

STATE OF VERMONT
Agency of Administration

STANDARD STC State Technology Collaborative	ORIGINAL POLICY ADOPTED BY STC DATE: 2/8/07	ORIGINAL POLICY NUMBER
	EFFECTIVE DATE 2/8/07	ASSOCIATED DOCUMENTS Data Protection Policy Password Policy Password Standard

STATUTORY REFERENCE

OR OTHER AUTHORITY: Personnel Policies and Procedures
 ELECTRONIC COMMUNICATIONS AND INTERNET USE -
<http://www.State.vt.us/pers/er/pm/pm117.htm>

APPROVAL DATE: 2/8/07

APPROVED BY: Secretary of Administration

STANDARD TITLE: Data Protection

STANDARD STATEMENT: As governed by the State of Vermont *Data Protection Policy*, this *Data Protection Standard* identifies the State's current **standards and best practices** in protecting its electronically stored data. Data protection includes (but is not limited to) the safeguards and preventative measures taken to:

- Guard State data against malicious intent, unauthorized access, modification or loss.
- Ensure that devices containing the State's electronically stored data files are kept physically secured and backed up to reliable sources.

The following information pertains to all State employees, non-employees, and/or vendors who operate, maintain, and/or transport devices containing electronic data belonging to the State of Vermont. Such devices include (but are not limited to) computers, laptops, handheld devices (i.e. Palm's™, Blackberry's™, cell phones, etc), file servers, and data storage hardware (i.e. thumb drives, external hard disks, iPODS™, disk arrays, NAS, SAN, etc.) and removable media (i.e. floppy disks,

backup tapes, CD, DVDs jaz/zip disks, etc).

While the handling, storage, and recycling/shredding of State data in paper form also requires appropriate protection, specific reference to paper is not included in the scope of this standard.

STANDARDS FOR DATA SECURITY

1. All individually assigned equipment including personal computers, workstations, laptops (including those used with docking stations), portable storage and hand held devices.

1.1 Wherever based upon the sensitivity of the data involved prudence requires additional security, it must be implemented and used. Sensitivity of data can be based upon privacy concerns, statutory or regulatory obligations for data handling, or risk of financial loss to the state or its clients, business associates, or citizens. It is the responsibility of managers, supervisors, and users to identify when data should be treated as sensitive, giving rise to the need for enhanced security. It is the responsibility of IT staff to identify appropriate responses to such needs and to arrange for such measures, as available or obtainable resources permit.

1.2 Store all data on the user's home directory or other shared resource on their Department's local area network (LAN) server, where it is protected and backed up. Exceptions to this include the temporary storage of data on portable devices in order to meet a business need for the data to be accessed when the LAN is not reasonably available. Use of this exception should be limited; use to meet an employee's desire to routinely have data available for personal convenience to work away from the office should not be considered a business need. Once the business need to maintain the data off the LAN has passed, the data must be taken off the portable device and maintained on the LAN."

2. All shared equipment, including application, database and file servers (all platforms), fixed data storage (i.e. NAS/SAN/TAN).

2.1 Require the use of a password to obtain access (as outlined in the State Password Standard), and configure to "time-out" and transition to screen saver mode after 15 minutes or less of inactivity.

2.2 Equip with a backup power supply (i.e. UPS) and configured to shut down gracefully.

2.3 Store data with tape backup (or similar technology), to copy data files to an alternative media that can be used to restore from as needed.

2.4 Store backup tapes (or other media) in an appropriate State (or State approved) building other than the one in which the device is located. Follow applicable guidelines such as those identified in HIPPA regulations, to perform the backups and secure media in a controlled location that is kept locked and only accessible to authorized personnel.

2.5 Equip with firewalls and malware software (where applicable), to manage appropriate data traffic, filter unwanted data, and reject unauthorized access.

BEST PRACTICES FOR DATA SECURITY

1. All Individually assigned equipment including personal computers, workstations, laptops (including those used with docking stations), portable storage and hand held devices.

1.1 Equipped with a power strip that regulates and conditions the alternating current supplied to the device (not applicable to portable storage and handheld devices).

1.2 In certain scenarios where it applies, equipped with a backup UPS and configured to shut down gracefully.

1.3 In certain scenarios where it applies, equipped with tape backup (or similar technology), to copy data files to an alternative media that can be used to restore from as needed. If applicable, store backup tapes (or other media) in an appropriate State (or State approved) building other than the one in which the device is located. Follow applicable guidelines such as those identified in HIPAA regulations, and secure media in an environmentally controlled location that is kept locked and only accessible to authorized personnel.

1.4 Use the native encryption provided with the device operating system (i.e. Windows encryption). For data determined to be sensitive and/or confidential by Agencies/Departments, implement a more secure form of encryption. Examples include PGP encryption and solutions whereby the encryption key is stored on another appliance separate from the device being encrypted (i.e. thumb drive).

1.5 Equipped with data encryption technologies to secure data transferred over the Internet.

1.6 Do not allow use of alternate startup files from secondary storage media (i.e. floppy/jaz disks, thumb drives, CD's, DVD, etc) to boot up computers.

1.7 Erase storage drives before discarding or sending to surplus, consistent with NIST or FIPS standards.

1.8 Safeguard equipment from extreme temperatures and weather (i.e. cold, rain).

2 All shared equipment, including application, database and file servers (all platforms), fixed data storage (i.e. NAS/SAN/TAN).

2.1 Safeguard equipment from extreme temperatures and weather conditions.

2.2 Operate with data encryption technologies to secure data transferred over the Internet, and/or when hosting a web based application that is accessed by end users outside of the WAN (i.e. GovNet, K12).

2.3 Erase storage drives before discarding or sending to surplus, consistent with NIST or FIPS standards.

BEST PRACTICES FOR PHYSICAL SECURITY

3. Computers and workstations.

3.1 Store in secure location that is only accessible to authorized personnel. Exceptions include kiosks and similar devices left available to the general public within the confines of a State facility that is staffed with State employees and/or security guards (i.e. lobbies, libraries, etc.).

3.2 Before moving equipment, ensure all data files are backed up and/or stored on a LAN.

3.3 Ensure equipment is secured and protected from damage during transportation (i.e. padding around device).

4. Laptops, portable storage and hand held devices.

4.1 Ideally stored in an environmentally controlled location that is kept locked (where applicable) and only accessible to authorized personnel.

4.2 Transport laptops in protective carry cases (when applicable) which conceals its contents and is labeled with the employees name and contact information. In extreme situations where the cost of the device is high and/or the data contained is confidential, such carry cases should be equipped with locks.

4.3 Do not leave devices in unattended vehicles. If a device must be left in an unattended vehicle, it should be for a limited time and the device should be secured (i.e. trunk, glove box, etc.) and/or concealed from view through windows, with all windows closed and doors locked.

4.4 Do not leave devices unattended while at an off-site facility. If it is left overnight at an off site premise, it should be secured and/or concealed in an area that is kept locked and only accessed by authorized personnel.

4.5 Label all devices with an asset tag that can be referenced if necessary.

5. File servers (all platforms) and large scale data storage (i.e. NAS/SAN/TAN).

5.1 Store in an environmentally controlled location that is kept locked and only accessible to authorized personnel. This is not the general office area, but rather an area dedicated to the secure storage of such devices.

5.2 Rack mount in lockable storage racks, when available and affordable.