Encryption and Data Classifications

This article contains basic information about security, data classification, and encryption.

Information

Data must be encrypted if it is considered 2-lock (moderate risk) or 3-lock (high risk) data. To make best use of TPM features, the computer should be configured with UEFI and SecureBoot.

1. If data is determined to be 2 or 3 lock data, take one of the following actions:
   1. If possible (the user does not need the data), shred the data.
   2. If certain values are not needed, de-identify the data
   3. Encrypt the disk and proceed to step 2.

A. HIGH RISK DATA

Yale Data are classified as High Risk if (i) they could be exploited for criminal or other wrongful purposes and Yale is obligated by statute or regulation to keep them confidential; (ii) Yale is contractually obligated to keep them confidential; (iii) they identify an individual and would customarily be shared only with the individual’s family, doctor, lawyer, or accountant; or (iv)

Examples:

- Personally identifiable patient and human subject information
- Social Security, driver’s license, and passport numbers
- Credit card and bank account numbers
- Export controlled information under U.S. laws
- Confidential information about Yale donors
- Databases used for payroll, tax, health care, and other critical functions
- Information pertaining to animal research protocols and researchers

Related Policies and Procedures

- Protected Health Information (PHI) and Human Subject Data
- For all other High Risk Data, please visit https://your.yale.edu/policies-procedures
- … or email it.compliance@yale.edu

B. MODERATE RISK DATA

Yale Data are classified as Moderate Risk if they are not High Risk and (i) they are not available to the public; or (ii) the loss of their confidentiality, integrity, or availability could cause limited harm to Yale’s mission, safety, finances, or reputation.

Note: if any data in a dataset or file contain data attributes or combinations of attributes that are defined as High Risk, the data set must be treated as High Risk.

Examples:

- Unpublished research data
- Student and applicant data
- Employment applications and personnel files
- Non-public contracts
- Internal memos and email, non-public reports, budgets, plans, and financial information
- Engineering, design, and operational information regarding Yale infrastructure

Related Policies and Procedures

Visit https://your.yale.edu/policies-procedures or email it.compliance@yale.edu

C. LOW RISK DATA
Yale Data are classified as Low Risk if they are not Moderate or High Risk and (i) Yale chooses or is required to disclose them to the public, or (ii) the loss of their confidentiality, integrity, or availability would cause no harm to Yale’s mission, safety, finances, or reputation.

Examples:

- Information that Yale has made available to the public on its website
- Policy and procedure manuals designated by Yale as public
- Job postings
- Yale directory information not designated by the individual as "private"
- Information in the public domain
- Publicly available campus maps

2. **Identify the data** as high (3-lock), moderate (2-lock), or low (1-lock) risk.

3. Identify all devices on which the data will be stored or otherwise accessed. This includes computers used to remotely access a computer storing the protected data (laptop RDC to desktop)
   1. All of these devices must be encrypted
   2. All of these devices must be physically secured using a cable lock or other locking mechanism when the user is not present.

4. **Windows computers** must be encrypted using Bitlocker.
   1. Strip the user’s profile of admin permission.
      1. Do this for any user profile on the system with the exception of somadmin and the built in administrator account.
   2. Ensure UAC is enabled on all local admin accounts.
   3. Look for and uninstall:
      1. P2P software (Kazaa, iMesh, Napster etc)
      2. non-business filesharing and chat applications (WeChat)
      3. TOR applications (untraceable browsers)
      4. unsupported software (Quicktime).
   4. Scan system for and remove viruses.
   5. Ensure machine has all available security patches.
      1. This includes Windows, Office, Acrobat, Flash and browsers.
   6. Ensure machine is reporting to BigFix of SCCM (whichever is in use at the time)
   7. Ensure CrashPlan is functional (ensure it is actively backing up under the user's account)
      1. Ensure the backup is complete. Do not begin encryption until a full, recent backup is obtained.
   8. Set a screensaver to go on every 15 minutes and require a password to unlock the machine.
      1. Run gpedit.msc then navigate to User Configuration > Administrative Templates > Control Panel > Personalization and select "Prevent changing screen saver"
      2. Enable the policy
      3. Click OK
   9. Ensure MAC addresses are net-registered and do not have an expiration date. (Sam Chevalier and Dana Augur can check this, otherwise, submit a sub-task to the systems team.)
   10. A TPM chip is required to use ITS’ managed bitlocker. Check for a TPM chip using these instructions. Configure BitLocker using ITS’ management server using these instructions.
   11. If no TPM chip is present, the user must enter a pre-OS password to authenticate and additional configuration steps are required.

5. **Apple computers** must be encrypted using FileVault 2 (present in 10.7 Lion and above)
   1. Strip the user profile of admin permission.
   2. Look for and uninstall:
      1. P2P software (Kazaa, iMesh, Napster etc)
      2. non-business filesharing and chat applications (WeChat)
      3. TOR applications (untraceable browsers)
   3. Scan system for and remove viruses.
   4. Ensure machine is reporting to BigFix of SCCM (whichever is in use at the time)
   5. Ensure CrashPlan is functional (ensure it is actively backing up under the user's account)
      1. Ensure the backup is complete. Do not begin encryption until a full, recent backup is obtained.
   6. Set a screensaver to go on every 15 minutes and require a password to unlock the machine.
   7. Ensure MAC addresses are net-registered and do not have an expiration date. (Sam Chevalier and Dana Augur can check this, otherwise, submit a sub-task to the systems team.)

6. **Mark the system as Encrypted in Insight using the comments field for now.**

7. **Inform the user of the appropriate means for sharing protected data.**

8. **When user leaves or machine is replaced or otherwise disposed of:**
   1. If data can be deleted according to user, shred the data.
   2. Be sure to check Insight comments on the computer object to see if it was encrypted at some point. Alternatively, check this page for linked JIRA issues relating to encryption.
   3. Dispose of the system in accordance with: 1609 PR.01 Disposal of Media Containing Confidential or Protected Health Information

Link the JIRA issue to this confluence document.
Related articles

- Sharing Protected Data
- BitLocker - TPM
- Troubleshooting BitLocker with TPM
- Encryption and Data Classifications
- BitLocker - No TPM