Foundational Information Security Controls

What are Foundational Security Controls and why are they important?

Foundational controls are the software tools and policies that the University requires to keep computers and institutional information, resources and data safe. In conjunction with you, they work to protect University data from compromise.

What Foundational Security Controls does SATS implement?

SATS implements five major Foundational Security Controls:

1. **Patch Management**: Systems are required to have a process through which security patches (i.e., Windows Updates) are installed, operational and regularly updated.

   Installed software, including your Operating System, receives security patches on a regular basis. If these patches are not installed in a timely manner, your system could get infected despite having an antivirus solution and firewall in place. Patch Management ensures that we are sending the security patches to your computer on a regular basis to keep your system and data safe. We use software to help us with patch management and to notify you about important IT issues in Student Affairs and Campus Life. You may sometimes see a small KACE popup that gives you important information.

   ![Example KACE Popup](image)

   *If you have a laptop you are responsible to log into the campus network at least every 30 days by either physical connection to a campus Ethernet jack, Eduroam, or UMass VPN.*
2. **Anti-Virus/Anti-Malware:** Anti-malware solutions must be installed, operational and regularly updated for applicable information technology resources.

   All Student Affairs computers come preinstalled with McAfee EndPoint Solutions and AntiMalware Enterprise. This software works in the background to help your computer remain uninfected and your data secure.

3. **Firewall:** Systems are required to have software installed and configured to block incoming network connections unless explicitly allowed.

   A firewall works to make sure that nobody can connect to your computer over the network unless you give them permission. The firewall also tries to prevent any malicious software from sending University data to a third party.

4. **Encryption:** All institutional information, research data and technology resources stored on systems are required to be encrypted. This includes flash drives and external hard drives.

   Encryption scrambles data using one-way mathematical functions. This means that you need a decryption key – in this case, your password - to access the data. Without the decryption key, the data will not be accessible to anyone.

   If your encrypted computer is lost or stolen, it will be difficult (but not impossible) for University data to be accessed.

   If your drive is not encrypted and your computer is lost or stolen, University data can be easily accessed. We may receive significant fines if University data is compromised.

   Example: If an unencrypted laptop is lost or stolen, someone could boot it using a CD or flash drive and they could have full access to everything on it. If the drive is encrypted, it would be extremely difficult for someone to access the data. The encryption is either tied to your login ID and password or a provided encryption key, which must be kept secure. Do not write down your login ID and password or encryption key and store with your laptop.

5. **Secure Disposal:** All information technology resources that contain institutional information or research data must be disposed of in an authorized manner, including having hard drives destroyed by UMass IT.

   The SATS Help Desk will collect University-owned systems and fill out appropriate paperwork and complete the secure disposal. Photo copiers and fax machines also contain hard drives and must have data removed and be disposed of securely.
This control also applies to personal computer or electronic device that contain institutional information or research data. You are responsible for secure disposal.

What is your role as a staff member?

Your knowledge, commitment and actions are one of the most important security controls.

a. **Avoid Phishing/Phishing Awareness:** Read about [phishing](#) and find out how you can prevent being the victim of a phishing attack where your credentials and data are stolen. Look at [some recent examples](#) of phishing at UMass to learn what phishing emails look like. Watch and share the UMass Cybersecurity Project [Phishing video](#) to learn more about STOP – THINK - ASK. If you see a phishing email **do not** click on the link. Report it to UMass IT by forwarding the email as an attachment to itprotect@umass.edu. If you’re not sure if an email is suspicious, contact the SATS Help Desk at sats-hd@sacl.umass.edu or 413-577-SATS (7287). Don’t open or respond to unsolicited or suspect emails.

b. **Password Security:** Choose a strong password that is different than all of your other passwords. Passwords should be a minimum of 10 characters and include at least three of the following - Uppercase, Lowercase, numbers, symbols. Do not write it down or leave it in a publicly accessible place or in your laptop bag. Do not share your password with anyone. Do not save passwords when requested by software. Change passwords at least every 6 months.

c. **Use standard user/non-admin accounts:** User accounts on SATS computers are non-administrative. This limits exposure if the system is compromised and limits a virus’ ability take full control of the entire system. It is also important to consider using a non-administrative account for routine use of your personal computer.

d. **Safe Web Browsing:** Practice safe browsing habits. In the course of your work duties, if you notice that a website looks illegitimate, do not browse to it. If Google or McAfee displays a notification that a site is unsafe, do not proceed. Do not browse to websites by clicking on links in emails. At the first sign of any issues, contact the SATS Help Desk.

e. **Safe Email Practices:** Do not open email attachments unless you know the sender, recognize the attachment, and are expecting the attachment. Do not send confidential or restricted data within an email or as an attachment. [UMass Box](#) is a good resource to securely share confidential and restricted data with other individuals that need access to this data.

f. **DATA Classifications:** Learn about [University data classification standards](#). Some data in the University needs to be given significant protection; other data does not
need to be treated with such thorough methods. Knowing about data classifications will help you make choices about where you can safely store and share University data. No confidential information should be downloaded, moved, copied or otherwise stored on non-university owned devices.

g. Secure Unattended Devices: Workstations and electronic devices that contain or can access university information should be locked and not left unattended. Screen Savers are enabled via Policy and force the machine to lock after a 10 minute period of inactivity. This is a backup in case you forget. You should always lock your machine whenever you leave it to prevent unauthorized access. Use Windows key + L to lock your Windows workstation whenever you leave it. Tablets and phones should be locked and require a passcode to unlock. Portable devices (flash drives, USB hard drives) and portable media containing university data should be secured in desk/cabinet when not in use.

h. Use Only Authorized Software: Do not install software or plug ins on your computer without authorization from your IT support group.

i. Confidential Data Handling: Do not download, copy, or move confidential or restricted University data on to a non-university device. University Data should not be put into the cloud unless it is an approved cloud.

Who do I contact if I have questions?

If you see something that looks out of the ordinary, please contact us at sats-hd@sacl.umass.edu or 413-577-SATS (7287) or ask any SATS staff member.

Where can I find more information about Foundational Security Controls?

In addition to this resource, the UMass IT website contains a section on minimum foundational controls with detailed technical information.

Other important Information Security Resources:

- University of Massachusetts Amherst Information Security Policy - [https://www.umass.edu/it/policies/informationsecuritypolicy](https://www.umass.edu/it/policies/informationsecuritypolicy)
- Confidentiality of Institutional Information Technology Resources Policy [http://www.umass.edu/it/security/conf-policy](http://www.umass.edu/it/security/conf-policy)
- Records Retention and Disposition Schedules [http://www.umass.edu/records/record-retention-and-disposition-schedules](http://www.umass.edu/records/record-retention-and-disposition-schedules)
- UMass Amherst IT Security Center [http://www.umass.edu/it/security](http://www.umass.edu/it/security)