Data Use Standards

Purpose

East Stroudsburg University has developed Data Use Standards as part of its Data Classification Policy. These standards outline requirements for handling and protecting all the University's institutional data, whether it be Public, Internal Use Only, or Confidential.

Scope

All members of the East Stroudsburg University community (staff, faculty, students, contractors, consultants, visitors, etc.) must safeguard East Stroudsburg University data. Accordingly, all members should be able to readily identify the data classification of the information resources they encounter and are responsible for ensuring that the minimum standards of treatment are met.

Policy

The following table defines the required safeguards for protecting data and data collections based on their classification. In addition to the following data security standards, any data covered by federal or state laws or regulations or contractual agreements must meet the security requirements defined by those laws, regulations, or contracts.

Security Control Category	**Data Classification**		
	Public	**Internal Use Only**	**Confidential**
Access Controls	- No restriction for viewing	- Viewing and modification restricted to authorized individuals as needed for business-related roles - Authentication and authorization required for access	- Viewing and modification restricted to authorized individuals as needed for - business-related roles - Authentication and authorization required for access - Confidentiality agreement required
Copying/Printing (applies to both paper and electronic forms)	- No restrictions	- Data should only be printed when there is a legitimate need - Copies must be limited to individuals with a need to know	- Data should only be printed when there is a legitimate need - Copies must be limited to individuals authorized to access the data and who have signed a confidentiality agreement

		- Data should not be left unattended on a printer	- Data should not be left unattended on a printer
Network Security	- Protection with a network firewall recommended - IDS/IPS protection recommended	- Protection with a network firewall required - IDS/IPS protection required - Servers hosting the data should not be visible to the entire Internet	- Protection with a network firewall with only minimal access permitted - IDS/IPS protection required - Servers hosting the data cannot be visible to the entire Internet, nor to unprotected subnets such as the guest wireless network - The firewall ruleset should be reviewed periodically
Virtual Environments	- May be hosted in a virtual server environment - All other security controls apply to both the host and the guest virtual machines	- May be hosted in a virtual server environment - All other security controls apply to both the host and the guest virtual machines	- May be hosted in a virtual server environment - All other security controls apply to both the host and the guest virtual machines
Physical Security	- System must be locked or logged out when unattended	- System must be locked or logged out when unattended - Hosted in a secure location required; a Secure Data Center is recommended	- System must be locked or logged out when unattended - Hosted in a Secure Data Center required
Remote Access to systems hosting the data	- Access restricted to local network or FSU Virtual Private Network (VPN) service	- Access restricted to local network or FSU Virtual Private Network (VPN) service - Remote access by third party for technical support limited to authenticated, temporary access via FSU Virtual Private Network (VPN) service	- Restricted to local network or secure VPN group - Unsupervised remote access by third party for technical support not allowed
Data Storage	- Storage on a secure server recommended	- Storage on a secure server recommended	- Storage on a secure server required

	- Storage in a secure Data Center recommended	- Storage in a secure Data Center recommended - Should not store on an individual's workstation or a mobile device. This includes personal and/or contractor-owned equipment. - Storaged in a contracted cloud drive i.e., Microsoft One Drive	- Storage in Secure Data Center required - Should not store on an individual workstation or mobile device (e.g., a laptop computer); if stored on a workstation or mobile device, must use encryption. This includes personal and/or contractor-owned equipment. - Portable media (e.g., portable hard drives, flash drives, and SSD's) must be stored in a secure location - Storaged in a contracted cloud drive i.e., Microsoft One Drive - Paper/other hard copy: do not leave unattended where others may see it; store in a secure location
Transmission	- No restrictions	- No requirements - Encryption recommended (for example, via SSL or secure file transfer protocols)	- Encryption required (for example, via SSL or secure file transfer protocols) - Cannot transmit via e-mail unless encrypted and secured with a digital signature
Backup/Disaster Recovery	- Backups required; daily backups recommend - recommended	- Daily backups required - Off-site storage recommended	- Daily backups required - Off-site storage in a secure location required
Media Sanitization and Disposal (hard drives, CDs, DVDs, tapes, etc.)	- See “East Stroudsburg University Media Disposal Procedures”	- See “East Stroudsburg University Media Disposal Procedures”	- See “East Stroudsburg University Media Disposal Procedures”

Training	- General security awareness training recommended - System engineer or admin recommended	- General security awareness training required - System engineer or admin recommended	- General security awareness training required - System engineer or admin required - Applicable policy and regulation training required

Revision History

Version Number	***Date***	***Author***	***Description***
1.0	*March 2022*	*Robert E. Smith, Ed.D.*	*Initial Document*