MANDELL on SAFETY & SECURITY

Information Security Policy & Guidelines

Local, state, and federal laws require that certain types of information (e.g., individual student records) be protected from unauthorized release This facet of information security is often referred to as protecting confidentiality. While confidentiality is sometimes mandated by law, common sense and good practice suggest that even non-confidential information in a system should be protected as well-not necessarily from unauthorized release as much as from unauthorized modification and unacceptable influences on its accessibility.

Components of Information Security

- Confidentiality - Preventing unauthorized disclosure and use of information
- Integrity - Preventing unauthorized creation, modification, or deletion of information
- Availability - Preventing unauthorized delay or denial of information

Information Threats

Examples of information threats include:

- Natural events (e.g. lightning strikes, and aging and dirty media)
- Intentional acts of destruction (e.g., hacking and viruses)
- Unintentionally destructive acts (e.g., accidental **downloading** of computer viruses, programming errors, and unwise use of magnetic materials in the office)

Transmit Information Securely (including e-mail):

- *Use email only for routine office communication:* Never send sensitive information as email. If email absolutely must be used, encrypt the file and send it as an attachment rather than in the text of the e-mail message.
- *Physically protect your data encryption devices and* ***keys****:* Store them away from the **computer** but remember where you put them. Use the same common-sense principles of protection you should be giving your bank card personal identification number (PIN).
- *Inform staff that all messages sent with or over the organization's computers belong to the organization:* This is a nice way of saying that everything in the office is subject to monitoring.
- *Verify the receiver's authenticity before sending information anywhere:* Ensure that users on the receiving end are who they represent themselves to be by verification.

Present Information for Use in a Secure and Protected Way:

- *Practice "views" and "table-design" applications*: A "view" selects only certain fields within a table of information for display, based on the user's access rights. Other table fields are excluded from the user's view and are thus protected from use. For example, although a school record system may contain a range of information about each student, Food Services staff can view only information related to their work and Special Education staff can view only information related to their work. This type of system maintains information much more securely than traditional paper systems, while at the same time increasing statistical utility and accountability options. *In short, use the system controls for limiting information to a carefully determined set of users based on their function and authority.*

- *Use "key identifiers" to link segregated information:* If record information is maintained in a segregated manner (e.g., testing files are kept in a different **database** than special education files) for security purposes, a common file identifier (e.g., a Social Security Number) can be used to match records without unnecessarily divulging the identity of individuals and compromising confidentiality.

Back up Information Appropriately:

- *Back up not only information, but also the **programs** you use to access information:* Back up **operating system** utilities so that you retain access to them even if your **hard drive** goes down. Also maintain current copies of critical **application software** and documentation as securely as if they were sensitive data. Caution: Some proprietary software providers may limit an organization's legal right to make copies of programs, but most allow for responsible backup procedures. Check with your software provider.
- *Consider using backup software that includes an encryption option when backing up sensitive information:* Encryption provides additional security that is well worth the extra effort, since it ensures that even if unauthorized users access your backup files, they still can't break confidentiality without also having access to your encryption key. If you adopt this recommendation, be sure to change your encryption key regularly.
- Choose a backup program that has a verification feature.
- *Maintain a log of all backup dates, locations, and responsible personnel:* Accountability is an excellent motivator for getting things done properly. Remember to store the logs securely.
- *Avoid over-backing up:* Too many backup files can confuse users and thereby increase the possibility of exposing sensitive information. Clear hard drives, servers, and other **storage media like thumb drives** that contain old backup files to save space once you have properly secured (and verified) the last complete and partial backup.
- *Test your backup system:* This point has been made numerous times throughout the document, but it truly cannot be overemphasized!

Store Information Properly:

- *Apply recommended storage principles as found in this document to both original and backup files alike:* Backup files require the same levels of security as do the **master files**(e.g., if the original file is confidential, so is its backup).

- *Restrict handling of sensitive information to authorized personnel:* Information, programs, and other data should be entered into, or exported from, the system only through acceptable channels and by staff with appropriate clearance.
- ***Write-protect*** *important* ***files:*** Write-protection limits accidental or malicious modification of files. Note that while write-protection is effective against some viruses, it is by no means adequate virus protection in itself.
- *Communicate clearly and immediately about security concerns:* Train staff to promptly notify the system administrator/security manager when data are, or are suspected of being, lost or damaged.

Dispose of Information in a Timely and Thorough Manner:

- *Institute a specific information retention and disposal policy as determined by the organization's needs and legal requirements:* All data have a finite life cycle. Consult local, federal, and state regulations for guidance before implementation.
- Establish a realistic retention policy.
- Mark files to indicate the contents, their expected life cycle, and appropriate destruction dates.
- Burn, shred, or otherwise physically destroy storage media (e.g., paper) that cannot be effectively overwritten or degaussed.