University of Colorado Boulder

Minimum Requirements for Non-DDS Managed Endpoints

1. Required to use University owned equipment (includes any equipment purchased through the procurement center).
2. Unique user id and password required at login.
3. Must be encrypted with whole disk encryption using BitLocker for Windows or FileVault for MacOS.
4. Operating system must be fully updated to latest version and OS security updates applied promptly.
5. Run campus provided Microsoft Defender for real-time scanning to prevent, detect, and remove malware or potential vulnerabilities.
6. All installed applications should be updated to latest versions and application security updates applied promptly.
7. Local firewall (native Mac OS X, Windows, and Linux are sufficient) must be enabled and functioning (blocking all non-stateful incoming traffic).
8. Use Microsoft O365 OneDrive, Teams and SharePoint and other approved and supported enterprise cloud storage solutions to backup and protect University data from loss. The Preserve is an approved and supported platform developed for use by campus researchers.