Washington University in St. Louis

Office of Information Security
University Information Security Policies

Electronic Messaging Security Policy

Statement of Policy
Washington University in St. Louis (WashU) is committed to conducting all university activities in compliance with all applicable laws, regulations, and university policies. WashU has adopted this policy to outline the security measures required to protect electronic information systems and related equipment from unauthorized use.

Objective
The policy and associated guidance provide direction for electronic messages (i.e. email, chat, and other electronic messages) containing WashU confidential and/or protected information.

Applicability
This policy is applicable for all WashU electronic messages, services provided by WashU for electronic messages, and WashU community member accounts used for electronic messages.

Audience
The audience for this policy is all WashU faculty, staff, and students. It also applies for all other agents of the university with access to WashU information and network for contracted services. This includes, but not limited to partners, affiliates, contractors, temporary employees, trainees, guests, and volunteers. The titles will be referred collectively hereafter as "WashU community".

Roles & Responsibilities

Policy
Electronic message services are provided by WashU for university functions. All WashU community members are expected to comply with the following while using electronic message services:

- State laws
- Federal laws
- Washington University in St. Louis policies

WashU may permit access to review, monitor, or disclose electronic messages from services provided by the university as it is necessary upon approval from Human Resources or the Office of the General Counsel. Users are responsible for providing electronic messages not retained

by WashU that may be relevant upon request by Human Resources or the Office of the General Counsel.

Encryption

Electronic messages containing confidential and/or protected information that may travel across external networks will utilize a physical or logical encryption mechanism to ensure the confidentiality and integrity of the information.

WashU community members are responsible for encrypting attachments (Microsoft Office, Adobe PDF, etc.) that contain WashU protected and/or confidential information and validating the recipients email address or other contact information prior to sending any messages.

Protected and/or confidential information will not be entered in the subject line of any electronic message.

Departments and schools will establish processes and procedures for the use of electronic messages containing WashU protected and/or confidential information.

Encryption exceptions are as follows:

- WashU BJC communication – secure network
- Patient has opted out of encryption per Email Consent Form

External electronic message services

- Workforce members will not provide their WashU login ID or password to another person or vendor due to potential security risks
- Auto-forwarding WashU email accounts containing protected information to any external mail service (Google, Yahoo, etc.) is not permitted
- Public electronic message services will not be used for communication regarding patient care

WashU community members will not use their Washington University email accounts for personal matters such as financial or banking transactions.

WashU email signature line

Refer to the HIPAA Privacy Office for the security measures required to comply with privacy policies for information on creating automatic signatures.

Policy Compliance

The Office of Information Security (OIS) will measure the compliance to this policy through various methods, including, but not limited to - reports, internal/external audits, and feedback to the policy owner. Exceptions to the policy must be approved by the OIS in advance. Non-

compliance will be addressed with management, Area Specific Compliance Office, Human Resources, or the Office of Student Conduct.

Related Policies
Encryption Policy
Computer Use Policy

Reference
None

Policy Review
This policy will be reviewed at a minimum every three years.

Title: Electronic Messaging Security Policy
Version Number: 3.0
Reference Number: SC-01.02
Creation Date: April 2, 2008
Approved By: Security and Privacy Governance Committee
Approval Date: February 27, 2017
Status: Final
Scheduled Review Date: March 1, 2022
Revision Date: February 26, 2019
Revision Approval Date: March 15, 2019
Policy Owner: Office of Information Security