4. Removable Media: Acceptable Use Policy

This policy must be followed to safeguard both personal and State information and applies to all State employees and anyone using State computer systems, including other State agency staff, contract staff and vendors. All State entities must take measures to ensure that encryption procedures are consistently implemented. The use of third party tools to enforce this policy is one approved alternative; the use of Windows technologies, such as Active Directory Group Policy and native Windows encryption utilities, is another option. This policy represents a minimum standard. Agencies are free to use stricter standards deemed appropriate. The effective date of this change is October 1, 2012.

1. USB ports are essential for most personal computers and are universally allowed to support the connection of keyboards and mice. USB ports can also be used for approved peripheral devices.

2. The following Removable Media Devices must be "State owned assets" and controlled through an authorized approval process: flash drives, external hard drives, memory sticks, audio/video devices (tablets, iPods, MP3 players or similar hybrid devices), smartphones, cell phones or cell phone hybrids, micro drives and non-standard PDAs. The controls that apply to connecting devices by USB also apply to other methods of connecting these devices and failure to comply with such controls will also violate this policy. Examples of other connection methods include but are not limited to: Bluetooth, Infrared, Firewire, Serial/Parallel ports, Optical (CD/DVD/Blu-ray), eSATA, or SCSI.

3. The level of encryption on any Removable Media Device is required to be tailored to confidentiality requirements for the data on the device. A data classification process compliant with FIPS 199[1] is required before deciding on the level of encryption for a media device. The security personnel affiliated with the agency along with the agency leadership will be responsible for the execution and accuracy of the data classification. After the data on the device is classified, the following apply:

a. Data that is not determined to be sensitive data, as defined below, is allowed to reside on an unencrypted device. The Office of the Director of Compliance must be informed at helpdesk@omes.ok.gov prior to any use of a non-encrypted device and if the Director of Compliance disapproves of any use of such non-encrypted device, the device will not be used until encrypted. The possibility of the presence of sensitive data will mandate the use of an encrypted device.

   When used in this policy, "sensitive data" is defined as any data that includes Personal Identity Information (PII), information deemed confidential by the nature of the agency's business, or information regulated by federal, state, and local regulations. Personal identity information includes social security numbers, tax identification numbers, bank account numbers, credit card numbers, personal health information (PHI) and drivers' license numbers. Current and former State employee personal contact information, such as home telephone numbers and addresses and information related to electronic communication devices are considered sensitive information by State statute.

[1] FIPS PUB 199: Federal Information Processing Standards Publication "Standards for Security Categorization of Federal Information and Information Systems", February 2004. - http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

b. If any external regulations apply to the data on the device, the device owners are required to comply with the stricter regulation applicable to the data.

c. An agency may request a temporary exemption from compliance with this policy by submitting a written request to the Office of the Director of Compliance setting forth the reasons for the requested exemption and the Director of Compliance shall deliver a written approval or denial of such request to the agency.

4. All removable devices identified by the preceding section 3b must include a data encryption algorithm and a strong password, both of which must be implemented so they cannot be removed by anyone other than an authorized administrator. Only encryption alternatives for Removable Media Devices from the approved list below and provided through statewide contract, or other approved purchasing method, are approved for use. If data resides on an unapproved Removable Media Device, the data must be migrated to an approved device or an authorized designated network location.

5. If any Removable Media Device is lost, stolen or accidentally destroyed, the incident must be reported to agency management and to the Office of Management and Enterprise Services ("OMES") service desk electronically at helpdesk@omes.ok.gov or by telephone at 866-521-2444 or 405-521-2444 within 48 hours. Any misplacement of a device for at least 48 hours is also required to be reported to the OMES service desk. OMES must inform the Governor's Office within 24 hours after a report is made to the OMES service desk of any incident described in this section.

6. This policy must be enforced using "active policies", such as Microsoft Active Directory "group policies", on the Windows platforms involved (servers, desktops, directories, etc.), or an equivalent methodology on other operating systems.

7. Violations of this policy, including abuse of administrator privileges, may be cause for criminal, civil, or disciplinary action including the possibility of termination.

SOFTWARE ENCRYPTION ALTERNATIVES (MOBILE COMPUTING AND REMOVABLE MEDIA)

1. Symantec Endpoint Encryption 8.0
2. McAfee Endpoint Encryption (for Removable Media)
3. Sophos SafeGuard RemovableMedia
4. Checkpoint Media Encryption
5. LANDesk Endpoint Security (CREDANT Mobile Guardian)
6. TrueCrypt (Note: This is an open source solution that does not offer any local or remote administration software and should not be considered for medium to large organizations, unless the organization has an administration tool that is or can be customized to be compatible with devices on which this product is used.)
7. BitLocker-to-Go (Note: With Windows 7, BitLocker Drive Encryption helps protect sensitive data from being accessed by unauthorized users who come into possession of lost, stolen, or improperly decommissioned computers. BitLocker-to-Go extends BitLocker data protection to USB storage devices, enabling the devices to be restricted with a passphrase. In addition to having control over passphrase length and complexity, IT administrators can set a (AD Global) policy that requires users to apply BitLocker protection to removable drives before being able to write to the drives.

HARDWARE ENCRYPTION ALTERNATIVES (USB FLASH DRIVES—OTHERS MAY BE ADDED IF APPROVED) – CURRENT APPROVED AND VETTED LIST OF DEVICES

1. IronKey: https://www.ironkey.com/enterprise
2. Kanguru Defender: https://www.kanguru.com/index.php/flash-drives/secure-storage
3. McAfee USB Standard Encrypted Hard Drive Non-Bio http://www.mcafee.com/us/products/encrypted-usb.aspx (for those who already have McAfee ePolicy Orchestrator)
4. Kingston DataTraveler Locker: http://www.kingston.com/ukroot/flash/dt_Locker.asp

Note 1: The Dell contract has provisions for ordering hardware encrypted disk drives directly from Dell. However, the disk drives are not manageable from the administrative tools provided by most software encryption vendors.

Note 2: (Vulnerabilities may exist in devices currently in use):

A. There is a known flaw in the (built-in or onboard) software encryption process that impacts several major vendors of software encrypted USB flash drives (and some hardware encrypted devices). These vendors have a vulnerability flaw that can be exploited by those with knowledge of the weakness. A flaw was identified in the way the authentication works from the software to the drive itself. The worst part is that multiple vendors used the SAME KEY, and these drives actually passed low-level government certification. The vendors identified so far include:
   - Kingston
   - Verbatim
   - SanDisk

   For more information, see http://www.darkreading.com/insider-threat/167801100/security/encryption/222200174/index.html

B. Hardware encrypted devices are inherently more secure (for organizations that must use such devices for sensitive or confidential information) because hardware encryption is less vulnerable to software modifications that can be used to break or circumvent the encryption algorithms, is designed to erase the contents after some number of failed attempts at password guessing and typically performs better (faster read/write times) for organizations that use such devices extensively or for large amounts of data storage and transfer.

5. Mobile Computing Devices: Acceptable Use Policy

This policy refers to the use of mobile computing devices, including but not limited to all notebooks/laptops, netbooks, tablets (iPads, Xooms, PlayBooks, Motion, etc.) and all forms of smartphones. This policy must be followed to safeguard both personal and State information and applies to all state employees and anyone using State computer systems, including other State agency staff, contract staff and vendors. The only exception is for visitors making ad hoc use of state-owned public WiFi infrastructure. All State entities must take measures to ensure these procedures are consistently implemented. This policy represents a minimum standard. State agencies are free to use stricter standards deemed appropriate. The effective date of this policy is October 1, 2012.

1. Mobile computing devices must be encrypted if used on the State infrastructure, including, but not limited to: connecting the devices to a State-owned Computer, connecting the devices to the State-owned Network (excepting the state-provided public WIFI infrastructure) and connecting the devices to a state provided service (e.g. Exchange, Databases, File Shares). See ***Removable Media — Acceptable Use Policies*** for instructions regarding using these devices as data containers connected to agency assets.

2. Centrally managed software requires a minimum of the following security settings:

   a. State data at rest must be encrypted. If technology allows, a secure, encrypted logical container for the State data is acceptable. Otherwise, the internal storage and the auxiliary storage (where applicable) must be encrypted. The encryption standards must follow Section 3 of the ***Removable Media: Acceptable Use Policy***.

   b. Password protection of the device and/or the container of State data must comply with section 2.1 of the **State of Oklahoma Information Security Policies, Procedures, and Guidelines** and with the following additions and deviations from that policy:
      i. Minimum 6 (six) character password for the device or secure application partition unless other federal or state regulations require higher complexity;
      ii. Device wipe or lockout after 10 unsuccessful authentication attempts; and
      iii. Device lockout after 15 minutes, requiring reentry of the password.

   c. Remote wiping of the device is required upon the occurrence of any of the following scenarios:
      i. Employee is terminated;
      ii. Employee loses control of the device, either by theft, misplacement, change of ownership or the device is upgraded;
      iii. OMES detects a policy or data breach, or malware; or
      iv. OMES has any other reason to believe the device is corrupted or not trustworthy, including but not limited to, tampering with protection or management mechanisms.

3. Personal smartphones and tablets may be used for State business provided the devices have been equipped and configured to meet the following State minimum security requirements for such devices:

a. Personal devices must meet the agency-owned device requirements for security set forth in the preceding section 2 of this policy and

b. Personal Devices must follow any regulatory compliance demanded by current applicable legislation and policy, including this policy. In doing this, agencies should know that the sensitivity of some data will prohibit the agency from allowing some or all of its employees to use personal mobile computing devices for State business.

4. Personal smartphones, tablets and other smart devices may only be used for State business on a voluntary basis as a privilege for an employee. Prior to use of such device for State Business, a **Bring Your Own Device Agreement** ("BYODA") must be executed by the employee, the agency for which the employee works and OMES – ISD management. Pursuant to the BYODA, a copy of which is appended to and incorporated by reference into this policy, the employee is wholly responsible for the additional risks, responsibilities, and costs that might arise from using smart devices for State business.

   The additional risks and costs will include, without limitation:

   a. Exposure to regulations concerning State data, including but not limited to, Data Destruction legislation[2], Records Maintenance Act[3], the Open Records Act[4] and Attorney General Opinion 09-12;

   b. Exposure to legal proceedings against the agency resulting in temporary or permanent loss of the mobile computing device;

   c. Extra data and/or voice costs associated with the use of personal smart devices for State business;

   d. Risk of rendering the smart device inoperable due to errors in the management software or interoperability issues with the operating system; and

   e. Loss of personal data resulting from wipe commands.

5. If a mobile computing device is lost, stolen, destroyed, upgraded or a change in ownership has occurred, it must be reported within 48 hours to management of the agency for which the employee works and to the Office of Management and Enterprise Services ("OMES") service desk electronically at helpdesk@omes.ok.gov or by telephone at 866-521-2444 or 405-521-2444. Any misplacement of a device for at least 48 hours is also required to be reported to the OMES service desk. OMES must inform the Governor's Office within 24 hours after a report is made to the OMES service desk of any incident described in this section.

6. Violations of this policy, including abuse of administrator privileges, may be cause for criminal, civil, or disciplinary action including the possibility of termination.

---

2 62 O.S. §41.5a-4

3 67 O.S. §§201 - 215

4 51 O.S. §§24A.1 - 24A.29