INFORMATION PRIVACY AND SECURITY QUICK REFERENCE GUIDE

Overview

All of us share responsibility for protecting Stanford systems and data from unauthorized access.

Key Resources

- University Privacy Office - https://privacy.stanford.edu
- Information Security Office - https://security.stanford.edu
- Risk Classifications - https://dataclass.stanford.edu
- Verifiable Encryption - https://encrypt.stanford.edu

Roles and Responsibilities

Faculty and Staff
1) Understand the Low, Moderate, and High Risk Data classifications - https://dataclass.stanford.edu
2) Keep your laptop/desktop software up to date - https://patching.stanford.edu
3) Verifiably encrypt all of your devices used for Stanford business - https://encrypt.stanford.edu
4) Request a Data Risk Assessment for new systems handling High Risk Data - https://dra.stanford.edu
5) Backup your laptop/desktop - https://backup.stanford.edu
6) Watch the information security awareness video - https://accounts.stanford.edu/manage
7) Be vigilant for phishing and other social engineering schemes - https://phishing.stanford.edu
8) Report lost or stolen devices to the University Privacy Office - https://privacy.stanford.edu
9) Be familiar with security policies and HIPAA regulations - https://security.stanford.edu
10) Use “Secure:” in subject line to send High Risk Data via email - https://secureemail.stanford.edu
11) Use Medicine Box for PHI data storage and collaboration - https://med.stanford.edu/box.html

Department Management
- Perform periodic monitoring and oversight to ensure faculty and staff roles and responsibilities are performed in compliance with policies and regulations.

Questions? Program Leadership Contacts

Information Security Office - https://security.stanford.edu
Chief Information Security Officer, Michael Duff - mjduff@stanford.edu or ciso@stanford.edu

University Privacy Office - https://privacy.stanford.edu
Chief Privacy Officer, Wendi Wright - wendiw2@stanford.edu or privacy@stanford.edu