University of Wisconsin-Platteville

Email Policy
Published: 01/26/2015
Section of: University Security Policies
Target Audience: Faculty, Staff, Students & Guests
PUBLIC
Page 1 of 12

University of Wisconsin-Platteville is hereinafter referred to as "the university."

1.0 Overview
Email is an essential component of communication; however it presents a particular set of challenges due to its potential to introduce security threats to the network. Email can also have an effect on the university’s liability by providing a written record of communications, so having a well thought out policy is essential. The university owns and maintains all legal rights to its email systems and network, and thus any email passing through these systems is owned by the university and it may be subject to use for purposes not anticipated by the user. Additionally, individuals should be advised that email sent through the university system is considered public record. This policy outlines expectations for appropriate, safe, and effective email use.

2.0 Purpose
The purpose of this policy is to detail the university’s usage guidelines for the email system. This policy will help the university reduce risk of an email-related security incident, foster good communications both internal and external to the university, and provide for consistent and professional application of the university’s email principles.

3.0 Scope
The scope of this policy includes the university’s email system in its entirety, including desktop and/or web-based email applications, server-side applications, email relays, and associated hardware. It covers all electronic mail sent from the system, as well as any external email accounts accessed from the university network. Email use is a privilege, not a right, and appropriate use in accordance with university policies is expected from all individuals. Some sections of this policy may apply specifically to expectations for university employees.

4.0 Policy

4.1 Proper Use of University Email Systems
Individuals are asked to exercise common sense when sending or receiving email from university accounts. Additionally, the following applies to the proper use of the university email system.

4.1.1 Sending Email
When using a university email account, email must be addressed and sent carefully. Individuals should keep in mind that the university has no control of email once it is sent. Users must exercise extreme care when typing in addresses, particularly when email
address auto-complete features are enabled; using the "reply all" function; or using distribution lists; in order to avoid inadvertent information disclosure to an unintended recipient. Careful use of email will help the university avoid the unintentional disclosure of sensitive or non-public information.

4.1.2 Incidental Personal Use and General Guidelines
Incidental personal usage of university email systems by employees is permitted as long as A) such usage does not negatively impact the university computer network, and B) such usage does not negatively impact the job performance of a university employee.

- The following is never permitted by any individuals: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited.
- Individuals are prohibited from forging email header information or attempting to impersonate another person.
- Email is an insecure method of communication, and thus information that is considered confidential to the university, or protected by data privacy regulations, may not be sent via email, regardless of the recipient, without proper encryption.
- It is university policy not to open email attachments from unknown senders, or when such attachments are unexpected.
- Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size.

Please note that the topics above may be covered in more detail in other sections of this policy.

4.1.3 Operational Communications and Email
The university uses email as an important communication medium for operations. University employees are expected to check and respond to email in a consistent and timely manner during business hours.

Additionally, faculty, staff, and students are asked to recognize that email sent from a university account reflects on the university, and, as such, email must be used with professionalism and courtesy.

4.1.4 Email Signature & Disclaimers
Email signatures (contact information appended to the bottom of each outgoing email) may or may not be used, at the discretion of the individual user. Users should keep any email
signatures professional and courteous in nature. Political and religious references are not encouraged.

Email disclaimers, usually as text appended to the end of outgoing mail messages, are not required. However, they are useful as a component of the university’s risk reduction efforts, and are recommended when sending official email communications from a university account. See an example of an email disclaimer below.

The preceding e-mail message (including any attachments) contains information that may be confidential, protected by the attorney-client privilege or other applicable privileges, or constitute non-public information. It is intended for the designated recipient(s) only. If you are not an intended recipient of this message, please notify the sender by replying to this message and then delete it from your system. Use, dissemination, distribution, or reproduction of this message by unintended recipients is prohibited.

4.1.5 Auto-Responders
The university recommends the use of an auto-responder (if the email system is equipped with such a feature) if an employee will be out of the office for an entire business day or longer. The auto-response should notify the sender that the employee is out of the office, the date of the employee’s anticipated return, and who the sender should contact if immediate assistance is required. The auto-response should not contain sensitive internal university information due to the automatic nature of the replies.

4.1.6 Mass Emailing
The university makes the distinction between the sending of mass emails and the sending of unsolicited email (spam). Mass emails may be useful for both internal operational and external purposes (such as when communicating with the university’s employees or student base), and is allowed as the situation dictates. The sending of spam, on the other hand, is strictly prohibited.

It is the university’s intention to comply with applicable laws governing the sending of mass emails. For this reason, as well as in order to be consistent with good business practices, the university requires that email sent to more than twenty (20) recipients external to the university have the following characteristics:

1. Wherever possible, the email must contain instructions on how to unsubscribe from receiving future emails (a simple "reply to this message with UNSUBSCRIBE in the subject line" will do). Unsubscribe requests must be honored immediately.
2. The email must contain a subject line relevant to the content.
3. The email must contain contact information, including the full physical address, of the sender.
4. The email must contain no intentionally misleading information (including the email header), blind redirects, or deceptive links. Note: Emails sent to university employees, existing faculty, staff, students, or persons who have already inquired about the university’s services are exempt from the above requirements.

4.1.7 Opening Attachments
Users must use care when opening email attachments. Viruses, Trojans, and other malware can be easily delivered as an email attachment. Users should:

- Never open unexpected email attachments.
- Never open email attachments from unknown sources.
- Be cautious of clicking links within email messages unless the individual is certain of the link's safety. It is often best to retype the URL, as specially-formatted emails can hide a malicious URL. Example: If you receive an email that includes a link to www.wisconsin.gov, opening a browser and directly typing in that URL can ensure that you are going to the state of Wisconsin’s website and not to a site that spoofs it.

The university may use methods to block what it considers to be dangerous or emails or strip potentially harmful email attachments as it deems necessary.

4.1.8 Monitoring and Privacy
The University is subject to the State of Wisconsin open records laws. URL: http://www.wisfoic.org/index.php?option=com_content&view=article&id=64:text-of-open-records-law&catid=39:text-of-laws&Itemid=69 Individuals should not have an expectation of privacy when using the university’s network or university resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. The university reserves the right to monitor any and all use of the computer network. To ensure compliance with university, state, and federal policies this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media. Additionally, all university emails are subject to the state of Wisconsin open records law and may be published in accordance with that law.

4.1.9 University Ownership of Email
Faculty, staff, students, and guests should be advised that the university owns and maintains all legal rights to its email systems and network, and thus any email passing
through these systems is owned by the university and it may be subject to use for purposes not be anticipated by the user. Keep in mind that email may be backed up, otherwise copied, retained, or used for legal, disciplinary, or other reasons. Additionally, individuals should be advised that email sent through the university system is considered public record.

If the university utilizes a hosted email solution, then the regulations and acceptance policy of that vendor (e.g. Microsoft) also applies to the user account.

4.1.10 Contents of Received Emails
Users must understand that the university has little control over the contents of inbound email, and that this email may contain material that the user finds offensive. If unsolicited email becomes a problem, the university may attempt to reduce the amount of this email that the users receive, however no solution will be 100 percent effective. The best course of action is to not open emails that, in the user's opinion, seem suspicious. If the user is particularly concerned about an email, or believes that it contains illegal content, the individuals should notify a supervisor, the UW-Platteville Helpdesk, or the UW-Platteville Information Security office.

4.1.11 Access to Email from Mobile Phones
Many mobile phones or other devices provide the capability to send and receive email. The university permits users to access the university email system from a mobile phone. Refer to the Mobile Device Policy for more information.

4.2 External and/or Personal Email Accounts
The university recognizes that users may have personal email accounts in addition to their university-provided account. The following sections apply to non-university provided email accounts:

4.2.1 Use for University Business
Employees must use the university email system for all business-related email. Employees are prohibited from sending business email from a non-university-provided email account.
4.2.2 Access from the University Network
Employees are permitted to access external or personal email accounts from the university network, as long as such access uses no more than an incidental amount of the users' time and university resources.

4.2.3 Use for Personal Reasons
Employees are strongly encouraged to use a non-university-provided (personal) email account for any non-business communications. Employees must follow applicable policies regarding the access of non-university-provided accounts from the university network.

4.3 Confidential Data and Email
The following sections relate to confidential data and email:

4.3.1 Passwords
As with any university passwords, passwords used to access email accounts must be kept confidential and used in adherence with the Password Policy. At the discretion of the Assistant Vice Chancellor for Information Technology, the university may further secure email with certificates, two factor authentication, or other security mechanisms.

4.3.2 Emailing Restricted Data
Email is an insecure means of communication. Users should think of email as they would a postcard, which, like email, can be intercepted and read on the way to its intended recipient.

Emailing of information classified by the university as restricted should be limited to an as needed basis. The university requires that any email containing confidential information sent external to the university be encrypted using commercial-grade, strong encryption. Encryption is encouraged, but not required, for emails containing confidential information sent internal to the university. When in doubt, encryption should be used.

Further guidance on the treatment of confidential information exists in the university's Restricted Data Policy. If information contained in the Restricted Data Policy conflicts with this policy, the Restricted Data Policy will apply.
4.4 University Administration of Email
The university will use its best effort to administer the university's email system in a manner that allows the faculty, staff, students, and guests to both be effective while utilizing their email as well as reduce the risk of an email-related security incident.

4.4.1 Filtering of Email
A good way to mitigate risk from email is to filter it before it reaches the user so that the user receives only safe, appropriate messages. The University uses a hosted email solution, and therefore is subject to the vendor's current filtering standards. No method of email filtering is 100 percent effective, so the user is asked additionally to be cognizant of this and use common sense when opening emails.

Additionally, many email and/or anti-malware programs will identify and quarantine emails that it deems suspicious. Emails deemed as suspicious by the vendor’s filtering will be stored in a “Junk” folder. Each individual should periodically check their junk folder to ensure that no legitimate email was flagged by the vendor’s filter.

4.4.2 Retention and Backup
Email should be retained and backed up in accordance with the applicable policies, which may include but are not limited to the: Data Classification Policy, Restricted Data Policy, Backup Policy, and Retention Policy.

4.4.3 Email Deletion
Emails containing information covered by the university’s record management schedules must be retained in accordance with those schedules.

Faculty, staff, students, and guests are encouraged to delete email periodically when the email is no longer needed for business purposes. The goal of this policy is to keep the size of the user's email account manageable, reduce the burden on the university to store and backup unnecessary email messages, and comply with university record management schedules.

However, users are strictly forbidden from deleting email in an attempt to hide a violation of this or another university policy. Further, email must not be deleted when there is an active investigation, litigation, or open records request where that email may be relevant.

Unless otherwise indicated, for the purposes of backup and retention, email should be considered internal data.
4.4.4 Address Format
Email addresses must be constructed in a standard format in order to maintain consistency across the university. The university has chosen lastnamefirstinitial@uwplatt.edu as its standard email format. Requested deviations to that format must be submitted in writing to the university help desk. The intent of this policy is to simplify email communication as well as provide a consistent and professional appearance. Due to system restrictions and duplicate names, abbreviations or expansions on this naming convention may occur.

Email Aliases
Often the use of an email alias, which is a generic address that forwards email to a user account or office or group of individuals, is a good idea when the email address is widely used in the public domain. Aliases reduce the exposure of unnecessary information, as well as (often) the names of university employees who handle certain functions. Keeping this information private can decrease risk by reducing the chances of a social engineering attack.

Examples of commonly used email aliases are:
- concerns@universitydomain.com
- techsupport@universitydomain.com
- communications@universitydomain.com
- info@universitydomain.com

The university may or may not use email aliases, as deemed appropriate by the Assistant Vice-Chancellor for Information Technology and/or executive team. Aliases may be used inconsistently, meaning: the university may decide that aliases are appropriate in some situations but not others depending on the perceived level of risk.

4.4.5 Account Activation
Email accounts will be set up for each individual determined to have a valid need to send and receive university email. Accounts will be set up at the time a new hire starts with the university, or when a promotion or change in work responsibilities for an existing employee creates the need to send and receive email. Provisional accounts are created for prospective students, and transitioned to long-term accounts for enrolled students. Guest accounts may be created upon request to accommodate non-conventional university employees, vendors, business or community partners.

At times, email accounts may be given to non-employees, contractors, or other individuals
Email Policy

Section of: University Security Policies

Target Audience: Faculty, Staff, Students & Guests

Page 9 of 12

authorized to conduct certain aspects of the university's business. In these cases, the university should consider designating the temporary or non-employee status of the account in the account name, such as:

- lastnamefirstintitial@temporary.universitydomain.com
- lastnamefirstintitial@contractor.universitydomain.com
- lastnamefirstintitial@consultant.universitydomain.com

4.4.6 Account Termination

When an individual leaves the university, or his or her email access is officially terminated for another reason, the university will disable the individuals access to the account by password change, disabling the account, or another method. The university is under no obligation to block the account from receiving email, and may continue to forward inbound email sent to that account to another user, or set up an auto-response to notify the sender that the user is no longer employed by the university.

4.5 Prohibited Actions

The following actions shall constitute unacceptable use of the university email system. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the university email system to:

- Send any information that is illegal under applicable laws.
- Access another user's email account without A) the knowledge or permission of that user - which should only occur in extreme circumstances, or B) the approval of university administration in the case of an investigation, or C) when such access constitutes a function of the employee's normal job responsibilities. Note: During emergencies, or upon request from the UW-Platteville police department, authorization can be made by the Assistant Vice Chancellor for Information Technology, the Deputy CIO for Information Technology, or the Information Security Officer.
- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, harassing, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
- Send emails that create a hostile environment. This includes sending emails that are intentionally inflammatory. Employees should not send emails that cause disruption to the workplace environment or that include information that is not conducive to a professional working atmosphere.
  - Make fraudulent offers for products or services.
  - Attempt to impersonate another person or forge an email header.
  - Send spam, solicitations, chain letters, or pyramid schemes.
University of Wisconsin-Platteville

Email Policy
Published: 01/26/2015
Section of: University Security Policies
Target Audience: Faculty, Staff, Students & Guests
PUBLIC
Page 10 of 12

- Knowingly misrepresent the university's capabilities, operational practices, services, fees, or policies.

The university may take steps to report and prosecute violations of this policy, in accordance with university standards and applicable laws. Employee violations should be taken to the senior staff in that area, who will contact Human Resources. Human Resources will involve the appropriate parties. Student violations should be taken to the Dean of Students, who will then involve the appropriate parties.

4.5.1 Data Leakage
Data can leave a network in a number of ways. This often occurs inadvertently by a user with good intentions. For this reason, email poses a particular challenge to the university's control of its data.

Emailing of university data, restricted or otherwise, to non-university email accounts for the purpose of saving the data is prohibited, unless explicitly authorized. If an employee needs access to information from external systems (such as from home or while traveling), that user should notify his/her supervisor rather than emailing the data to a personal account or otherwise removing it from university systems. An employee’s supervisor can work with the UW-Platteville Information Technology Services department to provide a secure solution for accessing the university’s data.

The university may employ data loss prevention techniques to protect against leakage of confidential data at the discretion of the Assistant Vice Chancellor for Information Technology.

4.5.2 Sending Large Emails
Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size. The current vendor hosted email solution restricted email attachments sent or received to 25MB or less.

4.6 Applicability of Other Policies
This document is part of the university's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies will be reviewed as needed.
5.0 Enforcement

This policy will be enforced by the Assistant Vice Chancellor for Information Technology in consultation with Human Resources and/or the Dean of Students. Violations may result in disciplinary action, which, for students is outlined in Chapter 14 and Chapter 17 of the student conduct agreement and for all individuals may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of university property (physical or intellectual) are suspected, the university may report such activities to the applicable authorities.

6.0 Definitions

Auto Responder  An email function that sends a predetermined response to anyone who sends an email to a certain address. Often used by employees who will not have access to email for an extended period of time, to notify senders of their absence.

Certificate  Also called a "Digital Certificate." A file that confirms the identity of an entity, such as a university or person. Often used in VPN and encryption management to establish trust of the remote entity.

Data Leakage  Also called Data Loss, data leakage refers to data or intellectual property that is pilfered in small amounts or otherwise removed from the network or computer systems. Data leakage is sometimes malicious and sometimes inadvertent by users with good intentions.

Email  Short for electronic mail, email refers to electronic letters and other communication sent between networked computer users, either within a university or between companies.

Encryption  The process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored.

Mobile Device  A portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

Password  A sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also known as a passphrase or passcode.

Spam  Unsolicited bulk email. Spam often includes advertisements, but can include malware, links to infected websites, or other malicious or objectionable content.
University of Wisconsin-Platteville

<table>
<thead>
<tr>
<th>Email Policy</th>
<th>Published: 01/26/2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section of: University Security Policies</td>
<td>Target Audience: Faculty, Staff, Students &amp; Guests</td>
</tr>
<tr>
<td>PUBLIC</td>
<td>Page 12 of 12</td>
</tr>
</tbody>
</table>

**Smartphone**  A mobile telephone that offers additional applications, such as PDA functions and email.

**Two Factor Authentication**  A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

**7.0 Revision History**

Published 1.0 1/26/2015