



---

## Data Security Policy

---

Original Adoption: January 2, 2018  
Effective Date: January 2, 2018  
Reviewed: January 12, 2018  
Last Revision: January 22, 2018

---

### INTRODUCTION

Today, information technology (IT) permeates all aspects of teaching, learning, research, outreach, and the business and facilities functions of the College. Safeguarding information and information systems is, therefore, essential to preserving Northwest Louisiana Technical College's ability to perform its missions and meet its responsibilities to students, faculty, staff, and the constituents whom it serves. Federal and State statutes, rules, and regulations, State Office of Information Technology policies and standards, Louisiana Board of Regents policies, Louisiana Community and Technical Colleges System (LCTCS) policies and other explicit agreements also mandate the security of information and information systems. Failure to protect the College's information technology assets could have financial, legal, and ethical ramifications.

### PURPOSE

The Northwest Louisiana Technical College (NWLTC) is committed to preserving the security, confidentiality, integrity and availability of all forms of information used and maintained on behalf of faculty, staff, and students consistent with Northwest Louisiana Technical College System's mission. Improper disclosure, modification, or destruction of information may result in harm to the operation of NWLTC in support of its mission. As a result, specific procedures will be developed to help administer and manage the storage, processing, and use of information.

### INFORMATION TECHNOLOGY TASKFORCE (ITT)

NWLTC currently does not have a stand-alone information technology department. Under the guidance of LCTCS Information Technology, several NWLTC leaders work together as a team to oversee the management, protection and distribution of its sensitive information and the framework for securing its technology resources. Along with the Director, the following positions serve on this taskforce: Campus Deans, Chief Academic & Student Affairs Officer, Chief Finance Officer, Chief Financial Aid Officer, Chief Human Resources Officer, Chief Institutional Research Officer, Registrar, and Computer Analyst / IT Technician.

## **TASKFORCE’S VIEW AND ENFORCEMENT OF SECURITY**

NWLTC acknowledges that no individual is immune from investigation when there are reasonable suspicions of theft, fraud, or misuse of its information technology resources.

In accordance with the [Louisiana Community and Technical College System \(LCTCS\) Use of Technology Resources Policy Statement and Northwest Louisiana Technical College Network and Computer Access Agreement](http://www.nwltc.edu/wp-content/uploads/2017/01/7.001-Northwest-LTC-Network-and-Cmputer-Access-Agreement.pdf), <http://www.nwltc.edu/wp-content/uploads/2017/01/7.001-Northwest-LTC-Network-and-Cmputer-Access-Agreement.pdf> use of NWLTC computer resources is limited to NWLTC faculty, staff, currently enrolled students, and authorized guests, for legitimate academic and business purposes consistent with the College's mission. Use of technology resources of this institution is a privilege and not a right. Abuse of these privileges may result in the loss of such privileges, possible employment termination, student expulsion, and/or prosecution.

The unauthorized use of another's logon id and password will be viewed as theft of a College resource and computer fraud. The result of such abuse may be the loss of all computer privileges and/or other disciplinary action.

## **POLICY STATEMENT**

It is the policy of NWLTC to protect personally identifiable information of employees and students. The electronic restrictions and safeguards outlined in this policy provide guidance for students and employees that have access to protect personally identifiable information retained by the College to ensure compliance with state and federal regulations such as:

- Family Education Rights to Privacy Act (FERPA) - federal law that protects the privacy of student education records.
- Health Insurance Portability and Accountability Act (HIPAA) - federal act that sets standards for protecting privacy of patients' health information.
- Gramm–Leach–Bliley Act (GLBA) - federal law that imposes restrictions on the disclosure of consumers' personal financial information.

### **Reason for Policy**

To ensure that anyone that collects or uses personally identifiable information at NWLTC does so in compliance with state and federal regulations and best practices for information security in higher education.

### **Entities Affected by this Policy Who should Read it**

This policy will affect students and employees that have been granted access to resources containing personally identifiable information.

## **Definitions**

A. Personally Identifiable Information - is any information pertaining to an individual that can be used to distinguish or trace a person's identity. Some information that is considered Personally Identifiable Information is available in public sources such as telephone books, public websites, College listings, etc. This type of information is considered to be Public Personally Identifiable Information and includes:

1. First and Last name
2. Address
3. Work telephone number
4. Work e-mail address
5. Home telephone number
6. General educational credentials
7. Photos and video

B. Protected Personally Identifiable Information - is defined as any one or more of types of information including, but not limited to:

1. Social security number
2. User name and password
3. Credit card number/Banking information
4. Driver's License number
5. Date and place of birth
6. Mothers maiden name
7. Criminal, medical, and financial records
8. Educational transcripts
9. Photos and video including any of the above

C. NWLTC Information System – a collection of computing resources that are accessible through privileged access such as a login or key. Usually a software package designed to store student and employee data. Examples: Banner, Canvas, Document Imaging, and Databases.

D. Secure Deletion – Secure deletion of an electronic file is accomplished by overwriting the full file contents with random data multiple times.

E. Breach of Data Security - means the compromise of the security, confidentiality, or integrity of computerized data or physical files containing data that result in the unauthorized acquisition of and access to personal information maintained by an agency or person. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of security of the system, provided the personal information is not used for, or is subject to, unauthorized disclosure.

## **SECURITY POLICY OBJECTIVES AND METHODS**

This policy attempts to outline security practices and how the College intends to manage, protect and distribute its sensitive information and the framework for securing its technology resources while participating in the world-wide cyber space community.

As a means of securing its technology resources, the College utilizes one or more of the following measures:

### **Authentication**

Traditionally, a *logon id* and *password* is used as assurance or verification that the resource (human or machine) at the other end of the session really is what it claims to be before being granted access to College resources. Authenticated users may have different types of permissions based on their authorization levels. As a means of authentication and control, a user may be required to provide proof of identification before being granted access to any College computer resource.

### **Authorization**

Most computer security systems are based on a two-step process with the first stage being authentication and the second stage being authorization. The authorization process allows a user access to various resources based on identity. It protects against unauthorized access to a system or to the information it contains by the types of permissions granted – Access Control.

### **Confidentiality**

Recognizing that confidentiality is critical to total data security, a number of tools are used to safeguard the confidentiality of NWLTC's information, integrity, and non-repudiation of data (proof to receiver that sender is the originator of the information) and to assure that sensitive information remains private and is not visible to an eavesdropper. This includes but is not limited to:

- Encryption ensures that classified information is not adversely affected;
- Virus Control helps protect against file corruption;
- Electronic Data Exchange by use of secure protocols, digital certificates and the Secure Socket Layer (SSL) to help ensure confidentiality and integrity when transmitting data across the network.

### **Audit**

Security-relevant events are monitored to provide logs of access attempt.

Audit service tools will be provided to audit personnel to generate reports to analyze and review information technology security.

### **Administration**

The management of technology resources protection scheme ensures that only authorized users can access objects on the system. This is handled by creation, maintenance, and monitoring security information such as access control policies, authorized user profiles, security parameters, and ownership identification.

## **NETWORK/CYBER SECURITY**

NWLTC utilizes a multi-layered approach as protection of its data and technology resources against unauthorized access from untrusted network environments, as well as, malicious attacks from untrusted cyberspace environments. These network security strategies include but are not limited to:

- Firewalls
- Intrusion prevention and detection
- Anti-virus
- Anti-spam
- Access control lists
- Network monitoring

In the event of a network/cyber security incident, the following approach is utilized in response and implemented:

### **Step 1 - PREPARATION**

The amount of preparation one does before an event occurs to successfully handle an incident.

### **Step 2 – DETECTION**

Determine whether or not an actual incident has occurred.

### **Step 3 – CONTAINMENT**

Limit the scope and magnitude of an incident in order to keep it from getting worse.

#### **Step 4 - ERADICATION**

To ensure that the problem and vulnerabilities that allow re-entry to the system are eliminated.

#### **Step 5 - RECOVERY**

Ensure that the system is returned to a fully operational status.

#### **Step 6 - FOLLOW-UP**

Meet, discuss, identify lessons learned and make recommendations that will prevent future incidents.

### **EMAIL**

In accordance with the NWLTC Network and Computer Access Agreement, <http://www.nwltc.edu/wp-content/uploads/2017/01/7.001-Northwest-LTC-Network-and-Computer-Access-Agreement.pdf>, NWLTC employees and students have access to electronic mail (E-Mail) both internally and through the Internet. This E-mail access is the property of the College and may be subject to auditing and monitoring.

- Use of NWLTC's E-mail system provides communication between staff, faculty, students, external entities, clients, and others.
- It is intended for business and academic use only.

#### **E-mail Privacy**

- Users should not have any expectation of privacy when using and storing information on any computer resource of the College.
- The College reserves the right to review and copy any data or other information stored on any computer resource without notice to the user. E-mail created or distributed through NWLTC's E-mail system is the property of NWLTC .
- Users should be aware that under certain circumstances, the Office of Information Technology staff may need to access and review E-mails sent and received.
- Users should remember that all E-mail sent or received through this system is the property of NWLTC , and is subject to audit and monitoring.
- There is no guarantee of security or confidentiality for inappropriate use of the E-mail system.

#### **E-mail Usage**

- E-mail should be transmitted based on business or academic need.
- Under no circumstance is it permissible for NWLTC employees to conduct business of any kind that would infringe on the beliefs of the College.

- Users should not use E-mail to transmit messages that contain remarks, images, or content that can be considered defamatory, offensive, harassing, disruptive, derogatory, racial or ethnic slurs or as pornographic comments or images.
- It is strongly recommended that E-mail is not used to transmit passwords or any other authentication information for NWLTC's systems.
- It is strongly recommended that confidential information is not sent in detail via the E-mail system when communicating with the Human Resource office (i.e., Password, SSN, DOB, Pin, etc.)
- It is prohibited that student grades or any sensitive material be transmitted in violation of FERPA guidelines.
- Users should never E-mail or otherwise transmit any attachment that is suspect of being a virus.
- Inappropriate use of the E-mail system may result in immediate loss of E-mail privileges and possible disciplinary action up to and including termination.
- Examples of inappropriate usage include, but are not limited to, sending electronic chain mail or mass unsolicited mail, and altering email or Internet headers to hide the identity of the sender/poster or to attribute the email or posting to someone other than the sender/poster or intended recipient.
- Only responsible administrators or their designees are authorized to send broadcast e-mail communications to all faculty and staff. These general office email accounts have been set up to allow certain academic and administrative departments to disseminate highly targeted communications throughout the NWLTC community. All NWLTC responsible administrators and designees will retain their individual e-mail accounts.
- The Responsible Administrator for each area must sign a *Network and Computer Access Agreement* form that states his/her responsibility. The user agreement authorization form is kept on file in the Office of Human Resources.
- Canvas Community users are expected to adhere to the same policies regarding sending broadcast email communications to all faculty and staff.
- Only specifically identified email accounts are authorized to send broadcast email communications to students
- Email accounts are provided to adjunct faculty when requested by the division for the time period as specified on the request.
- Only individuals authorized by their respective divisions are allowed to retrieve and distribute access letters to adjunct faculty.

## **INTERNET**

NWLTC provides Internet access for its employees so they can obtain up-to-date information that may be useful in performing their job responsibilities and duties.

## **Proper Internet Usage**

- No illegal or pirated information or software should be downloaded or viewed.
- Passwords for personal use should be of different variation from those used within NWLTC.
- NWLTC prohibits employees from using the Internet to visit sites that are pornographic, sexually explicit, racial or ethnically biased or harassing or offensive in any way, either graphic or in text form, other than authorized academic purposes.
- NWLTC reserves the right to monitor any and all network activities to and from your computer including Internet access. Such activities may be archived and monitored at a future date.
- Similarly, the unauthorized copying of commercial software packages for which the College is liable through licensing agreements or the introduction of any unauthorized software to a College computer is considered inappropriate and a violation of Internet usage and/or copyright laws and may be prosecuted.
- The NWLTC website on the Internet is an official publication of the College. All web pages linked to it are also official publications of the College. As such, the content of these pages should promote the College, its programs, faculty and staff in a positive light, consistent with its mission.
- The creation and maintenance of web pages by units within the College are encouraged as a means of promoting NWLTC, its programs, faculty, and staff.
- These pages require the Director and Public Relations Committee's before publication and must be administered according to the College's Internet Web Pages policy.
- Inappropriate Internet usage will result in the loss of Internet access and may result in further disciplinary action, up to and including termination.

## **WIRELESS ACCESS**

### **Wi-Fi Purpose**

- NWLTC is the host to a Wi-Fi network that is available to employees, students, and authorized guests.
- Employees and students use their NWLTC email account username to connect to the Wi-Fi network.
- Upon request, a special user account can be set up for doing business with the college for a specified time period.

### **Wi-Fi Usage**

- Wi-Fi coverage is campus-wide at all NWLTC locations.
- Access is available to connect to the Internet via devices such as laptops and mobile phones.
- Individual users must configure personal devices for wireless network connection.



## **END USER ACCOUNTS**

The College is linked to the Internet and to other networks either directly or indirectly. Access to these networks by faculty, staff, and students is granted because of employment or enrollment at the College.

NWLTC faculty and staff members may be granted access to the College's network and mainframe if deemed appropriate for their position or department. For detailed instructions on how to become a user of the College's network and/or mainframe systems, employees should refer to the College's Technology Services policy.

Since user account access is an integral part of security for the College's technology infrastructure, access is granted based on a number of general practices. The following guidelines have been established.

### **Account Creation**

- A request for account access is submitted electronically via the IT Help Desk system. When a request is submitted, it is electronically routed for approval to the employee's supervisor and data manager, if applicable.
- The employee's job function and department requirements will determine the level of access to system resources.
- At a very minimum, all accounts require both a username and a password.
- Sharing of end-user accounts between users is prohibited.
- When an account has been established, electronic notification will be sent to the requestor and the new employee's supervisor.

### **Account Logons and Passwords**

NWLTC faculty, staff and students may be issued logon ids that are used to access various information technology systems and resources provided by the College. This logon id will remain valid for the period the individual is associated with the College.

All users with logon ids and passwords to the College's technology resources should be aware of the following:

- The logon id owner is responsible for all actions and functions performed by his/her logon id.
- Passwords used in association with the logon ids are to be safeguarded and neither logon ids nor passwords are to be shared by any two individuals. (*with the exception of general office email accounts*)
- Logon ids or passwords may not be shared with another person other than a designated IT representative.
- Proper use of the logon id is the responsibility of the individual under whose name it has been assigned.

## **Password Selection and Management**

Potentially, serious damage can occur if a user's password is not safeguarded. Therefore, passwords should be changed regularly. Passwords are used to authenticate an end-user's identity and to establish accountability. A password that is easily guessed is not an effective password and compromises security and accountability of actions taken by the logon id, which represents the end-user's identity.

- All end-users with logon ids and passwords to the College's technology resources should practice the following:
- The recycle or re-use of passwords shall be reasonably limited.
- Users are advised to change the initial password on a new account immediately.
- Passwords should be selected that are difficult to guess by others.
- Mainframe passwords should be at least eight (8) characters in length, must be in lower case, and may consist of a combination of letters, characters, and numbers (alphanumeric).
- Network passwords should be at least eight (8) characters in length.
- Network password complexity must contain at least 3 of the following 4 categories: English upper case characters (A-Z), English lower case characters (a-z), Base 10 digits (0-9), and non-alphanumeric characters (e.g. %, &, !).
- It is strongly suggested that passwords should not include your logon id, your name, your spouse's name, children's or pet's name, or any other names commonly known to others.
- Users will be held accountable for password selection and protection.
- A user's password must not include anything derogatory, offensive, or defamatory.
- It is strongly suggested that passwords are not written down or stored in a place that can be accessed easily by others.
- All passwords shall be changed whenever it is determined that a system security may have been compromised.
- When requesting a password reset, individuals will be asked a security question(s) to verify the identity of the person requesting the action.
- Passwords are encrypted and will not display when typed.

Mainframe passwords should periodically be changed. However, it will automatically expire every 180 days; the system will prompt you when the time approaches. Note: The 180th day for each individual may be different.

Network passwords should periodically be changed.

Some general management rules to practice are: 1) do not leave your computer logged on and unattended for an extended period of time, 2) do not log on to your system if someone can see you keying in your password, 3) turn off your computer when you leave for the day, 4) if you use a remote access program and you need to leave your computer on, be sure that it is in a locked

room, and 5) use a screen-saver access program to secure the computer from unauthorized access.

### **Temporary or Contracted Employees**

All temporary and contractual employees with access to the network or mainframe should be aware of the following:

- Accounts are created for Temporary or Contracted employees using the same process as regular employees.
- All Temporary or Contracted employees must be set up with a temporary account containing an account expiration date, if applicable.
- Upon approval, the Office of Information Technology will provide a logon id and password for temporary access and application use.

### **Account Modification**

Current employees may request changes to their access by contacting Computer Analyst/IT Technician. The employee's supervisor must approve the request electronically. However, this does not automatically guarantee that the request will be granted, as it may require the approval of a data manager, if applicable.

### **Account Removal**

All employees with access to the network or mainframe should adhere to the following:

- When IT is notified of an employee's separation from the College, access to technology resources will be disabled. Access is not removed until confirmation of separation is received from the Human Resources office.
- Access to technology resources will be restricted by the close-of-business on the employee's last working day, unless otherwise instructed by Human Resources.
- In the event of immediate access suspension, an authorizing College administrator contacts the Office of Information Technology Assistant Vice Chancellor/CIO or the Executive Director. The Assistant Vice Chancellor/CIO or Executive Director notifies the appropriate security personnel so that the access to technology resources is immediately disabled.
- Retirees will not retain access to their email account upon separation from the college.
- Student email accounts are purged annually. Student email accounts are purged from the email database based on criteria provided by the College Registrar.

### **Remote Access**

- NWLTC adheres to the Louisiana Community and Technical College System's policy regarding remote access.

- Remote access users shall not violate any college policies, perform any illegal activities, and be used for outside business interests.
- Remote access privileges will be strictly limited and evaluated on a case by case basis.

## **PRIVACY OF STUDENTS**

The Family Educational Rights and Privacy Act (FERPA) protect educational records of a student from public disclosure without written permission of the student. NWLTC adheres to these rules and guidelines to protect the rights of its student body. The College's computing information and network resources are used in a manner that complies with this privacy.

## **CONFIDENTIALITY**

All computer information is considered confidential unless a user has received permission to use it. Accessing or attempting to access confidential data is strictly prohibited. Confidential information should only be used for its intended purpose. Using confidential information for anything other than its intended use, without prior approval, is prohibited.

NWLTC strives to maximize the confidentiality and security of its information systems and services within the limitations of available resources. As with paper-based systems, no technology can be guaranteed to be 100% secure. All users should be aware of this fact and should not have an expectation of total privacy regarding information that is created, stored, sent, or received on any networked system. The College reserves the right to review and copy any data or other information stored on any computer resource without notice to the user. This also includes the monitoring of all Internet use, email, and other activities accessed on or through computer resources of the College. Such monitoring, without limitation, may include, but is not limited to, review of all sites accessed by a user and e-mails transmitted and/or received.

The Internet environment offers tremendous opportunities to provide convenient access to information and services to authorized individuals wherever they may be. Users who serve as data managers of institutional information should be particularly aware of the potential for unauthorized access to or tampering with online information and services in the Internet environment.

## **DATA SECURITY & BACKUPS**

Data of value (data that would be missed if lost and cannot be easily recreated as from an OS installation) must be backed up on a regular basis. The Computer Analyst/IT Technician must ensure that a means of backing up and restoring vital data is provided; in keeping with this responsibility, a backup strategy for the College's network and mainframe systems is conducted on a daily basis.

## **Networking**

The entire backup process is hosted by NWLTC. *DataVault* Agents are installed on each server/workstation requiring backup. Each agent is configured to transmit and store the backed-up data at the secure data vault located at NWLTC.

The backup process is completely automated requiring minimal intervention from the Computer Analyst/IT Technician. The backup process consists of two strategies, which are the “incremental” and “full” backup strategy. The incremental backup runs daily and full backup runs on Saturday evenings.

## **Mainframe**

- Daily backups of the College’s mainframe computing system are performed to ensure availability and integrity of data. The backup process consists of basically two strategies, “incremental” and “full” backups.
- Each day incremental backups are taken of all DASD datasets to which modifications have been made since the last backup taken.
- Periodically, full volume backups are made of each disk pack. These full volume backups occur automatically as a new generation of backups.
- In addition to the generation that is currently being built, four complete generations are available from which restorations may be done.
- Two copies of each backup/archive are made. One copy is vaulted offsite for disaster recovery purposes and the other copy remains onsite for system restoration, if needed.
- A Tape Management System (TMS) vaulting procedure is used to automate the vaulting rotations.

## **DATA SECURITY – AUDITING AND MONITORING**

The Office of Information Technology is responsible for the monitoring and periodic audits of the College’s technology resources including, but not limited to, technology systems, software development, and operating systems. To facilitate this effort, a number of tools are used, such as:

- **Audit Logs** – logs are maintained that can provide sufficient data to reconstruct events and actions, such as dates, times, individual and/or process authorizing an activity/operation.
- **Archives** – information is archived to ensure that important assets are maintained in a reliable long-term retrieval state for specified periods that may be utilized for special needs (i.e. – legislation, statutes, government, etc.).
- **Monitoring Products** – a number of monitoring utilities are used to monitor the College’s network infrastructure. These tools allow for the monitoring of Internet connectivity, servers, routers, switches, ports and the like.
- **Audit Files** – are available through the College’s administrative applications that allow for audit tracking of data elements in the databases. Reports can be generated indicating

the before and after values of the data element. Event logs on the network automatically record network activity and ‘flag’ possible suspicious activity or concerns.

### **DATA SECURITY – ENCRYPTION**

As stated in the State of Louisiana IT Policy #IT-POL-014, sensitive data, defined as data not subject to the Louisiana Public Records Act (L.R.S. 44:1 et seq), is to be encrypted on all approved portable storage devices. The state’s preferred encryption freeware is “TrueCrypt,” which is available to download and view tutorials at <http://www.truecrypt.org>.

### **DATA SECURITY – RETENTION AND COMPLIANCE**

It is recommended that data/files are maintained for a period of five (5) academic/calendar years.

### **TECHNOLOGY SECURITY VIOLATIONS**

Reporting incidents is an ethical responsibility of all members of the NWLTC community. A critical component of security is to address security breaches promptly and with the appropriate level of action. Below are guidelines for reporting and handling security incidents:

All users of NWLTC technology resources computers have the affirmative obligation to report, directly and without undue delay, any and all information concerning conduct that they know to involve corrupt or other criminal activity or conflict of interest to the College.

Activities that should immediately be reported include, but are not limited to:

- Attempts to circumvent established computer security systems;
- Use, or suspected use, of virus, Trojan Horse, or hacker programs;
- Obtaining, or trying to obtain, another user’s password;
- Using the computer to create and/or disseminate harassing or defamatory messages;
- Using the computer to communicate inappropriate messages or jokes that may be considered offensive by others;
- Illegal activities of any kind;
- Attempts to breach facility security should be reported to Campus Dean;
- Incidents of security violations, willful or intentional, of secured resources are considered to be misconduct under applicable student and employee conduct standards. Users engaged in such conduct may be denied access to technology resources and may be subject to other penalties and disciplinary actions including termination or expulsion.

Under appropriate circumstances, NWLTC may refer suspected security incidents to law enforcement authorities, and provide access to necessary data for investigation as permitted by law.

Technology security violations can be reported in two ways:

- 1) Send email to [ronaldriley@nwltc.edu](mailto:ronaldriley@nwltc.edu)

2) Call IT Help Desk (318-371-3035 ext 1155)

## **Procedures**

### A. Maintaining and discarding Personally Identifiable Information.

All electronic files that contain Protected Personally Identifiable Information will reside within a protected NWLTC information system. All physical files that contain Protected Personally Identifiable Information will reside within a locked file cabinet or room when not being actively viewed or modified. Protected Personally Identifiable Information is not to be downloaded to personally owned, employee workstations or mobile devices (such as laptops, personal digital assistants, mobile phones, tablets or removable media) or to systems outside the protection of the college. Personally Identifiable Information will also not be sent through any form of insecure electronic communication such as e-mail or instant messaging systems. Significant security risks emerge when Personally Identifiable Information is transferred from a secure location to a less secure location or is disposed of improperly. When disposing of Personally Identifiable Information the physical or electronic file should be shredded or securely deleted. For help with secure deletion please contact the Campus Dean.

### B. Exceptions

If there is an operational or business need to store protected Personally Identifiable Information outside a NWLTC controlled information system please contact the Campus Dean or Director for assistance in securing the information.

## **Containment, Classification, and Reporting**

The first priority after a breach of data security is discovered is to contain the breach and notify supervisory personnel as quickly as possible. The data must be secured and the reasonable integrity, security, and confidentiality of the data or data system must be restored. After consulting with the Director, a member of the NWLTC IT Taskforce must also inform the USDOE of the breach within an hour of the breach discovery (on the same day of discovery):

1. Email [cpssaig@ed.gov](mailto:cpssaig@ed.gov) & copy NWLTC IT Taskforce Team
2. **Data to include in the email:**
  - i. Date of breach (suspected or known)
  - ii. Impact of breach (# of records, etc.)
  - iii. Method of breach (hack, accidental disclosure, etc.)
  - iv. Information Security Program Point of Contact - email and phone details
  - v. Remediation Status (complete, in process – with detail) & Next steps (as needed)
3. Call Education Security Operations Center (ED SOC) at 202-245-6550 with above data. ED-SOC operates 7x24.

4. Call or Email Tiina Rodrigue – [tiina.rodrigue@ed.gov](mailto:tiina.rodrigue@ed.gov) or 202-377-3887 – if both previous methods fail.

The exact nature of the breach of data security in terms of its extent and seriousness must be determined. The supervisor of the department where the breach occurred must take immediate action to determine the extent of the breach and to contain it or recover the missing data. Assistance from the IT Department or other personnel should be requested as soon as possible if necessary. The department supervisor should document the breach, the scope of the breach, steps taken to contain the breach, names and categories of the persons whose personal information was, or may have been, accessed or acquired by an unauthorized person.

### **Enforcement**

An employee found to be in violation of this policy may be subject to disciplinary action as deemed appropriate based on the facts and circumstances giving rise to the violation.

### **Retirees & Emeritus Retirees**

NWLTC Retirees shall not have active email accounts through NWLTC unless the retiree is designated an 'emeritus retiree' by vote and approval of the LCTCS Board of Supervisors. Emeritus retirees may be provided an active NWLTC email for life.

### **Policy Effective Date**

January 2, 2018

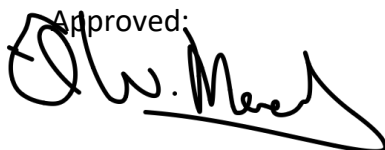
### **Review Date**

January 12, 2018

### **Revision Date**

January 22, 2018

Approved:



---

Earl W. Meador, JD  
Director