1 Unmanaged Client Zone

This network Zone includes all devices that are not managed by UCIT. Devices residing in this section of the network will only be protected by a single Edge firewall and are encouraged to run antivirus software. Users connected to this section of the network are responsible for the security of their own devices, which may be blacklisted if deemed compromised or acting suspicious.

Specifications:

- a. Unmanaged host computers from Students, staff and faculty
- b. All devices that cannot be assigned to any other network Zones shall reside in this Zone.
- c. Network access is provided via landline or wireless.

4.1.2 Computer Labs/Learning Environments

This network Zone includes all lab devices.

Specifications:

- a. Only approved lab devices are permitted in this Zone.
- b. Network access is provided via landline only.
- c. No public facing servers are allowed in this Zone
- d. All devices must be managed

4.1.3 Unmanaged Research Computing Zone

This network Zone is provided for research computing only. This is an unmanaged zone, so users with compliance requirements or confidential data are advised to use the Managed Research Server Zone instead. All users must apply for this zone and applications will be reviewed on an individual basis.

All systems in this zone must be part of research initiatives or actively involved in supporting research projects.

4.1.4 Third-Party Networks

This section provides ISP type network connectivity to business partners that are not UofC owned or managed such as government bodies, companies, or institutes.

Specifications:

- a. These networks are subject to security scanning and monitoring conducted by UCIT.
- b. Third Parties are responsible for the security of their own devices. Network service may be denied in the event of a security incident.
- c. All inbound internet access must be requested as it is denied by default.
- d. This zone will use the public address space (136.159.xxx.xxx)

4.2 Trusted Area

Traffic originating from this area is considered to be secure. This does not mean that it is free from a possible security outbreak, but incidents can be avoided and controlled. The Trusted area must be protected by a secondary firewall managed by UCIT

4.2.1 Managed Client Zone

This network Zone is provided to all UofC owned client computers that are managed by UCIT. A secondary firewall will restrict all inbound or incoming connections.

Specifications:

- e. Only client administrative computers are permitted in this Zone.
- f. Access is provided via landline or wireless through AirUC Secure
- g. No servers are allowed in this Zone
- h. All devices must be managed

4.2.2 Managed Isolated Zone

This is an isolated section of the network to provide data traffic to independent services that are free from any external access, except for management purposes. Services will

include control systems (HVAC) card systems access (including CampusOne) and other systems that require complete network isolation. Access to this Zone for the purposes of management will be granted point-to-point and under supervisory approval only.

Specifications:

- a. All devices permitted in this zone must be approved by Network Services.
- b. Network access is provided via landline or encrypted wireless.
- c. Isolated zones are logically segmented.

4.2.3 Managed Server Zone

This is a secure segment of the network and will include all servers that contain confidential or highly confidential information as defined in the U of C Data Classification Standard. Servers may include all 3-tier back end systems, databases and other storage solutions with restricted access.

Specifications:

- a. Only servers are permitted in this Zone.
- b. No public facing servers are allowed in this Zone.
- c. Clients in the Managed Client Zone are allowed to connect to systems in this Zone through a firewall.
- a. Network access is provided via landline only
- h. All devices must be managed
- i. Server administration and management must be done via the Managed Client Zone. Direct VPN access may be allowed when explicitly required and requested.

4.2.4 Managed Research Computing Server Zone

This zone follows the same specifications as the *Managed Server Zone*, but it is limited to research servers containing confidential or highly confidential data. Specifications for the Managed Server Zone apply.

All systems in this zone must be part of research initiatives or actively involved in supporting research projects.

4.2.5 Management Network

This zone is restricted to management protocols and services only. This includes availability monitoring, configuration protocols for the purposes of managing servers residing in the following zones:

- a. Demilitarized Zone (DMZ)
- b. Internal Demilitarized Zone (iDMZ)
- c. Managed Server Zone
- d. Managed Isolated Zone
- e. Managed Research Server Zone

All access to this zone must be requested from Network Services. The management network will be connected to specific management interfaces that support physical separation from the standard network connectivity port.

4.3 Semi-Trusted Area

This section of the network provides all user-facing services, internal and external to the Internet. This is considered a high-risk area for attacks and malicious activity; therefore services will be hardened and all traffic constantly monitored.

4.3.1 Demilitarized Zone (DMZ)

All managed client-facing services available to the Internet must reside in this Zone. This includes any service that allows direct connection from the *Untrusted Area*.

Specifications:

- a. Only servers are permitted in this Zone.
- b. Network access is provided via landline only
- b. All servers in this Zone are public-facing.
- c. Only non-confidential information may be stored locally on servers in this Zone.
- d. Service connections are accepted from anywhere unless blacklisted.
- e. Service connections are TCP/IP port or range specific
- f. Traffic inside this Zone will be controlled to enhance security
- g. Server traffic (back end services) to the Managed Server Zone is allowed point-to-point and through specific ports.
- h. All devices must be managed

4.3.2 Internal Demilitarized Zone (IDMZ)

All managed client-facing services only available to local networks must reside in this network segment. This includes any service that must be available to both *Untrusted* and *Trusted Areas*.

Specifications:

- a. All servers in this Zone are internal-facing only
- b. Only servers are permitted in this Zone.
- c. All data stored in this Zone may be available to all network zones; additional controls may restrict access to specific Zones or Areas.
- c. Network access is provided via landline only
- d. Servers in this Zone can further restrict access based on service requirements
- e. Service connections may be accepted from all local area networks (LAN) unless blacklisted.
- i. Service connections are TCP/IP port specific
- f. Traffic inside this Zone will be controlled to enhance security
- g. Traffic to the Managed Server Zone is allowed point-to-point and through specific ports.
- h. All devices must be managed

4.4 Storage Network AREA

This zone is restricted to storage protocols only and may be IP based or non-IP based storage. Only servers in the following zones are able to connect to the storage network directly:

- a. Demilitarized Zone (DMZ)

- b. Internal Demilitarized Zone (iDMZ)
- c. Managed Server Zone
- d. Managed Isolated Zone
- e. Managed Research Server Zone

The Storage Network Area will not accept direct client connections.

- Exceptions** **5** The CIO can approve exceptions to the above standard. Exemption requests must include detailed descriptions of:
- a. Why the exemption to the above standard is being requested
 - b. The compensating logical and physical security controls, which ensure the security of the applicable systems.
 - c. How this exemption maintains the integrity of all security Zones

- Related Standards** **6** Vulnerability Assessment Standard
Remote Access Standard

- History** **7** March 19, 2009 Initial Draft
September 10, 2010 Approved by CIO

=