Written Information Security Program

Ripon College Information Technology

Revision History:

Version Number	Revision Date
1.0	27/02/2023
1.1	3/7/2023

Policies, procedures and processes to insure effective administrative, technical and physical safeguards for protection of employees, faculty and student data.

1. OBJECTIVE:

The objective of Ripon College, in the development, maintenance and implementation of this comprehensive written information security program ("WISP") is to create effective administrative, technical, and physical safeguards for the protection of personal information of our employees, faculty, and students. This WISP sets forth Ripon College's procedure for evaluating and addressing our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information.

2. PURPOSE:

The purpose of this WISP is to better:

(a) Ensure the security, confidentiality, integrity, and availability of personal information Ripon College collects, creates, uses, and maintains;
(b) Protect against any reasonably anticipated threats to hazards to the security, confidentiality, integrity, or availability of such information;
(c) Protect against unauthorized access to or use of Ripon College's maintained personal information in a manner that could result in substantial harm or inconvenience to any customer or employee; and
(d) Define an information security program that is appropriate to Ripon College's size, scope, mission, and its available resources; and the amount of personal information that Ripon College owns or maintains on behalf of others, while recognizing the need to protect both student and employee information.

3. SCOPE:

This WISP applies to all employees, contractors, officers and directors of Ripon College. It applies to any records that contain personal information in any format and on any media, whether electronic or paper form.

(a) For purposes of this WISP, "personal information" means either a US 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.
    i. Social Security number;
    ii. Driver's license number, other government-issued identification number, including passport number or tribal identification number;
    iii. 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.
    iv. Health insurance identification number, subscriber identification number, or other unique identifier used by a health insurer.

v. Biometric data collected from the individual and used to authenticate the individual during transaction, such as an image of a fingerprint, retina, or iris; or

vi. 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.

(b) Personal information does not include lawfully obtained information that is available to the general public, including publicly available information from federal, state, or local government records.

4. INFORMATION SECURITY COORDINATOR:

Ripon has designated a Chief Information Security Officer responsible to implement, coordinate, and maintain this WISP. This designated employee (the "Data Security Coordinator") will be responsible for the following:

(a) Initial implementation of this WISP, including:

i. Assessing internal and external risks to personal information and maintaining related documentation, including risk assessment reports and remediation plans;

ii. Coordinating the development, distribution, and maintenance of information security policies and procedures;

iii. Coordinating the design of reasonable and appropriate administrative, technical, and physical safeguards to protect personal information;

iv. Ensuring that the safeguards are implemented and maintained to protect personal information throughout Ripon College where applicable;

v. Overseeing service providers that access or maintain personal information on behalf of Ripon College;

vi. Monitoring and testing the information security program's implementation and effectiveness on an ongoing basis;

vii. Defining and managing incident response procedures;

viii. Establishing and managing enforcement policies and procedures for this WISP, in collaboration with Ripon College HR and management.

(b) Employee and contractor training, including:

i. Providing periodic training regarding this WISP, Ripon College's safeguards, and relevant information security policies and procedures for all employees, and contractors who have or may have access to personal information;

ii. Ensuring that training attendees formally acknowledge their receipt and understanding of the training and related documentation, through written acknowledgement forms; and

iii. Retaining training and acknowledgment records.

(c) Reviewing the WISP and the security measures defined herein at least annually, or whenever there is a material change in The College's business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal information.

(d) 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 Ripon College's information security policies and procedures.

(e) Periodically reporting to management regarding the status of the information security program and The College's safeguards to protect personal information.

5. RISK ASSESSMENT

As a part of developing and implementing this WISP, Ripon College will conduct a periodic, documented risk assessment on a regular basis, or whenever there is a material change in College business practices that may implicate the security, confidentiality, integrity, or availability of records containing personal information.

(a) The risk assessment shall:

i. Identify reasonably foreseeable internal and external risks to the security, confidentiality, integrity, or availability of any electronic, paper, or other records containing personal information.

ii. Assess the likelihood and potential damage that could result from such risks, taking into consideration the sensitivity of the personal information.

iii. Evaluate the sufficiency of relevant policies, procedures, systems, and safeguards in place to control such risks, in areas that include, but may not be limited to:

A. Employee and contractor training and management;

B. Employee and contractor compliance with this WISP and related policies and procedures;

C. Information systems, including network, computer, and software acquisition, design, implementation, operations, and maintenance, as well as data processing, storage, transmission, retention, and disposal; and

D. Ripon College's ability to prevent, detect, and respond to attacks, intrusions, and other security incidents or system failures.

(b) Following each risk assessment, The College will:

i. Design, implement, and maintain reasonable and appropriate safeguards to minimize identified risks;

ii. Reasonably and appropriately address any identified gaps.

iii. Regularly monitor the effectiveness of The College's safeguards, as specified in this WISP.

6. INFORMATION SECURITY POLICIES AND PROCEDURES

As part of this WISP, Ripon College will develop, maintain, and distribute information security policies and procedures in accordance with applicable laws and standards to relevant employees and contractors, to:

(a) Establish policies regarding:

i. The collection of personal information that is reasonably necessary to accomplish The College's legitimate business transactions or to comply with any and all federal, state or local regulations;

ii. The storage of personal information that is limited to the time reasonably necessary to accomplish The College's legitimate business transactions or to comply with any and all federal, state or local regulations;

iii. Information classification;

iv. Information handling practices for personal information, including the storage, access, disposal, and external transfer or transportation of personal information;

v. User access management, including identification and authentication (using passwords or other appropriate means);

vi. Encryption;

vii. Computer and network security;

viii. Physical security;

ix. Incident reporting and response;

(b) Detail the implementation and maintenance of The College's administrative, technical, and physical safeguards.

7. SAFEGUARDS

Ripon College will develop, implement, and maintain reasonable administrative, technical, and physical safeguards in accordance with applicable laws and standards to protect the security, confidentiality, integrity, and availability of personal information that The College owns or maintains on behalf of others.

(a) Safeguards shall be appropriate to The College's size, scope, and business; its available resources; and the amount of personal information that The College owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information.

(b) Ripon College shall document its administrative, technical, and physical safeguards in The College's information security policies and procedures.

(c) Ripon College's administrative safeguards shall include, at a minimum:

i. Designating one or more employees to coordinate the information security program;

ii. Identifying reasonably foreseeable internal and external risks, and assessing whether existing safeguards adequately control the identified risks;

iii. Training employees in security program practices and procedures, with management oversight;

iv. Selecting third party service providers that are capable of maintaining appropriate safeguards, and requiring service providers to maintain safeguards by contract; and

v. Adjusting the information security program in light of business changes or new circumstances;

(d) Ripon College's technical safeguards shall include maintenance of a security system covering its network (including wireless capabilities) and computers that, at a minimum, and to the extent technically feasible, supports:

i. Secure user authentication protocols, including:

A. Controlling user identification and authentication with a reasonably secure method of assigning and selecting passwords (ensuring that passwords are kept in a location or format that does not compromise security) or by using other technologies, such as biometrics or token devices;

B. Restricting access to active users and active user accounts only, including preventing terminated employees or contractors from accessing systems or records; and

C. Blocking access to a particular user identifier after multiple unsuccessful attempts to gain access or placing limitations on access for the particular system.

ii. Secure access control measures, including:

A. Restricting access to records and files containing personal information to those with a need to know to perform their duties; and

B. Assigning unique identifiers and passwords (or other authentication means, but not vendor-supplied default passwords) to each individual with computer or network access that are reasonably designed to maintain security.

iii. Encryption of all personal information traveling wirelessly or across public networks.

iv. Encryption of all personal information stored on laptops or other portable or mobile devices.

v. Reasonable system monitoring for preventing, detecting, and responding to unauthorized use of or access to personal information or other attacks or system failures.

vi. Reasonably current firewall protection and software patches for systems that contain (or may provide access to systems that contain) personal information.

vii. Reasonably current system security software (or a version that can still be supported with reasonably current patches and malware definitions) that (1) includes malicious software ("malware") protection with reasonably current patches and malware definitions, and (2) is configured to receive updates on a regular basis.

(e) Ripon College's physical safeguards shall, at a minimum, provide for:

i. Defining and implementing reasonable physical security measures to protect areas where personal information may be accessed, including reasonably restricting physical access and storing records containing personal information in locked facilities, areas, or containers.

ii. Preventing, detecting, and responding to intrusions or unauthorized access to personal information, including during or after data collection, transportation, or disposal.

iii. Secure disposal or destruction of personal information, whether in paper or electronic form, when it is no longer to be retained in accordance with applicable laws or accepted standards.

8. SERVICE PROVIDER OVERSIGHT

Ripon College will take reasonable steps to select, retain and oversee each of its third party service providers that may have access to or otherwise create, collect, use, or maintain personal information on its behalf by:

(a) Evaluating the service provider's ability to implement and maintain appropriate security measures, consistent with this WISP and all applicable laws and The College's obligations.

(b) Requiring the service provider by contract to implement and maintain reasonable security measures, consistent with this WISP and all applicable laws and The College's obligations.

(c) Monitoring and auditing the service provider's performance to verify compliance with this WISP and all applicable laws and College obligations.

9. MONITORING

Ripon 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 information. Ripon College shall reasonably and appropriately address any identified gaps.

10. INCIDENT RESPONSE

Ripon College will establish and maintain policies and procedures regarding information security incident response. Such procedures shall include:

(a) Documenting the response to any security incident or event that involves a breach of security;

(b) Performing a post-incident review of events and actions taken; and

(c) Reasonably and appropriately addressing any identified gaps.

11. ENFORCEMENT

Violations of this WISP may result in disciplinary action, in accordance with The College's information security policies and procedures and human resources policies. Please see Ripon College's HR policy for details regarding The College's disciplinary process.

12. PROGRAM REVIEW

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

(a) Ripon College shall retain documentation regarding any such program review, including any identified gaps and action plans.

13. EFFECTIVE DATE

This WISP is effective as of March 7, 2023.