

Internet Services (Server) Registration Policy

POLICY:

All devices connected to the Darton College network that are intended to “serve” information to on or off campus users must be registered with Office of Information Technology (OIT).

Rationale:

The rising frequency of security incidents involving network-attached devices significantly increases the probability of major disruptions to the internal computer systems of the College. Current server technology is easily implemented but the platforms if not properly configured provide an extremely vulnerable and high risk opportunity for exploitation and significant damage to other connected devices, other external devices, and other users. Registration of all such serving devices with accompanying procedures for verifying security configurations will significantly reduce the potential for this type of damage and also greatly shorten the time needed to identify and isolate equipment which has been inadvertently compromised. Additionally, care taken in build and deployment of serving devices provides a greater level of protection to other devices connected to the network. Establishing policy centrally and issuing standards and utilities from a central authority allows for rapid incident response and continuous update of protection methods.

Standards & Procedures:

Standards:

Compliance. Chairs and Vice Presidents are responsible for monitoring compliance with this policy and associated standards by: (1) directing the registration of machines within their respective organizations that meet the standard definition of servers; and (2) directing reviews of, and action on, reports on unregistered serving devices connected to the College network that are generated by OIT .

Definition of Servers. Typically, servers are machines that have intentionally been set up to provide services to others on campus or the Internet. These provided services could include Web (http) servers, FTP servers, file sharing servers, etc. Most of these services are not typically offered by end-user workstations. However, if an end-user workstation has installed or turned on web server, FTP server, etc. services, this machine would be required to register as a serving device.

Server Registration. As a minimum, OIT must be provided the following information on each device currently or intended to be attached to the College network for the purpose of “serving” information either on or off campus:

- Brand of hardware platform
- Operating system version
- Equipment MAC address
- Requested DNS name

- Assigned or requested IP address
- Person responsible for management of the device (including phone number and email address)
- Device physical location
- Internet services being offered by the platform
- Security Protection measures applied to the device

As a continuing activity associated with normal network management, OIT will periodically scan for network-connected devices. Any unregistered serving devices found during these scans will be isolated from the network until proper registration is accomplished. When it has been determined by the College Information Security Officer that a security incident or compromise has occurred, failure to have accomplished registration will result in deactivation of network ports associated with the serving device.

Server Security Audits. Administrative departments are responsible for developing and administering their own local procedures for initial verification of server security configuration as well as for ensuring that updated security patches are applied to serving devices within their respective organizations. Assistance from the College Network Support Specialist is available for initial system verification and for periodic scans of systems. OIT will provide minimum requirements for server configurations. Failure to meet these minimums will result in the serving device being isolated from the network.

Procedures:

[Register an Internet Services \(Server\) Device](#)

[Ensure Currency of Patches for Internet Services \(Server\) Devices](#)

Register, view, update, or delete existing information for Internet services devices attached to the University network.

About:

The **Internet Services Registration Policy** requires that Internet services devices (servers) be registered with Office of Information Technology. A server is defined as any device attached to the College network for the purpose of "serving" information either on or off campus. The registration process requires very specific technical information; therefore, it is suggested that each Department designate one or more technical staff members to register devices for their area.

Register a Device:

1. Complete the form "DNS Request" in Public Folders under Office of Information Technology.
You will be contacted (usually within 24 hours) with your information.

Help:

If you have questions, or need assistance, please contact the Helpdesk (229-317-6704) or helpdesk@darton.edu.

Ensure that steps are taken to provide current security patches on server devices that are to be attached to the Darton College Network and the Internet.

Guidelines for Securing a Device to be Attached to the Network and the Internet:

1. **Protect the device before it is attached to the network.**

Devices can be compromised or infected with a virus within minutes of connection to the network. Do the following before attaching the device to the network:

 - Install current security patches for the device
 - Install anti-virus software
2. **Use Antivirus software.**

Antivirus software is a necessity for windows operating system devices. Configure it to:

 - Scan for viruses in real time
 - Daily automatically update of virus signatures
 - Periodically perform a full virus scan of the device
3. **Shut down unnecessary services.**

Disable services that are not required for the desired function of the device. Devices often come with many services enabled by default that are not necessary. Services that are not running cannot be used to penetrate the device.
4. **Install and configure a firewall.**

A device may be protected by either an internal host based firewall or an external stand alone firewall. A firewall stance of "everything that is not explicitly denied is not allowed" is the industry best practice.
5. **Enable and enforce password standards.**

Configure the device to require strong passwords. Enable as many of the following standards as possible:

 - Length of 6 characters or more
 - No word that can be found in a dictionary
 - A mixture of upper case, lower case, numerals and special characters
 - Password must be changed every 90 days
 - Passwords may not be reused
6. **Enable and configuring logging.**

Typically, very little logging is enabled by default. Logging is extremely useful for detecting and unsuccessful and successful attempted penetrations.
7. **Stay up to date on security patches.**

Security is an ongoing process. Apply security patches or workarounds promptly.
8. **Keep informed on security issues.**

There are many security mailing lists and web pages available on the Internet. At a minimum, you should join the security alert mailing from the manufacturer of the network device if one is available. Here are links to sites for some major vendors as well as general security and antivirus information web sites. Many of these sites have mailing lists you may join to alert you to new security
9. **Vulnerabilities and patches.**
 - SANS – Sysadmin, Audit, Network, Security Institute
<http://www.sans.org>
 - CERT – Computer Emergency Response Team Coordination Center
<http://www.cert.org>
 - CIS - Center for Internet Security
<http://www.cisecurity.org>
 - Security Focus
<http://www.securityfocus.com>

- Microsoft Security Information
<http://www.microsoft.com/security/default.asp>
- Sun Microsystems Security Information
<http://sunsolve.sun.com/pub-cgi/show.pl?target=security/sec>
- Apple Security Information
<http://www.info.apple.com/usen/security/index.html>
- Linux Security Information
<http://www.linuxsecurity.com/>

Help:

If you have questions, or need assistance, please contact the Help Desk (229-317-6704) or helpdesk@darton.edu).