ISO 305 - Email Use

Friday, April 26, 2019 8:45 AM

Written by: cjohnson@uwsp.edu (2019.04.26)

Updated by: cjohnson@uwsp.edu (2019.04.26)

Approved by: Information Security Office

Applicable to:

- All users that conduct university business or instruction.
- All users of UWSP email services.

Terms:

- University Business – All matters officially connected to the operation of the university, whether it is academic in nature, or support operations. Any actions taken by an individual in their official capacity connected to their appointment(s) at the University of Wisconsin – Stevens Point is considered university business.
- Third-Party Account - Third-party email accounts include any addresses not assigned to the user by the University for the purpose of conducting university business. Services such as gmail, hotmail, and personal outlook accounts, are examples. This is considered a third-party address even if the user has procured the account for business purposes, whether that business be personal, another company/organization (for example, moonlighting). This also includes third-party accounts procured for the purpose of conducting university business, but not issued by the University for that purpose.

1. Introduction

1.1. Background

The ever-increasing use of digitized and networked information at the University intensifies the risk of data being copied, modified, hidden or encrypted, accessed by unauthorized persons, stolen or destroyed. Furthermore, unless systems are appropriately secured, there is an increased risk that they will be used to mount attacks against other organizations, affiliates, or persons, potentially damaging the reputation of the University. In addition, it is essential for the protection of those who administer and manage IT facilities to do so within the framework of the numerous laws that concern data and information, so that individuals do not find themselves liable to criminal proceedings because of their activities.

The technical controls that are used within the University provide an essential element of the required protection. However, these only deliver part of the solution, the most effective defense being achieved through awareness and good working practices. This document forms the University's Email Use Policy in support of its Information Security Policy. Compliance with this Policy will ensure that consistent controls are applied throughout the University to minimize exposure to security breach.

The University's Information Security Policy and a full list of Supporting Policies can be found at https://www.uwsp.edu/infotech/Pages/Policies/Policies.aspx

UW System administrative policies can be found at https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/

The UW Board of Regent policy on Acceptable Usage of Technology Resources can be found at

https://www.wisconsin.edu/regents/policies/acceptable-use-of-information-technology-resources/

1.2. Applicability

This Policy is primarily aimed at faculty and staff of the University of Wisconsin – Stevens Point, but all users of UWSP email services are subject to this Policy. Compliance with this Policy is conditional for continued access to this service. All accounts for computer systems and services that are used for university business are subject to this policy. Applicability naturally extends to anyone else who is subjected to the Policy who undertakes activities governed by this Policy. It is the personal responsibility of each person to whom this Policy applies to adhere fully with its requirements. However, Deans and chairs of departments are responsible for implementing this Policy within their respective faculty/department and for overseeing compliance by staff under their direction or supervision. Monitoring and technical controls to ensure compliance with this Policy are the responsibility of the UWSP Information Security Office.

1.3. Purpose

Policy Purpose Electronic mail services are provided on university owned computing and networking resources to further the mission of learning, instruction, administration and public service. The purpose of this policy is to ensure the proper use of the University of Wisconsin-Stevens Point electronic mail communication system and make users of the email system aware of what the University of Wisconsin-Stevens Point deems to be acceptable and unacceptable use. This policy is intended to maintain an ethical and amicable working environment and to meet the requirements governing the use of university email resources. Violations of computing policies may result in loss of access to systems, appropriate administrative sanctions and/or legal action.

1.4. Statement

Email is an essential means of communication in support of the university's daily academic, educational, public service and administrative functions. The university encourages using the university email system to improve communications, share information, transact university business and exchange ideas. Those who use university email are expected to do so responsibly, that is, to comply with state and federal laws, with this and other policies and procedures of the University, and with normal standards of professional and personal courtesy and conduct. These responsibilities include understanding and observing appropriate use of email resources and other resources as outlined in the Acceptable Use of Information Technology Resources Policy.

2. Acceptable Use

Acceptable Use The university has established email as an official means of communication with students and employees. Email resources are provided primarily as a medium of expression for academic programs and university operations. Therefore, everyone should use non-university resources for extensive or recurring communication not related to university purposes. The university email system may be used for incidental personal purposes provided that such use does not:

- Interfere with the operation of the campus email system.
- Burden the University with noticeable incremental cost.
- Interfere with the user's employment obligations.

Each user is responsible for using the email system with normal standards of professional and personal courtesy in an ethical and lawful manner.

2.1. Examples of Unacceptable Use

Unacceptable and inappropriate behavior includes, but is not limited to:

• Using your university email account to join email based special interest groups for personal purposes (e.g., gardening, food, coupons, eBay, shopping, fantasy gaming, investment email lists, etc.).
• Allowing anyone else to use your email account. You are responsible for any correspondence originating from your account.
• Sending or forwarding Highly Sensitive data as defined in the UW System – 1031.A Data Classification Policy without proper authorization or without using required controls.
• Sending a campus wide mailing or a mailing to large groups of people without first checking with the email administrator (postmaster@uwsp.edu).
• Using email to harass, intimidate or otherwise annoy another person, such as broadcasting unsolicited messages or sending unwanted email, is expressly prohibited. This also applies to material originating from this campus but sent to other sites or persons on the Internet.
• Sending chain letters, email hoaxes, viruses, worms, spyware, or any form of malware.
• Using the email system for personal gain or for commercial activities not associated with the university.
• Using a pseudonym or writing anonymous mail that appears to disassociate you from responsibility for your actions is almost always inappropriate. Concealing or misrepresenting your name or affiliation to mask irresponsible or offensive behavior is a serious abuse. Using identifiers of other individuals as your own constitutes fraud.
• Attempting to gain access to another person's email files or to use another person's email account unless permission was granted by the proper authorities.
• Sending or forwarding material that could be construed as obscene, threatening, offensive, or libelous.
• Sending materials to a mailing list which are not consistent with the purpose of the mailing list.

2.2. The Use of Third-Party Email Accounts

The use of third-party email accounts for strictly personal use while on campus technology assets will be tolerated, provided the following conditions are met:

• Does not interfere with technical operations, violate security policies, or conflict with any other institutions policies, procedures, or standards.
• Does not burden the University with noticeable incremental cost.
• Does not interfere with the user's employment obligations.

The use of such accounts for conducting university business is strictly forbidden without an exception granted by the UWSP Chief Information Officer and the UWSP Information Security Office. This practice constitutes a violation of institution security policy and a significant risk to the University.

2.2.1. Email Forwarding to Third-Party Accounts

The forwarding of email from university email services to third-parties is strictly forbidden, and is a violation of administrative security policies. The University's technical services monitors for the exfiltration of email to non-approved sources, and will take steps to enforce this policy. Exceptions to this policy are granted on a case-by-case basis by the Information Security Office, and are provided in writing. For the purposes of email forwarding, other UW institutions, schools, and organizations are not considered third-parties, provided they abide by the same UW System administrative policies regarding data classification and protection. This policy applied to university faculty, staff, and student staff. Student accounts with access to student emails are assumed to not contain correspondence related to university business, and are exempt from the email forwarding restriction, provided they do not use their student email account to conduct business on behalf of the university.

2.3. Mass Emails and Solicitations

Email services at the university is created and maintained for the purpose of supporting the mission of the university. This is primarily academic endeavors, but the service must also be available to support

the necessary business functions. In an effort to ensure we are best able to complete our academic objectives, use of the email service primarily supports those efforts. Use of email services is therefore necessarily limited in some ways that may not be consistent with non-academic organizations.

2.3.1 Email Solicitations to UWSP Mailboxes

As a public university activity conducted on university equipment or business is subject to Wisconsin Chapter 19.32 Open records requests. This includes the directory information of our students, for which the Registrar charges a modest service fee. However, this statue does not ensure that emails sent to the addresses collected per these requests are delivered to university mailboxes.

Solicitation to university mailboxes is allowable, provided the messages conform to the requirements of this policy and the following stipulations:

1. The sender will not release more than 500 messages per day to the university.
2. The sender must include, and honor, an unsubscribe or "opt out" link within the body of the email.
3. The sender must include specific language indicating the message is an email solicitation somewhere in the body of their message that is clearly visible.
4. The sender must acknowledge, in writing, that the university makes no guarantee of delivery in any case, and provides no service to third-parties to ensure delivery of these messages. This includes, but is not limited to, delivery confirmation, adjusting security rules, or tracking delivery.

Failure to abide by these stipulations will result in the message being filtered by automated systems, or manually blacklisted.

2.3.2 Contracting third-parties for email services

Contracting third-parties for the purpose of mass communication or emails is sometimes a necessary part of the business or academic process. The use of email surveys for data collection, or the sending of emails for recruiting, for example. As such, the use of email services for these purposes is allowed, but our reputation demands we carefully follow the standards outlined in this policy.

All services that will send emails using email addresses in the uwsp.edu domain must be approved by the Information Security Office. A security review will be conducted, and implementation must include the use of DKIM/DMARC/SPF in accordance with the Information Security Office's current standards to ensure compliance and integrity.

Email solicitations for academic purposes must be approved through appropriate channels on the university. This is required if the solicitation or survey is intended to be sent on-campus only, or to the public. The requestor must ensure the experimental methodology or solicitation has been approved by the Institutional Review Board. If the message is to be sent to a large group of people, approval must be granted from ra-chanc@uwsp.edu (Chancellor.) The survey must be sent by an approved vendor. The Center for Inclusive Teaching and Learning (CITL) has and existing contract with a service provider. Additional vendors will only be approved in the event that there is a demonstrable technical limitation to sending with the existing vendor.

3. Public Records Requests

Personal and university related email of university faculty, staff, student employees, and student organizations may be considered to be a public record. The definition of what is in scope for these request is found in Wisconsin Chapter 19.32. Email messages in your mailbox (either on the server or on your workstation) may need to be provided if requested. When an email message has been deleted from your Deleted Items folder of your mailbox for more than 30 days, it is no longer available and subject to a public records request.

In cases where a request has been made by university executives, human resources, legal counsel, or

law enforcement, a litigation hold may be placed on your account to preserve email beyond the 30 day limit. Due to the sensitive nature of this measure, these requests are kept strictly confidential. The Information Security Office is not permitted to share with the user when their mailbox has been placed into a litigation hold.

Regular IT services may also extend the 30-day deadline in your mailbox. Occasionally, various IT processes may require the archiving of some or all of an individual mailbox or several mailboxes. In these cases, confidentiality of these archives are maintained as if they were active mailboxes, to the level of assurance stipulated in Section 3.1 of this policy.

3.1. Limitations to Privacy in Electronic Communication

Normally you can expect the contents of what you write, create, store and send to be seen only by those to whom you intend or give permission. However, this policy does not imply the complete privacy of your email account. Circumstances where authorized university personnel may need access to your email include but are not limited to the following:

- troubleshooting
- protecting the integrity of the university's technology services
- protecting the rights and property of the university
- protecting the rights of individuals working in collaborative situations
- protecting intellectual property rights as required by law
- handling abandoned email accounts

Authorized university personnel are required to report possible improper or illegal activities they discover. Enforcement Violations will be handled through existing disciplinary, grievance, and hearing procedures. Policy infractions may incur sanctions up to and including dismissal or expulsion.

4. Continuance of Email Service

The university Information Technology department strives to provide technology services to maintain the university's mission. There are times when resources must be appropriated to support that mission. In the case of technology services, it is not always practical or possible to provide services to former faculty and staff members if doing so presents an obstacle to maintaining the academic mission of the university. This section details the services available for retired and emeriti faculty and staff as it pertains to email services.

It should be noted in this policy that the Information Security Office runs a procedure when any faculty or staff retire to sanitize their mailbox for sensitive data. An automated process runs to discover sensitive data, such as SSNs and credit card numbers. The system redacts any such data.

4.1 Volunteers, Gratis Instructors, and Part-Time Employees

Many times when a faculty or staff member retires, they only retire from part of their duties. They continue to provide service to the university in a part-time capacity, or by volunteering. When this occurs, there is no change to email services. While their status with HR and entitlements may change, their email service will continue with their existing mailbox. The Information Security Office will still perform the data sanitization procedure to preserve the integrity of the email system.

The change in status requires an entitlement review from the Information Security Office and a signed Volunteer Agreement on file with Risk Management. Continuation of the account requires a written request from the sponsoring department. IT requires a service fee for maintaining accounts for these individuals to cover the cost of licensing, which will be invoiced to the department. The exact amount can be found by contacting IT Purchasing.

4.2 Complete Retirement / Separation from the University

In the event that a faculty or staff member retires with no intention of providing any additional service to the university, the individual's account will be decommissioned in accordance with System and institution administrative policy. A new account with entitlements appropriate for this arrangement will be provisioned. For the purposes of data security, this ensures the cleanest and quickest way to ensure compliance with policy. Exceptions to this rule are available only with the approval of the Information Security Office, as such action must be carefully managed to ensure we remain within the bound imposed upon us by policy.

4.2.1 Department Access to Email

In the event of a retirement as above, the user's mailbox may be archived and made available to the department as institutional data. This request must be submitted in writing to the Information Security Office, and will only be granted upon the approval of Human Resources. In this case, access to the mailbox will be delegated to appointed individuals for the purpose of archiving and retaining department data. This archive can be retained for up to three months before the archived account is deleted.