Removable Media Acceptable Use Procedures—Clarification and Guidance

The following includes additional clarification and guidance related to recent updates to the statewide Information Security Policy, Procedures and Guidelines, along with some examples of questions asked about the new Removable Media Acceptable Use Procedures.

Encryption Clarification

1. The basic requirement is "to ensure that all removable media is encrypted" and the restrictions related to the use of "hardware encrypted" USB flash drives applies to those areas of any organization working with information that must be kept secure due to legislation and/or regulatory requirements. (See Additional Guidance below.)
2. As a general rule all other information can be encrypted using software encryption techniques.
3. When using removable media to distribute information to external third parties (including the public), as long as it is not controlled by a legislative or regulatory body and has been formally classified as "public access" in terms of the Open Records Act, encryption is not required.
4. Currently, encryption is required for all notebooks/laptops, netbooks, tablets (iPads, Xooms, PlayBooks, Motion, etc.) and all forms of Smartphones, flash drives, external hard drives, memory cards/sticks, audio/video devices (iPods, MP3 players or similar hybrid devices), cell phones or cell phone hybrids, micro drives and non-standard PDAs.

Additional Guidance

From a policy standpoint, we need to take steps to ensure personal identity information (PII) is not disclosed inadvertently through loss or theft of a device. The "Removable Media" revision was circulated among the cabinet secretaries in July and has been discussed in CIO meetings and IT security meetings for about 4 months prior to the adoption of the policy. It includes references to allow the use of approved 3rd party tools to facilitate software encryption for users that do not typically work with data that is classified as sensitive, confidential or controlled by legislation or regulations. We included seven (7) software encryption alternatives, including one (1) open source product and Microsoft's built-in solution with Windows 7 (Bit Locker/Bit Locker to go).

The following is intended to clarify the new acceptable use procedures:

1. The overarching goal is to encrypt all removable media used by anyone accessing state infrastructure;
2. There are two basic options:
    a. Hardware encryption is the recommended solution for all users that work with information controlled by:
        i. Statutes (Federal or State Legislation)
            1. Federal Deposit Insurance Corporation (FDIC)
            2. Internal Revenue Service (IRS)
            3. Gramm-Leach-Bliley Act (GLBA) Interagency Guidelines
            4. National Credit Union Administration
            5. Health Insurance Portability and Accountability Act (HIPAA) Security Rule
            6. Criminal Justice Information Services (CJIS) Security Policy
            7. State Data Breach and Privacy Laws (HB2245, HB2357, SB81/HB2332 [E-Media Destruction], A.G. Opinion No. 99-30 [state employee home contact information])

ii. Examples of the above include:
    1. Bank accounts and routing codes
    2. Tax payer IDs, social security numbers (SSN) and related data
    3. Automated Clearing House (ACH) and Electronic Fund Transfer (EFT) data
    4. Drivers license numbers
    5. Personal Health Information
    6. Law enforcement data, information/documents related to active criminal proceedings, investigations, evidence, electronic discovery, and personal identity information related to undisclosed protection or investigative assignments
    7. State employee home contact information, birth dates and SSNs

iii. Regulations
    1. Payment Card Industry (PCI) Data Security Standard
    2. Federal Financial Institutions Examinations Council (FFIEC)
    3. Critical Infrastructure Protection Program (CIP)
    4. North American Electric Reliability Council (NERC)

iv. Examples of the above included:
    1. Credit card numbers (personal account number [PAN] and card validation value [CVV or CVV2])
    2. Bank account numbers and routing codes, Automated Clearing House (ACH) and Electronic Fund Transfer (EFT) data
    3. "Critical infrastructure" is defined by federal law as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."
    4. Information relating to the control of or interface with bulk power systems in North America

b. Software encryption is recommended for all users that work with information that is not controlled by legislation or regulations.

3. Additional hardware and software encryption alternatives will be considered, if there is a business justification for their use and they have been tested to verify they are acceptable and have no known vulnerabilities.

We do not want to impede business processes or increase expenses beyond what is necessary and prudent to provide appropriate controls that will prevent the loss of state information and ensure compliance with state and federal legislation and regulatory requirements.

Additional frequently asked questions may be found on the OSF website at http://www.ok.gov/OSF/faqs.html#c271

The following notation is being included with all new purchases containing removable media:
"Refer to OSF's Mandatory Encryption Procedures for all state-owned mobile and removable devices containing electronic media and connecting to state infrastructure (http://www.ok.gov/OSF/documents/InfoSecPPG.pdf); for additional guidance refer to OSF's website at: (http://www.ok.gov/OSF/Information_Services/Publications_&_Standards/)."