# **Summary of Cal State LA’s Security Standards and Guidelines**

1. University computers and equipment are intended for university business. While incidental personal use is permitted, never use them for running outside business.
2. Do not expect privacy on university owned computers. The university will generally protect your privacy; exceptions are when authorized officers of the university are required to access your data to carry out their official duties or fulfill legal obligations.
3. Employees are required to take Data Security and FERPA training every 2 years.
4. You are required to change your computer account password annually under Cal State LA’s Password Standard.
5. Keep the password of your Cal State LA user account unique. Do not reuse the passwords from your other accounts. Do not share your passwords with others.
6. Use only Cal State LA email account for official university business.
7. You are expected to protect Cal State LA’s sensitive data (Level 1 and Level 2 data.) Sensitive data access will be granted based on a need-to-know basis. Do not share sensitive data without proper authorization from the data or business process owners. Sensitive data sharing with third parties should only be shared on authorized secured data exchange channels (e.g., MoveIt, Secured FTP servers, or authorized portal of business partners, etc.)
8. Sensitive data must be backed up. Level 1 data is required to be encrypted per CSU Information Security Policy.
9. Multi-Factor Authorization (MFA) is required for access to critical Cal State LA systems.
10. You can report security concerns to IT Security (ITSecurity@calstatela.edu) or ITS Helpdesk via ServiceNow self-service tickets. You can also learn more about Cal State LA security programs at <https://www.calstatela.edu/its/it-security-and-compliance>