Passwords - general rules are:

- NO ONE but you should know your password- do NOT share (activity will show under your name, your responsibility, you will be held accountable not the 'intruder')
- Change passwords regularly and don't use the obvious - words, dates, numbers, especially those related to you personally or displayed in your work area
- Commit to memory – if written down, keep somewhere secure and separate from your computer. Not on post it notes or paper on or near your computer
- Treat as carefully as you would your banking PIN number.

Electronic Information is indispensable in our organization; but brings security risks. Email, faxes, Instant Messaging (IMS), and working away from office are all security challenges. Be sure you are familiar with what constitutes confidential data; it MUST be handled with extreme care and caution.

- **Email** and email attachments are NOT secure in the standard format; anyone intercepting can read and use. To secure confidential data at a minimum password protect it but encryption is better.
    - Be selective of how you use email
    - Do NOT send confidential data/documents without being encrypted or password protected
    - DON'T propagate chain emails or hoax warnings
    - Be aware that all email in your Outlook Box is stored on your hard drive and should be cleaned up regularly.
    - For more detail refer to the Association Security Policy.
- **Phishing** – fraudsters send phony emails that look legitimate and authentic, requesting that you verify or change personal or confidential information such as id, passwords, account numbers. **NEVER** respond via email contact the company and ask questions. Examples are: Fresno State help desk, Paypal, eBay, banking institutions (Citibank & BOA recent issues)
    - Report suspicious or malicious email to the help desk IF it appears to be from a @csufresno.edu email extension; otherwise report to the institution
- **Working away from office –** do NOT send confidential data/documents via email or USB or flash devices or save them to the hard drive unless the data is encrypted. If you need to, you can connect to our servers from any location just as if you were at your desk and data/documents should be saved to the servers. If you must carry an electronic or hard copy of saved data, keep it safe and locked up at all times.

Computing resource thefts, i.e. laptops, computers, flash or USB drives, are being targeted for there value. However, if the equipment contains confidential data or any kind it creates a required and necessary reaction by the corporation. **Immediately notify** the Executive Director and the MIS Director of any theft or break-in where electronic devices is stolen, including office locations, home addresses, personal cars, purses, etc. Electronic equipment is defined as anything that could contain data, i.e. computers, laptops, USB or flash devices, CD or DVDs.

Things to think about BEFORE sending an email w/ confidential data

1. Is there confidential data within?
2. Is the confidential data really necessary for the task?
3. Is there a better way to share the information w/o compromising the confidentiality?
4. Is email the best way to communicate the message/data?
5. Does the recipient have a real ‘need to know’
6. Is the confidential data encrypted or password protected?
7. Who can retrieve, see or gain access to the information once it leaves your hands?
8. Ask yourself, ‘if this was my confidential information, would I be sharing it?’
9. Protect as if it were your identity potentially being compromised or stolen
10. Slow down, think and pay attention!