Lake Region State College
Policy and Procedure Manual

SECTION 1500.04
CUSTOMER INFORMATION SAFEGUARDING PROGRAM

Purpose:
The Gramm-Leach-Bliley (GLB) Act of 2000 requires financial institutions to ensure the security and confidentiality of customer information. Universities and colleges are deemed to comply with the privacy provision of the Act if they are in compliance with Family Educational Rights and Privacy Act (FERPA) of 1974; however, universities and colleges are still subject to the requirements of administrative, technical and physical safeguarding of customer information. The written safeguarding program outlined below will address the administrative, technical and physical safeguarding of customer information. The objectives of the safeguards are as follows:

1. Ensure the security and confidentiality of customer information,
2. Protect against any anticipated threats or hazards to the security or integrity of such information, and
3. Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.

Scope:
This program applies to all members of the Lake Region State College community.

Related Documents/Policies:

Gramm Leach Bliley Act	http://www.ftc.gov/privacy/privacyinitiatives/glbact.html
Payment Card Industry Standards	https://www.pcisecuritystandards.org/tech/index.htm http://www.discovernetwork.com/resources/data/data_security.html www.visa.com/cisp
PCI (Payment Card Industry) Compliance Policy	Lake Region State College Policy & Procedure Manual
Information Security Response Policy	Lake Region State College Policy & Procedure Manual
Identity Theft Prevention Program (Red Flag)	Lake Region State College Policy & Procedure Manual
North Dakota University System Policy Section 1912: Public Records and	https://ndusbpos.sharepoint.com/:w:/s/NDUSPoliciesandProcedures/EeJcbOWn6K5KvYtMb3PdXNABMoPSC-Eiwt20sObOZkvhTQ
NDUS Procedure Section 1912.1: Information Security Procedures.	https://ndusbpos.sharepoint.com/:w:/s/NDUSPoliciesandProcedures/EV6QWSLvSxBCh1ZnfgfzSeIBfT4epx_CdnmV5-If8YSQqQ

Family Education Rights and Privacy Act (FERPA)	http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Definitions:

Customer Information	any record containing nonpublic personal information as defined in 16 CFR 313.3(n) about a customer of Lake Region State College, whether in paper, electronic or other form (16 CFR 314.2(b)).
Confidential Information	Confidential Information, further defined in the NDUS policy 1901.2, is information that is not to be publicly disclosed. The disclosure, use, or destruction of Confidential Information can have adverse affects on Lake Region State College and possibly carry significant civil, fiscal, or criminal liability.
Covered data and information	Student financial information and any other financial information required to be protected under GLB and includes both paper and electronic records.
Customer	Individual who obtains or has obtained a financial product or service from Lake Region State College that is to be used primarily for personal, family, or household purposes (16 CFR 313.3(e),(h)).
North Dakota Higher Education Computer Network (HECN)	The HECN is a cooperative effort among the eleven campuses of the North Dakota University System for the provisioning of enterprise-wide IT services

Responsibility for Lake Region State College's Customer Information Safeguarding Program is assigned to the Information Security Response Team (the Coordinators for the Customer Information Safeguarding Program) See Information Security Response Policy re: Team members. The Team consists of the Accounting Supervisor, Chief Information Officer, Director of Financial Aid, and Director of Marketing & Communications.

Risk Management:
Lake Region State College recognizes that there are both internal and external risks at three different levels: 1) ND Higher Education Computer Network (HECN), 2)Lake Region State College Information Technology Services (ITS) department, 3) other Lake Region State College department systems. These risks include but are not limited to:

1. Unauthorized access of protected information by someone other than the owner of the covered data and information
2. Compromised system security as a result of system access by an unauthorized person
3. Interception of data during transmission
4. Loss of data integrity
5. Physical loss of data in a disaster
6. Errors introduced into the system
7. Corruption of data or systems
8. Unauthorized access of covered data and information by employees

9. Unauthorized requests for covered data and information
10. Unauthorized access through hardcopy files or reports
11. Unauthorized transfer of covered data and information through third parties.

Lake Region State College recognizes that this may not be a complete list of the risks associated with the protection of customer information. Since technology growth is not static, new risks are created regularly.

Responsibilities:

Information Security Response Team	• Review & update this Customer Information Safeguarding Program regularly.
	• Work together and be responsible for coordinating LAKE REGION STATE COLLEGE's information security program, including the following:
	  ○ Identify reasonably foreseeable internal/external risks to the security that could result in unauthorized disclosure, misuse of information;
	  ○ Design and implementation of the safeguard program;
	• Regularly monitor and test the sufficiency of any safeguards in place to control risks in the following areas:
	  ○ Employee Management & Training;
	  ○ Information Systems; and
	  ○ Managing System Failures.

North Dakota Higher Education Computer Network (HECN)	• Obligations are addressed in SBHE Policy Section 1912: Public Records and NDUS Procedure Section 1912.1: Information Security Procedures.

Lake Region State College Information Technology Services (ITS) department systems	• Provide a secure computing environment for the faculty, staff and students of Lake Region State College, this includes but not limited to network infrastructure; file servers, and email systems.
	  • Access to the networking equipment is controlled by passwords. Physical access to the networking equipment is controlled by physical key, with only those people needing to maintain the infrastructure itself having access.
	  • The storage area on the file server consists of individual and shared directories. The individual storage is password protected for the specific individual account. Access to the administrative file server and shared areas for the department are authorized by the department and implemented by the system administrator.
	  • Access to covered data and information via computer information systems shall be limited to those employees who have a business reason to know such information. Each employee shall be assigned a user name and password in compliance with a password procedure. Databases containing personal covered data and information, including, but not limited to, accounts, balances, and transactional information, shall be available only to employees in appropriate departments and positions.
	  • Lake Region State College requires the deletion or change of

	administrative system access for terminating or transferring employees. • Provide secure data transmission. • When disposing of electronic devices -- wipe the data or physically destroy diskettes, tapes, hard drives etc • No passwords are maintained in plain text. No passwords are altered for an individual or given to an individual until it has been determined that that individual is the person entitled to access to the account.
Lake Region State College administrative departments and employees that have access to confidential customer information.	Management and control responsibilities for Lake Region State College departmental information systems and employees rest with the department heads and the chain of command shown in the Lake Region State College organizational chart. Management and control responsibilities fall under three general categories: A) Employee Management and Training, B) Information Systems, and C) Managing System Failures. A) Employee Management and Training The success or failure of any security plan largely depends on its employees. Because certain customer information (such as: social security numbers) is available to a large number of Lake Region State College employees via the administrative systems, risk of failure is slightly higher in this area. As a result of this risk, the following steps will be taken: • All departments shall check references and conduct criminal history background checks as required by law or SBHE or Lake Region State College policy prior to hiring employees. • Every employee with administrative computer system access to name and address information will be notified and reminded of Lake Region State College Information Security policies and the need to keep customer information confidential and properly safeguarded. • Employees will be reminded to take steps to maintain security & confidentiality of customer information, such as: -locking rooms and filing cabinets where records are stored -recognizing any fraudulent attempts to obtain customer information -limiting access to data in software programs • Impose sanctions for any breaches B) Information Systems Information systems include network and software, information processing, storage, transmission, retrieval and disposal. Department heads will notify employees annually of the following standards for information system security: • Store records in a secure area and only authorized employees have access • Store paper records in a room or file cabinet that is locked when unattended. • Store electronic customer information on a secure server, data is accessed with passwords and the server is in a secure area.

	• Dispose of customer information in secure manner. Shred customer information according to the retention periods. • Covered data and information such as customer information must be encrypted during transmission. Confidential data must be encrypted, whenever it is stored outside of a password protected centralized server. Confidential data may not be stored or backed up to DVD, CD, or other non-encrypted media. • No passwords are maintained in plain text. • All computers, DVD/CDs, diskettes, tapes, hard drives etc. should be returned to the ITS department for proper disposal. C) Managing System Failures An effective security management includes the prevention, detection and response to attacks, intrusions and system failures. Department heads will notify employees of the following Lake Region State College standards for managing system failures: • Takes steps to preserve security, confidentiality and integrity of customer information. • Store customer information on servers which backup the data regularly. Notify customer promptly if nonpublic information (NPI) is subject to loss, damage or unauthorized access. • Maintain systems and procedures to ensure that access is limited to authorized employees. • Notify ITS of a breach and move items around for priority.
Employees contracting with Service Providers	Follow PCI (Payment Card Industry) Policy

History
Administrative Council Approved 04/14/09