Duke Clinical Research Institute
From Thought Leadership to Clinical Practice

July 1, 2016

MEMORANDUM

To: **All Users of DCRI Computing Equipment and Network Resources**

From **Lesley H. Curtis, PhD, Interim Executive Director, DCRI**

Subject: **Secure System Usage**

The purpose of this memorandum is to inform you of the DCRI-wide policy regarding the proper use and management of all DCRI computing equipment and network resources. This information contained in this directive supersedes all other DCRI policies and guidelines related to the use of computing equipment and network resources. A copy of the *Secure System Usage Memo* may be found at https://dcrihome.dcri.org/IT/Documents/PoliciesForms/Secure%20System%20Use%20Memo.pdf.

Some DCRI Functional Groups or Key Research Programs have regulatory requirements that further define appropriate use of a workstation. All DCRI employees should be well informed of additional regulatory requirements unique to their work activities.

General Responsibilities

Computing equipment and information system resources at the DCRI are provided to facilitate the DCRI's vital research functions. The integrity, security, and stability of our networks, databases, and systems are of the utmost importance. All computing and electronic communications systems, as well as the associated equipment and data that are transmitted, received, or archived in University information systems are the property of Duke University (intellectual property rights are governed by the "Duke University Policy on Intellectual Property – Appendix P" in http://provost.duke.edu/faculty-resources/faculty-handbook/). The DCRI acts as the agent of Duke University and the School of Medicine with respect to the oversight and administration of policies and procedures related to computing and electronic communications systems at the DCRI.

As a user of DCRI computing systems, it is your responsibility to:

- Respect the freedom and privacy of others.
- Use systems and other resources for authorized purposes only.
- Use only legal versions of copyrighted software and do so in compliance with vendor licensing requirements.
- Access only that information which is publicly available or for which you have been given access rights.
- Protect the integrity of DCRI databases by not making unauthorized modifications.
- Protect user IDs/passwords and systems from unauthorized use.
- Use shared resources in a responsible manner. Refrain from monopolizing systems, overloading networks with excessive data, or participating in any other activity that could degrade system performance (wasting computer time, connection time, disk space, printer paper, or other resources).

Passwords

Passwords are an essential component of computer security. Failure to protect a password can compromise data, as well as the enterprise-wide network itself. Avoid writing your passwords on paper (e.g. sticky / post-it notes). If you need assistance remembering and managing your passwords, Duke has licensed the LastPass utility, which can be used to generate strong passwords and store them in a secure fashion. Contact the DCRI Service Desk at 919-668-8916 for assistance with LastPass.

- As a DCRI network user, you are expected to abide by the following with regard to the use of passwords for the DCRI system. Your individual account is issued to you, and its password must not, for any reason, be shared with any other individual or group (including administrative assistants, managers, and IT staff).
- If a password is shared, it is compromised and must be changed immediately.
- IT and other technical support staff do not need passwords to troubleshoot a system. If you are approached by a staff member claiming to need a password, do not disclose your password, and contact the Service Desk immediately.
- Your initial system password issued to you by the Service Desk should be used only once and then changed.
- Guard your passwords from “shoulder surfers.” Do not verbalize a password in front of others or openly write a password down. Passwords may be written if they are stored securely in a location accessible only to you.
- If you have been given access to several systems, you may use the same password for each system. However, this password should not be used for access to other, non-Duke sites or systems.
- You may not use computer programs to decode passwords.

The DCRI allows only strong passwords, which must be chosen in accordance with these guidelines:

- Must contain at least 8 characters
- Must be changed at least every 180 days (or more frequently based on entity procedures) or when it is believed or known to have been compromised, whichever comes first
- Must not be re-used in less than three years
- Must contain at least 5 unique characters (no aaaabbbb, for instance)
- Must contain a mix of at least 3 of the following 4 categories of characters: uppercase letters, lowercase letters, numbers, and special characters (e.g., %)
- No dictionary words (even spelled backward) of four or more characters
- No personal information, such as family names or phone numbers
- No character substitution (e.g., using $ for s in a word)
- No password similar to one's user ID

Use of Equipment, Systems, and Supplies

The primary use of DCRI electronic resources is for the work activities of the DCRI. The DCRI recognizes, however, that users may occasionally wish to use equipment and systems for personal use not directly related to DCRI business. Sound personal judgment, honesty, and integrity should regulate the amount and frequency of such use. Any personal use of equipment and systems that may create a hostile work environment, impact the productivity of any employee, or result in wasted resources is inappropriate.

Employees and other authorized personnel are accountable for using DCRI-provided equipment, systems, and supplies in accordance with University policies and work rules. Therefore, electronic equipment and systems, including telephones, may not be used to access, create, communicate, download, send, print, or copy offensive, harassing, or potentially disruptive material. Do not use the Duke e-mail system for any of the following activities:

- Sending junk mail or chain letters
- Promoting commercial ventures, religious beliefs, or political causes
- Inappropriately sending, receiving, or downloading copyrighted materials, trade secrets, proprietary financial information, or similar materials
- Supporting, establishing, or conducting any private business operation or commercial activity
- Intentionally disseminating or accessing obscenity as defined by law or providing a hyperlink to same

Security

Duke users frequently are targeted by phishing emails and phone calls. Phishing refers to the act of a malicious individual attempting to gain access to sensitive information, such as usernames and passwords, by impersonating a trustworthy party. It is critical for everyone to be on the lookout for suspicious communications. For tips on identifying potential phishing messages, visit http://security.duke.edu/internet-safety/phishing.

Think before you click on links and attachments in emails. Inspect email addresses and web site URLs for contents that point to unfamiliar sites, and be suspicious of any that ask for your Duke NetID or password. Never open an email attachment if you do not trust the source, or if you were not expecting the file. Contact the DCRI Service Desk at 919-668-8916 to report any suspicious behavior.

As a DCRI network user, you are responsible for taking appropriate measures to ensure the security of protected health information and other confidential information. Employees are personally accountable for all activity performed under their identity / credentials. Appropriate measures include the following:

- Protecting the security of health information by equipping computer monitors in potentially public areas with security screen filters
- Maintaining a password-protected screensaver that automatically activates after no more than 15 minutes of system inactivity (1 hour in enclosed offices)
- Immediately retrieving confidential information from printers in any public area
- Locking workstations prior to leaving them unattended in any public area
- Ensuring that mobile workstations (e.g., laptops and hand-held or tablet devices) are returned to a physically secure environment when not in use
- Immediately notifying the immediate supervisor and the Service Desk of any theft or destruction of workstation equipment
- Never attempting to circumvent or subvert system or network security measures
- Never engaging in any activity to purposely harm systems or information stored thereon, such as by creating or propagating viruses or worms, disrupting services, damaging files, or making unauthorized modifications to University data
- Protecting the data on laptop hard drives or removable media from loss or inappropriate disclosure

DCRI network users are expected to inform the Service Desk of any potential security incidents, including the following:

- Any unauthorized use of DCRI systems in ways that compromise system availability, performance, or integrity
- Suspicion that a password has been compromised or has been locked without the user’s knowledge
- Loss of any DCRI confidential data or protected health information
- Discovery of protected health information or other confidential information on a workstation or printer that is unattended

Stand-Alone Media Security

Stand-alone media are any media that are not integrated into equipment. Examples include CDs, memory sticks and flash drives. Users are responsible for maintaining the physical security of these devices and their contents. Protected health information must be encrypted. Lost media containing PHI or sensitive information must be reported to the Service Desk and the immediate supervisor.

Users who need to dispose of any stand-alone media must deliver the media to the Service Desk or contact them and arrange for pickup. Printouts of sensitive information must be recycled in the secure recycling bins on each floor.

Privacy Limitations

The DCRI respects the privacy of users and does not routinely inspect or monitor individual use of computing or networking resources. However, in accordance with the *Acceptable Use Policy*, which is found at http://security.duke.edu/duke-acceptable-use-policy, the DCRI reserves the right to access, inspect, and disclose any information contained in its electronic information systems as deemed necessary and appropriate for its business purposes, without the permission or notification of the employee. This includes the contents of voice mail, computer files (regardless of medium), local hard drives, e-mail and computer conferencing systems, and systems output (such as printouts). The DCRI also reserves the right to restrict access to inappropriate or potentially harmful sites on the Internet.

Investigation of Misuse

Users should expect that the DCRI will inspect and monitor network communication—without notice—in any situation where one or more of the following conditions exist:

- It is considered reasonably necessary to maintain or protect the integrity, security, or functionality of University or other computer resources or to protect the organization from potential liability
- There is reasonable cause to believe that a user has violated any University policy and/or Duke’s *Workplace Expectations and Guidelines* http://www.hr.duke.edu/policies/staff_handbook.pdf or otherwise misused computing resources
- There appears to be unusual or excessive activity
- As is otherwise required by law

Supervisory Access

With the prior approval of the Functional Group or KRP Leader **and** the Chief Human Resources Officer, DCRI or designee supervisors may access the e-mail or files of staff within their unit without user permission for either legitimate business purposes or to investigate a user's alleged misconduct, when such access is reasonable under the circumstances.

IT Access

The DCRI IT Group conducts regular scanning of network files to ensure data integrity, data storage capacity, and data security. Files are reviewed if they are taking up a considerable amount of network storage or if they pose a risk in terms of their inappropriateness for storage on business storage systems.

Downloading Software

Any software installed by non-DCRI IT that compromises the security and integrity or performance of DCRI systems may be stopped from running without notice by the IT group, and continued use may be considered a violation of Duke *Workplace Expectations and Guidelines* http://www.hr.duke.edu/policies/staff_handbook.pdf.

Data Backups

Data backups are performed on all DCRI servers. It is a DCRI policy that business critical documentation must be stored on shared storage areas that are backed up. It may be appropriate to save working files locally on the hard drives, however, hard drives are not backed up.

Encryption

No form of patient data or sensitive business information from any computer system may be sent outside the protected network without encryption. The approved form of encryption for documents is via the encryption mechanism in, for example, WinZip or PGP software. If you have questions about these or other encryption packages, contact the Service Desk for more information. Email containing SEI that is sent outside of Duke Medicine must be sent using the Secure Email feature in the Duke E-mail system. This may be done using the “Sensitive Electronic Information” button in Outlook, or if that is not available in your email client, by placing the text “(secure)” at the beginning of the Subject line of your email.

Acknowledgment

"I have read and understand the policy described in this memorandum and agree to abide by the requirements set forth for users of DCRI computing equipment and network resources. I further understand my network access privileges may be discontinued and/or that I may be subject to disciplinary action, up to and including termination, for any violation of these policy requirements."

Signature ______________________________ Date ______________