SUNY RF
The Research Foundation for
The State University of New York

Guidelines for Protecting Research Foundation Data

Every employee plays a critical role in ensuring the security of Research Foundation (RF) information and data. By taking the precautionary measures outlined in this document, you can reduce the risk of unauthorized access to or use of RF data, protect against identity theft, prevent unintentional security breaches and prevent the spread of computer viruses.

Protect paper documents

- Do not leave sensitive documents in plain view on your desk or on fax machines or copiers.
- Store sensitive documents in locked drawers or file cabinets.
- Shred confidential paper documents when they are no longer needed. Protect electronic files.
- Do not leave sensitive documents in plain view on your computer screen.
- Store data to a network drive such as your Y: drive to ensure it is backed-up.
- Secure confidential shared network files so that only authorized personnel may view them.
- Do not store confidential data in an unsecured network or public drive.
- Do not store confidential data on a laptop or other mobile device that can be easily stolen.
- Routinely review electronic files and purge files that are no longer needed.

Secure your computer

- Always lock your computer screen when away from your desk.
- Never give your computer ID and password or personal information to anyone.
- Avoid using simple, obvious or predictable passwords; use a combination of alphanumeric characters or sentences.
- Avoid writing down passwords or posting them in public view.
- Always change temporary passwords assigned by an administrator.
- Take extra precautions to secure laptops and other mobile devices when away from your desk or traveling.

Exercise caution

- Do not open e-mail attachments from an unknown source or an attachment you weren't expecting, even it appears to be coming from someone you know.
- Do not visit unknown Internet sites.
- Do not download software without approval; requests should be submitted through Customer Services.
- Do not reply to SPAM (unsolicited commercial emails).
- Avoid sending personal or confidential information in an email whenever possible.
- Do not provide information over the phone without knowing if the person on the other end is authorized to receive it and without being certain of their identity.
- Maintain a constant awareness about information and data in any format to prevent unauthorized personnel from seeing or overhearing information they should not.
- Report suspicious activity to your supervisor, the RF's Information Security Officer, or the Director of IT Operations.