Office of Information Security
UNIVERSITY OF COLORADO **BOULDER**
OFFICE OF INTEGRITY, SAFETY AND COMPLIANCE

Working remotely while using a personally-owned device in a secure manner

This guidance is primarily targeted at student employees of CU, who are unlikely to have access to a CU-issued device and may encounter CU data in the course of their work. The scope of this is for Public or Confidential data handling or processing on a personal computer. We recommend that a CU-issued device is used, if available, though we understand this is not always possible.

Access applications or documents to work "in the cloud" and avoid downloading sensitive information to your personally-owned device, when possible. Some great campus services make this easy: Sharepoint, OneDrive, Google Docs, etc. More information can be found at: https://oit.colorado.edu/services/messaging-collaboration. The guidance provided in this document includes a combination of free CU-supported services and recommendations for free software that is not affiliated with or officially supported by CU.

In the event that the following list of Highly Confidential data is accessed, stored, processed, or transmitted as part of regular day-to-day operations, this document is not applicable. Please contact the Office of Information Security at security@colorado.edu for further guidance.

Common Highly Confidential Data Types:

ITAR/EAR Proposals, ITAR/EAR Research Plans and Results, Grievances/Disciplinary Actions, Disability, Race, Ethnicity, Citizenship, Legal Presence, Visas, Religion, SSN, NID, Financial Aid (except work study), Loan and Bank Account Numbers, Health Information, Sexual Orientation, Taxpayer ID, National Origin, Any Business Document Containing Highly Confidential Data

Additionally, the following fields are considered Highly Confidential if they relate to any or all CU employees: Age, Sex, Marital Status, Disability, Military Status, Veteran Status, Dependent Information

More information about data classification can be found at:

https://www.cu.edu/security/data-classification

https://www.cu.edu/security/student-data-use-guidelines

https://www.cu.edu/security/employee-data-use-guidelines

https://oit.colorado.edu/services/it-security/guidelines-storing-documents-cloud

Office of Information Security
UNIVERSITY OF COLORADO **BOULDER**
OFFICE OF INTEGRITY, SAFETY AND COMPLIANCE

Follow these minimum security standards to safeguard your devices and CU data:

	Implementation Guidance
Training	Complete this 30 minutes course that explains information security principles, as they apply to information at the University of Colorado. Skillport Course
Access Control	Password protect your device. For CU applications, do not save account information and passwords to auto-fill – especially if you are working from a shared device.
Least Privilege	Accounts should be configured with the least privileges necessary for you to perform your job.
Limit System Complexity	Disable or uninstall unnecessary services or programs.
Patching	Install OS and 3rd-party software updates as soon as practical. Ninite
Malware Protection	All capable workstations should have antivirus software. Download Antivirus
Firewall	OS firewall enabled, if applicable
Physical Security	Devices shall be protected from unauthorized physical access and theft. *Minimize or supervise access to your computer by other household members. Unauthorized individuals may unknowingly put your computer or CU data at risk.*
Backups	Regularly backup your folders or sync your files to minimize possibility of data loss. Configure this to occur automatically, when possible. Ex) OneDrive, Google Drive affiliated with your employee IdentiKey
Data Security	Follow this guidance and implement PCI DSS, HIPAA, or FERPA controls, as applicable.
Disposal of equipment/data	Sanitize your device by destroying all CU data before disposal or transfer. Eraser

Optional, for additional protection:

Encryption	Use whole disk encryption. PGP
Remote Access	VPN may be used to access University resources from off-campus. Cisco AnyConnect

For additional security guidance, see https://www.cu.edu/security/top-10-actions-reduce-risk.