Lakeland Community College

PROCEDURE TITLE:	WRITTEN INFORMATION SECURITY PROCEDURE
PROCEDURE NO:	ITS25-06
ORIGINALLY APPROVED DATE:	07/15/25
REVISED DATE:	ANNUALLY
EFFECTIVE DATE:	07/15/25
NEXT REVIEW DATE:	ANNUALLY
RELATED POLICY:	3354-2-11-03, INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY 3354-2-11-04, DATA SECURITY AND PRIVACY ASSURANCE 3354-2-11-05, IDENTITY THEFT PREVENTION
RELATED PROCEDURES:	ITS25-05 COMPUTER & COMMUNICATION HARDWARE/SOFTWARE
RELATED DEPARTMENTAL GUIDELINES:	ADMINISTRATIVE TECHNOLOGIES > GUIDELINES > ADMINTECH GENERAL EXPECTATIONS AND PROCEDURES CURRENT.DOCX ADMINISTRATIVE TECHNOLOGIES > GUIDELINES > LIFECYCLE REPLACEMENT GUIDELINE.DOCX ADMINISTRATIVE TECHNOLOGIES > GUIDELINES > NETWORKING OPERATIONS STANDARDS AND PRACTICES CURRENT.DOCX ADMINISTRATIVE TECHNOLOGIES > INCIDENT RESPONSE > EMERGENCY PREPAREDNESS > EMERGENCY PREPAREDNESS PLAN CURRENT.DOCX
RESPONSIBLE OFFICE(S):	ADMINISTRATIVE TECHNOLOGIES/DATA SECURITY AND PRIVACY ASSURANCE COMMITTEE
APPROVED BY:	PRESIDENT'S CABINET

A. OBJECTIVES:

The objectives of this Written Information Security Procedure ("WISP") include defining, documenting, and supporting the implementation and maintenance of the administrative, technical, and physical safeguards Lakeland Community College has selected to protect the personal information it collects, creates, uses, and maintains. This WISP has been developed in accordance with the requirements of the Gramm-Leach-Bliley Act Safeguards Rule, Health Insurance Portability (HIPAA) and Accountability Act, Family Educational Rights and Privacy Act (FERPA) and considers addressing the requirements of other state's Data Security Regulations.

In the event of a conflict between this WISP and any legal obligation or other Lakeland Community College policy or procedure, the provisions of this WISP shall govern, unless

the Chief Information Officer or Security Engineer in coordination with the Data Security and Privacy Assurance Committee specifically reviews, approves, and documents an exception.

B. PURPOSE

The purpose of this WISP is to:

1. Ensure the confidentiality, integrity, and availability of personal [and other sensitive] information Lakeland Community College collects, creates, uses, and maintains.
2. Protect against any anticipated threats or hazards to the security, confidentiality, integrity, or availability of such information.
3. Protect against unauthorized access to or use of Lakeland Community College - maintained personal [and other sensitive] information that could result in substantial harm or inconvenience to any customer or employee.
4. Define an information security program that is appropriate to Lakeland Community College's size, scope, and business, its available resources, and the amount of personal [and other sensitive] information that Lakeland Community College owns or maintains on behalf of others, while recognizing the need to protect both student and employee information.

C. SCOPE

This Program applies to all Lakeland Community College employees, whether full- or part-time, including faculty, staff, contract and temporary workers, hired consultants, interns, and student employees, as well as to all other members of the Lakeland Community College community (hereafter referred to as the "Community"). It applies to any records that contain personal [or other sensitive] information in any format and in any media, whether in electronic or paper form.

1. For purposes of this WISP, "personal information" means either a U.S. resident's first and last name or first initial and last name in combination with any one or more of the following data elements, or any of the following data elements standing alone or in combination, if such data elements could be used to commit identity theft against the individual:
2. Social Security number;
3. Date of Birth;
4. Driver's license number, passport number, State ID, or tribal identification number, or other government-issued identification number;
5. Bank Account number, or credit or debit card number, with or without any required security code, access code, personal identification number, or password that would permit access to the individual's financial account, or any personally identifiable financial information or consumer list, description, or other grouping derived from personally identifiable financial information, where personally identifiable financial information includes any information:
    a. A consumer provides Lakeland Community College to obtain an education, financial product, or service;

b. About a consumer resulting from any transaction involving an education, financial product, or service with Lakeland Community College;
c. Information Lakeland Community College otherwise obtains about a consumer in connection with providing an education, financial product or service;

6. Health information, including information regarding the individual's medical history or mental or physical condition, or medical treatment or diagnosis by a health care professional/created or received by Lakeland Community College, which identifies or for which there is a reasonable basis to believe the information can be used to identify the individual and which relates to the past, present, or future physical or mental health or condition of the individual, the provision of health care to the individual, or payment for the provision of health care to the individual;
7. Health insurance identification number, subscriber identification number, or other unique identifier used by a health insurer;
8. Biometric data collected from the individual and used to authenticate the individual during a transaction, such as an image of a fingerprint, retina, or iris;
9. Email address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account;
10. Non-Directory FERPA Information including grades, GPA, major, grants, scholarships, test scores, Lakeland Identification (LID), high school, transcripts, disciplinary records, and class schedules;
11. Personal information does not include lawfully obtained information that is available to the public, including publicly available information from federal, state, or local government records or directory information as allowed by FERPA.

D. INFORMATION SECURITY COORDINATORS

Lakeland Community College has designated the Chief Information Officer with the Administrative Technologies Security Engineer in coordination with the Data Security and Privacy Assurance Committee to implement, coordinate, and maintain this WISP (as the "Information Security Coordinators"). The Information Security Coordinators shall be responsible for:

1. Implementation of this WISP including:
    a. Assessing internal and external risks to personal information and maintaining related documentation, including risk assessment reports and remediation plans (see Section E);
    b. Coordinating the development, distribution, and maintenance of information security policies and procedures (see Section F);
    c. Coordinating the design of reasonable and appropriate administrative, technical, and physical safeguards to protect personal information (see Section G);

d. Ensuring that the safeguards are implemented and maintained to protect personal information throughout Lakeland Community College, where applicable (see Section G);
e. Overseeing service providers that access or maintain personal information on behalf of Lakeland Community College (see Section H);
f. Monitoring and testing the information security program's implementation and effectiveness on an ongoing basis (see Section I);
g. Defining and managing incident response procedures (see Section J); and
h. Establishing and managing enforcement policies and procedures for this WISP, in collaboration with Lakeland Community College human resources and management (see Section K).

2. Employee, contractor, and (as applicable) stakeholder training, including:
   a. Providing periodic training regarding this WISP, Lakeland Community College's safeguards, and relevant information security policies and procedures for all employees, contractors, and (as applicable) stakeholders who have or may have access to personal information;
   b. Ensuring that training attendees formally acknowledge their receipt and understanding of the training and related documentation, through TechGuard/Infosec training system and Security Request Form; and
   c. Retaining training and acknowledgment records.
3. Reviewing this WISP and the security measures defined here at least annually, or whenever there is a material change in Lakeland Community College's business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal information (see Section 11).
4. Defining and managing an exceptions process to review, approve or deny, document, monitor, and periodically reassess any necessary and appropriate, business-driven requests for deviations from this WISP or Lakeland Community College's information security policies and procedures.
5. Annually reporting to the Board of Trustees and periodically reporting to Lakeland Community College management regarding the status of the information security program and Lakeland Community College's safeguards to protect personal information.

E. RISK ASSESSMENT

As a part of developing and implementing this WISP, Lakeland Community College will conduct a periodic, documented risk assessment using the IT Risk Assessment spreadsheet provided by Educause typically annually, or whenever there is a material change in Lakeland Community College's business practices that may implicate the security, confidentiality, integrity, or availability of records containing personal information. Any changes or improvements to be made will be documented in the Lakeland WISP Remediation Plan.

Lakeland Community College believes the College's current safeguards are reasonable and, considering current risk assessments made by Administrative Technologies, are

sufficient to provide security and confidentiality to confidential data maintained by the College. Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information.

F. INFORMATION SECURITY POLICIES AND PROCEDURES

As part of this WISP, Lakeland Community College has developed, maintains, and distributes information security policies and procedures in accordance with applicable laws and standards to relevant employees, contractors, and (as applicable) other stakeholders to include policies and procedures to:

1. Information classification has been determined to not be needed by outside counsel.
2. Information handling practices for personal [and other sensitive] information, including the storage, access, disposal, and external transfer or transportation of personal [and other sensitive] information.
3. User access management, including identification and authentication (using passwords or other appropriate means).
4. Encryption.
5. Computer and network security.
6. Physical security.
7. Incident reporting and response.
8. Employee and contractor use of technology, including our Information Technology Acceptable Use Policy that includes personal devices; and
9. Information systems acquisition, development, operations, and maintenance.

G. SAFEGUARDS

Lakeland Community College has developed, implemented, and maintains reasonable administrative, technical, and physical safeguards in accordance with applicable laws and standards to protect the security, confidentiality, integrity, and availability of personal [or other sensitive] information that Lakeland Community College owns or maintains on behalf of others.

1. Access to the Data Center outlined in our Administrative Technologies department guidelines, which includes physical locking, sign-in forms, cameras, and motion detection alerts.
2. All systems are thoroughly erased before delivering disposal or resale, while server systems are DOD wiped.
3. Our file share data resides in Microsoft OneDrive/Teams. Allowing us to scan for and identify documents with PII and provides that all files at rest and in transport are inherently encrypted. With a policy in Microsoft 365 that does not allow external sharing of the files containing more than 10 records of PII and a warning if a file contains even 1 record when emailing or sharing.
4. An external security scan of all public websites is performed annually, mitigated, and then rescanned.
5. Annually we have had security awareness training in multiple forms. Held optional in person training, sent out newsletters discussing the topic, performed internal scans and informed people to remove specific information and the

external sharing policy shows up automatically when a person shares the data. We have engaged an external resource to provide web-based training and phishing simulator.

6. Data containing any PII or FERPA-protected information that is retained in file format must follow Lakeland's data protection and lifecycle standards. Files stored in secure locations such as OneDrive or Teams must still be protected using sensitivity labels where available. From day 0 to 6, files may remain unencrypted but should be labeled if possible. From day 7 to 30, files must be encrypted using either sensitivity labels, Microsoft Office password protection, or 7-Zip with AES-256. At 30 days, files should be deleted unless a documented exception exists. For approved exceptions, files retained beyond 30 days and up to 18 months must be encrypted using 7-Zip or an equivalent method that restricts access and ensures data security. Even encrypted files originally pulled from secure databases must be deleted in accordance with records retention policies. While this is the general rule, documented exceptions may apply in cases where legal, regulatory, or departmental records retention requirements necessitate longer storage, provided the files remain securely encrypted and access-controlled throughout their lifecycle.
7. The network is protected by redundant Cisco firewalls and our Cisco Firepower Intrusion detection system. In addition, the network servers are divided into separate DMZ's to protect the Banner/Financial system and other critical devices. Each building within Lakeland is also separated by their own VLAN and credit card processes are also on a separate VLAN. Our windows servers are patched about once a month and our Linux and oracle systems are patched as needed.
8. Lakeland's firewall, server, and network device logs are actively monitored through a centralized security information and event management (SIEM) system. Wazuh collects logs from all major network devices and server systems, with alerting configured based on industry best practices. Our security vendor, Oculus IT, provides 24x7x365 monitoring and sends automated alerts for suspicious activity. In addition to real-time alerts, Lakeland's internal team reviews all logs and security dashboards on a weekly basis to ensure proactive threat detection and response.
9. User ID security:
    a. Password controls include the following requirements:
    b. With the deployment of Multi Factor Authentication, passwords will be required to be changed every 365 days. Passwords will have a minimum number of 10 characters, and at least 3 out of the 4 following: Uppercase, Lowercase, Numbers, or Non-alphanumeric Special characters. Passwords will not allow utilizing part of your username, dictionary words, or more than 3 consecutive characters.
    c. If a user attempts to change their password to an older password, this will not be allowed. The system will remember the previous three passwords so they cannot be used again.

d. Users will have up to 10 attempts to login, but after 2 attempts they will be presented with a ReCAPTCHA to continue their tries. Once the account is locked, users will not be able to try again for 30 minutes.
e. Multifactor Authentication has been added for all employees and security questions can only be used to reset the password. When a password is reset, the users are notified.
f. Administrative and Service accounts have higher requirements.

10. We use Active Directory, that is integrated into our Portal system to provide SAML2.0 complaint logins or LDAP to authenticate for nearly all systems. As soon as HR places a person into the "Let's go" system all relevant IT personnel are notified via email. At times HR will notify us ahead of time, and we will ensure access removal during the termination session. Once a person's Active Directory ID is disabled, they lose access immediately.
11. Annually, we require the Data Access Managers to review/print/and sign off on Banner user access using the "Audit Sign-Off Roster."
12. Access to systems containing PII data must be requested and approved for additional access to display PII data, otherwise the data is masked. When the user requests access they agree to a confidentiality agreement and to the proper handling of data.

H. SERVICE PROVIDER OVERSIGHT

Lakeland Community College oversees each of its service providers that may have access to or otherwise create, collect, use, or maintain personal [or other sensitive] information on its behalf by:

1. Evaluating the service provider's ability to implement and maintain appropriate security measures, consistent with this WISP and all applicable laws and Lakeland Community College's obligations.
2. Requiring the service provider by contract to implement and maintain reasonable security measures that address the standard of care, encryption, information security, security breach procedures, return or destruction of personal information, service level agreements and compliance with ADA/Digital Accessibility laws, consistent with this WISP and all applicable laws and Lakeland Community College's obligations.
3. Monitoring and auditing the service provider's performance to verify compliance with this WISP and all applicable laws and Lakeland Community College's obligations.
4. Utilizing third-party risk intelligence tools such as Bitsight to assess the ongoing cybersecurity posture of a select group of key vendors, allowing Lakeland to identify potential risks that may warrant further review or follow-up.

I. MONITORING

Lakeland Community College will regularly test and monitor the implementation and effectiveness of its information security program to ensure that it is operating in a manner reasonably calculated to prevent unauthorized access to or use of personal [or other

sensitive] information. Lakeland Community College shall reasonably and appropriately address any identified gaps, using the Lakeland WISP Remediation Plan.

J. INCIDENT RESPONSE

Lakeland Community College has established and maintains Policy Number: 3354:2-11-04, Title: Data Security and Privacy Assurance regarding information security incident response.

1. Such procedures shall include:
2. Documenting the response to any security incident or event that involves a breach of security.
3. Performing a post-incident review of events and actions taken.
4. Reasonably and appropriately addressing any identified gaps.
5. Follow the EIncidentCheckList2019.docx provided by Educause.

K. ENFORCEMENT

Violations of this WISP will result in disciplinary action, in accordance with Lakeland Community College's information security policies and procedures and human resources policies. Please see Lakeland Community College's policy page for details regarding the College's disciplinary process.

L. PROGRAM REVIEW

Lakeland Community College will review this WISP and the security measures defined herein at least annually, or whenever there is a material change in Lakeland Community College's business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal [or other sensitive] information.

Lakeland Community College shall retain documentation regarding any such program review, including any identified gaps and action plans.

M. EXCEPTIONS

While every exception to a standard potentially weakens protection mechanisms for Lakeland's systems and underlying data, occasionally exceptions are necessary. When requesting an exception, users are required to submit a business justification for deviation from the standard in question. Request will be accepted using the Security Exception Request form.

N. DOCUMENT CONTROL

Updates to the Written Information Security Procedure will be announced to employees via public website, management updates, and/or email announcements. Changes will be noted in the Record of Changes to highlight the pertinent changes from the previous policies, procedures, standards, and guidelines.