DePaul University Computing Policy

Category: Operations
Responsible Department: Information Services
Responsible Officer: Vice President for Information Services
Effective Date: 10/9/2015

Policy Summary

This policy provides general principles, guidelines and security requirements for all computing environments at DePaul University.

Scope

This policy affects the following groups of the University:

- Hiring/Supervising Managers
- Executive Offices
- Assoc. / Assist Vice Presidents
- Full-Time Staff
- Part-Time Staff
- Full-Time Faculty
- Part-Time Faculty
- Budget Managers
- Student Employees
- Vice Presidents
- Deans
- Directors/Department Chairs

This policy applies to all members of the above groups.

Policy

In order to protect university data and provide a safe computing environment on campus, this policy must be followed for all computing devices or environments that are purchased by DePaul University or used to access DePaul University data. If you are unsure whether or how this policy applies to your circumstances, please contact Information Services (IS) for clarification. IS may detect devices found to be in non-compliance with this policy and will make reasonable attempts to identify a responsible party and remedy the issues. IS reserves the right to disconnect devices from

the DePaul network as needed to ensure a safe and secure computing environment. Individuals, departments, or units owning computing devices shall bear the costs of ensuring compliance with this policy. If you are unable to comply with portions of this policy, please contact Information Services to discuss exceptional situations

General Principles for All Computing Environments

Passwords

- Devices must be protected by strong passwords that are resistant to dictionary attacks.
- Configurations and selected passwords should follow the password guidelines detailed in the Access to and Responsible Use of Data policy.
- Passwords must be encrypted in transit and in storage.
- Default passwords should always be changed when initially configuring a device.

User Accounts

- Use of group or shared user accounts is strongly discouraged so DePaul University can maintain individual accountability across its technology systems.
- Guest accounts should be disabled.
- Default superuser accounts should be renamed when possible on Windows operating systems.
- On an ongoing basis, system administrators are responsible for ensuring that only authorized users retain access to resources. Further details regarding review requirements for access to sensitive data can be found in the Access to and Acceptable Use of Data policy.

Updates and Patches

- Patches impacting the functionality or availability of software or systems must be applied in a timely fashion.
- Critical security patches (as designated by the vendor) should be applied immediately or as soon as reasonably practical.
    - Testing the patch (or validation that others have tested it) before applying it to production environments is recommended to avoid unintended service disruptions.
    - While Information Services will deploy critical security patches for some software and systems, end-users and other administrators are responsible for the rest. Generally speaking, though not in all cases, the person or entity which performed the initial system or software installation should be responsible for patching. For a list of what software and systems Information Services will patch, visit https://offices.depaul.edu/information-services/services/computers/Pages/Updates-and-Patching.aspx.
- For assistance assessing the potential impact and importance of released patches, contact Information Security at security@depaul.edu

General Controls

- Configure auto-logoff or auto-screen locking to trigger after 30 minutes of inactivity, requiring a password on wake.
- If a device outside DePaul University's datacenters is network connected, and the operating system includes a software firewall, activating the firewall is a minimum requirement.
- Display the following notice prior to allowing access to the system:

This is a DePaul University resource. This computer system, and all related equipment, networks, and network devices are provided for authorized use only and are subject to DePaul's Acceptable Use Policy. DePaul may access and monitor university computing resources and any information stored on or transmitted through them in accordance with applicable laws for legitimate business purposes including, but not limited to, system monitoring and maintenance, complying with legal requirements, and administering DePaul Policies.

- Remote administrator access methods must use at least 128-bit encryption.
- Unneeded services should be removed or disabled.
- Lost or stolen computing devices containing any DePaul University data must be reported to Information Security (security@depaul.edu) immediately. Other reporting responsibilities are described in the Fixed Asset Management policy.

Computers

- Information Services is responsible for determining which computing devices, systems, and methods of access are acceptable for conducting university business.
- When purchasing computers with university funds, employees must choose the device which suits them best from the list of Approved Desktop/Laptop/Tablet Computers at https://offices.depaul.edu/information-services/services/administration/computer-replacement/Pages/computer-standards.aspx
- Computers purchased from the Approved Desktop/Laptop/Tablet Computers list will be deployed by Information Services with the university image.
    - The university image complies with the general computing principles detailed in this policy.
    - The university image includes enterprise-licensed software and services which will not be available to computers not running the image.
- Exceptions may be granted by the Vice-President of Information Services in cases where business needs cannot be met by any of the pre-approved computer options. IS technical staff will assist in the selection of alternate models.
- DePaul owned desktop, laptop, and tablet computers must be covered by a manufacturer's warranty in order to receive hardware support from IS. IS recommends a 3 to 4 year life cycle for most computers.
- DePaul University owned computers that have reached the end of their service life must be disposed of via the Salvage of University-Owned Equipment policy.
- Computer support and repair work must be completed by DePaul University employees, original equipment manufacturers (i.e. Apple, Dell), or other service providers authorized by IS.
- Employees are responsible for keeping any self-installed software up to date, and safely configured. The Software Licensing policy details requirements and procedures associated with acquiring and installing software.

- Full disk encryption is strongly recommended for all computers. Additionally, employees should reference the data classification matrix in the Access to and Responsible Use of Data policy to know which data must be encrypted, no matter where it is stored. Additional information about data encryption, including instructions, can be found here.
- Systems must have anti-virus software installed. Anti-virus software should be configured to update daily and perform real-time scanning.
- Employees are responsible for backing up their own data. IS recommends use of the U: drive for storage of university data. IS centrally backs up data on the U: and W: drives and retains the ability to restore recently lost files saved to this environment.
- Personally owned computers used on the DePaul University network should follow the general computing principles detailed in this policy.

Mobile Devices

- Employees should note the requirements of the Mobile Devices policy.
- University owned mobile devices that have reached the end of their service life must be disposed of via the Salvage of University-Owned Equipment policy.
- Employees are responsible for keeping mobile devices up to date, and safely configured.
- It is strongly recommended that DePaul data stored on mobile devices be encrypted.
- Personally owned mobile devices used on the DePaul University network should follow the General Computing Principles detailed in this policy.
- Mobile devices used to access DePaul data are required to issue a user challenge (such as a PIN or password) before granting access to the device.

Network Connected Devices

- Operating devices, servers, or services which may disrupt DePaul University network services are prohibited. Examples of prohibited equipment and services are:
    - DHCP Servers
    - DNS Servers
    - Network Address Translation or IP Masquerading Services
    - Routers
    - Wireless Access Points
- Permanent use of network switches or hubs is not allowed and may lead to service disruptions.
- If you have questions about other network devices, please contact the technology support center.
- When purchasing printers with university funds, departments must choose the printer which best suits their needs from the selections made available by Procurement Services.
- Personally owned devices used on the DePaul University network should follow the general computing principles detailed in this policy.
- Scientific devices which need an internet connection should be reviewed by, and setup in consultation with Information Services.

Cloud Services

- Using cloud services may introduce risk to the university. Information Services (IS) and the Office of General Counsel (OGC) are resources available to help understand these risks. Refer to the Purchasing Authority and Responsibilities policy for determination of which purchases of cloud services must be reviewed by Information Services. Additionally, IS has published Guidelines for Selecting Cloud Services, to aid decision-making and provider assessments in this area.
- As determined by the Security Classifications & Controls Matrix in the Access to and Responsible Use of Data policy, DePaul data classified as internally restricted or highly sensitive may not be stored on cloud devices unless they have been reviewed by IS, and the relevant contracts and/or terms of use have been reviewed by OGC pursuant to the Contract Requirements and Procedures policy, regardless of dollar amount. For example, this includes services like Dropbox, desktop backup to the cloud, email services, and iCloud.

Servers

- Servers connected to the DePaul campus network must be located in one of the university datacenters.
- Special circumstances may exist which prevent a server from being located in a datacenter. In these cases:
    - Exceptions must be approved by the Vice-President of Information Services
    - As directed by Information Security, servers granted exceptions may require additional setup, departmental funding for additional risk mitigation, or a university officer to submit a Risk Acceptance form.
    - Servers must be housed in a locked, physically secure area accessible only to those requiring access.
- Systems should have anti-virus software installed. Anti-virus software should be configured to update daily and perform real-time scanning.
- Information Services provides a hosting service for customers who wish to perform and be responsible for application administration functions themselves. In exceptional cases, a transfer of departmental resources may be required to ensure that IS has adequate physical resources to offer this service. A more in-depth explanation of the IS hosting service is provided at: https://offices.depaul.edu/information-services/services/administration/Pages/Hosted-Infrastructure.aspx.

Glossary of Terms

- **Server:** A computer that provides data or other services to other computers or users over a network.
- **Computer:** Refers to devices traditionally referred to as personal computers, and are available in desktop, laptop, and tablet form factors. These devices run fully featured desktop operating systems like Microsoft Windows and Apple OSX.
- **Mobile Device:** Refers to devices such as tablets and smartphones which run mobile operating systems like Android, iOS, and Windows Phone.
- **Tablet:** A portable computing device which uses a touchscreen as its primary input device.
- **University Datacenter**: Centralized facilities run by Information Services to house servers, data storage, and associated components.

- **University Image:** A custom configured operating system with bundled software and services developed, maintained, and supported by Information Services.
- **Encryption:** the process of encoding messages or information in such a way that only authorized parties can read it
- **Default Password**: Where a device needs a username and/or password to log in, a default password is usually provided that allows the device to be accessed during its initial setup, or after resetting to factory defaults. The default password is set by the manufacturer and is common to all implementations of the technology, anywhere.
- **Guest Account:** A default (often restrictive) set of permissions and privileges given to non-registered users of a system or service.
- **Default Superuser Accounts**: Special user accounts used for system administration which typically allow the highest levels of system access. Depending on the operating system (OS), the actual name of this account might be: root, administrator, admin or supervisor.
- **Authorized User:** A user that has been granted permission to use a system or service by the administrator or other responsible party.
- **Patches:** A piece of software designed to update a computer program or its supporting data, to fix or improve it.
- **Software Firewall:** A software-based network security system that controls incoming and outgoing network traffic based on a set of rules.
- **Remote Administration:** Refers to any method of controlling a computer from a remote location (examples are SSH and Windows Remote Desktop).
- **Full Disk Encryption:** The process of encrypting all the data on the hard drive used to boot a computer, including the computer's OS, and permitting access to the data only after successful authentication to the Full Disk Encryption product.
- **Network Switch or Hub:** A computer networking device that connects devices together on a computer network.
- **System Administrator:** A person who is responsible for managing a multi-user computing environment, including establishing and managing user accounts.

Procedures

Information Services has provided a number of detailed how-to guides and instructions on the web at https://is.depaul.edu.

For additional questions, policy interpretation, or assistance needed to comply with this policy, contact the IS Technology Support Center via phone at 312-362-8765, via e-mail at tsc@depaul.edu, or log a ticket online via the Technology Support Center link in Campus Connect.

Divisional Collaborations

None

Contact Information

Information Services can be reached by phone at 312-362-8200, by e-mail at Information_Services@depaul.edu, or visit our website: https://is.depaul.edu .

Employees in the College of Computer Science and Digital Media should contact helpdesk@cdm.depaul.edu for additional interpretation of and exemptions to this policy

Appendices

None

History/Revisions

Origination Date: 10/09/2015
Last Amended Date: 10/09/2015
Next Review Date: N/A