SECTION 1500.01
INFORMATION SECURITY

Purpose:
Many departments and offices maintain files, both electronic and paper, of personal, biographical, academic, health, financial and admission records. These records may include personal billing information, Perkins loan records, student institutional loans and personal correspondence with employees, students and parents. The Information Security policy outlines how Lake Region State College will respond to an incident covered by the campus's policies to ensure compliance with Gramm-Leach-Bliley ACT (GLB), Family Education Rights and Privacy Act (FERPA), Payment Card Industry security standards (PCI), Identity Theft Prevention program (Red Flag). System and application security, and internal control procedures provide an environment where risks are mitigated.

Events that jeopardize the security and privacy of institutional and personal data will occur, in spite of the most vigilant efforts to minimize their occurrence. The Information Security Response Team responds to and investigates major incidents related to misuse or abuse of Lake Region State College information and information technology resources, regardless of the campus or department involved. This includes computer and network security breaches and unauthorized disclosure or modification of institutional or personal information. The role of the Information Security Response team is to coordinate a consistent and effective response to such events. Each member of the campus community should be watchful and prepared to report incidents.

The campus network, information systems, and data are critical resources for accomplishing the mission of Lake Region State College. All campus users have an interest in the security of these resources, and share in the responsibility for protecting them. Prompt and consistent reporting of and response to Information Security incidents protects and preserves the integrity, availability, and privacy of data and IT resources and helps the campus to comply with applicable law.

Scope of Policy:
This policy applies to all members of the Lake Region State College community.
The Information Security Response Team will be comprised of:

Department	Position
Administrative Affairs	Accounting Supervisor
Information Technology Services	Chief Information Officer
Student Affairs	Director of Financial Aid
Public Relations	Director of Marketing and Communications

Related Documents/Policies:

Gramm Leach Bliley Act	http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

Lake Region State College Customer Information Safeguarding Program (Gramm Leach Bliley Act)	Lake Region State College Policy & Procedure Manual
Payment Card Industry Standards	https://www.pcisecuritystandards.org/tech/index.htm
Lake Region State College PCI (Payment Card Industry) Compliance Policy	Lake Region State College Policy & Procedure Manual
Lake Region State College Identity Theft Prevention Program (Red Flag)	Lake Region State College Policy & Procedure Manual
Family Education Rights and Privacy Act (FERPA)	http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
"What To Do If Compromised" VISA USA Fraud Investigations and Incident Management Procedures	https://usa.visa.com/legal/privacy-policy.html.html
SBHE Policy 1901.2 Computing Facilities	https://ndusbpos.sharepoint.com/:w:/s/NDUSPoliciesandProcedures/EcNDwdojgP9Gm9dkA8uwgPIBX78yZqhKzSZV0e0lHK4l8g
NDUS Procedure 1901.2	https://ndusbpos.sharepoint.com/:w:/s/NDUSPoliciesandProcedures/EbKGBu_mHxhOiSGyOaBmBZcBGi-W2Xs4cOIG4D-GRWETYQ

Definitions:

Confidential Information	Confidential Information, further defined in the SBHE policy 1901.2 and NDUS Procedure 1901.2, is information that is not to be publicly disclosed. The disclosure, use, or destruction of Confidential Information can have adverse effects on Lake Region State College and possibly carry significant civil, fiscal or criminal liability.
Personal Identifying Information (PII)	Information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.
Campus Information Technology Security Officer	Individual designated by the Institution to fill this role.
Data Custodian	The individual who has ultimate responsibility and ownership for a particular set of data (e.g. a department head, V.P., or President)
Merchant Bank	The Merchant Bank for Lake Region State College is the Bank of North Dakota

Forensic Image	The process of making a duplicate of the computer system hard drive(s) using some form of hardware write protection, such as a hardware write blocker, to ensure no alterations are made to the original drive. There are two goals when making an image: 1. Completeness (imaging all of the information) 2. Accuracy (copying it all correctly)
Information Technology (IT) Incident	An activity or event that results in damage to, misuse of, or loss of an IT resource. Incidents include but are not limited to: • Loss of a computing device (misplaced, stolen, vandalized) • Detection of a malicious program, such as a virus, worm, Trojan horse, keystroke logger, rootkit, remote control bot, etc. • Detection of unauthorized users, or users with unauthorized escalated privileges. • Detection of a critical or widespread vulnerability or misconfiguration that might lead to a compromise affecting the confidentiality, integrity, or availability of university systems or data.
Major Incident	An IT incident which: • Involves a device or system containing confidential data • Threatens the business continuity of the college or department • Affects multiple systems or servers • Involves the violation of North Dakota state or U.S. federal law
Information Technology (IT) Resource	A computing asset provided by the College to further ITS' mission. Examples include, but are not limited to, network bandwidth, networking equipment, workstations, computer systems, SmartBoards, IVN equipment, data, databases, servers and printers.

Principles:
In the event of an Information Security incident concerning the possible exposure or loss of confidential institutional or personal data, you must take immediate action to report the incident to the Information Security Response Team as soon as the incident is suspected.

Procedures:

1. Reporting incidents involving confidential data (as soon as the incident is suspected)
    a. Immediately call, no matter what time of the day or night or weekday or weekend or holiday, until you get a human. Try in this order:
        i. Security Officer 701-662-1511
        Or 701-351-8547 (24x7)
        Or 701-662-8025 (after hours)
        ii. Information Security Response team at 701-662-1502 (during office hours)
        Or 701-351-3633 (after hours)

b. Please also e-mail lrsc.helpdesk@lrsc.edu with details of the suspected exposure. Please do not simply leave a voicemail or send e-mail - please ensure you reach a human, because it is critical that we begin response procedures immediately.

2. Safeguarding the compromised computer (if a computer is part of the incident):
    a. Step away from the computer.
    b. Do not touch it, or take any other action until advised by the Campus Information Technology Security Officer.
    c. Do not attempt to login, or alter the compromised system.
    d. Do not power it off. These actions will delete forensic evidence that may be critical to your incident.
    e. Do not discuss the incident with any other parties until you are authorized. This is critical to ensure that only accurate information is disseminated, rather than suppositions or guesses as to what happened.
    f. Begin writing a detailed description to be shared with the Information Security Response Team: what made you suspect the incident, what you know happened thus far, information on the machine and the data affected and what actions have been taken so far.

The information Security Response Team is charged with investigation and coordination of incidents where confidential institutional or personal data is suspected to have been exposed, and it has experienced forensic NDUS staff to assist.

When a Campus Information Technology Security Officer is notified, the Information Security Response Team will immediately be assembled to advise and assist in containing and limiting the exposure, investigating the attack, obtaining the appropriate approvals, and handling notification to the affected individuals and agencies. The incident still "belongs" to the department experiencing the exposure; the mission of the Information Security Response Team is to assist you.

Time is critical

Immediately containing and limiting the exposure is first priority. In certain situations, we must notify the NDUS Security Officer within two business days of becoming aware of the incident. In others, we must notify the Merchant Bank involved within one business day. Also, individuals involved in such incidents expect expeditious notification to them so that they can monitor their accounts. The most common complaints after an incident are about how long it took the organization to contain the exposure and to send notifications. At Lake Region State College, our goal is to notify the individuals affected within one week of our becoming aware of the possible exposure.

3. Reporting other types of suspected incidents
    a. For non-emergency reports of information and information technology security or abuse incidents, send email to lrsc.helpdesk@lrsc.edu or contact the ITS Department. If you are reporting an incident related to an email message you received do not delete the original email. It will be needed for the investigation.

Responsibilities:

All Employees	• Classify information; any data not yet classified by the custodian shall be deemed Private. • Report any IT or information security incidents to the Campus

	Information Technology Security Officer(s). • Follow the procedures for safeguarding a compromised computer involving confidential information .
Data Custodian/Department	• Work with the employee(s) to identify the scope of the incident, including users affected and the type of data compromised. • Notification to the affected individuals in case of a major incident with guidance from the Information Security Response Team. • Identify reasonably foreseeable internal/external risks to the security that could result in unauthorized disclosure or misuse of information. • Take the lead in minimizing the risks with assistance from the Information Security Response team.
Information Security Response Team	• In the case of major incidents, advise and assist in containing and limiting the exposure, investigating the attack, identifying the users involved, obtaining the appropriate approvals, and overseeing notification to the affected individuals and agencies which may include, but are not limited to, the Data Custodian, President, NDUS Security Officer and the Bank of North Dakota. • Work with Data Custodian/Department to minimize risks. • Design and implementation of the Information Security Education and Training program. • Regularly monitoring and testing the sufficiency of any safeguards in place to control risks in the following areas: ○ Employee management and training ○ Information systems ○ Managing system failures
Campus Information Technology Security Officer	• Determine if the incident is a major or minor incident. • In the case of a minor incident, work with ITS to contain the treat and restore the system. • In case of a major incident work with the Information Security Response Team.

History
Administrative Council Approved 05/09
Administrative Council Approved 07/14/09
Administrative Council Approved 06/11/15