UNIVERSITY of MARYLAND
SCHOOL OF PHARMACY

Policy and Procedures for PRC Secure Server Training

Last Updated: July 2019
Effective Date: July 2019
Modification Date:

Purpose

PRC maintains a secure server that safeguards data with personally identifiable information (PII).
This document details information on PRC's Required Annual Secure Server Training.
PRC follows the National Institute of Standards and Technology (NIST) recommended guidelines for security awareness, control, requirements and training in the workplace. Users on the PRC server are required to attend an annual security training that covers NIST Special Publications- 800-50, 800-53 R4, 800-171, and 800-181. Included in the training are security and privacy controls, protecting controlled information, as well as PRC housed data specific policies. Ultimately, PRC ensures that all system users are aware of the security risks associated with their activities and of the applicable policies, standards and procedures related to the security of the PRC system.

Specific standards are outlined as such in NIST Special Publication 800-171:

> *"Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems."*

Security measures are in affect to prevent or minimize compromises to PRC's secure server system; compromises include data breaches or unnecessary server shutdowns.
All PRC users are accountable to these system security measures.

1. Follow U.S. Government IT Security Laws
2. Follow all University of Maryland Baltimore's Security Standards
3. Follow all of the University of Maryland's School of Pharmacy's Security Standards
4. Follow HIPAA Privacy and Security Rules
5. Follow all PRC's instructions given to you specifically as well as to all users
6. Adhere to the DUA
   - Stay within cell size limit
   - Given 24 hours to reduce file size within defined limits
7. Protect your server account
   - Keep passwords protected and to yourself
   - Never allow others to use your account
8. Never download raw data from the server to an external location (e.g. USB, email)
9. No moving data to alternate file locations without prior PRC approval
10. Do not share detail data externally
    - Data screen captures, printing, or emailing can be considered unauthorized disclosure
11. Work within a project's approved workspace
12. Be efficient in utilizing our resources
    - Never max out our servers' temporary workspace
13. Logoff after all active server sessions
14. Never leave an active terminal session unattended

15. Always lock all terminals when unattended
16. Report all security breaches whether your breach or that of others

Policy:

1. PRC will conduct security training annually for all approved PRC system users. A system user is someone who has successfully met a set of minimum standards and successfully received certifications to include:
   - Health Insurance Portability and Accountability Act (HIPAA) 125 and 201
   - Collaborative Institutional Training Initiative (CITI)
   - PRC Annual Security Training
2. Members of PRC's user community will be invited to attend formal training dates.
3. New users throughout the year can attend semi-annual training offered by PRC or opt to pay PRC for individualized training as needed to fulfill the requirement.
4. System users, who compromise PRC's system security, default to the Progressive Discipline Policy of PRC's System Security.

Protect PRC's system and your digital footprint; conduct only approved activity.
Report all security breaches to the PRC director.

\\prcw.rx.umaryland.edu\SAMBA_PRC\PRC_Operations\Policy_and_proc\draft\Current working drafts to be finalized\PRC_Mandatory_SecurityTraining.docx