NMC INFORMATION TECHNOLOGY POLICIES AND PROCEDURES

Table of Contents

Suite 301, 4200 W Jemez Rd, Los Alamos, NM 87544
505-412-4200, fax 505-212-0049, info@newmexicoconsortium.org

NMC Information Technology Policies and Procedures

I. Overview

The purpose of these Information Technology (IT) Policies and Procedures is to establish guidelines for the use and management of IT resources (workstations, laptops, servers, printers, networks, etc.) by New Mexico Consortium (NMC) and for the implementation of a level of security which will provide for the protection of data and information technology resources from accidental or intentional unauthorized disclosure, modification, or destruction from within or outside the company.

The procedures listed in this document establish the methods NMC will use to protect the confidentiality, integrity, availability, and reliability of all information technology resources used to support the needs of our researchers and the mission of the organization.

These policies and procedures apply to all employees of NMC, to non-NMC individuals performing work using NMC IT resources, and to all IT resources whether owned, leased, or contracted by NMC.

NMC's Chief Information Officer (CIO) is responsible for implementing and monitoring the policies and procedures described in this document.

II. User Access

Access to NMC's servers, computers and system resources by NMC or outside sources will be determined by CIO in coordination with the Director, PIs, and managers. Each staff's position requirements will be taken into consideration in determining the staff's level of access.

In order to have access to the company's IT resources (e-mail, servers, workstations, printers) all users must obtain a user account from the NMC's Tech Support (techsupport@newmexicoconsortium.org). Once the accounts are established, users will set their own passwords to gain access to those resources. Passwords are required for the network account, e-mail account, access to the databases and any other account the user may be assigned to. Network administrator may require passwords being changed on a regular basis (e.g., every 90 days), or passwords to be unique (i.e., once a password has been used, it can never be used again.). If there are reasons to suspect a password has been compromised, the network administrator has the authority to disable an account or change a user's passwords, temporarily suspending user access to the account(s).

Upon request, NMC staff may be assigned a specific network drive to store their work.

In the case where several users need common access to some files on the server, Tech Support staff will create special shared network folders for that purpose.

III. Software Installation and Management

1. Only Tech Support staff are authorized to install, update, or remove NMC-owned software from a workstation or laptop.

2. All software installed in computer property of NMC is either in the public domain or has been legally purchased or leased by NMC.

3. Any software found installed on a workstation or laptop, which violates the policies stated in this document, will be immediately deleted upon detection

4. The Tech Support staff will assign each server, workstation, laptop or notebook an administrator password that will be known only to the authorized personnel. The Tech Support staff will then establish user profiles in order to protect the programs and data in a computer from being accidentally or intentionally deleted by users, prevent the installation of unauthorized or conflicting software, prevent users from saving information to specified locations, prevent the access, installation or removal of printers and other hardware and, in general, prevent users from changing a computer's configuration. Only authorized staff can install, update or remove NMC-owned software from servers and computers, to add or delete printers and, in general, to change computer settings.

5. Tech Support staff ensure that the software installed on company computers has been legally purchased or leased by NMC. The IT department will keep a log of installed software to make sure that the number of licenses purchased or leased is not exceeded. Clear communication is the key to preventing these problems. Employees should discuss installation of any additional software on the NMC-owned computers with their supervisor or IT manager prior installation.

6. If it is determined that an individual has violated company policy by installing illegal or unauthorized software on an NMC machine, or that inappropriate non-work related data is stored on the NMC computer, the finding will be reported to the management, and a disciplinary action may be taken against the employee who installed the unauthorized software.

IV. IT Security

A. User Responsibilities

Although the CIO has overall responsibility for the security of the NMC's IT Resources, every member of the NMC community is responsible for protecting the security of NMC information and information systems by adhering to the NMC policies and using safe computing practices.

1. Understand phishing. The classic phishing trap is when a malicious person sends you an email with a request that you follow an embedded link in the email, and then has you enter your password or other personal information. They have redirected you to their own web site and are collecting the information you type. If you are faced with a request to follow a link from an e-mail and then enter any information, stop, then read this. The only way to stop phishing attacks is by being vigilant. Here is the link to the Wikipedia page about what phishing is: https://en.wikipedia.org/wiki/Phishing
   New phishing techniques emerge every day. Be aware.

2. Don't download and open an attachment unless you know and trust the sender. Again, the only way to avoid this is to be vigilant.

3. Open PDF documents with Adobe Acrobat READER. Don't use Acrobat or Acroread unless you need to edit a PDF document. There are several alternative PDF viewers for simple reading (OS X default viewer "preview", Skim, Foxit for Windows, several great ones for GNU/Linux). Don't use Adobe products for simple PDF viewing!

4. Keep all your software (operating system, browser, office) updated with the most current versions. The software developers release updates whenever they identify a security vulnerability. Generally, they are staying on top of these issues. However, you have to update your software to take advantage of this. The recent trend in malware is to operate through vulnerabilities in office software like Word and Adobe Acrobat. So all your software needs to be updated all the time. Don't ignore that request to update your software and set updates to weekly or daily, not monthly.

5. Think before you enter your administrative password. If you are surfing the Web and you are all of a sudden prompted for your administrative password, it is almost certain that something is wrong unless you are installing or updating software. Regular Web surfing should never require your administrative password.

6. Report lost computers immediately. We may need to move quickly to change passwords if they may have been exposed.

7. Evaluate the risks of computing and the value of the data on your machine:
    i. if you would like to encrypt your hard drive, we can arrange that.
    ii. if you like to have virus protection software, we can do that.
    iii. if you would like to operate on a non-administrative account, we can arrange that.
8. Users should be aware that NMC:
    i. may be liable for any e-mail originating out of its corporate account.
    ii. reserves the right to monitor e-mail use by its staff.
    iii. monitor Internet access at any time

B. CIO Responsibilities

CIO (Chief Information Officer) is responsible for advising NMC staff in security practices relating to these areas:

1. Financial information and transactions (CFO – Chief Financial Officer)
2. Health information (HR – Human Resources)
3. Personnel information (HR – Human Resources)
4. Confidentiality (Operations, Tech Support Staff)
5. Infrastructure, communications, and systems security (Tech Support Staff)
6. Legal issues (COO – Chief Operating Officer)
7. Research data and sponsored programs information (Director, researchers)

C. Protecting Personally Identifiable Information (PII)

PII means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, public websites, and university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any

single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.

Examples of PII include but are not limited to the following:

1. Social security numbers in any form
2. Place of birth associated with an individual
3. Date of birth associated with an individual
4. Mother's maiden name associated with an individual
5. Biometric record associated with an individual's
    i. Fingerprint
    ii. Iris scan
    iii. DNA
6. Medical history information associated with an individual's
    i. Medical conditions, including history of diseases
    ii. Metric information, e.g. weight, height, blood pressure
7. Criminal history associated with an individual
8. Employment history and other employment information associated with an individual
    i. Ratings
    ii. Disciplinary actions
    iii. Performance elements and standards (or work expectations) are PII when they are so intertwined with performance appraisals that their disclosure would reveal an individual's performance appraisal.
9. Financial information associated with an individual
10. Credit card numbers
11. Bank account numbers
12. Security clearance history or related information (Not including actual clearances held)

Protected PII means an individual's first name or first initial and last name in combination with any one or more of types of information, including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal, medical and financial records, educational transcripts. This does not include PII that is required by law to be disclosed.

Storing PII on NMC computers requires COO's and CIO's written approval and normally is not allowed. PII can be stored on approved devices on an encrypted file system, and access is restricted to only those who need access by passwords and file system permissions.

On-site, computers with PII are located in a restricted access area and are password protected.

PII may be stored on off-site computers when necessary on an encrypted file system.

D. Vendors

Vendors providing hosted services and vendors providing support, whether on premises or from a remote location, are subject to NMC IT policies and will be required to fill out the acknowledgement form on part IX.

E. Other Registered Entities

Any entity that is a registered user and connected to the NMC network is responsible for the security of its computers and network devices and is subject to the following:

a. The provisions of these IT Policies and Procedures.

b. All other laws, regulations, or policies directed at the organization and its individual users.

F. Server Security

All NMC servers will be placed in a secure location, such as in a locked room with restricted access. In cases when it is not possible to place a server in a locked room, it will be placed in a lockable case, ensuring that the case is always locked.

Additional server and computer security is provided by a combination of firewalls, VLANs, and routers.

Anti-virus and adware removal software may be installed on NMC machines at CIO's discretion.

G. E-mail/Internet Access

Both Internet access from NMC property and NMC e-mail accounts should be used almost exclusively for work-related purposes, and neither can be used in a way which is offensive to an individual or a group of individuals. Internet access and the use of NMC e-mail can and will be monitored by IT staff at their discretion. Our web-based e-mail is hosted by Google, which puts more resources than anyone else in protecting Internet communication from malware.

H. Reporting of IT Security Incidents

A critical component of security is to address security breaches promptly and with the appropriate level of action. All users of NMC computing resources are responsible for reporting incidents in which they suspect data, computer or network security may have been compromised. The NMC Incident Report Form will be used to report an IT security incident. The issue will be addressed as prescribed by the incident reporting procedures.

V. Backup and Recovery

A. The NMC IT team will make every effort to ensure that users' data is protected via backup and recovery procedures. Whole-computer backups will typically not be completed unless for mission critical servers where rapid disaster recovery is required. Backup schedules are determined based on criticality of the data on the individual computer as determined by CIO(Chief Information Officer), COO (Chief Operating Officer), and CFO (Chief Financial Officer).

- **Laptops**: These devices are highly mobile and employees usually carry laptops with them between the workplace and their home, or if they are on travel. NMC IT Staff will install a backup software (such as CrashPlan) on each laptop, and make sure that an initial backup of the user's files is completed. Incremental backups are then taken regularly as network connectivity permits (usually while employee is on NMC premises), or via VPN.

- **Desktops**: Desktop computers are usually stationed in offices. Users' home directories or other requested directories are backed up using a backup software (such as CrashPlan). Other directories, such as project directories with data specific for the research performed on such computers are encouraged to be kept on a network drive, or specifically requested to be backed up by the researcher maintaining that computer. Depending on the size of the data to be backed up, prior approval may need to be requested by the IT team from the CIO (Chief Information Officer).

- **Servers:** NMC servers are often part of critical infrastructure and for this reason are always backed up.

- **Financial**: This data is critical to the NMC operations and will be protected by multiple levels of backup, both on-site and off-site. Off-site backups are currently managed through a cloud provider (currently Armada Backup), and can be restored from any place with an Internet connection.

- **ADP**: Our payroll system is hosted in the cloud, and the NMC holds ADP accountable for backing up the payroll information in their system. ADP reports are stored as encrypted files on a restricted-access server only.

- **Personal devices**: The NMC is not responsible for backing up or protecting employees' personal compute devices (laptops, tablets, phones, etc…) brought to work. If a personal device is used for NMC work purposes, the tech Support staff must be informed and data protection and backup may be provided by NMC.

B. Backup schedules. To guarantee that critical backups are not destroyed along with the originating server(s) in case of a natural disaster, at least two copies of the backup data will be stored at locations different than where the original data resides. The first copy is kept at an alternate NMC location (when multiple viable locations are available) and the second copy is located with a trusted cloud backup provider. If no alternate NMC locations are available, both copies shall be stored at external backup providers. The criticality of data is determined by the COO and CIO, in collaboration with the users of the data.

Backups shall be performed incrementally and increasingly often directly related to the criticality of the data. For example, financial data that is accessed and modified multiple times per day should be backed up multiple times per day. However, data which is modified once a month does not have to be backed up several times per day. Due to the differences in data, the backup infrastructure also has to be tired. I.e., tape backups runs only once every night or less often whereas backups of critical data is done to a fast network server with disks. Those fast disk backups, are then accumulated on slower media (such as tape) later on.

C. Disaster recovery. In addition to the criticality of the data itself, is also important to understand how rapidly backed up data can be recovered following a disaster. The most critical data must also be quickly recoverable - therefore, data such as finances must be immediately recoverable. That is why such data is stored encrypted in the cloud, and backed up multiple times per day. Any off-site tape backup could take a very long time to retrieve. The following table outlines the types of data and corresponding levels of recoverability:

Data type	**Typical data size**	**Recovery time**
Critical Infrastructure Servers	~50GB	<2 hours
Financial & Administrative	~50GB	<8 hours
Home directories	~3TB	<24 hours
Desktop / Laptop computers (with current backup)	~25GB/machine	<2 days
Project directories (portions that are backed up)	~50TB	<1 week

VI. Cell Phones and Tablets

NMC may provide some employees with additional communication technology devices or services as authorized by the NMC Director:

- NMC-owned cellular phone voice/text/data messaging service,
- NMC-owned cellular wireless modems associated with tablets or Verizon Mi-Fi devices
- NMC-owned tablets

Some of these devices may be given to employee upon separation from NMC. IT staff must clear the device prior releasing it to the separated employee.

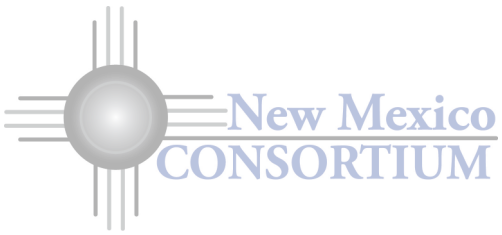
VII. Biolab

The NMC Biolab is located about 5 miles away from the main office. The two buildings are connected with a direct Ethernet (provided by REDInet) circuit at 10 Gbit/s. The Biolab is wired up with Cat6 cables at over 100 locations around the building, and wireless service is provided throughout the building and the attached greenhouse.

Non-NMC residents at the Biolab may use non-NMC computers. NMC provides Internet connectivity, and printing services to non-NMC staff at the Biolab. Support requests outside these basic services are subject to CIO / Director approval and may incur extra charges.

VIII. Troubleshooting and Maintenance

For all IT related issues - a support request should be sent to techsupport@newmexicoconsortium.org. Techsupport can also be reached on the phone at (505) 412-6543 but email is the preferred medium of contact.



IX. Acknowledgement of NMC IT Policies and Procedures

By signing this, I (name)_____ on behalf of (company) _____ acknowledge that I have read, understood and will comply to the NMC IT Policies and Procedures.

Signature: _____

Title: _____

Date: _____