Protecting the Security of Grant Applications

Security Awareness Guidelines for Peer Reviewers

Grant applications, critiques, and scores are considered highly confidential information. By following the **best practices** below, you will be doing much towards protecting the information entrusted to your care.

Think Electronic Security

1. ***The Single Most Important Advice:*** Download applications to a secure PC and not to unsecured network drives or servers.
2. Make sure these files are never exposed to the Internet. Applications should never be posted on a peer reviewer's (or institution's) website because the files can be "discovered" by internet search engines, e.g., *Google*.
3. Have a strong password for file access and never share it.
4. If you leave your office, close out of the *eRA Commons* system, or out of your application file. You can also lock your computer.
   - Some systems can be locked by simultaneously hitting the Ctrl, Alt and Delete key and then selecting "Lock Computer" from the Task Manager.
   - Consider installing a password-enabled screen saver that activates after 15 minutes of inactivity.
   - Systems can also be put into a *sleep* mode which should then have a password-enabled *wake* mode.
5. Refrain from discussing application-related information in email—it's not secure—and you never know who could be intercepting it. If you must send information related to an application, carefully review the message content and double check the accuracy of the recipients before sending the message.
6. Most operating systems have the ability to natively run an encrypted file system (Windows = EFS and Mac OSX = File Vault). Consider running this type of system, especially for laptops, which can be stolen or misplaced.

Think Physical Security

1. If the application and/or related data are in hard copy or reside on portable media, e.g., on a CD, flash drive or laptop), treat it as though it were cash.
   - Don't leave it unattended or in an unlocked room.
   - Consider locking it up.
   - Exercise caution when traveling with portable media, i.e., take extra precautions to avoid the possibility of loss or theft (especially flash drives which are small and can easily be misplaced).
2. Refrain from discussing review information in public—you never know who is listening.

When the Review Session is over—destroy all review-related materials

1. Shred hard copies – preferably using a cross-cut.
2. Delete electronic files securely:
   - At minimum, delete the files and then empty your recycle bin.
   - Optimally, use a ***secure*** method, e.g., an electronic "shredder" program that performs a permanent delete and overwrite.
   - CDs can be broken or crushed, incinerated, shredded, melted or returned to the SRA.

For more information:

- Visit the NIH Information Security Training website at: http://irtsectraining.nih.gov/.
- Review the NIH Information Security Orientation brochure at: http://irm.cit.nih.gov/security/Sec-Orient-for-New-Users.doc.
- Review the NIH Laptop Computer Security Brochure at: http://irm.cit.nih.gov/security/laptop_sec_broch.doc.