SECURITY

Safe. Simple. Secure.

SECURITY HANDBOOK

Security Best Practices

1. Restrict access rights by limiting the use of administrator privileges. This will help prevent the potential installation of malware and other unwanted software by unsuspecting users.

2. Keep systems updated with all of the current security patches. Where possible, turn on automatic updates to apply operating system security updates. When using images to support multiple systems, be sure the image is updated regularly with all applicable patches and virus definitions.

3. Automatic updates offered by Windows and Macs do not always patch third party applications such as FireFox, Flash, Java, etc. Be sure to check regularly for updates to these applications or consider using an automated patching solution.

4. Make sure all data is deleted from computers before they are sent to property management.

5. Where possible, set passwords on your mobile devices (i.e. Smartphones).

6. Do not save sensitive information to portable drives. Be sure to encrypt sensitive data wherever it is stored.

7. Enable computer firewalls. Mac and Windows computers come with built-in firewalls.

8. Use antivirus software and update the definitions regularly. Free antivirus software is available on the IT website for students, faculty and staff.

9. Back up your data frequently. A free backup service, Tivoli Storage Manager, is provided by IT and is available for faculty and staff computers

10. Educate users about safe browsing habits.

11. Create and enforce policies to prevent the installation of unlicensed/unapproved software.

12. When changing your password, remember to change your password in all locations where you may have your credentials stored to prevent account lockout.