Questions for ISO 27001 Duke University IT Department

**7.1** Are we compliant with the control that states security perimeters should be defined and used to protect areas containing information and associated assets?

Locate desktops in an access-controlled environment. Keep laptops with you at all times or stored in a secured location. Locate servers in an access-controlled environment and limit physical access. Log physical access for Sensitive systems.

**7.2** Is the IT department compliant with the control to protect secure area through appropriate entry controls and access points?

We have a strict visitor management process in place. Visitors are required to sign in, provide identification, and receive badge before entering any secure areas. They are escorted by authorized personnel throughout their visit.

**7.3**  Is the IT department compliant with the control to design and implement physical security measures for offices, rooms, and facilities?

We have implemented a comprehensive access control system that includes measures such as card readers, biometric scanners, or keypads to restrict entry into secure areas. Only authorized personnel are granted access through these controlled entry points.

**7.4** Is the IT department compliant with the control to continuously monitor premises for unauthorized physical access?

Duke University deploys cameras (closed circuit and network cameras) to meet operational, physical ty or public safety requirements.

**7.5** Is the IT department compliant with the control to design and implement protection against physical and environmental threats?

**7.6** Is the IT department compliant with the control to design and implement security measures for working in secure areas?

Our university is currently not fully compliant with the control for security measures in secure areas. We are actively working on implementing standardized security measures, including risk assessments, policies and procedures, access controls, security awareness training, and regular audits.

**7.7** Are clear desk rules for papers and removable storage media, as well as clear screen rules for information processing facilities, defined and appropriately enforced by the IT department?

At present, there is no specific policy or guideline in place that mandates employees to adhere to clear desk rules

**7.8** Is the IT department taking measures to provide Equipment siting and protection?

The IT department has ensured that equipment is securely sited in access-controlled areas, with sensitive tools positioned to prevent unauthorized viewing. We mitigate environmental risks through fire suppression systems, continuous monitoring of temperature and humidity, and lightning protection measures. Additionally, university-owned IT equipment is segregated from personal or third-party devices to maintain security.

**7.9** Is the IT department implementing measures to prevent loss, damage, theft, or compromise of off-site devices and to avoid interruptions to the organization's operations?

The IT department keeps off-site devices safe by using strong passwords, encrypting data, erasing information if a device is lost, and teaching employees about security. This helps avoid problems a keeps devices secure when they're not at the office.

**8.1** Is the IT department implementing measures to prevent loss, damage, theft, or compromise of user endpoint devices and ensure the continuity of the organization's operations?

the IT department has implemented several measures to prevent loss, damage, theft, or compromise of user endpoint devices. These include using whole-disk encryption, enrolling devices in our endpoint management services, and installing malware protection software. Additionally, devices are required to be stored securely when not in use, and we have a comprehensive patching and vulnerability management process to keep systems up-to-date and secure.

**8.2** Is the IT department implementing measures to secure privileged access rights and prevent unauthorized access or misuse of critical systems and data?

The IT department secures privileged access rights by following the principle of least privilege, ensuring that access to critical systems and sensitive data is limited. Multi-factor authentication (MFA) is used for administrator logins, and strong password policies are enforced. We also configure laptops and desktops to prohibit anonymous access and require password-protected screensavers.