Best Security Practices
and
Examples of How to Secure Personal Information

In an effort toward keeping electronic Personal Information secure, these are items that should be discussed with your information technology and business departments, or other district personnel as appropriate.

Best Practices

Definition: Personal Information

Personal Information means an individual's first name or first initial and last name, in combination with any one or more of the following data elements: Social Security Number; driver's license or California identification card number; account number, credit or debit card number, in combination with any required code or password that would permit access to the individuals financial account; medical information; health insurance information or medical information as defined by California Civil Code section 1798.29(g)(2) and (3); a username/email address in combination with a password or security question which would permit access to any online account of an individual. Personal Information also includes any other such information obtained from the System which, if disclosed, would constitute an unwarranted invasion of a person's privacy.

1. Promptly log off and close the Internet browser when not using System that contains Personal Information.

2. Any local drive (including a cloud-based server, physical server, virtual disk, workstation computer, or portable device) onto which Personal Information is downloaded or exported from the System should be encrypted so that Personal Information data at rest is protected.

3. Files being viewed or prepared for import into the System from a local drive (including a cloud-based server, physical server, virtual disk, workstation computer, or portable device) should also be encrypted.

4. Emailing of Personal Information is only permissible if the data or file itself is encrypted before it is emailed.

5. File Sharing of Personal Information should be encrypted. This would include, but not be limited to, network drives (either physical or virtual) or drives using a cloud based service.

Examples of How to Secure Personal Information

Several means of encryption are acceptable:

1. An encrypted virtual disk, also called a virtual hard disk (VHD), is an ordinary data file whose contents are strongly encrypted, and which when opened with the correct encryption passkey, appears to the local computer as an ordinary hard disk. Any data written to this virtual disk is automatically encrypted. When the virtual disk is "unmounted" the data remains in the virtual disk file, and cannot be accessed without re-entering the passkey.

   The Windows Bitlocker VHD function is an example of a virtual disk.

   http://howtogeek.com/193013

2. An encrypted hard drive is a hardware feature of certain portable devices, in which all data on the device's hard disk or solid state disk is continuously encrypted "at rest". Should the portable device be lost, the drive cannot be accessed without first entering the hardware encryption password, even if the drive is removed from the portable device and attached to another computer.

   The Dell Data Protection - Mobile service is a typical hard-disk encryption offering: http://www.dell.com/learn/us/en/19/campaigns/dell-data-protection-solutions

3. An encrypted USB "thumb" drive is a small, portable, solid-state storage device which has embedded hardware encryption technology such that a password must be entered any time the drive is attached to a computer.

   The Imation IronKey is an example of an encrypted USB key:

   http://www.ironkey.com/en-US/encrypted-storage-drives/f100.html

4. Email can be secured by emailing the Bitlocker file, or by using an encryption algorithm such as: 7zip http://www.7-zip.org/ on the attachment. Be careful to not copy Personal Information content into the body of an email.

5. Technologies can be combined in order to achieve complete encryption protection. For example, an encrypted virtual disk could be stored on an ordinary unencrypted USB drive, resulting in a total system that maintains encryption for any data moved onto the virtual disk on the USB drive.

6. When sending an encrypted file, do not include the password. Separately call or U.S. mail the password to the recipient.

7. The following criteria may be helpful in creating a secure password:

    - Passwords should be 8-20 characters long.
    - Passwords should not contain: your name, NetID, dictionary words, or simple patterns.
    - Passwords must include 3 of the following: uppercase letters, lowercase letters, numbers, special characters (!, @, #, $, etc.).