Encryption Standard Guidelines

The Encryption Standard issued by the State Security Office requires organizations to encrypt information that has been classified as Level C Very Sensitive or Level D Extremely Sensitive by the Data and System Security Classification Standard if the information is to leave the organization. Organizations can refer to their Data and System Security Classification grid to see if the information they intend to transmit or remove from the organization is subject to the Encryption Standard. Data subject to encryption is data transmitted outside a network or residing on a mobile data storage device such as a thumb drive, a laptop, a PDA (personal digital assistant), or other type of device. Backups of data containing Level C and Level D data are also to be encrypted.

The following information is meant to serve as guidance for ways to use technologies to encrypt information for differing scenarios. Refer to the glossary at the end of this document for definitions of the acronyms.

Sending files electronically

Use digital certificates
Use PGP
Turnkey encryption package
Encrypted VPN/SSH
Secure FTP methods

Email

S/MIME using digital certificates
Use PGP
Use one email server with accounts for all people who need to exchange emails securely

Laptops

Encrypt with Windows 2000 or higher – encrypt files, folders, or whole drive
Add-on encryption packages for those using lower systems
Encrypt with vendor encryption software such as PGP, MAC's FileVault

FTP

Use FTP-TLS or FTP-SSL
Switch to WebDAV over SSL
Encrypted VPN/SSH

Media leaving agency

Use thumb drives capable of acceptable encryption
Use PGP
Turnkey encryption package

Remote Access (includes dialup)

Encrypted VPN/SSH
HTTPS
Secure FTP methods

Glossary

File Transfer Protocol (FTP)

An application layer protocol that uses Transmission Control Protocol (TCP) and telnet services to transfer bulk-data files between machines or hosts.

Flash drive

Flash drives, also referred to as thumb drives or USB drives, are portable storage devices that use flash memory and are very lightweight and small. Flash drives can be used in place of a floppy disk, zip drive disk, or CD.

HTTPS

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a Web protocol developed by Netscape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering.

Personal Digital Assistant (PDA)

A PDA is a small handheld device that combines computing, information storage, telephone, fax, and/or Internet.

Pretty Good Privacy (PGP):

PGP uses RSA public key encryption for key management, IDEA for bulk encryption of data and MD5 for authenticity. PGP does not use Certification Authorities but relies instead on a “web of trust”.

Secure Shell (SSH)

Secure Shell (SSH), sometimes known as Secure Socket Shell, is a Unix-based command interface and protocol for securely getting access to a remote computer. Both ends of the client/server connection are authenticated using a digital certificate and passwords are encrypted. SSH uses RSA public key cryptography for both connection and authentication. SSH-1 is considered obsolete as it is susceptible to man-in-the-middle attacks. SSH-2 replaces SSH-1.

Telnet

Telnet is a network protocol that is used to connect to remote computers for the purpose of executing commands on a remote machine. Telnet is considered to be insecure due to several well-known vulnerabilities.

Transport Layer Security (TLS)

The successor to SSL, Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol provides connection security with some encryption method such as the Data Encryption Standard (DES). The TLS Handshake Protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged.

Secure Virtual Private Network (VPN)

A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols. In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted. An additional level of security involves encrypting not only the data, but also the originating and receiving network addresses.

WebDAV

Web Folders, or WebDAV, is a file transfer protocol that supports secure file transfer over intranets and the Internet. With Web Folders, you can upload, download, and manage files on a remote computer across an intranet and the Internet. Web Folders is similar to File Transfer Protocol (FTP); however, Web Folders provides a more secure environment for transferring files over the Web.