Protecting the Security of NIH Grant Applications

Security Awareness Guidelines for Members of NIH Scientific Review Groups

NIH grant applications and related materials such as appendices, prior summary statements, reviewer rosters and critiques, additional review documents, impact scores and criterion scores are considered highly confidential information and may contain sensitive data. Thus, you must take every reasonable precaution to safeguard these materials entrusted to your care. The **best practices** below will aid you in this task.

Think Electronic Security

1. **The Single Most Important Advice:** Download applications and related materials to a secure PC under your control; do not use unsecured wireless, network drives or servers (i.e., computers and Wi-Fi in business centers or hotels). If using a home-based wireless connection, consider using Wi-Fi Protected Access 2 (WPA2) instead of WEP (Wired Equivalent Privacy—which can be hacked in minutes). Consider downloading materials to a directory so that the documents can be easily purged after the meeting.

2. Never post grant applications and related materials on any website or save them "in the cloud" because the files can be "discovered" by internet search engines, *e.g., Google or Bing*. Make sure you do not disclose any sensitive grant-related information via social media websites.

3. Have a strong password for computer access and never share it. Because professional hackers have software programs that can correctly guess most passwords in less than 10 minutes, please ensure that your passwords are complex and have at least eight characters.

4. If you leave your office, close the Internet Assisted Review (IAR) site or your application file, or lock your computer.
   - Windows-based systems can be locked by hitting the Ctrl, Alt and Delete keys simultaneously and selecting "Lock Computer" from the Task Manager.
   - Consider installing a password-enabled screen saver that activates after 15 minutes of inactivity.
   - Systems can be put into a *sleep* mode and should require a password to wake up.

5. Refrain from sending sensitive application-related information in email (even to yourself); it's not secure and could be intercepted. If you must send information related to an application, ask the Scientific Review Officer to send you an email message using the NIH Secure Email and File Transfer Service (https://secureemail.nih.gov/); you can reply to the SRO's message with the confidential material attached and the information will be encrypted in transit. Alternatively, you may send the information to the SRO through email, if it is encrypted and password protected, and if the SRO knows how to remove the password protection. Before sending the information, carefully review the message content; eliminate any unneeded confidential information and then double check the accuracy of the recipients before hitting the send button.

6. Most operating systems can run an encrypted file system to protect files while they are on your hard drive (e.g., Windows - BitLocker and Mac - File Vault 2 and/or encrypted disk images). Consider applying such encryption on your PC. All laptops; however, **must** be encrypted due to the risk of their being stolen or misplaced.

7. All mobile devices (including Blackberries, iPhones and iPads) and portable media (including flash drives, CDs, DVDs etc.), containing grant applications, previous summary statements, appendix materials and any other grant-related sensitive materials) **must** be encrypted. Please be aware that handling, storing, or accessing sensitive information on a mobile device is not recommended.

8. Full disk encryption is highly recommended, especially for laptops.

Think Physical Security

If the applications and/or related materials are in hard copy or reside on mobile devices or portable media (e.g., CD, Smart Phones, flash drive or laptop), *treat them as though they were cash*.

- Do not leave them unattended or in an unlocked room.
- Consider locking them in a locked cabinet or drawer.
- Keep sensitive information out of sight when visitors (or family members) are present.
- Take extra precautions with mobile devices and portable media. Mobile devices are more susceptible to lost and theft, anti-virus software is not as effective for them; they can store as much or more data than a PC, and can access networks faster.
- Be particularly careful with flash drives which are small and easily misplaced.
- Monitor your laptop as it passes through TSA security at the airport and promptly pick it up. Never place it in checked baggage.

When the review meeting is over, destroy all review-related materials.

1. Shred hard copies – preferably using a cross-cut shredder.

2. Delete electronic files securely:
   - At minimum, delete the files and then empty your recycle bin.
   - Optimally, use a ***secure* erasure** method, e.g., an electronic "shredder" program that performs a permanent delete and overwrite.
   - CDs can be broken, crushed, incinerated, shredded, melted or returned to the Scientific Review Officer.

IMMEDIATELY REPORT lost, stolen, or inappropriate disclosure of an NIH-generated CD, laptop or other data-storage device that contains sensitive data or application material. Report to your Scientific Review Officer within 24 hours:

- The Scientific Review Group meeting in which you are or were a participant.
- All materials that are missing and whether they were encrypted.
- Circumstances surrounding their disappearance (stolen from your office, left in a taxi, etc.)

Additional information is available at:

- The NIH Information Security Training website: http://irtsectraining.nih.gov/.
- The NIH Guide Notice NOT-OD-08-071: http://grants1.nih.gov/grants/guide/notice-files/not-od-08-071.html