This is a copy of the official, signed Policy on file.

Policies and Procedures

SUBJECT: Computer Services Policy

POLICY #: 202.3
PROCESS OWNER: Information Technology

RELEASE DATE: 09/18/2009
EFFECTIVE DATE: 12/10/2013
BOARD/CEO APPROVAL:

PURPOSE/OVERVIEW/INTENT:

This policy applies to all authorized users. Authorized users include MRN employees, contractors, consultants, collaborators, temporaries, and other workers, including personnel affiliated with third parties utilizing VPN access to MRN's network, granted an MRN domain account, and e-mail. IT services ensures that systems and applications operate effectively and provide appropriate confidentiality, integrity, network availability, and protects information commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access, or modification. These services include functionality such as network access, data storage, electronic mail (e-mail), network security, and network management. The scope of this policy applies to both MRN and non-MRN issued computers/devices that access the MRN network.

This policy outlines proper and improper behaviors, defines misuse and incidental use, explains rights and responsibilities, and briefly reviews the repercussions of violating these codes of conduct.

All MRN policies, including, but not limited to, access control, export control, harassment, hostile work environment, intellectual property, research data, data security, and confidentiality shall apply to the use of computing services.

GUIDELINES / GENERAL RULES / POLICY:

Rights and Responsibilities

MRN computing services must be used in an appropriate, ethical, and lawful manner. MRN does not provide a warranty, either expressly or implied, for the computing services provided. MRN reserves the right to limit a computer user's session if there are insufficient resources, and also to cancel, restart, log, record, review, or hold a job, process, or program to protect or improve system or network performance if necessary.

All users of MRN's Computer and Network Infrastructure (CNI) have no rights of privacy, or any reasonable expectations of privacy, for any materials stored or viewed and/or located on MRN's CNI. All communications performed or transmitted either on or through the use of the organizations network, may be, and at times will be, monitored, accessed, viewed, disclosed, and/or recorded to secure systems and operations.

Suspected violations of this policy (e.g., any incidents involving unauthorized access to, destruction of, or misuse of computing services by staff, students, or authorized third-party users) must be brought to the attention of MRN management. In the case of a criminal violation by employees or non-employees, MRN will notify the appropriate law enforcement authorities.

1. User Responsibilities

Users are responsible for all of their activities using computing services and shall respect the intended use of such services. Users must understand and keep up-to-date with this policy and other applicable MRN computer policies and procedures.

a. Copyrights

Software licenses are purchased either with systems or individually to provide required functionality and compatibility within the institute. Users shall use the software only in accordance with the licensing agreement. According to U.S. Copyright Law, a person or corporation that engages in the illegal reproduction of software or documentation can be subject to civil damages. MRN does not support the illegal duplication of software, documentation, and employees who make, acquire, or use unauthorized copies of computer software or documentation shall be disciplined, which may include termination. Non-employees may lose access for such behavior.

Users shall respect all copyrights including software, music, and movie copyrights. Users shall not reproduce copyrighted work without the owner's permission unless there are clear and documented Fair Use or TEACH Act exceptions. In accordance with copyright laws, including the Digital Millennium Copyright Act, MRN, upon receipt of official notice from a copyright owner, may authorize blocking access to information alleged to be in violation of another's copyright. Any such information violating copyright law will be uninstalled from MRN computing systems.

b. Software Licenses

Only software that is legally permitted or licensed shall be installed on MRN-owned computers, communications devices, personal digital assistants, etc. If unlicensed or illegal software is discovered on such an MRN-owned device, the software must either be uninstalled immediately or “made legal” through the acquisition of a legitimate license. MRN employees are also responsible for ensuring that any hardware or software that is installed on to or connected to an MRN-owned device (a) has been properly evaluated and tested; (b) does not contain any malicious software (e.g., computer virus, software Trojan program, software worm program); (c) will not negatively impact the performance of MRN's computing services or impede others from accomplishing the education, research, and public service mission of MRN; and (d) has been specifically authorized. Computer users may not install software or hardware on MRN computing equipment without prior approval from the IT Department.

c. Personally Identifiable Information

Personally identifiable information is protected information and must be kept confidential and shall not be transmitted unless encrypted. Examples of this type of information include, but are not limited to, social security numbers, driver’s license numbers, birth dates, medical information, and insurance policy numbers. When in doubt, individuals should contact MRN Information Technology or the MRN Privacy Officer.

d. Computer Security and Anti-virus Software

MRN Information Technology staff shall ensure anti-virus software is installed on MRN-owned equipment and keep the software active and up-to-date. This requirement applies to all computer servers as well as all MRN-issued desktop and laptop computers.

Individuals using computing services are responsible for (a) safeguarding all data, information, and MRN digital assets; (b) encrypting all data that is categorized as “Export Controlled” or "Protected Health Information" regardless of whether it is stored (at rest) or being transmitted over communication networks (in motion); and (c) keeping accounts and passwords confidential.

2. Unacceptable Computer Use

MRN reserves the right to sanction a user (pursuant to Section 6 herein) if it is determined, after an investigation by the appropriate office, that the user violated federal or state law or MRN policy by misusing MRN computing services. MRN will disclose illegal or unauthorized activities to appropriate personnel and/or law enforcement agencies.

a. Obscene Material

Users shall not access, store, display, distribute, edit, or record obscene, pornographic, lewd, or lascivious material using MRN resources. In the case of research where the display or use of such materials falls within legitimate job responsibilities, the Chief Operating Officer may exempt a user from the requirements of this subsection by documenting, in writing, the scientific value or purpose of having said material. The Chief Operating Officer issuing the exemption letter

shall keep the letter on file for three (3) years after the user is no longer employed by, or has a contract with, or otherwise provides services to MRN. The incidental and unsolicited receipt of such material, such as might be received through email, shall not constitute a violation of this section, provided that the material is promptly deleted and neither stored, nor forwarded to, other parties.

b. Security Violations

All Users of MRN computing services shall not:

- attempt to defeat or circumvent any security measures, controls, accounts, or record-keeping systems;
- use computing services to gain unauthorized access to computing services of MRN or any other entity;
- intentionally alter, misappropriate, dismantle, disfigure, disable, or destroy any computing information and/or services;
- knowingly distribute or launch computer viruses, worms, Trojans, or other rogue programs;
- physically or electrically attach any additional device (e.g., an external disk, printer, wireless access point, video system, or storage device) to a MRN issued computer or non-MRN computer, communications device, or network connection without specific pre-authorization.

c. Legal Violations

All Users of MRN computing services shall not:

- use computing services for harassment of any kind as defined in the MRN Anti-Harassment Policy;
- use computing services for unlawful purposes including fraudulent, threatening, defamatory, harassing, or obscene communications;
- invade the privacy rights of anyone;
- disclose student records in violation of FERPA Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99);
- disclose faculty or staff records;
- use computing services to access or disclose financial information in violation of any other MRN policy;
- use computing services to access or disclose any non-public or personally identifiable information about a patient, research subject, employee, or student without having a legitimate MRN purpose;
- use computing services to access or disclose medical information about a research subject, patient, employee, or student without having a legitimate MRN purpose or in violation of HIPAA except as permitted by MRN policy and applicable state and federal law and regulations; or
- use computing services to violate MRN policy, state law, or federal law, including copyright and child pornography laws.

d. Other Misuse

All Users of MRN computing services shall not:

- use computing services in violation of any MRN contractual obligation, including limitations defined in software and other licensing agreements;
- use computing services in a way that suggests MRN endorsement of any commercial product or service (unless a legal agreement exists and any communication or computing activity has been pre-approved by an appropriate manager);
- use computing services to masquerade or impersonate another person or entity.

3. Personal Use

The personal use of computing services or communication devices for extenuating circumstances is permitted. Personal use of computing services, however, should not interfere with an employee fulfilling his or her job responsibilities. Use should be infrequent, limited, and non-routine and should not:

- consume significant time or resources,
- interfere with other users' access to computing services, or

- be excessive as determined by management.

4. Electronic Protected Health Information

Electronic Protected Health Information (ePHI) must be protected under various laws and regulations and shall be encrypted wherever it is stored and whenever it is transmitted. MRN will provide encrypted storage media to any employee required to transfer ePHI. Personally owned storage media will not be used to store or transmit ePHI or other MRN data. Principal Investigators will document the transfer of data in accordance with the MRN Research Data Policy.

5. Privacy Limitations

MRN reserves the right to monitor individual usage of its computing services. The normal operation and maintenance of MRN computing services requires the backup and storage of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities as are necessary for the rendering of services. It is the right of MRN to monitor and review any activities on its resources. It is best, therefore, to assume that any and all actions taken or activities performed using MRN computing services are not private. MRN reserves the right to monitor or scan personal laptops, computers, smart devices, or other electronic equipment or media that have been used to access or store MRN data in the course of investigating a security or policy violation.

MRN may also specifically access and examine the account of an individual user under the following circumstances and conditions:

- to ensure compliance with federal or state law,
- to examine an account if there is reasonable suspicion that a law or MRN policy has been violated and access is needed to investigate the apparent violation. or
- to preserve public health and safety.

Information stored electronically may be made available in administrative or judicial proceedings.

6. Sanctions

The misuse, unauthorized access to, or destruction of MRN computing services and resources in violation of applicable laws or MRN policy may result in sanctions, including but not limited to withdrawal of use privilege, disciplinary action up to and including expulsion from the MRN or discharge from a position, and legal prosecution. MRN reserves the right to sanction if it is determined, after an investigation by the appropriate office, that the user violated federal or state law, or MRN policy.

7. Computer Hardware and Software Purchases

Computer equipment and software purchases require approval by the Director of IT. Software and hardware disposition shall be coordinated with the Help Desk. A functional requirement and technical review for any specialized system or network component is required as part of the purchasing process. This review identifies compatibility with MRN's network systems, network requirements, and hardware and software license requirements. The review must verify the system meets the functional requirements as designated to the best of the ability of the reviewer. Requests shall be submitted through the MRN Help Desk ticketing system.

8. Electronic mail (email)

The MRN email system shall not to be used for the creation or distribution of any disruptive or offensive email messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Transmission of Protected Healthcare Information (PHI) in unencrypted form is also prohibited. Employees who receive any email with this content from any MRN employee should report the matter to their supervisor immediately.

Email messages are limited to 25Mbs in size including the attachments.

Information, the loss, or misuse, or unauthorized access to or modification of which could adversely affect MRN or an individual requires proper handling and protection. The following markings will be included in the Subject line of all electronic mail containing Sensitive Information, depending on its type:

MRN Sensitive
or
MRN Sensitive - Export Controlled

Email marked with the term "MRN Sensitive" in the subject line will automatically be encrypted to external users and they will be sent a HTTPS SSL link to log on to receive the message and any attachments. This does not guarantee the recipient, only that the message sent was encrypted.

For example:
MRN Sensitive - Investigation Results
MRN Sensitive - Export Controlled - Patent idea

Email can be accessed through Microsoft Outlook, web client through the use of an Internet browser, and/or a smart device (a smart device can include personal cell phones, iPad, and other wireless accessible devices). Personal phones that are configured to receive company e-mail are subject to review when an employee leaves or is terminated from the Institute.

9. Encryption

All MRN-owned laptops and remote desktops (those not on site at MRN) must have encryption software. MRN Information Technology staff shall ensure encryption software is installed on MRN-owned equipment and will keep the software active and up-to-date.

Proven, standard algorithms such as 3-DES, Blowfish, RSA, RC5, AES and IDEA should be used as the basis for encryption technologies. Symmetric cryptosystem key lengths must be at least 128 bits using 2048 bit or larger certificates. Asymmetric crypto-system keys must be 256bit or of a length that yields equivalent strength.

MRN's key length requirements will be reviewed annually as part of the annual review of this policy and upgraded as technology allows. No encryption technology other than that approved and distributed by IT may be used to protect restricted data. The use of proprietary encryption algorithms is not allowed for any purpose. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

10. Data Storage on Networks Storage

Users are allocated storage space in a personal (Home Directory) and a group folder. Any data requiring backup shall be stored on the network storage. For proper file management, the following storage rules apply:

- Monitor storage in home directories. Keep it free of excess or unnecessary files such as outdated documents, data, or graphic files.
- The designated group folder owner shall monitor data storage utilization. The folder owner shall ensure the data volume is minimized.

Note: MRN IT monitors disk quotas and will contact folder owners when quota reaches 90% full.

11. Cloud Computing

MRN recognizes the significance and utility of "cloud" computing services including data storage. It is the responsibility of MRN to protect the institute's data, ensure compliance with the agreements that govern our sponsored research programs, and various regulatory agencies compliance. Refer to the MRN's Privacy and Information Security Training for specific details regarding the HIPAA Privacy Rule and Security Standards, and best practices for information security.

It is the responsibility of MRN staff, external collaborators, and volunteers that store data on non-MRN managed "cloud' services to ensure that the logical security measures adequately protect the information being stored.

Any cloud computing services provider that is being used to store, transmit, or transform any MRN data must adhere to this set of standards. "MRN data" includes but is not limited to:

- Research data produced by MRN faculty, staff, and external collaborators, including:
    - All raw and processed experimental data, both pre- and post- publication
    - Generated study data
    - Grant applications and supporting documentation/data
- MRN business and employee data including:
    - Personnel information
    - Employee contact information
    - Procurement of other business data processed by outside services in a hosted environment

The "cloud" is not a long-term storage solution. Remove the data once the purpose of usage the "cloud" is accomplished.

REVISION HISTORY:

DATE	REVISION	DESCRIPTION OF CHANGE
09/18/2009	**0**	Original Release
07/15/2010	**1**	Issuance of exemption letter by Chief Research Officer Instead of Chief Science Officer.
08/30/2010	**2**	Added volunteer and collaborator.
12/10/2013	**3**	Updated sections to reflect current services, support, and electronic mail (email), added section 7. Computer and Software Purchases, section 8. Electronic mail (email), section 9. Encryption, 10 Data Storage on Network Storage, and 11. Cloud Computing.