Sheps Center Rules of Behavior

Introduction

It is recommended that every System Security Plan (SSP) contain Rules of Behavior (ROB). ROB apply to the system users and list specific responsibilities and expected behavior of all individuals with access to or use of the named information system. In addition, ROB outlines the consequences of non-compliance and/or violations.

ROB is part of a complete program to provide good information security and raise security awareness. ROB describes standard practices needed to ensure safe, secure, and reliable use of information and information systems.

This ROB covers all staff and partners of the Sheps Center working with sensitive data. This includes contract personnel and other funded users, if applicable. The Sheps Center information system environment covered by this ROB includes the UNC central email system, the Sheps Cecil file server, the Sheps office IT infrastructure located at the Sheps Building, and the Sheps Secure Dataset Servers (SDS).

Consequences for Violating the Rules of Behavior?

Penalties for non-compliance may include, but are not limited to, a verbal or written warning, removal of system access, reassignment to other duties, demotion, suspension, reassignment, termination, and possible criminal and/or civil prosecution.

Application and Organization Rules

A. *Passwords*

1. Passwords should follow the standards stated in the UNC "Password Policy for General Users". Among them:
   Minimum length: 8 characters
   Combination of letters, numbers and special characters (such as *#$ %).
   Dictionary words should not be used.
2. Passwords will be changed at least every 90 days and should never be repeated. Compromised passwords will be changed immediately.
3. Passwords must never be shared by that user with other users. For example, colleagues sharing office space must never share each other's password to gain system access.
4. Passwords must never be stored in an unsecured location. Preferably, passwords should be memorized. If this is not possible, passwords should be kept in an approved storage device, such as an encrypted vault.

B. *Encryption*

1. Laptop computers accessing sensitive data must utilize Whole Disk Encryption.
2. Files that contain direct identifiers and other PHI require encryption before transmission and should be encrypted while stored on a computer's hard disk drive. Direct identifiers include: name, SSN, address, phone number, identifying license numbers, etc.

Transmission of data with direct identifiers must be authorized by research project Principal Investigator or Sheps management prior to transmission.
NOTE: The storage of direct identifiers at Sheps should stored under the direction of the Sheps Security Liaison.

3. Sensitive information that travels over wireless networks and devices must be encrypted.

C. *Internet Usage*

1. With the exception of systems administrators, accessing the Internet from the SDS via X-Windows or command line is strictly prohibited.
2. Visiting websites including, but not limited to, those that promote, display, discuss, share, or distribute hateful, racist, pornographic, explicit, or illegal activity is strictly prohibited.
3. Using a Sheps computer and the Internet to manage, run, supervise, or conduct personal business enterprises is prohibited.

D. *Email*

1. Except for limited personal use, non-work-related e-mail on the UNC email system is prohibited. The dissemination of e-mail chain letters, e-mail invitations, or e-mail cards is prohibited.
2. E-mail addresses and e-mail list-serves constitute sensitive information and are never to be sold, shared, disseminated, or used in any unofficial manner.
3. Using an official e-mail address to subscribe to any non-work related electronically distributed newsletter or magazine is prohibited.

E. *Working from Home/Remote Dial-up Access*

1. Users must connect to the UNC Virtual Private Network (VPN) to access Sheps file servers.
2. Users must be certain to log-off and secure all connections/ports upon completion.
3. Users who work from home must ensure a safe and secure working environment free from unauthorized visitors. At no time should a “live” Sheps connection be left unattended.
4. When doing Sheps work on sensitive data from home, users must use an official Sheps computer maintained by Sheps Computing staff to limit vulnerability to an intrusion and increase security.
5. Home users connected to the Internet via a broadband connection (e.g. DSL or a cable-modem) must install, routinely update, and have operational a hardware or software firewall.
6. No official Sheps sensitive material may be stored on a user’s personal computer.

F. *Unofficial Use of UNC Equipment*

Except for limited personal use, UNC equipment including, but not limited to, fax machines, copying machines, postage machines, telephones, and computers are for official UNC use only.

For any piece of Sheps equipment taken off-site and used off-site, user must maintain a signed, up-to-date Off-Campus Use Agreement filed with the Sheps Computer Support office.

G. *Other Rules of Behavior*

1. A user is responsible for secure handling of assigned Sheps Building keys. User must never share his/her entry keys with anyone.
2. A user is responsible for secure handling of assigned RSA SecurID, where applicable. User must never share his/her SecurID with anyone.
3. Users who no longer require Sheps system access (as a result of project completion, job change, job transfer, or reassignment of job responsibilities) must notify Sheps management immediately after a changing event.
4. When not in use, workstations must be physically secured and powered off (turned off) unless remote desktop connectivity is required to perform work.
5. Screen-savers must be password protected.
6. Movable media such as DVDs, CDs, external hard drives and thumb drives that contain sensitive data must be encrypted and secured when not in use.
NOTE: Some DUAs prohibit the placement of data on movable media. In these situations, the restrictions of a DUA override other rules.
7. Altering code, introducing malicious content, denying service, port mapping, engaging a network sniffer, or tampering with another person's account is prohibited.
8. If a user is locked out of the system, the user should not attempt to log-on as someone else. Rather, the user should contact the system administrator.
9. Printed material that contains sensitive data must be protected and disposed of according to UNC Security Policies. Sensitive Information must not be copied, printed, or stored in a manner that would leave it vulnerable to unauthorized access.
10. Users must follow UNC Security Policies

H. *Additional Rules of Behavior for System Administrators*

1. System administrators may only access or view user files with the expressed consent of the user and/or management.
2. System administrators may track or audit user accounts without the expressed consent of the user and/or management for security auditing purposes.
3. System administrators must make every reasonable effort to keep the network free from viruses, worms, Trojans, and unauthorized penetrations.
4. System administrators must implement, monitor, and keep updated vulnerability scans for the Sheps servers housing sensitive data.
5. It is the system administrators' responsibility to account for all system hardware and software that is part of the Sheps SDS.

6. System administrators must dispose of hardware and software according to UNC Security Policies. Hardware that has stored sensitive data must be disposed of according to the UNC Standards for Electronic Media Disposal.

Acknowledgment

I have read and understand the Rules of Behavior governing my use of Sheps servers and computers housing sensitive data. By signing below, I agree to abide by them.
I understand that failure to do so may result in disciplinary action being brought against me, up to and including dismissal.

User Name (please print) ______________________________________

User Signature____

Organization____

Date____