Endpoint Security Standard
St. Bonaventure University

When considering endpoint security one has to include any and all devices that potentially connect to SBU related services that could provide personally identifiable information (PII) and protected university data to unwanted users if not protected properly. At no point should any personally owned device be allowed to access SBU servers containing high or critical levels of PII or any protected university data.

The list below attempts to identify any and all devices that qualify as endpoints of concern as of this writing as well as recommendations by the Information Security Council for protection against breach of PII associated with St. Bonaventure students, employees and all constituencies who may rely on the confidentiality of such data.

Definitions

Personally owned devices – technology devices owned by an individual (computer, cell phone, etc.)

SBU Devices – technology devices used by SBU employees but owned by St. Bonaventure University

Data Security Levels – Critical, High and other levels of data sensitivity are defined in the St. Bonaventure Data Classification Standard

Endpoints of concern / recommendations

a. Computers

SBU Office Desktops

- All SBU desktops will enforce a screen saver password after a maximum of 15 minutes of system inactivity.
- All SBU desktops being disposed of or re-purposed will be wiped to ensure that no data can be recovered from the system's hard drive.

Laptops

- The university will continue to identify users who have access to highly or critically sensitive data and encrypt the hard drives of these systems.
- All SBU laptops will enforce a screen saver password after a maximum of 15 minutes of inactivity from the system.
- All SBU laptops being disposed of or re-purposed will be wiped to ensure that no data can be recovered from the system's hard drive.
- It is strongly recommend that any personally owned laptop being used for work purposes has a screen saver password after a period of 15 minutes of inactivity from the system.

- No SBU related data of high or critical sensitivity will be stored on personal owned devices.

b. Mobile Devices
   - All mobile devices connecting to SBU systems (i.e. SBU email) will require a lock code to access the device.
   - All mobile devices connecting to SBU systems will require a lock screen (screen timeout) to initiate upon a maximum of 5 minutes of inactivity on the device.
   - No mobile devices will contain files that meet the highly or critically sensitive level as defined in the Data Classification Standard.
   - SBU employees must report any missing mobile device that connects to SBU systems immediately, but no later than 48 hours after you discover it being lost.
     1. The user must change their password immediately upon noticing that their mobile device is missing.
     2. SBU mobile devices will be erased remotely in the event that a user reports their phone missing.
   - No passwords for apps linked to SBU databases will be stored on mobile devices.

c. Portable drives (i.e. flash drives, external hard drives, CD/DVD's)
   - Any files containing data classified as highly sensitive must be password protected prior to storing them on portable drives.
   - Any files that meet the critically sensitive level in data classification should not be stored on portable drives.

d. SBU Photocopiers
   - Any SBU photocopier containing an internal hard drive will have data wiped from the system prior to disposal and show a certificate verifying data removal from vendor

Securing Data in Public Areas:

- University computers and office spaces should both be locked by employees any time they leave their office for an anticipated time longer than 5 minutes. If an employee shares a workspace with other personnel the computer must be locked anytime you leave your immediate workspace area.
- Any employee using public computer systems (i.e. labs or classrooms) must log off the system immediately upon finishing use of the computer