Standard Security Controls

Using a set of standardized controls allows IT Security to ensure all University and Medical Center areas are protected from threats. By applying these standards, departments no longer need to manage the security concerns themselves but can leverage the knowledge and skills of the University's IT Security team.

There are four basic categories of controls:

- **Computer Controls**
- **Data Protection**
- **Network Protections**
- **User Authentication**

You can download a more detailed listing of these controls HERE.

Computer Controls

- **AntiVirus/AntiMalware –** Users can unknowingly install viruses and other malicious programs by simply visiting a compromised website or clicking on a link in an email. Anti-virus programs can monitor and block these programs before they can be exploited.
- **Centralized Patch Management –** Microsoft, Apple, and other software providers regularly release patches, updates, and other fixes to address security vulnerabilities and operational issues. Using a centralized tool means the patches are tested and rolled out in a controlled fashion and saves manual work on the part of the departments.
- **Domain Membership –** When computers are joined to a domain, administrators can more easily manage security and user settings.
- **Email Protection –** Email is one of the most challenging aspects of information security. Viruses, malware, phishing attacks, and more can be delivered by an email indistinguishable from a regular email to the average user. Email Protection tools monitor for and remove those malicious components.
- **Endpoint Detection and Response –** Monitoring for viruses and malware is an important baseline, but as hackers grow more sophisticated, better tools are needed. EDR programs look for suspicious activity, block it, and can collect samples to help improve the tools.
- **Standard Operating System Image –** Setting up computers with a standard image means all users start with a consistent, secure, vetted set of applications and programs.

Computer Controls (Continued)

- **Standard System Hardening –** Centrally managed computers start with preconfigured settings that make it more difficult for malware to affect the system and can be sent updates when a program is vulnerable or prone to malicious behavior.
- **Vulnerability Management Authenticated Scans –** New vulnerabilities are always discovered in computer software. A central scanning tool can find the areas of weakness and give system administrators a clear roadmap for what they need to fix.

Data Protection

- **Full Disk Encryption –** When laptops, mobile phones, and USB drives get lost and stolen, the data can stay safe if the device is encrypted.
- **Media Destruction –** If old devices are not properly cleaned before being disposed of, sensitive data can end up in the wrong hands.

Network protections

- **Flow Monitoring –** The NetFlow protocol allows for the collection, analysis, and monitoring of network traffic flows, aids in detecting abnormal traffic, and helps diagnose security and operational issues.
- **Logging of network and system activity –** Collecting logs in one place gives us a comprehensive picture of network and system activity, allowing Incident Response to better react to potential threats.
- **Network Border Protections –** Standard network protections are provided to departments, ensuring a secure perimeter against potential threats.
- **No firewall bypasses –** Restricting publicly exposed servers to the DMZ and not allowing passthrough traffic prevents protecting the internal network from external threats. This is key in minimizing the attack surface and preventing attackers from getting an internal foothold.

User authentication

- **2-Factor Authentication –** Passwords are easy to guess and often compromised. When you add a second factor, like a push to your phone, you make it much harder for anyone to gain unauthorized access.
- **Local Administrator Password Solution –** Using LAPS allows admins to give out the local admin password when needed, knowing that it will be changed. This replaces the need to change the passwords manually.
- **Password Change –** Password changes on end-user accounts help reduce the risk of brute force attacks. Using Active Directory to enforce annual password changes removes manual work for the department.
- **Privileged Account Management – Admin Accounts –** A Privileged Account Manager allows for removing elevated privileges from end-user accounts and enforcing automated password changes. The passwords can be changed much more frequently than standard password change policies for end-users. By using a Privileged Account Manager, departments remove the manual work of changing passwords when someone leaves, or an account is compromised.