Policy
This policy identifies the practices and requirements for faculty, staff, students and other university constituents in regards to the security of the university's information resources.

Authority
The UW-River Falls Chancellor issues this policy in accordance with the Administrative Policy process.

The Chief Information Officer and the Division of Technology Services are responsible for the administration of this policy. To request an exception to this policy, maito: administrative-policy@uwrf.edu.

Sanctions and Appeals Process
Failure to adhere to the provisions of this policy may result in appropriate disciplinary action as provided under existing procedures applicable to students, faculty, and staff, and/or civil or criminal prosecution.

Procedure
Section I. Privacy Protection

The University of Wisconsin-River Falls is committed to safeguarding all personally identifiable information we obtain about our students, staff, other constituents and visitors, whether internal or external. The only personally identifiable information the university collects via electronic mail, administrative systems or the campus web site, including those web sites currently being maintained by third-party, trusted providers is that which is voluntarily provided by our constituents and visitors. Tracking information is collected and analyzed so that we may improve our service offerings to our users. This tracking information is kept confidential to the University of Wisconsin-River Falls.

The University of Wisconsin-River Falls will share personally identifiable information about its students, per FERPA standards and definitions, to entities external to the UW System only when:

- We have your consent to share the information;
- We need to send the information to companies/agencies who work on behalf of the University of Wisconsin-River Falls. These companies do not have and will not be granted any right to use the personally identifiable information we provide to them beyond what is necessary to assist us;
- We respond to legally issued subpoenas, court orders or a legal process;
• We find it necessary to protect and defend the legal rights or property of the University of Wisconsin-River Falls;
• We must comply with Federal or State law.
• We must comply with laws of other nations where our students, faculty and staff may travel.

Section II. Access, Security and Control of Data and Information Policy

Purpose and Scope

The University of Wisconsin-River Falls maintains both paper records and computer information systems to carry out its educational mission. Federal and State laws and regulations govern access to these records. The university establishes local policies and procedures to ensure compliance with these laws and regulations and to protect the integrity of university records and the privacy of individuals. The following policy statements are applicable to all areas of the university and must be observed by all persons dealing with such information, including all university employees and students, as well as other individuals or entities that share university information for business purposes. This policy shall not conflict with or supersede any federal or state mandates for which protection of data under which University departments may be custodians.

Policy and Principles

Data contained in the university's information systems are the property of the University of Wisconsin and represent official university records. Exceptions to this policy are: faculty developed curricular material, student developed curricular material, certain licensed information such as electronic journal subscriptions and personal data or personal information that may be temporarily stored on a university owned electronic device. Questions regarding exemptions should be discussed with the Chief Information Officer.

Users who accept access to university data, regardless of the medium, also accept responsibility for adhering to certain principles regarding the use and protection of that data. These principles are:

1. Information systems within the university shall be used only for and contain only data necessary for fulfillment of the university's mission.
2. University data shall be used solely for the legitimate business of the university.
3. Due care shall be exercised to protect university data and information systems from unauthorized use, disclosure, alteration or destruction.
4. Personally identifiable or financial information in university data, regardless of who collects or maintains it, shall only be shared among those faculty or staff whose responsibilities require knowledge of such data.
5. Summary data that contains no personally identifiable or personal financial information may be distributed freely at the university's discretion.
6. Applicable federal and state laws and university policies and procedures concerning storage, retention, use, release, transportation and destruction of data and/or all information systems, content and components shall be observed.
7. Appropriate university procedures shall be followed in reporting any breach of security or compromise of safeguards.

8. University computerized information systems shall be constructed in such a manner to assure that:
   a. Individual staff shall work with the Division of Technology Services so that a centralized catalog of information can be maintained and the expertise of the staff leveraged to carry out these requirement's;
   b. Accuracy and completeness of all system contents are maintained during storage and processing;
   c. Data, text and software stored and processed can be traced forward and backward for audit purposes;
   d. Information system capabilities can be reestablished in the event of infrastructure or equipment failures or calamities within an acceptable period of time;
   e. Actual or attempted breaches of security can be detected promptly.

9. Any employee engaging in, or allowing others to engage in, unauthorized use, disclosure, alteration or destruction of information systems or data in violation of this policy shall be subject to appropriate disciplinary action. All employees making use of university information systems shall be informed annually as to their proper, ethical and legal use.

10. Any student engaging in unauthorized use, disclosure, alteration or destruction of information systems or data in violation of this policy shall be subject to appropriate disciplinary action. All students making use of university information systems shall be informed annually as to their proper, ethical and legal use.

11. Users may not use, query, release or print data in any application which they have not been given deliberate access to, which can include but is not limited to:
   a. Transcripts, grade reports, enrollment reports;
   b. Financial Aid information;
   c. Personnel, leave, salary reports;
   d. Reports for government or funding agencies;
   e. Fund-raising activities;
   f. Mailing lists and labels; and
   g. Private or public release of data to outside parties such as student, parents, and the news media.

12. The university shall take steps to ensure that proper consent has been granted by users for the use of electronic transactions. Such consent shall be considered in effect from the point in time that it is consented until such time as the on-going relationship between the university and the user is severed. Should a severed relationship be renewed, a new consent must be granted by the user. Should any changes in the university's business practices occur that have a substantive effect on this consent, a revised consent must be granted which will supersede the previous consent.

13. All requests for information under the Freedom of Information Act, the Wisconsin Public Records Law, law enforcement agencies, subpoenas, etc. must be referred to the Assistant Chancellor for Business and Finance before releasing any records. Records will only be released at the direction of the Assistant Chancellor for Business and Finance, the Provost, the Chancellor or their properly designated representatives in concert with established policies and procedures.
Responsibilities
Safeguarding of university information systems and data shall be the responsibility of each faculty, staff or student with knowledge of the system or data. Specific responsibilities are as follows:

- **Management** - All levels of management are responsible for ensuring that system users within their area of accountability are aware of their responsibilities as defined in this policy. Specifically, managers are responsible for validating the access requirements of their staff and student employees according to their job functions prior to submitting requests for access, and for ensuring a secure office environment with regard to university information systems. Managers of major university offices should appoint an individual within their staff to ensure these responsibilities are observed. Managers are also responsible for ensuring and documenting that their staff and student employees attend appropriate training sessions offered by the university. Managers are also responsible for ensuring that their staff and student employees are in compliance with applicable laws, regulations and policies and practices that affect their area.

- **Employees** - Faculty, staff, and student employees, are responsible for the protection, privacy, and control of all university data they access or create, regardless of the data storage medium. All employees must ensure that the data and data media are maintained and disposed of in a secure manner. Employees are responsible for reading, understanding and complying with the applicable laws, regulations, policies and practices that affect their area. All employees are responsible for understanding the meaning and purpose of the data to which they have access, and may use this data only to support the normal functions of the employees' administrative or academic duties. All employees are responsible for all transactions occurring under their user ID. Passwords and other security access secrets may not be shared with anyone under any circumstances unless the Chief Information Officer, in consultation with the university administration, approves an exception.

- **Students** - Students are responsible for protecting their passwords and other security access secrets so that no unauthorized persons would have access to their university records. Students are responsible for reading, understanding and complying with the applicable laws, regulations, policies and practices that affect them. Students should participate in university sponsored training sessions to improve their understanding of how to safeguard their own privacy.

- **The Chief Information Officer** is responsible for providing administrative, technical and educational support in the area of information security for all users of the information systems. This support includes but is not limited to: security framework assessment; compliance and auditing; computer account management; system and network security administration; firewall management; and an information security education program.
Section III. Compliance with FTC Safeguard Rules

The Gramm-Leach-Bliley (GLB) Act requires financial institutions to ensure the security and confidentiality of personal information that is collected from customers, such as their names, addresses and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers. As part of its implementation of the GLB Act, the Federal Trade Commission (FTC) has issued the Safeguards Rule. This Rule requires financial institutions under FTC jurisdiction to secure customer records and information. The FTC has ruled that colleges and universities are financial institutions for the purposes of this Rule, and must be in compliance by May 23, 2003.

Section IV. Compliance with PCI-DSS Credit Card Framework

The Payment Card Industry Data Security Standard (PCI-DSS) is a framework of security requirements, technology techniques and data protocols that were established to encourage the safe processing of electronic financial transactions using a “credit” or “debit” card. These requirements are of university merchants by the financial institutions that process these transactions on our behalf. All university employees are required to comply with these requirements and must remain diligent in maintaining them daily to prevent a breach of financial information. The University Controller, in conjunction with the Chief Information Officer, or their designees, are responsible in overseeing that all applicable laws, rules, regulations, policies and practices are accounted for in the payment processing chain. Departments are responsible for a portion of the campus wide costs to maintain PCI-DSS safe technology environments and may also incur directly associated fees of compliance and non-compliance.

This policy (AP-05-301) sets out to satisfy PCI-DSS Version 3.0 Requirement 12.1 where the University shall “establish, publish, maintain and disseminate a security policy.” Any campus merchant that is processing transactions that involve a credit card in any manner must comply with PCI-DSS and have a formal PCI-DSS security policy in their department that complies with PCI-DSS requirements. It is the responsibility of departmental management to contact the University Controller or designee to establish a PCI-DSS security program prior to beginning any efforts to acquire credit card transactions. Each merchant must comply with all requirements at the direction of the University Controller and Chief Information Officer, or designees, prior to and thereafter processing credit card transactions.

Section V. Electronic Payment Processing

All departments wishing to transact electronic payments through any means, regardless of method or technology used now or in the future, are required to receive approval from the University Controller and Chief Information Officer prior to doing so. The Chief Information Officer, in conjunction with the University Controller, is responsible in overseeing that all the department is meeting all applicable laws, rules, regulations, policies and practices are accounted for in the payment processing chain.
Section VI. Breach Reporting

All faculty, staff, students and University constituents shall immediately upon detection of, or immediately upon suspicion of, a breach of personal identifiable information (PII) or financial information, report the breach to the Chief Information Officer.

Section VII. Solicitation of Sensitive Information through Email

Sensitive Information: SSN, Credit Card Number, Driver’s License, University Passwords, Passport number, Financial account numbers, student class rosters, student ID numbers, and personal health information.

University departments, staff and constituents shall not transmit sensitive information through insecure transmission methods including email, instant messaging, learning management systems, social media networks, third party file sharing applications or any other method not under the direct control of the Division of Technology Services.

The Division of Technology Services, Chief Information Officer and/or Chief Information Security Officer should be consulted about any process prior to proceeding to use methods of information sharing. This is so they can assist with assuring compliancy with this guideline.

If the email communication is requesting someone give or submit sensitive information, either of the following requirements must be met:

1. The email communication contains no URLs:
   The organization sends the email as themselves, directing the person to an existing, well-known portal or website. From there, the person can be directed to a 3rd party site, or information collected and securely transferred to the 3rd party.
   a. For example, instead of linking to http://3rdparty.site.com/user?ba=2817&id=110282, the email states “Refer to our homepage at www.university.edu, select “Human Resources”, then “Background Check Process”.
   b. All websites involved must use an internet recognized SSL certificate so the person can verify the authenticity and integrity of the websites.

2. If the email communication contains URLs:
   a. Have a valid, internet recognized digital certificate attached which verifies the authenticity of the sender.
   b. If the email contains a link to a web page that requests a login, or a place to enter personally identifiable information, then the web pages involved need to be secured with an Extended Validation web certificate.
   c. If the email comes from a third party, it should state plainly it originated from the third party, and which UW institution they are working with. It should not come from the third party pretending to be from the university (i.e. “spoofed”).
d. The following language (or equivalent) should be added to the message:
   i. “To verify the authenticity of this email, you may contact <insert a local campus phone number for a person who can verify the email as legitimate>”.

e. If possible, there should be prior communication with the intended recipient of the email letting them know:
   i. to expect this email (so they will not delete/ignore/report it)
   ii. who it will be from
   iii. roughly what the contents will be
   iv. what action(s) we expect them to take
   v. that this process protects their privacy

If either of these requirements cannot be met in their entirety, the email communication must be cleared by the Chief Information Officer.

Background
This policy was developed in order to be compliant with:
- The Gramm-Leach-Bliley Act;
- The Federal Trade Commission's Safeguard Rule;
- The requirements of the University of Wisconsin System Legal Office.
- 15 USC 6801 – Protection of nonpublic personal information.
- 2005 WI Act 138 – Wisconsin Statute 134.98 – defines PII (personally identifiable information) and defines handling of breach notifications.

This policy supplants the previous Data Security Policy.

Related Documents
Contact
To direct questions about this policy, mailto: administrative-policy@uwrf.edu.