



# NFISD Department of Technology

## Computer & Network Security Procedures

Procedures Document No.

Effective Date:

Last Revised:

**Directly in support of the following policy documents:**

Status

- Draft
- Under Review
- Approved

The following are responsible for the accuracy of the information contained in this document

**Responsible District Officers**

**Responsible Coordinating Office**

North Forest Department of Information Technology (NFIT)

## 1. Summary and Scope

The purpose of these procedures is to provide specific requirements to protect North Forest ISD information technology resources and the information stored on those resources, while appropriately governing employees' and students' behavior. These procedures may be superseded by unit-level information technology procedures which are officially approved by the unit head, NFIT, and North Forest ISD Board of education.

(NOTE: Phrases shown in *italics* at their first occurrence in this document are defined in the associated IT Policy Definitions - Standards Document No. 00.00.00)

## 2. General Procedures

### 2.1. Users

#### 2.1.1. General NFIT Faculty/Staff Security Responsibilities

Security responsibilities associated with NFIT information technology resources must be communicated to users. This training must become part of the unit-level induction procedure for all new hires. This should be supplemented with periodic additional training. The following topics must be included:

- Password policy and how to choose good passwords.
- Prohibition of unmanaged modems/cellular modems/remote access communication lines.
- Defense against "social engineering" tactics to gain unauthorized access to systems, or to obtain sensitive information. This should specifically include information about *phishing*, *spyware*, and web browsing concerns, and current scams.
- The fundamental insecurity of e-mail.

### ***Computer & Network Security Procedures***

- Location and identity of their unit computer support, the Director/Manager for their division, and the NFIT Information Security office.
- How to access this policy and [NFIT Data Access Policy](#) online.
- Recommendations about physical security (e.g., lock up your office when leaving, protect information on portable drives when traveling).
- How to report an incident.
- Other topics as deemed necessary or timely by the Dean, division Director, Chair, or the newly hired person's unit computer support.
- Review the information security tutorial located online: (website address)

#### **2.1.2. Employee termination and clearance**

The unit must establish a procedure to revoke or revise access rights to NFIT resources (information or physical) immediately following any significant shift in job responsibilities (e.g. transfer between operational areas within the unit, transfers outside the unit within NFIT, retirement, termination, or reclassification).

#### **2.1.3. Incident response**

Refer to NFIT's Incident Responses Procedures for detailed guidance.

#### **2.1.4. Investigative contact**

If anyone is contacted by a representative from an external law enforcement organization (District Attorney's Office, FBI, DPS, ISP security officials, etc.) that is conducting an investigation of an alleged violation involving NFIT computing and networking resources, they must inform the NFIT Office of Legal Affairs (need number) immediately.

### **2.2. System/Network Management**

Specific computer system and network management details are noted in this section for implementation by the unit technical lead. The technical lead and the technical support team hold system administration authority and the associated responsibility.

#### **2.2.1. Administrators**

Every NFIT-owned networked device (e.g. server, workstation, laptop) must have a designated system administrator, by default a member of the technical support team. If the administrator is not a member of the *technical support team*, he or she must sign a document (physical or electronic) accepting the administrative privileges and responsibilities (see sample form in Appendix A). All exception cases must be approved by the technical lead. System administration privileges include all of the following:

- Physical access to the system at all times
- Ownership of the controlling account for the computer (e.g., "root" or "Administrator")
- Control over the assignment of access rights on the administered system and providing access to systems as noted by the data coordinator or data steward.
- Authority to change the system configuration, reboot the system, and/or disconnect/connect the system to the NFIT network as needed
- Authority to manage the system logs, security logs, user access logs, etc.
- Installation or modification of system software or hardware

System administration responsibilities include full compliance with all applicable policies and procedures as well as the Data Protection Safeguards.

### **2.2.2. System and network performance monitoring**

As part of its enterprise services and network management responsibilities, NFIT is responsible for providing scanning for malicious content (e.g. *viruses*, web pages crafted to compromise computers), scanning wasteful content (e.g. *spam*), and monitoring network performance in a manner appropriate to NFIT as a whole. Centralized scanning by NFIT is in addition to the scanning activities normally undertaken at the unit.

### **2.2.3. Inspection of files and monitoring system and network usage**

A system administrator may access others' files for the maintenance of networks and computer and storage systems, such as to create backup copies of media. In the event of unintentional discovery of unlawful content, federal and state laws compel system administrators and technical support to report situations that are against the law (e.g. child pornography).

The District may specifically monitor the activity and accounts of individual users of the District's computing resources, including individual login sessions and communications, without notice. This monitoring includes all network-based traffic, wireless traffic, and NFIT systems' use (e.g. e-mail, *voice over IP communications (VoIP)*), content on computers owned by NFIT, sponsors, and contracted entities). This monitoring may occur in the following instances:

- i. The user has voluntarily made the files accessible to the public.
- ii. It reasonably appears necessary to do so to protect the integrity, security, or functionality of the District or to protect the District from liability.
- iii. There is reasonable cause to believe that the user has violated, or is violating, NFIT information technology policies.
- iv. An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns.
- v. Upon receipt of a legally served directive by appropriate law enforcement agencies.

Any such individual monitoring other than that specified in point (i) above, required by law, or necessary to respond to bona fide emergency situations, must be authorized in advance by the Chief Legal Advisor and the Director for Information Technology or their designee(s). In all such cases, the appropriate unit head will be informed as time and the situation allows. In all cases, all individuals' privileges and right of privacy are to be preserved to the greatest extent possible.

### **2.2.4. Procedure for requesting new or extended network service**

The online user request form, "Request for Service" web form, should be used whenever possible as described in the previous section, using email, fax or calling the HelpDesk only as backup alternatives. The following information must be included in the request:

- In the "Campus/Dept." field, enter "Your Campus location", room number, phone number, your name, email address.
- In the "Hardware/Software Problems" field, check the appropriate issue, next, enter more detailed information in "Description of Problem" field.

If the NFISD online user request form is not accessible, the request may be sent via email to support@nfisd.simhouston.com, faxed to (713) 491-1090 or can be “called in” to the HelpDesk at (713) 491-1031. In all cases, the above information (Summary and Detail) must be conveyed in order to process the request in a timely manner.

**2.2.5. Procedure for requesting networking policy exemptions**

The online user request form, “Request for Service” web form, should be used whenever possible as described in the previous section, using email or calling the HelpDesk only as backup alternatives. The following information must be included in the request:

- In the “Campus/Dept.” field, enter “Your Campus location”, room number, phone number, your name, email address
- In the “Hardware/Software Problems” field, check the appropriate issue, next, enter more detail information in “Description of Problem” field.

**2.2.6. Standards for information publication**

The Department of Communication and Public Affairs office maintains the standards for information publication (website address). These standards include information intended for District-wide communications or communications intended for the public.

**2.2.7. Logon banners**

All computers and remote user communications facilities, if capable, must be configured to display the following or similar *pre-logon banner*:

Unauthorized system access is prohibited. System use is governed by the NFIT Computer and Network Usage and Security Policy and the NFIT Data Access Policy.

**2.2.8. Malicious software control**

The network manager is responsible for implementing protective security measures (e.g. workstation firewall, anti-spyware, anti-virus scanning on workstations, e-mail servers, and mail servers).

**2.2.9. Ancillary systems backup and disaster recovery**

In order to maintain the *availability* component of information security, the technical lead must have a system implemented, maintained, managed, and tested that duplicates and preserves business, research, and instructional-critical data. Depending on the criticality of the information, some duplicate copies of the data may be kept “off-site”, or preserved against physical damage from fire, water, theft, erasure, etc. A “system” includes hardware, software, and trained staff with published procedures to follow.

This system should be tested after initial implementation, major system changes, and annually.

The unit must have a practical IT disaster recovery plan created with all technical support and managers fully familiar with this plan and in agreement about how it should be executed. The procedure for briefing a newly hired manager or technical support person should include an overview of backup procedures and the disaster recovery plan, and a copy of these plans and procedures for their files.

#### **2.2.10. Physical security**

Information security requires maintaining physical security, including:

- Major file and application servers should be placed in *limited-access room(s)*. At least one full copy of a system backup should be stored away from the system or off-site.
- Network equipment and cable patch points should be placed in limited-access rooms, with only authorized support staff permitted access.
- Individual computers (generally for one person's use) should be in rooms that are locked during non-work hours.
- Only system administrators, technical leads, and/or technical team members may add or remove parts from a computer.

#### **2.2.11. Accountability and auditing**

Computers must have password-protected screen savers enabled. Computers actively used by more than one person should be set up to maintain user accountability and auditability. On systems which can have effective access controls (e.g. Windows NT/2000, UNIX), a login process should always be required which can capture the userID of the person logging on and the time at which they logged on and off. "Autologin" procedures are limited to accounts for auditing and centralized, automated administration. On systems where the security need is higher based on data classification or other operational criteria set by the unit head, the audit log will be reviewed as prescribed in the Data Protection Safeguards ([website address](#)). For remote user communication facilities, this information should *always* be captured and saved, and backed up for at least 90 days, and regularly analyzed for evidence of attempted security breaches.

Users who access sensitive data should consult the Data Access Policy for additional requirements.

### **2.3. Workstation Application Selection and Configuration**

While servers are unique and have specific requirements based on function, workstations should be as generic as possible, with special administration being undertaken only with careful consideration of the appropriate academic or business need. To the greatest extent possible, the number of *different* brands, models, sizes, and versions of equipment, software, and operating systems should be minimized to limit the cost and complexity of support.

Hardware and software purchases should be made from an approved technology list maintained by the technical lead (Director of IT) or with a written waiver from the technical lead.

## **2.4. Data Management & Retention**

Although the Institute Data Access Policy, Data Access Procedures, and Data Protection Safeguards provide in-depth details for data management based on data categorization, the following procedures should be implemented.

### **2.4.1. Data Categorization**

All data at NFIT must be categorized into the following four categories: (1) Public Use, (2) Internal Use, (3) Sensitive, and (4) Highly Sensitive. All media containing sensitive and highly sensitive data must be clearly labeled with the corresponding data category.

### **2.4.2. Data Responsibility**

All significant collections of data, data critical to scholarly or business function, and data categorized as “Sensitive” or “Highly Sensitive” must have an established *Data Steward*, *Data Coordinator(s)*, and *Data Administrator(s)*.

### **2.4.3. Data Protection**

All information must be protected as specified in the Data Protection Safeguards based on the data category. All servers containing “Sensitive” or “Highly Sensitive” information must be registered with NFIT.

### **2.4.4. Data Retention**

Much of the data handled electronically is subject to specific federal, state, and/or Board of Trustees retention, archiving and record keeping requirements. It is the responsibility of the Data Stewards to know specific regulatory requirements, and to abide by these requirements. For data without specific retention requirements, users are advised not to retain the data for longer than operationally necessary.

## **2.5. Computer Lab Management**

Computer labs are run both as a centralized resource and within specific units. Each computer lab must be administered in compliance with the following requirements.

### **2.5.1. Acceptable use**

- Users must obey all posted rules (e.g. Food and tobacco products are not permitted in any computing lab at any time for any reason).
  - All use must be authenticated by ID and password or other means
  - All use must be in compliance with the Computer & Network and Security Policy (CNUSP) and the Data Access Policy (DAP).
- See board approved acceptable use policy

### **2.5.2. Software installation and system images**

Lab workstations should be configured to allow software installation only by the lab director/manager. When appropriate (based on lab size), each lab should maintain a standardized image for easy restoration of systems in the event of a failure. Systems should be reformatted and reinstalled or re-imaged at least every other month.

Computers in labs will be erased and re-imaged multiple times during each semester. Therefore, lab users should have no expectation of data retention on individual systems

between uses. Notice of this practice will be clearly posted in each lab as a reminder to not save important files on local hard drives of any lab computer.

## **2.6 Data Requests**

Many programs require student data to be supplied, from our student information system (SIS). All such requests must be made in writing, including the date of the request, the deadline and all necessary contact information. Please allow up to one (1) month for data to be prepared for an application.

# **3. Access Procedures**

## **3.1 Computer / Program Access**

In order to safeguard our network from unauthorized access, it is imperative that all user access is coordinated with the technology department in advance. All requests for computer or program access should be made no less than five (5) business days in advanced.

### **3.1.1 E-mail / Computer Access**

All computer and e-mail access is coordinated through the Human Resources department. Once an employee's information is filed with HR, technology receives the position and location information, and issues a username and password to the campus principal.

### **3.1.2 Finance Plus**

Requests for access to Finance Plus must be made in writing to the technology department using the *Finance Plus Authorization Form*. This form can be requested from the Finance or Technology department. Any access to the financial or budgeting systems, other than entering / approving requisitions, requires a signature from the Director of Finance. Any access to the human resources package requires a signature from the Director of Human Resources.

### **3.1.3 eSchoolPlus**

eSchoolPlus access can be requested from the Technology Department or Student Services. All teachers, with schedules, have access to the system automatically, and do not require additional paperwork. All requests for administrative access (i.e. counselors, PEIMS, principals, etc), must be made using the eSchoolPlus Authorization Form. This form must be signed by the highest level campus principal, as well as the Director of Student Services.

**3.1.4 Forgotten Passwords**

Any user, who forgets their password, will need to contact the technology department either in person or by phone. When making the request, the requestor may be asked to verify by their district ID number and/or a portion of their social security number (Last four digits). (Note: This does not include the district's Cambridge software)

## Appendix A – System Administration Selection

The following document designates the system administrator as noted in section 2.2.1 of the procedures:

### System Administrator Designation

This form designates the system administrator for the following system:

|               |       |      |       |
|---------------|-------|------|-------|
| Manufacturer: | _____ | OS:  | _____ |
| Model:        | _____ | IP:  | _____ |
| Host          | _____ | MAC: | _____ |
| Firewall:     | _____ |      |       |
| Other         | _____ | DNS: | _____ |
| Security:     | _____ |      |       |

#### Administration Responsibilities

System administration responsibilities are completely described in the NFIT Computer & Network Security Procedures. A few of these responsibilities include:

- ⌚ Install only appropriate, licensed software on the system
- ⌚ Apply all operating system and application patches as required by NFIT's Computer & Network Usage and Security Policy (CNUSP), its associated documents, the Data Access Policy, and the Computer & Network Security Procedures.
- ⌚ Supply system and application access only to appropriate NFIT employees and students (unless the target audience is the internet at-large and your director approves in writing)
- ⌚ Maintain appropriate security software (e.g. firewall, intrusion detection, and virus scanning)

#### System Administration Selection – Select one of the following options:

- ⌚ I assume all responsibilities for system administration as noted above. I agree to handle the operating system(s) maintenance, hardware additions, application installations, application maintenance and access in a secure manner to protect the computing assets of NFIT.
- ⌚ will maintain the operating system(s), applications, and access to my system in a secure manner to protect the computing assets of NFIT. I understand that I may not receive administrator/root access to this system.

System Administrator's Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Print Name: \_\_\_\_\_ Unit: \_\_\_\_\_

Phone Number: \_\_\_\_\_ E-mail Address: \_\_\_\_\_

**Computer Policy Compliance**

I understand that I am responsible for complying with the NFIT's CNUSP, the NFISD Data Access Policy, the NFIT Computer & Network Security Procedures, my home unit's information technology procedure (if any), and appropriate federal and state laws when operating this computer.

System Owner's Signature: \_\_\_\_\_ Date:

\_\_\_\_\_  
Print Name: \_\_\_\_\_ Phone Number:

\_\_\_\_\_  
E-mail Address:  
\_\_\_\_\_