Fredonia Secure the Human Reference Guide

You Are the Shield

- Cyber and physical security is *everyone's* responsibility.
- You are the most important line of defense for the University for cyber security attacks and data breaches.
- Be vigilant and report any suspicious activity. Cyber security incidents should be reported to the ITS Service Center (673-3407) while physical security incidents should be reported to the University Police Department (673-3333).

Social Engineering

- Social Engineering is the art of human manipulation. Cyber attackers will pretend to be someone or something you trust or know then use that trust to get what they want, often by simply asking for it (e.g. requesting confidential information via email, phone or in person etc..).
- Be suspicious if you are ever being asked for confidential information (e.g. usernames & passwords etc..) or other indicators such as people using a lot of confusing terms or people creating a sense of urgency to get information.

Email, Phishing & Messaging

- Phishing is a type of social engineering attack that attempts to trick someone into thinking an email is real and then completing an action such as clicking on a link, opening an attachment or completing an online form.
- Messages coming from a suspicious address; requiring immediate action; targeted towards a generic user (e.g. customer); claiming to be from an official organization; having grammar or spelling mistakes; using a personal email address; requesting confidential or sensitive information.
- Requests for personal or confidential information should always be scrutinized.
- Never click on links or attachment or provide sensitive information via email. Report the phishing attempt by calling the ITS Service Center (673 - 3407) and they will assist in retrieving the email and header information.

Browsing

- Always use the latest version of browsers.
- Check for HTTPS at the start of the website's address for a secure connection and that the padlock icon in the status bar is closed.
- Do not save passwords in browsers.
- Always log off from websites after you are finished using them.
- Ensure your browser and plugins are updated and running the latest version.

Social Networking

- Use a strong and unique password.
- Use two-step verification whenever it is available.
- Only install apps from trusted sources and only install what you need.
- Be aware of social engineering and never post confidential information.
- Ensure your privacy controls are set to share information to only those that you trust.
- Assume any information that you post will eventually become public.

Mobile Devices

- Always use a screen lock (e.g. PIN).
- Always encrypt your operating system, use firewalls and ensure your device has up to date anti-virus software.
- Enable remote wiping when available.
- Only use apps from trusted sources and only install what you need.
- Never "jail break" or "hack" your device.
- Disable wireless and Bluetooth when not in use.
- Always ensure that your device has the latest operating system and software updates.

Passwords

- Passwords are private and should never be shared with anyone.
- Use strong passwords and protect them. Consider using passphrases for your password. Your password must include at least 8 characters and contain 3 out of 4 of the following: uppercase letters, lowercase letters, numbers, special characters.
- Do not use more than two consecutive characters as they appear in your username or your full name.
- Your eServices account is used as a Single Sign On (SSO) so it may have access to many systems at the University.
- Personal information and common words should never be used as passwords.
- Passwords should be changed regularly at least every semester. Some systems require you to change your password every 30, 60, or 90 days.

Need Assistance?

- ITS Service Center- P: 673-3407 E: itsservicecenter@fredonia.edu W: http://home.fredonia.edu/its/
- ResNet Office – P: 673-3668 E: resnet@fredonia.edu W:http://home.fredonia.edu/its/resnet/
- Internal Control – P: 673-4925 W: http://fa.fredonia.edu/internalcontrol/
- Information Security Office – W: www.fredonia.edu/its/security
- University Police – P: 673-3333 W: http://students.fredonia.edu/upd

- Do not use work passwords for personal accounts.
- Do not create a password that is information that could be widely known about yourself.
- Consider using a password manager to keep track of your personal and professional accounts. This is a computer program that securely stores your passwords in an encrypted vault.
- Use two step or two factor authentication whenever possible.

Data Security and Destruction

- Data security is how we store, transmit and destroy our University's information. Data security is *everyone's* responsibility.
- Only use authorized systems for the storage, processing, transmitting and the destroying of University owned data.
- Do not copy or send anything to an unauthorized system or account.
- Keep our system secure by only using ITS authorized and licensed software.
- Cloud storage (e.g. Google Drive, Dropbox etc..) should *never* be used to store or share sensitive information.
- Always physically secure sensitive information by storing it in a locked cabinet or drawer.
- Always lock your computer when unattended.
- When sensitive information is requested from you, always authenticate the person's identity using approved procedures.
- Always use approved and secure methods that use strong encryption when sending sensitive information.
- Email is not secure and should *never* be used to share or store sensitive information.
- If you have administrative (elevated) privileges on a system, always use a non-privileged unique account to log in and then elevate your privileges as needed.
- Never share sensitive information with a 3rd party unless they are approved and have a current Non-Disclosure agreement (NDA).
- Always follow approved date retention and destruction policies.
- Please contact the ITS Service Center for approved data destruction methods.

Hacked

- Notify the ITS Service Center immediately when you suspect that you may have been hacked.
- Symptoms of being hacked may include the following: anti-virus warning, browser is randomly sending you to websites, passwords are changed, contacts receive random emails, unauthorized or suspicious software running on computer etc.
- Create regular backups using approved storage solutions (e.g. PGP secure fredshare for sensitive data, U Drive for non-sensitive data).

Personally Identifiable Information (PII)

- Includes any information that can identify a specific individual such as medical records, bank accounts, credit card numbers, social security numbers, passports, academic transcripts or grades, and driver's license number.
- Single pieces of PII data can be linked together to steal an identity or breach sensitive data.
- Only collect PII that you are authorized to collect and that you absolutely need.
- Be on the lookout for PII so that they can be secured properly.
- Always use an approved secure method to send PII to a recipient and only send what they need.
- Never email or fax PII data.
- Always follow approved policies and procedures when storing, accessing, and transmitting PII data.
- Memorize your Fredonia I.D. as it replaces the use of the SSN.
- If you have any questions about how to handle PII contact the ITS Service Center (673 - 3407).

Cloud Services

- Remember, you never know where data is being stored when using Cloud Services.
- Use only ITS approved Cloud Services and never store sensitive information.
- Never use personal cloud services for work.
- Always use strong and unique passwords for Cloud Services.
- Always scan downloads from Cloud Services with an up to date antivirus software application.
- Never purchase or sign up for Cloud Services unless they have been approved by ITS and Purchasing.
- Configure your Cloud account so that it does not share any information or files with anyone by default.

Data Retention

- Be aware of the Records Retention Policy and how it applies to your position.
- Be mindful that all email, Google Drive and all other approved electronic storage systems are FOILable.
- Keeping unnecessary multiple unauthorized copies of data increases risk for the University.
- Properly destroy records when there is no longer a legal, historical or operational need for the information.
- Always use an approved encrypted storage solution (e.g. Symantec PGP Fredshare) for storing University owned sensitive information.

Need Assistance?

- ITS Service Center- P: 673-3407 E: itsservicecenter@fredonia.edu W: http://home.fredonia.edu/its/
- ResNet Office – P: 673-3668 E: resnet@fredonia.edu W:http://home.fredonia.edu/its/resnet/
- Internal Control – P: 673-4925 W: http://fa.fredonia.edu/internalcontrol/
- Information Security Office – W: www.fredonia.edu/its/security
- University Police – P: 673-3333 W: http://students.fredonia.edu/upd