

# LENOIR-RHYNE UNIVERSITY

## Policy and Procedure

Title: Data Handling and Storage Policy

Division/Department: University Wide

### Purpose

To establish a policy for the protection of sensitive data that is created, received, maintained or transmitted by faculty, staff or students of Lenoir Rhyne University. This policy is intended to ensure that the information is uniformly used and disclosed in accordance with all university policies and applicable state and federal laws.

### Policy

Institutional data is information that supports the mission of Lenoir Rhyne University. Institutional data is considered a vital asset and is owned by the University. Due to the essential nature of institutional data, its quality and security must be ensured to comply with legal, regulatory, and administrative requirements. Authorization to access institutional data varies according to its sensitivity. This policy sets forth the university's standards with regard to the handling and storing institutional data.

### Procedure

#### DEFINITIONS:

**Archival/Storage:** The act of physically or electronically moving inactive or other records to a storage location until the record retention requirements are met or until the records are needed again.

**Institutional Data:** Information that supports the mission of Lenoir Rhyne University.

**Personally Identifiable Information (PII) or Sensitive Data:** Data requiring the highest level of protection including, but not limited to, data protected by law, data protected by legal contracts, or security related data. It also includes data that is not open to public examination because it contains information which, if disclosed, could cause severe reputation, monetary or legal damage to individuals or the college or compromise public activities. Examples include: passwords, intellectual property, ongoing legal investigations, medical or grades information protected by FERPA or HIPAA, social security numbers, people code ID's, birth dates, professional research, graduate student work, bank or credit card account numbers, income and credit history.

**Restricted Data:** Data whose access is restricted by federal or state statute (i.e. HIPAA, FERPA). For purposes of this policy, restricted data is a subset of PII data.

# LENOIR-RHYNE UNIVERSITY

## Policy and Procedure

### ARCHIVAL/STORAGE PROCEDURES:

Enterprise Resource Programs (ERP): The system(s) that maintain enterprise-wide institutional data that is considered PII and requires the greatest security. At all times, personnel should use internal identifiers in lieu of social security numbers. These systems include but are not limited to: PowerCAMPUS, PowerFAIDS, and Dynamics.

The ERP is backed up nightly to a back-up server that is also backed up nightly. The data is being backed up but not the entire database structure. OIT will be able to restore the data after the replacement and build of a new database server.

Electronic Mail (E-Mail): The E-mail system is a delivery system for electronic communication and is treated as Institutional Information.

E-Mail is backed up nightly and moved to a Storage Area Network that is backed up weekly to a server in a secondary data center. The mailbox stores are being backed up but not the entire Exchange environment. OIT will be able to restore the data after the replacement and building of a new Exchange server.

File Servers: The servers used to store all non-ERP related information that is vital to the mission of the University.

The File Server is backed up nightly to a server in a secondary data center.

Learning Asset Management Project (LAMP) – The portal that functions as the university's learning management system.

LAMP is hosted by the Appalachian College Association, a consortium of 36 small, private liberal arts colleges and universities in the Southern Appalachian Mountains across five states (Kentucky, Tennessee, North Carolina, Virginia, and West Virginia).

LAMP is hosted off-site; therefore, no back-ups are maintained by Lenoir Rhyne University.

### ACCESS CONTROLS:

- Only authorized users may access, or attempt to access, sensitive information.
- Authorization for access to sensitive data comes from the appropriate Vice President or department head, and is made in conjunction with an authorization form which is found on the login screen to PowerCAMPUS.
- Where access to sensitive data has been authorized, use of such data shall be limited to the purpose required to perform university business.

# LENOIR-RHYNE UNIVERSITY

## Policy and Procedure

- Users will respect the confidentiality and privacy of individuals whose records they access, observe ethical restrictions that apply to the information they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information.
- Notification of a user's termination or removal of authorized access to electronic sensitive information must be conveyed immediately to the Office of Information Technology (OIT). The Office of Public Safety must be notified to remove physical access to offices containing sensitive information.

### DATA TRANSFER OF PII:

- PII should not be transmitted through electronic messaging even to other authorized users unless security methods, such as encryption, are employed.
- PII must not be transferred by any method to persons who are not authorized to access that information. Users must ensure that adequate security measures are in place at each destination when sensitive data is transferred from one location to another.
- PII must not be taken off campus unless the user is authorized to do so, and only if encryption or other approved security precautions have been applied to protect that information.
- PII must not be stored on any mobile device such as a PDA, flash drive, thumb drive or laptop.
- Physical protection from theft, loss, or damage must be utilized for mobile devices that can be easily moved such as a PDA, flash drive, thumb drive or laptop.

### DATA STORAGE OF PII:

- Physical protection must be employed for all devices storing PII. This shall include physical controls that limit physical access and viewing, if open to public view. When not directly in use, office, lab, and suite doors must be locked and any easily transportable devices should be secured in locked cabinets or drawers.
- Users of laptop and other mobile computing devices need to be particularly vigilant and take appropriate steps to ensure the physical security of mobile devices at all times, but particularly when traveling or working away from the University.
- It is strongly recommended that institutional data not be stored on PCs or other systems in offices or laboratories. Institutional data (including word documents, spreadsheets and Access databases) that is created on a PC or similar system should be stored on a networked server managed by OIT.
- Individual desktop machines are not being backed up by OIT.

### DATA RETENTION AND DISPOSAL:

This will be the responsibility of each Vice President, Department Head or designee to determine for each department, school or college at Lenoir Rhyne University.

# LENOIR-RHYNE UNIVERSITY

## Policy and Procedure

### COMPLIANCE:

Compliance with this data protection policy is the responsibility of all members of the Lenoir Rhyne University community. Violations of this policy are dealt with seriously and include sanctions up to and including termination of employment. Users suspected of violating these policies may be temporarily denied access to LR's information technology resources during investigation of an alleged abuse. Violations can also be subject to prosecution by state and federal authorities.

### Author of Policy:

Chief Information Officer

### Individuals Affected:

All employees of the university

### Reviewed By/Concurrence From

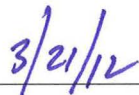
Chief Information Officer  
VP for Finance and Administration

### Approval



---

Chief Information Officer



---

Approval Date

Developed On: 01/08/2010

Revised On: 3/15/2010

3/24/2010

3/21/2012

Note: Please review the policies available online at <http://policies.lr.edu/> to confirm that this is the most recent version of the policy.