FITCHBURG STATE UNIVERSITY

# Faxing Policy

| | |
|---|---|
| **Version** 1.2 | **Last Updated:** 8/8/2025 |
| **Security Level:** Public | **Issued:** 12/12/2023 |

## Purpose

This policy aims to ensure the confidentiality, integrity, and availability of faxes transmitted through the University faxing solution, especially in adherence to HIPAA requirements.

## Scope

This policy applies to all system administrators within the Technology department who have access to the cloud faxing solution and physical faxing solutions.

## Policy

### Faxing Standard:

- All fax transmission of University information must be performed through an approved cloud-based fax service to minimize physical security risks and ensure auditability. Requests to deploy or use standalone (physical) fax machines are categorically denied; exceptions may be granted only by the CISO upon submission and approval of a written business case that documents the specific necessity, compensating controls, and risk mitigation measures.

### Fax Access and Confidentiality:

- System administrators are not permitted to access faxes belonging to other departments unless explicit written permission is obtained from the respective department head.
- Such access should be solely for the purpose of troubleshooting or maintaining the integrity of the University's faxing system.
- All accesses must be logged within the University's faxing software for auditing.

### Security and Compliance Requirements:

- Ensure the University’s faxing solution employs end-to-end encryption to protect data during transmission. This also includes data encryption at rest.
- The system will be configured to delete faxes automatically after fifteen days.
- Implement access controls to restrict unauthorized access to fax data. This includes permissions to only their faxes, user names, and passwords with complexity requirements, with password expiration and multi-factor authentication to gain access to the University’s faxing solution.

- Regularly update and patch the faxing system in line with the patch management policy
- Conduct periodic security audits and compliance assessments of the faxing system.
- The system must maintain a secure and routinely audited log of all system administrator activities related to fax access.
- Faxing should not be used to send or receive credit card information.

### Training and Awareness:

- All system administrators must undergo training regarding HIPAA compliance and the importance of maintaining the confidentiality of fax transmissions.
- Continuous education on evolving security practices and compliance requirements should be provided.

### Incident Reporting:

- Any breaches or suspected breaches of fax confidentiality must be immediately reported to the Chief Security Officer or the relevant authority.
- Fitchburg State's Incident Response procedure should be followed when responding to such incidents, including containment, investigation, and notification processes as required by HIPAA.

### Policy Review and Updates:

- This policy should be reviewed annually or as required to ensure ongoing compliance with HIPAA and other relevant regulations.
- Updates to the policy must be communicated promptly to all relevant personnel.

## Roles

Technology Security Team: Ensure awareness and compliance with this policy. Ensure that this policy and all component policies and procedures are maintained and implemented.

Technology Fax Administrators: Ensure that individuals assigned to access their applications are authorized. Ensure that the IT infrastructure is protected against unauthorized access. Administer the setup of new numbers, and application accounts, changes to existing accounts, and the disabling of accounts for terminated personnel in a timely manner. Maintain access control lists for review.

All Fax Users: Understand and adhere to this policy. Safeguard their user IDs and passwords. Access only those resources for which they are authorized. Immediately report suspected violations of this policy to their manager or to the Technology Department.

## Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including loss of access rights and/or termination of employment in adherence to their respective collective bargaining agreement. Students found to have violated this policy may have their access removed and may have additional actions taken as directed by the Student Code of Conduct.

## Revision History

| Date of Change | Revision | Responsible | Summary of Change |
|---|---|---|---|
| 12/12/2023 | 1 | Stefan Dodd, CIO<br>Eric Boughton, CISO | Creation of Policy |
| 5/8/2024 | 1.1 | Eric Boughton, CISO | Formatting |
| 8/8/2025 | 1.2 | Eric Boughton, CISO<br>Stefan Dodd, CIO | Formatting, Added Fax Standard Section, Changed scope to all faxing, not just cloud faxing. |