Colorado School of Mines
Office of the Provost

Executive Directive

March, 2014

Mandatory use of Encryption Software for Mobile Devices

This directive identifies the encryption requirements to comply with the latest revision(s) of:

- Colorado School of Mines Information Technology Appropriate Use Policy
- Colorado School of Mines Administrative Data Policy

Mines' Information Technology policies require that any mobile device containing institutional data must be encrypted[1]. The purpose of this requirement is to ensure that institutional data stored on a mobile device is appropriately protected in the event of loss, theft, or other mishap that may expose, compromise, or endanger the data stored on the mobile device. It is the user's responsibility to ensure that appropriate encryption methods are enabled and used to protect all institutional data stored on any device he or she uses whether the device is owned by the institution or the individual user. The Department of Internal Audit and Compliance will conduct random compliance audits.

Whole disk/device encryption is the preferred method for portable devices such as laptops, tablets, and smartphones since operating systems and applications may often leave remnants or copies of data stored in temporary files. Folder and file-level encryption can be appropriate for data stored on USB flash drives, CDs, DVDs, tapes, and similar devices - we recommend using Truecrypt to encrypt the files and folders on these devices that contain institutional data.

An updated list of recommended encryption applications and information about their use will be maintained on the ccit.mines.edu website in the security section. Some departments and users may be required to purchase and use the enterprise-level Symantec PGP Full Disk encryption package due to the nature of the data they may store on their portable devices. The current list of recommended applications follows:

Product	Platforms	Cost	Notes/Comments
Truecrypt	Windows, Mac OS X, Linux	Free	Full disk and folder encryption
FileVault	Mac OS X	Free	Comes with OS X
Bitlocker	Windows 8, 7	Free*	Free with Windows 7 Ultimate and Enterprise; Free with Windows 8 Pro and Enterprise.
LUKS	Linux variants	Free	Built in to Linux
Symantec PGP Full Disk Encryption	Windows, Mac OS X, Linux	$125	File, folder, whole disk, virtual disk encryption. Can securely wipe or shred individual files. Supports key escrow, other advanced features. License available from CCIT. *May be required for some users.*
iOS	iPad, iPhone, iPod Touch	Free	Built in – activate passcode, or preferably password.
Android	Smartphones, tablets	Free	Activate encryption in setup

The Symantec PGP Full Disk Encryption application is recommended if you store or travel with sensitive institutional data and may be required in some departments or for some users. This system is centrally managed via Symantec's PGP Universal Server and provides encryption key escrow and policy management services. Employees who travel internationally should be aware that some countries limit or forbid the use of encryption technology. It is the traveler's responsibility to ensure compliance with local laws. Rather than decrypting laptops when traveling to these countries, we recommend that you checkout a laptop from CCIT and load only the data you need for your trip onto the laptop.

CCIT staff will automatically install encryption software when building new mobile systems and will install it on existing systems upon request or as the opportunity arises.

HISTORY AND REVIEW CYCLE

The policy will be reviewed at least annually, or as needed by the Responsible Administrative Unit.
Last Issued: March 2014

[1]The encryption requirement can be waived for certain circumstances. Contact the Chief Information Security Officer (CISO) to seek an exemption. All exemptions must be approved by the CISO.