Guidelines for Remote Access
& Use of University Information Systems
University of Scranton
Planning & Information Resources Division

This document provides guidance for remote access to University information systems for academic and administrative purposes at the University of Scranton. A list of related University policies is provided at the end of this document for further reference. Individuals who require remote access to systems beyond what is available through the my.scranton portal should contact the Technology Support Center at techsupport@scranton.edu or 570-941-HELP.

Does This Apply to Me?

Remote access to University information systems includes any of the following activities:

- Using a computer to work from a non-University location
- Connecting from off-campus to campus networks or systems, such as:
  - Your desktop workstation
  - Enterprise systems such as my.scranton, Live@edu, Banner, Argos, ANGEL, etc.
  - File systems, shared drives, or shared servers, such as RoyalDrive
  - Equipment or other instrumentation
- Conducting University business over a non-University network
- Using a non-University computer for University-related work, including one that is shared by non-University employees, family, or friends

There are many reasons why faculty, staff, and sometimes vendors or contractors, need to have remote access to University systems. There are also many risks to the privacy and security of the information that is being accessed. These guidelines are intended to assist you to reduce the risk associated with accessing University systems remotely.

Standards and Guidance

University information management and security policies (see page 4 for links to related policies) apply to all devices used for University business purposes, regardless of ownership or location. Information Resources recommends that only University owned and supported devices and applications be used for remote access activities; however the guidance below applies to any device used for remote access.
Department heads are responsible for making sure that staff and faculty engaging in any of the activities listed above are authorized to do so and are aware of the relevant University policies that apply to remote access of information systems.

**Remote Access Devices**

Remote access to University information classified as *restricted or confidential* should be limited to the use of a University owned and managed device. If that is not possible, a personally owned device may be used if the device is configured and secured to the standards of a University owned device, at a minimum:

- Running up-to-date, resident, anti-malware program – such as Microsoft Security Essentials
- Operating system up-to-date with all critical patches
- Third party applications, such as Java or Adobe, up-to-date with all critical patches
- Internet connection provided by a trusted source, optimally a residential service paid for by the individual.

Unprotected and unauthorized wireless networks, i.e. public Wi-Fi services, should never be used to do work involving restricted or confidential information. Wireless connections that are used should be secured with strong transport encryption, e.g. Wi-Fi Protected Access II (WPA2).

- Reasonable measures taken to ensure the physical security of the device.

University owned laptops should be connected to the campus network at least once-a-month to insure that the proper updates are installed.

Lost or stolen devices containing restricted or confidential information must be reported to the Information Security Office, even if the device was not University-owned. Be aware that even if you have deleted the restricted or confidential information it may still be resident on the device and should be reported.

**Information Management**

**Data Storage**

University information classified as *restricted or confidential* should be stored on a University owned and managed device. Use of the Royal Drive file management system is recommended. If a copy of restricted or classified data is needed for analysis on a properly protected personally owned device (see above), you should store the minimum amount of data necessary, and delete it as soon as possible.

---

**Tips for Securely Accessing University Systems**

*Shut down or restart your computer at least weekly and whenever your programs tell you to in order to install updates. This will help ensure that software and security updates are properly installed.*

*Microsoft Security Essentials and Sophos for Apple systems are recommended, free anti-virus products for personal devices.*

*When using a shared computer, make sure to log out of all applications, clear web cookies and history, and quit the browser and all programs when you are done. Clear any stored passwords and password protect sensitive files.*
Restricted or confidential data should be encrypted in storage. If the device is not capable of encrypting data with at least a 128-bit encryption key protected by a strong password, then it is not suitable for storage of University data. Encryption and decryption keys for the device should be kept in escrow, using a tool such as KeePassPortable, with a trusted source known to your department head. Keys for University-owned devices are kept in escrow by IT Services for business continuity and regulatory reasons.

**Email**

Email affords the same level of privacy as a postcard. As such, information classified as *restricted or confidential* should not be sent using email. If restricted information needs to be sent via email, it is best practice to:

- Save the information in RoyalDrive
- Send the intended recipient an email containing a password-protected RoyalDrive ticket to the information.
- Call the recipient and relay the password information to them.

Personal email accounts should not be used to conduct University business.

**Paper Records**

Individuals accessing University information systems remotely should minimize their usage of paper records containing restricted or confidential information. When usage of paper records cannot be avoided, ensure that storage and disposal of those records is done in a manner consistent with University Records Management & Retention and other information security policies.

**Contracts and Temporary Employees**

Vendors, contractors or other individuals with temporary access to University information systems should be asked to agree in writing or contractually to abide by all relevant University information security policies before their remote access request is granted. All remote access requests for contractors or other temporary circumstances should include an access termination date.

**Tips for keeping information safe**

*Web pages that have https (not http) in the web address encrypt the information that you enter. Check for this before you enter any restricted information, including your password, online.*

*Information sent via standard wireless is especially easy to intercept. Only use known, encrypted networks when working with restricted information. Check the wireless settings on your portable devices to make sure they aren’t set to auto-connect to any wireless networks they detect – this can put your data at risk.*

*Make sure a strong password is required for access to your computer. Don’t use the same passwords for University systems as for non-University systems.*
Related Resources

Known restricted data fields: credit/debit card numbers, bank account numbers, PIN numbers, Social Security Numbers, driver’s license or state identification number, authentication secrets such as passwords or private keys, patient information as specified by the Health Insurance Portability & Accountability Act

Student record data protected under the Family Educational Rights and Privacy Act (FERPA) is classified as confidential. For a complete list of information that the University classifies as confidential, consult the Information Classification & Protection Policy (see link below).

Related University Policies
Information Classification & Protection Policy
Information Access Policy
Strong Password Guidelines
http://www.scranton.edu/pir/policies.shtml

Records Management & Retention Policy
http://matrix.scranton.edu/Governance/university-policies%20.shtml

Mobile Device Center
http://matrix.scranton.edu/pir/its/techservices/mobile/index.shtml

Key Contacts

Technology Support Center
941-HELP techsupport@scranton.edu

Information Security Office
security@scranton.edu or x5816