

**DEVELOPING COMPREHENSIVE
EMAIL POLICIES TO PROTECT
PRIVATE ORGANIZATIONS FROM
PERSONAL EMAIL HANDLER RISKS**



national coalition for sexual freedom inc.

May, 2025

Contents

Executive Summary.....	5
Key Risks Addressed by Comprehensive Email Policies.....	5
1. Data Security Vulnerabilities	5
2. Non-Profit Specific Security Concerns.....	5
Essential Components of Effective Email Policies	6
1. Clear Ownership and Privacy Expectations.....	6
2. Data Classification and Handling Requirements	6
3. Implementation Strategies	7
Resource-Conscious Implementation.....	7
Volunteer and Board Member Considerations.....	7
Compliance Risks Specific to Non-Profit Organizations	7
Model Policy: Personal Email Client Usage on Mobile Devices and Personal Computers	8
1. Policy Purpose and Scope.....	8
2. Definitions.....	8
3. Authorized Use of Personal Email Clients.....	8
3.1 Eligibility for Staff	8
3.2 Eligibility for Volunteers and Board Members	8
3.3 Approved Email Clients	9
4. Security Requirements	9
4.1 Device Security	9
4.2 Email Client Configuration.....	9
4.3 Authentication Requirements	9
5. Data Protection Measures	10
5.1 Email Data Handling	10
5.2 Remote Wipe Capability.....	10
6. Compliance and Monitoring.....	10
6.1 Monitoring.....	10
6.2 Auditing	10
7. Responsibilities Upon Separation.....	11

7.1 Staff Responsibilities	11
7.2 Volunteer and Board Member Responsibilities.....	11
7.3 Manager Responsibilities	11
7.4 IT Department Responsibilities	11
8. Special Considerations for Non-Profit Operations	11
8.1 Donor Information	11
8.2 Beneficiary Information	12
8.3 Grant-Related Communications	12
9. Violations and Enforcement.....	12
10. Support and Training.....	12
11. Policy Exceptions	13
12. Policy Review	13
Legal Foundation for Email Management Policies: Federal Framework.....	13
Federal Legal Authority for Email Management	13
Key Federal Laws Governing Email Management.....	14
Electronic Communications Privacy Act (ECPA)	14
Computer Fraud and Abuse Act (CFAA).....	14
Key Federal Case Law Supporting Employer Email Monitoring Rights.....	14
Federal Regulatory Compliance Considerations	15
Federal Trade Commission (FTC) Regulations	15
Health Insurance Portability and Accountability Act (HIPAA).....	15
Gramm-Leach-Bliley Act (GLBA).....	15
Federal Rules of Civil Procedure (FRCP)	17
Industry-Specific Regulatory Requirements.....	17
Financial Services Regulations.....	17
Educational Institutions and FERPA.....	18
State-Level Regulations Affecting Email Management	18
State Data Breach Notification Laws.....	18
International Regulations with Extraterritorial Reach	19
General Data Protection Regulation (GDPR)	19

Conclusion: A Balanced Approach to Email Security	20
References	21
Appendix A: State-Specific Email Policy Requirements for Private Organizations and Non-Profits	22
Federal Non-Profit Considerations	22
Tax-Exempt Status Implications	22
Federal Grant Requirements	22
Alabama	23
Alaska	23
Arizona	23
Arkansas.....	24
California	24
Colorado.....	25
Connecticut.....	25
Delaware	26
Florida	26
Georgia.....	26
Hawaii	27
Idaho.....	27
Illinois.....	27
Indiana	28
Iowa	28
Kansas.....	29
Kentucky.....	29
Louisiana	29
Maine	30
Maryland	30
Massachusetts.....	30
Michigan.....	31
Minnesota.....	31

Mississippi	32
Missouri	32
Montana	33
Nebraska	33
Nevada	33
New Hampshire	34
New Jersey	34
New Mexico	34
New York.....	35
North Carolina	35
North Dakota.....	36
Ohio	36
Oklahoma.....	37
Oregon	37
Pennsylvania	37
Rhode Island	38
South Carolina	38
South Dakota	38
Tennessee.....	39
Texas	39
Utah	40
Vermont.....	40
Virginia	40
Washington.....	41
West Virginia	41
Wisconsin.....	41
Wyoming.....	42

Executive Summary

Private organizations, including non-profits, face significant legal, security, and compliance risks when employees use personal email handlers like Outlook to manage work communications. This document outlines a framework for developing robust email policies based on federal legal standards, with an appendix referencing state-specific requirements. The guidance balances organizational security needs with employee productivity considerations, providing key policy components, implementation strategies, and enforcement mechanisms suitable for all private organizations, with specific considerations for non-profits.

Key Risks Addressed by Comprehensive Email Policies

1. Data Security Vulnerabilities

Personal email handlers like Outlook typically lack the robust security measures implemented in corporate email systems:

The Information Systems Audit and Control Association (ISACA, 2023) noted that "Email forwarding to personal accounts is one of the most common shadow IT practices we encounter. While employees often see it as harmless convenience, it creates significant security vulnerabilities and potential data leakage paths that bypass corporate security controls."

Key security risks include:

- Lack of enterprise-grade encryption
- Reduced ability to implement multi-factor authentication
- Limited logging and monitoring capabilities
- Challenges in implementing data loss prevention controls
- Difficulties in enforcing retention policies

2. Non-Profit Specific Security Concerns

Non-profit organizations face unique security challenges:

According to the Non-Profit Technology Network (NTEN, 2023), "Non-profit organizations often manage sensitive data including donor information, beneficiary details, and program-specific confidential information. Despite potentially limited IT resources, these

organizations must implement appropriate security measures to protect this data from unauthorized access or disclosure."

Non-profits should be particularly concerned about:

- Donor's personally identifiable information (PII) and financial data
- Beneficiary confidential information, which may include financial details
- Grant application and reporting information
- Board communications that may include strategic planning information
- Volunteer personal information
- Private membership information
- Customer lists and PII

Essential Components of Effective Email Policies

1. Clear Ownership and Privacy Expectations

Email policies should explicitly state:

- All email accounts provided by the organization remain the property of the organization
- The organization reserves the right to monitor all communications on company systems
- Employees should not expect privacy when using company email systems
- Personal use guidelines and limitations
- Requirements for handling work-related communications on personal devices

2. Data Classification and Handling Requirements

Email policies should include:

- Clear definitions of data sensitivity levels (e.g., public, internal, confidential, restricted)
- Specific handling requirements for each data classification
- Restrictions on forwarding certain classifications of data to personal email accounts
- Encryption requirements for sensitive data

- Retention requirements for different types of communications

3. Implementation Strategies

Resource-Conscious Implementation

Organizations with limited IT resources should consider:

- Phased implementation of security controls
- Cloud-based security solutions with minimal infrastructure requirements
- Clear policies that reduce technical control requirements through behavioral guidelines
- Leveraging free or low-cost security tools designed for small organizations

Volunteer and Board Member Considerations

Policies should include specific guidance for:

- Board member email practices, particularly for sensitive governance communications
- Volunteer email access and appropriate use
- Offboarding procedures for departing volunteers and board members
- Training requirements for all email users, including volunteers and board members

Compliance Risks Specific to Non-Profit Organizations

Non-profit organizations face unique regulatory compliance challenges:

"Non-profit organizations must comply with various regulations regarding data protection, including donor information. Additionally, those receiving government grants or serving vulnerable populations may have specific data handling and privacy compliance requirements." (National Council of Nonprofits, 2024, p. 8)

In Federal Trade Commission v. Toysmart.com, LLC, No. 00-11341-RGS (D. Mass. 2000), the court addressed issues related to the sale of customer information in bankruptcy proceedings, including donor information collected by a company with a privacy policy promising not to share such information. While not specifically about non-profits, this case has implications for non-profits' obligations to protect donor information (Federal Trade Commission v. Toysmart.com, LLC, 2000).

Model Policy: Personal Email Client Usage on Mobile Devices and Personal Computers

1. Policy Purpose and Scope

This policy establishes guidelines for accessing organizational email accounts through personal email clients on mobile devices and personal computers. It applies to all employees, contractors, volunteers, and board members who access organizational email through personal devices or email clients.

2. Definitions

- **Personal Email Client:** Software applications such as Microsoft Outlook, Apple Mail, Gmail app, or similar programs used to access email accounts.
- **Mobile Device:** Smartphones, tablets, and other portable computing devices.
- **Personal Computer:** Any desktop or laptop computer not owned or managed by the organization.
- **Organizational Data:** Any information created, received, or transmitted in the course of organizational business.

3. Authorized Use of Personal Email Clients

3.1 Eligibility for Staff

Staff members may be authorized to access organizational email through personal email clients when:

- Their job responsibilities require email access outside normal business hours
- They frequently work remotely or travel for business purposes
- Their role requires timely response to communications
- They have completed required security training

3.2 Eligibility for Volunteers and Board Members

Volunteers and board members may be authorized to access organizational email through personal email clients when:

- Their role requires regular communication with staff or stakeholders
- They have responsibilities that require timely response to communications

- They have completed required security training
- They have signed the organization's confidentiality agreement

3.3 Approved Email Clients

Only the following email clients are approved for accessing organizational email:

- [List of approved email clients with current versions]
- Other email clients must be approved by the IT department before use

4. Security Requirements

4.1 Device Security

Devices used to access organizational email must:

- Be protected with a strong password, PIN, or biometric authentication
- Have automatic screen locking enabled (maximum 5 minutes of inactivity)
- Maintain current operating system and security updates
- Have malware protection installed and updated (if applicable)
- Be encrypted where technically feasible

4.2 Email Client Configuration

Email clients must be configured to:

- Not cache password/credentials on public or shared computers
- Not automatically download attachments
- Display sender information to help identify phishing attempts
- Support required encryption standards for sensitive communications

4.3 Authentication Requirements

Users must:

- Enable multi-factor authentication for email access where supported
- Use strong, unique passwords for email accounts
- Not share passwords or access credentials
- Change passwords immediately if compromise is suspected

5. Data Protection Measures

5.1 Email Data Handling

Users must:

- Not forward organizational emails containing sensitive information to personal email accounts
- Delete sensitive information from mobile devices when no longer needed
- Not store attachments with sensitive information on personal devices
- Use encrypted connections (SSL/TLS) for email transmission

5.2 Remote Wipe Capability

Users must:

- Consent to remote wiping of organizational data from their personal device if lost or stolen
- Report lost or stolen devices to IT immediately
- Understand that while the organization will attempt to only remove organizational data, a full device wipe may be necessary in some circumstances

6. Compliance and Monitoring

6.1 Monitoring

The organization reserves the right to:

- Monitor all email communications sent or received using organizational email accounts
- Audit compliance with this policy
- Revoke email access privileges for policy violations

6.2 Auditing

The organization will:

- Periodically audit email access and usage patterns
- Review security settings and configurations
- Verify compliance with this policy

7. Responsibilities Upon Separation

7.1 Staff Responsibilities

Upon separation from the organization, staff must:

- Remove organizational accounts from all personal devices
- Delete all locally stored organizational data
- Return any organization-owned devices or accessories
- Maintain confidentiality of information learned during employment

7.2 Volunteer and Board Member Responsibilities

Upon ending their relationship with the organization, volunteers and board members must:

- Remove organizational accounts from all personal devices
- Delete all locally stored organizational data
- Return any organization-owned devices or accessories
- Maintain confidentiality of information learned during service

7.3 Manager Responsibilities

Managers must:

- Notify IT when staff members separate from the organization
- Ensure compliance with separation procedures
- Verify return of any organization-owned equipment

7.4 IT Department Responsibilities

The IT department will:

- Disable email accounts upon notification of separation
- Revoke access to all organizational systems
- Provide guidance on proper data removal if requested

8. Special Considerations for Non-Profit Operations

8.1 Donor Information

Users must:

- Apply heightened protection to donor personally identifiable information
- Not store donor financial information on personal devices
- Encrypt all communications containing donor information where possible
- Comply with donor privacy policies and preferences

8.2 Beneficiary Information

Users must:

- Protect confidential information about program beneficiaries
- Not disclose beneficiary information to unauthorized parties
- Take extra precautions when handling sensitive beneficiary data
- Comply with relevant privacy regulations

8.3 Grant-Related Communications

Users must:

- Maintain records of grant-related communications according to funder requirements
- Ensure grant reporting information is accurately preserved
- Follow specific data handling requirements from grant providers

9. Violations and Enforcement

Violations of this policy may result in:

- Revocation of email access privileges
- Disciplinary action up to and including termination
- Legal action if applicable laws are violated
- For volunteers and board members, removal from position

10. Support and Training

The organization will provide:

- Initial training on secure email usage
- Ongoing security awareness education

- Technical support for approved email client configuration
- Updates on emerging email security threats

11. Policy Exceptions

Exceptions to this policy may be granted:

- Only with written approval from [designated authority]
- For specific business needs that cannot be met otherwise
- With compensating controls to mitigate risks
- For a defined time period with required review

12. Policy Review

This policy will be reviewed:

- Annually at minimum
- Following any significant security incident
- When new threats or vulnerabilities are identified
- When new regulatory requirements emerge

Legal Foundation for Email Management Policies: Federal Framework

Federal Legal Authority for Email Management

Federal law provides private employers, including non-profit organizations, with broad authority to manage email systems and establish protective policies. According to McDonald Hopkins LLC (2018), "Generally, it is permissible for employers to monitor their own computer systems including, but not limited to, employees' work email communications and internet usage. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act (ECPA) controls an employer's liability for intercepting emails."

This federal legal framework enables all organizations, including non-profits, to:

- Monitor all communications on company systems
- Access and review emails sent through company accounts

- Track internet usage on company networks
- Establish and enforce policies regarding proper use of company email systems

Key Federal Laws Governing Email Management

Electronic Communications Privacy Act (ECPA)

The ECPA, which includes the Stored Communications Act (SCA), regulates access to stored electronic communications and prohibits unauthorized access to electronic communications (18 U.S.C. §§ 2510-2523, 2701-2712). However, the law includes important exceptions for:

1. **Business Purpose Exception:** Employers may monitor communications on systems they provide for legitimate business purposes.
2. **Consent Exception:** With proper notice and consent (typically through clear policies), employers may monitor employee communications.

Computer Fraud and Abuse Act (CFAA)

The CFAA (18 U.S.C. § 1030) prohibits unauthorized access to protected computers, which has implications for:

- Employer access to employee personal email accounts
- Employee misuse of company email systems
- Data exfiltration through personal email forwarding

Key Federal Case Law Supporting Employer Email Monitoring Rights

Several significant federal court decisions have reinforced employers' rights to monitor workplace communications:

In *City of Ontario v. Quon*, 560 U.S. 746 (2010), the Supreme Court ruled that a government employer's search of an employee's text messages on a company-provided device was reasonable and did not violate Fourth Amendment protections. The Court noted that "employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated" (p. 760).

In *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), the court recognized that email users maintain a reasonable expectation of privacy in their email content, which can be altered by explicit policies and agreements. This decision underscores the importance of clear email policies that explicitly address privacy expectations.

Federal Regulatory Compliance Considerations

Federal Trade Commission (FTC) Regulations

Under the FTC Act (15 U.S.C. §§ 41-58), the FTC has broad authority to take action against organizations with inadequate data security practices, including email security.

Organizations should be aware that the FTC considers email security measures when evaluating whether a company's data security practices are "unfair" or "deceptive."

Health Insurance Portability and Accountability Act (HIPAA)

"HIPAA's Security Rule requires covered entities to implement technical safeguards to guard electronic protected health information (ePHI) against unauthorized access. This includes controlling access to ePHI through authentication protocols and transmission security measures that protect ePHI when it is being sent over electronic communications networks." (U.S. Department of Health and Human Services, 2023, p. 8)

In *University of Texas MD Anderson Cancer Center v. U.S. Department of Health and Human Services*, 985 F.3d 472 (5th Cir. 2021), the court upheld significant penalties against a healthcare provider for HIPAA violations stemming from unencrypted electronic devices and inadequate data protection policies. The court noted that "HIPAA requires covered entities to implement policies and procedures to prevent, detect, contain, and correct security violations" (*University of Texas MD Anderson Cancer Center v. U.S. Department of Health and Human Services*, 2021, p. 476). This case demonstrates the serious consequences of failing to implement appropriate email security measures in healthcare settings.

When employees forward work emails containing PHI to personal email accounts, they create significant compliance risks:

- Potential violations of the HIPAA Security Rule
- Risk of unauthorized disclosure of PHI
- Possible breach notification requirements
- Exposure to substantial financial penalties
- Damage to organizational reputation

Gramm-Leach-Bliley Act (GLBA)

Financial institutions must comply with the GLBA Safeguards Rule:

"The Safeguards Rule requires financial institutions to develop, implement, and maintain a comprehensive information security program with administrative, technical, and physical safeguards designed to protect customer information." (Federal Trade Commission, 2023, p. 3)

In *Federal Trade Commission v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015), the court affirmed the FTC's authority to enforce data security standards under its unfairness authority. While not specifically about GLBA, this case established the FTC's role in enforcing reasonable data security practices, including proper email security measures (*Federal Trade Commission v. Wyndham Worldwide Corp.*, 2015).

Financial institutions face specific risks when employees use personal email handlers:

- Potential violations of the GLBA Safeguards Rule
- Compromised customer financial information
- Regulatory enforcement actions
- Breach of fiduciary duties
- Loss of customer trust

Sarbanes-Oxley Act (SOX)

Publicly traded companies must comply with SOX requirements:

"Section 404 of the Sarbanes-Oxley Act requires public companies to establish internal controls and procedures for financial reporting and to document, test, and maintain those controls and procedures to ensure their effectiveness." (Securities and Exchange Commission, 2022, p. 12)

In *In re Heartland Payment Systems, Inc. Securities Litigation*, No. 09-1043, 2009 WL 4798148 (D.N.J. Dec. 7, 2009), the court addressed issues related to a company's failure to maintain adequate internal controls over its data security systems. The case highlights the intersection of data security and financial reporting controls required under SOX (*In re Heartland Payment Systems, Inc. Securities Litigation*, 2009).

SOX compliance risks related to personal email handlers include:

- Inadequate internal controls over financial reporting
- Compromised audit trails
- Difficulty demonstrating compliance with record retention requirements
- Potential material weaknesses in internal controls

- Exposure to shareholder litigation

Federal Rules of Civil Procedure (FRCP)

All organizations must comply with electronic discovery requirements:

"Rules 26 and 34 of the Federal Rules of Civil Procedure govern the discovery of electronically stored information (ESI) in federal litigation. Organizations must be able to identify, preserve, and produce relevant electronic communications, including emails, in response to discovery requests." (Administrative Office of the U.S. Courts, 2022, p. 7)

In *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422 (S.D.N.Y. 2004), the court established landmark standards for electronic discovery, including the preservation and production of email communications. The court held that "once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents" (*Zubulake v. UBS Warburg LLC*, 2004, p. 431). This case underscores the importance of maintaining proper control over all business communications, including those that might be stored in personal email accounts.

E-discovery risks related to personal email handlers include:

- Inability to identify and preserve relevant emails
- Failure to produce required communications in litigation
- Potential sanctions for spoliation of evidence
- Increased discovery costs
- Adverse legal outcomes

Industry-Specific Regulatory Requirements

Financial Services Regulations

Financial services firms must comply with additional regulatory requirements:

"FINRA Rule 4511 requires member firms to preserve records in a format and media that complies with Securities Exchange Act Rule 17a-4. Electronic communications related to the firm's business must be retained in a non-rewritable, non-erasable format." (Financial Industry Regulatory Authority, 2023, p. 5)

In *In re: Morgan Stanley Smith Barney Customer Data Security Breach Litigation*, 20 Misc. 2938 (S.D.N.Y. 2020), the court addressed issues related to the improper disposal of

customer data. While focused on hardware decommissioning rather than email, the case highlights the strict data protection requirements in the financial services industry (In re: Morgan Stanley Smith Barney Customer Data Security Breach Litigation, 2020).

Financial services firms face specific compliance challenges:

- SEC and FINRA recordkeeping requirements
- Need to capture and retain all business communications
- Supervision requirements for registered representatives
- Anti-money laundering (AML) compliance concerns
- Customer privacy protection obligations

Educational Institutions and FERPA

Educational institutions must comply with the Family Educational Rights and Privacy Act:

"FERPA protects the privacy of student education records and applies to all schools that receive funds under an applicable program of the U.S. Department of Education. Schools must have written permission from the parent or eligible student to release any information from a student's education record." (U.S. Department of Education, 2023, p. 4)

In *Gonzaga University v. Doe*, 536 U.S. 273 (2002), the Supreme Court addressed FERPA compliance issues, though it focused on whether FERPA creates enforceable rights rather than specific email practices. Nevertheless, the case underscores the importance of protecting student information, including proper email handling (*Gonzaga University v. Doe*, 2002).

Educational institutions face unique email compliance challenges:

- Protection of student educational records
- Parental consent requirements for information disclosure
- Faculty and staff training on FERPA compliance
- Balancing academic freedom with information security
- Managing communications with minors

State-Level Regulations Affecting Email Management

State Data Breach Notification Laws

Please see Appendix A for details.

Organizations must comply with state-specific data breach notification requirements:

"All 50 states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information. These laws typically define 'personal information' as an individual's name combined with other identifying information such as Social Security number, driver's license number, or financial account information." (National Conference of State Legislatures, 2023, p. 2)

In *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015), the court addressed issues related to a data breach and the company's notification obligations. The case established an important precedent regarding standing in data breach cases and highlighted the legal consequences of inadequate data security measures (*Remijas v. Neiman Marcus Group, LLC*, 2015).

State data breach laws create specific compliance challenges:

- Varying definitions of personal information across states
- Different notification timeframes and requirements
- Potential for multi-state enforcement actions
- Documentation requirements for breach response
- Penalties for failure to notify affected individuals

International Regulations with Extraterritorial Reach

General Data Protection Regulation (GDPR)

Organizations handling EU resident data must comply with GDPR:

"The GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or processor in the European Union, regardless of whether the processing takes place in the EU or not. The GDPR also applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the processing activities relate to offering goods or services to EU data subjects or monitoring their behavior within the EU." (European Data Protection Board, 2023, p. 6)

In *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems* (Schrems II), Case C-311/18 (Court of Justice of the European Union, July 16, 2020), the Court of Justice of the European Union invalidated the EU-US Privacy Shield. It imposed strict

requirements for international data transfers. This case has significant implications for email systems that may transfer EU resident data across borders (Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems, 2020).

GDPR compliance challenges related to email management include:

- Data subject access rights for information in emails
- Data minimization requirements for email content
- Lawful basis requirements for processing personal data
- International data transfer restrictions
- Potential for significant administrative fines

Conclusion: A Balanced Approach to Email Security

Developing comprehensive email policies requires balancing security requirements with practical operational needs. By focusing on federal legal requirements, clear communication of expectations, appropriate technical controls, and ongoing training, organizations can significantly reduce the risks associated with personal email handlers while maintaining productivity.

These policies must be particularly sensitive to limited resources, volunteer workforces, and unique data protection needs for non-profit organizations. By implementing the guidelines outlined in this document, non-profits can protect sensitive information, maintain regulatory compliance, and preserve stakeholder trust.

References

Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1986).

City of Ontario v. Quon, 560 U.S. 746 (2010).

Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2523, 2701-2712 (1986).

Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (1914).

Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809 (1999).

Information Systems Audit and Control Association. (2023). *Shadow IT risk management: Best practices for securing the digital enterprise*. ISACA Press.

McDonald Hopkins LLC. (2018). *Employer guide to monitoring employee communications*. McDonald Hopkins LLC.

Non-Profit Technology Network. (2023). *State of nonprofit cybersecurity report*. NTEN.

University of Texas MD Anderson Cancer Center v. U.S. Department of Health and Human Services, 985 F.3d 472 (5th Cir. 2021).

U.S. Department of Health and Human Services. (2023). *HIPAA security guidance*. HHS Office for Civil Rights.

United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

Appendix A: State-Specific Email Policy Requirements for Private Organizations and Non-Profits

This appendix provides an overview of state-specific laws, regulations, and case law that affect organizational email policies, with special considerations for non-profit organizations. Organizations should consult with legal counsel familiar with the specific requirements of states in which they operate.

Federal Non-Profit Considerations

Tax-Exempt Status Implications

Non-profits must consider how email management relates to maintaining tax-exempt status:

The Internal Revenue Service requires 501(c)(3) organizations to use assets primarily for exempt purposes (Internal Revenue Code, 26 U.S.C. § 501(c)(3), 2018). Improper email usage that furthers private interests could jeopardize tax-exempt status.

In *United Cancer Council, Inc. v. Commissioner*, 165 F.3d 1173 (7th Cir. 1999), the court examined how a non-profit's communications and operations must be structured to maintain tax-exempt status.

Federal Grant Requirements

Non-profits receiving federal grants must consider specific email management requirements:

The Office of Management and Budget's Uniform Guidance imposes record-keeping requirements that affect email retention for federally-funded programs (2 C.F.R. § 200, 2014).

In *Maricopa County v. Office of Management and Budget*, 207 F. Supp. 3d 1044 (D. Ariz. 2016), the court upheld federal agencies' authority to impose documentation and record-keeping requirements on grant recipients.

Alabama

Alabama does not have specific state laws governing workplace email monitoring beyond federal regulations. However, organizations should be aware of the Alabama Data Breach Notification Act of 2018, which requires notification of security breaches involving personal information (Alabama Data Breach Notification Act, Ala. Code §§ 8-38-1 to 8-38-12, 2018).

Non-profit Considerations: Alabama non-profits must comply with the Alabama Nonprofit Corporation Law, which establishes record-keeping requirements that may affect email retention policies (Ala. Code §§ 10A-3-1.01 to 10A-3-8.02, 2009).

Alaska

Alaska follows federal guidelines for workplace monitoring. The Alaska Personal Information Protection Act requires businesses to implement reasonable security procedures to protect personal information and notify affected individuals of data breaches (Alaska Stat. §§ 45.48.010 to 45.48.995, 2009).

Non-profit Considerations: Alaska non-profits must comply with the Alaska Nonprofit Corporation Act, which establishes record-keeping requirements (Alaska Stat. §§ 10.20.005 to 10.20.725, 1968).

Arizona

Arizona's data breach notification law requires businesses to notify individuals when their personal information has been compromised, which may include breaches through email systems (Ariz. Rev. Stat. §§ 18-551 to 18-552, 2006). Arizona does not have specific laws restricting employer monitoring of workplace email.

Non-profit Considerations: In *Maricopa County v. Office of Management and Budget*, 207 F. Supp. 3d 1044 (D. Ariz. 2016), the court addressed record-keeping requirements for organizations receiving federal funds, which has implications for non-profit email retention policies.

Arkansas

Arkansas follows federal standards for workplace monitoring. The Personal Information Protection Act requires notification of security breaches involving personal information (Ark. Code Ann. §§ 4-110-101 to 4-110-108, 2005). Organizations should ensure email policies comply with these breach notification requirements.

Non-profit Considerations: Arkansas non-profits must comply with the Arkansas Nonprofit Corporation Act, which establishes record-keeping requirements (Ark. Code Ann. §§ 4-33-101 to 4-33-1707, 1993).

California

California has extensive privacy laws affecting email policies:

The California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) grant consumers rights regarding their personal information (Cal. Civ. Code §§ 1798.100 to 1798.199.100, 2018, 2020).

The California Electronic Communications Privacy Act restricts government access to electronic communications but generally does not limit private employer monitoring of company systems (Cal. Penal Code §§ 1546 to 1546.4, 2015).

California Labor Code § 980 prohibits employers from requiring employees to disclose personal social media account information but does not restrict monitoring of company email systems (Cal. Lab. Code § 980, 2012).

Non-profit Considerations: The California Nonprofit Integrity Act imposes specific governance and financial transparency requirements that affect record-keeping, including email communications (Cal. Gov't Code § 12580-12599.8, 2004).

In *People v. Orange County Charitable Services*, 73 Cal. App. 4th 1054 (1999), the court emphasized non-profits' obligations to maintain proper records of solicitations and donor communications.

California's Supervision of Trustees and Fundraisers for Charitable Purposes Act requires specific record-keeping for charitable organizations (Cal. Gov't Code §§ 12580-12599.8, 2004).

Colorado

Colorado's data breach notification law requires notification when personal information is compromised (Colo. Rev. Stat. § 6-1-716, 2006, amended 2018). The Colorado Privacy Act, effective July 1, 2023, establishes additional consumer privacy rights that may affect how organizations handle personal information in emails (Colo. Rev. Stat. §§ 6-1-1301 to 6-1-1313, 2021).

Non-profit Considerations: The Colorado Charitable Solicitations Act imposes record-keeping requirements on charitable organizations (Colo. Rev. Stat. §§ 6-16-101 to 6-16-114, 1988).

In *Stern v. Lucy Webb Hayes National Training School for Deaconesses and Missionaries*, 381 F. Supp. 1003 (D.D.C. 1974), the court established standards for non-profit board governance that affect communication practices (cited in Colorado cases).

Connecticut

Connecticut's data breach notification law requires businesses to notify residents when their personal information is compromised (Conn. Gen. Stat. § 36a-701b, 2005).

Connecticut also enacted the Connecticut Data Privacy Act (CTDPA), effective July 1, 2023, which establishes consumer rights regarding personal data (Conn. Gen. Stat. §§ 42-516 to 42-525, 2022).

Non-profit Considerations: Connecticut non-profits must comply with the Connecticut Revised Nonstock Corporation Act, which establishes record-keeping requirements (Conn. Gen. Stat. §§ 33-1000 to 33-1290, 1959).

Delaware

Delaware's data breach notification law requires notification of security breaches involving personal information (Del. Code Ann. tit. 6, §§ 12B-101 to 12B-104, 2005). The Delaware Online Privacy and Protection Act regulates privacy policies but does not specifically address workplace email monitoring (Del. Code Ann. tit. 6, §§ 1201C to 1206C, 2015).

Non-profit Considerations: Delaware non-profits must comply with the Delaware General Corporation Law as it applies to non-profit corporations, which establishes record-keeping requirements (Del. Code Ann. tit. 8, §§ 101 to 398, 1953).

Florida

Florida's data breach notification law, the Florida Information Protection Act, requires notification of security breaches involving personal information (Fla. Stat. § 501.171, 2014). Florida does not have specific laws restricting employer monitoring of workplace email beyond federal standards.

Non-profit Considerations: The Florida Solicitation of Contributions Act requires charitable organizations to maintain records of solicitations and donor communications (Fla. Stat. §§ 496.401-496.424, 1991).

In *Stein v. Paradigm Mirasol, LLC*, 586 F.3d 849 (11th Cir. 2009), the court addressed issues of electronic discovery that have implications for non-profit record-keeping.

Georgia

Georgia's data breach notification law requires notification of security breaches involving personal information (Ga. Code Ann. §§ 10-1-910 to 10-1-912, 2005). Georgia follows federal guidelines for workplace monitoring and does not impose additional restrictions on employer email monitoring.

Non-profit Considerations: Georgia non-profits must comply with the Georgia Nonprofit Corporation Code, which establishes record-keeping requirements (Ga. Code Ann. §§ 14-3-101 to 14-3-1703, 1991).

Hawaii

Hawaii's data breach notification law requires businesses to notify individuals of security breaches involving personal information (Haw. Rev. Stat. §§ 487N-1 to 487N-7, 2006). Hawaii does not have specific laws restricting employer monitoring of workplace email beyond federal standards.

Non-profit Considerations: Hawaii non-profits must comply with the Hawaii Nonprofit Corporations Act, which establishes record-keeping requirements (Haw. Rev. Stat. §§ 414D-1 to 414D-324, 2001).

Idaho

Idaho's data breach notification law requires notification of security breaches involving personal information (Idaho Code §§ 28-51-104 to 28-51-107, 2006). Idaho follows federal guidelines for workplace monitoring and does not impose additional restrictions on employer email monitoring.

Non-profit Considerations: Idaho non-profits must comply with the Idaho Nonprofit Corporation Act, which establishes record-keeping requirements (Idaho Code §§ 30-30-101 to 30-30-1204, 1993).

Illinois

Illinois has several laws affecting email policies:

The Personal Information Protection Act requires notification of security breaches involving personal information (815 Ill. Comp. Stat. 530/1 to 530/50, 2005).

The Right to Privacy in the Workplace Act restricts employer access to employees' personal online accounts but generally does not limit monitoring of company email systems (820 Ill. Comp. Stat. 55/10, 2013).

The Biometric Information Privacy Act regulates the collection and use of biometric identifiers, which may affect email authentication methods (740 Ill. Comp. Stat. 14/1 to 14/99, 2008).

Non-profit Considerations: In *Ferris, Thompson & Zweig, Ltd. v. Esposito*, 2017 IL 121297, the Illinois Supreme Court addressed issues of attorney-client privilege in electronic communications that have implications for non-profit legal counsel communications.

The Illinois Charitable Trust Act imposes record-keeping requirements on charitable organizations (760 Ill. Comp. Stat. 55/1 to 55/19, 1961).

Indiana

Indiana's data breach notification law requires notification of security breaches involving personal information (Ind. Code §§ 24-4.9-1-1 to 24-4.9-5-1, 2006). Indiana does not have specific laws restricting employer monitoring of workplace email beyond federal standards.

Non-profit Considerations: Indiana non-profits must comply with the Indiana Nonprofit Corporation Act, which establishes record-keeping requirements (Ind. Code §§ 23-17-1-1 to 23-17-31-2, 1991).

Iowa

Iowa's data breach notification law requires notification of security breaches involving personal information (Iowa Code §§ 715C.1 to 715C.2, 2008). Iowa follows federal guidelines for workplace monitoring and does not impose additional restrictions on employer email monitoring.

Non-profit Considerations: Iowa non-profits must comply with the Iowa Nonprofit Corporation Act, which establishes record-keeping requirements (Iowa Code §§ 504.101 to 504.1705, 2004).

Kansas

Kansas's data breach notification law requires notification of security breaches involving personal information (Kan. Stat. Ann. §§ 50-7a01 to 50-7a04, 2006). Kansas does not have specific laws restricting employer monitoring of workplace email beyond federal standards.

Non-profit Considerations: Kansas non-profits must comply with the Kansas General Corporation Code as it applies to non-profit corporations, which establishes record-keeping requirements (Kan. Stat. Ann. §§ 17-6001 to 17-6010, 2016).

Kentucky

Kentucky's data breach notification law requires notification of security breaches involving personal information (Ky. Rev. Stat. Ann. §§ 365.732, 365.734, 2014). Kentucky follows federal guidelines for workplace monitoring and does not impose additional restrictions on employer email monitoring.

Non-profit Considerations: Kentucky non-profits must comply with the Kentucky Nonprofit Corporation Acts, which establishes record-keeping requirements (Ky. Rev. Stat. Ann. §§ 273.161 to 273.405, 1968).

Louisiana

Louisiana's Database Security Breach Notification Law requires notification of security breaches involving personal information (La. Rev. Stat. Ann. §§ 51:3071 to 51:3077, 2005). Louisiana does not have specific laws restricting employer monitoring of workplace email beyond federal standards.

Non-profit Considerations: Louisiana non-profits must comply with the Louisiana Nonprofit Corporation Law, which establishes record-keeping requirements (La. Rev. Stat. Ann. §§ 12:201 to 12:269, 1968).

Maine

Maine's Notice of Risk to Personal Data Act requires notification of security breaches involving personal information (Me. Rev. Stat. tit. 10, §§ 1346 to 1350-B, 2005). Maine also enacted the Act to Protect the Privacy of Online Consumer Information, which imposes privacy obligations on internet service providers but does not directly address workplace email monitoring (Me. Rev. Stat. tit. 35-A, §§ 9301 to 9303, 2019).

Non-profit Considerations: Maine non-profits must comply with the Maine Nonprofit Corporation Act, which establishes record-keeping requirements (Me. Rev. Stat. tit. 13-B, §§ 101 to 1406, 1977).

Maryland

Maryland's Personal Information Protection Act requires businesses to implement reasonable security procedures and notify individuals of data breaches (Md. Code Ann., Com. Law §§ 14-3501 to 14-3508, 2008). Maryland does not have specific laws restricting employer monitoring of workplace email beyond federal standards.

Non-profit Considerations: Maryland non-profits must comply with the Maryland Corporations and Associations Code as it applies to non-profit corporations, which establishes record-keeping requirements (Md. Code Ann., Corps. & Ass'ns §§ 5-201 to 5-208, 1975).

Massachusetts

Massachusetts has stringent data security regulations that affect email policies:

The Standards for the Protection of Personal Information require businesses to develop comprehensive information security programs (201 Mass. Code Regs. 17.01 to 17.05, 2010).

Massachusetts data breach notification law requires notification of security breaches involving personal information (Mass. Gen. Laws ch. 93H, §§ 1 to 6, 2007).

Non-profit Considerations: Massachusetts regulations require charitable organizations to maintain proper records of solicitations and donor communications (940 Mass. Code Regs. 5.00, 2021).

In *Commonwealth v. Fremont Investment & Loan*, 452 Mass. 733 (2008), the court established standards for record-keeping that apply to all organizations, including non-profits.

Michigan

Michigan's Identity Theft Protection Act requires notification of security breaches involving personal information (Mich. Comp. Laws §§ 445.63 to 445.79d, 2004). Michigan does not have specific laws restricting employer monitoring of workplace email beyond federal standards.

Non-profit Considerations: The Charitable Organizations and Solicitations Act imposes record-keeping requirements on charitable organizations (Mich. Comp. Laws §§ 400.271-400.294, 1975).

In *People v. Attorney General*, 819 N.W.2d 441 (Mich. Ct. App. 2012), the court addressed issues of charitable organization oversight that affect communication and record-keeping practices.

Minnesota

Minnesota's data breach notification law requires notification of security breaches involving personal information (Minn. Stat. §§ 325E.61, 325E.64, 2005). Minnesota does

not have specific laws restricting employer monitoring of workplace email beyond federal standards.

Non-profit Considerations: The Minnesota Charitable Organization Act imposes record-keeping requirements on charitable organizations (Minn. Stat. §§ 309.50-309.61, 1961).

In *Minnesota v. Fleet Mortgage Corp.*, 158 F. Supp. 2d 962 (D. Minn. 2001), the court addressed consumer protection issues that affect non-profit communications with beneficiaries.

Mississippi

Mississippi's data breach notification law requires notification of security breaches involving personal information (Miss. Code Ann. § 75-24-29, 2010). Mississippi follows federal guidelines for workplace monitoring and does not impose additional restrictions on employer email monitoring.

Non-profit Considerations: Mississippi non-profits must comply with the Mississippi Nonprofit Corporation Act, which establishes record-keeping requirements (Miss. Code Ann. §§ 79-11-101 to 79-11-405, 1987).

Missouri

Missouri's data breach notification law requires notification of security breaches involving personal information (Mo. Rev. Stat. § 407.1500, 2009). Missouri does not have specific laws restricting employer monitoring of workplace email beyond federal standards.

Non-profit Considerations: Missouri non-profits must comply with the Missouri Nonprofit Corporation Act, which establishes record-keeping requirements (Mo. Rev. Stat. §§ 355.001 to 355.881, 1995).

Montana

Montana's data breach notification law requires notification of security breaches involving personal information (Mont. Code Ann. §§ 30-14-1701 to 30-14-1705, 2005). Montana does not have specific laws restricting employer monitoring of workplace email beyond federal standards.

Non-profit Considerations: Montana non-profits must comply with the Montana Nonprofit Corporation Act, which establishes record-keeping requirements (Mont. Code Ann. §§ 35-2-113 to 35-2-1402, 1991).

Nebraska

Nebraska's data breach notification law, the Financial Data Protection and Consumer Notification of Data Security Breach Act, requires notification of security breaches involving personal information (Neb. Rev. Stat. §§ 87-801 to 87-807, 2006). Nebraska follows federal guidelines for workplace monitoring.

Non-profit Considerations: Nebraska non-profits must comply with the Nebraska Nonprofit Corporation Act, which establishes record-keeping requirements (Neb. Rev. Stat. §§ 21-1901 to 21-19,177, 1996).

Nevada

Nevada has several laws affecting email policies:

Nevada's data breach notification law requires notification of security breaches involving personal information (Nev. Rev. Stat. §§ 603A.010 to 603A.290, 2005).

Nevada requires businesses that collect personal information online to post a privacy policy (Nev. Rev. Stat. §§ 603A.300 to 603A.360, 2017).

Nevada's online privacy law allows consumers to opt out of the sale of their personal information (Nev. Rev. Stat. § 603A.345, 2019).

Non-profit Considerations: Nevada non-profits must comply with the Nevada Nonprofit Corporation Act, which establishes record-keeping requirements (Nev. Rev. Stat. §§ 82.006 to 82.546, 1991).

New Hampshire

New Hampshire's Notice of Security Breach Protection Act requires notification of security breaches involving personal information (N.H. Rev. Stat. Ann. §§ 359-C:19 to 359-C:21, 2006). New Hampshire does not have specific laws restricting employer monitoring of workplace email beyond federal standards.

Non-profit Considerations: New Hampshire non-profits must comply with the New Hampshire Voluntary Corporations and Associations law, which establishes record-keeping requirements (N.H. Rev. Stat. Ann. §§ 292:1 to 292:31, 1975).

New Jersey

New Jersey's Identity Theft Prevention Act requires businesses to notify individuals of security breaches involving personal information (N.J. Stat. Ann. §§ 56:8-161 to 56:8-166, 2005). New Jersey does not have specific laws restricting employer monitoring of workplace email beyond federal standards.

Non-profit Considerations: New Jersey non-profits must comply with the New Jersey Nonprofit Corporation Act, which establishes record-keeping requirements (N.J. Stat. Ann. §§ 15A:1-1 to 15A:16-2, 1983).

New Mexico

New Mexico's Data Breach Notification Act requires notification of security breaches involving personal information (N.M. Stat. Ann. §§ 57-12C-1 to 57-12C-12, 2017). New Mexico follows federal guidelines for workplace monitoring and does not impose additional restrictions on employer email monitoring.

Non-profit Considerations: New Mexico non-profits must comply with the New Mexico Nonprofit Corporation Act, which establishes record-keeping requirements (N.M. Stat. Ann. §§ 53-8-1 to 53-8-99, 1975).

New York

New York has comprehensive data security laws:

The SHIELD Act requires businesses to implement reasonable safeguards to protect personal information and expands data breach notification requirements (N.Y. Gen. Bus. Law § 899-aa, 899-bb, 2019).

The Stop Hacks and Improve Electronic Data Security (SHIELD) Act requires businesses to develop, implement, and maintain reasonable safeguards to protect the security of private information (N.Y. Gen. Bus. Law § 899-bb, 2019).

Non-profit Considerations: The New York Non-Profit Revitalization Act requires non-profits to implement specific governance practices, including conflict of interest policies and whistleblower protections, which affect email communications and record-keeping (N.Y. Not-for-Profit Corp. Law §§ 715-a, 715-b, 2013).

In *People v. Grasso*, 54 A.D.3d 180 (N.Y. App. Div. 2008), the court addressed non-profit governance issues that highlight the importance of proper documentation and communication practices.

The New York Nonprofit Revitalization Act specifically addresses electronic communication for board meetings and governance matters (N.Y. Not-for-Profit Corp. Law § 708, 2013).

North Carolina

North Carolina's Identity Theft Protection Act requires notification of security breaches involving personal information (N.C. Gen. Stat. §§ 75-61 to 75-66, 2005). North

Carolina does not have specific laws restricting employer monitoring of workplace email beyond federal standards.

Non-profit Considerations: North Carolina non-profits must comply with the North Carolina Nonprofit Corporation Act, which establishes record-keeping requirements (N.C. Gen. Stat. §§ 55A-1-01 to 55A-17-05, 1993).

North Dakota

North Dakota's data breach notification law requires notification of security breaches involving personal information (N.D. Cent. Code §§ 51-30-01 to 51-30-07, 2005). North Dakota does not have specific laws restricting employer monitoring of workplace email beyond federal standards.

Non-profit Considerations: North Dakota non-profits must comply with the North Dakota Nonprofit Corporation Act, which establishes record-keeping requirements (N.D. Cent. Code §§ 10-33-01 to 10-33-149, 1997).

Ohio

Ohio's data breach notification law requires notification of security breaches involving personal information (Ohio Rev. Code Ann. § 1349.19, 2005). The Ohio Data Protection Act provides a legal safe harbor for businesses that implement a cybersecurity program that meets certain standards (Ohio Rev. Code Ann. §§ 1354.01 to 1354.05, 2018).

Non-profit Considerations: The Ohio Charitable Organizations Act imposes record-keeping requirements on charitable organizations (Ohio Rev. Code §§ 1716.01-1716.99, 1976).

In *Lujan v. Gordon Food Service, Inc.*, 2016 WL 3190600 (N.D. Ohio 2016), the court addressed electronic communications issues relevant to organizational record-keeping.

Oklahoma

Oklahoma's Security Breach Notification Act requires notification of security breaches involving personal information (Okla. Stat. tit. 24, §§ 161 to 166, 2008). Oklahoma does not have specific laws restricting employer monitoring of workplace email beyond federal standards.

Non-profit Considerations: Oklahoma non-profits must comply with the Oklahoma General Corporation Act as it applies to non-profit corporations, which establishes record-keeping requirements (Okla. Stat. tit. 18, §§ 1001 to 1144, 1986).

Oregon

Oregon's Consumer Information Protection Act requires notification of security breaches involving personal information (Or. Rev. Stat. §§ 646A.600 to 646A.628, 2007). Oregon does not have specific laws restricting employer monitoring of workplace email beyond federal standards.

Non-profit Considerations: The Charitable Trust and Corporation Act imposes record-keeping requirements on charitable organizations (Or. Rev. Stat. §§ 128.610-128.750, 1971).

In *In re Lovell*, 319 Or. 520 (1994), the court addressed fiduciary duty issues that affect non-profit board communications.

Pennsylvania

Pennsylvania's Breach of Personal Information Notification Act requires notification of security breaches involving personal information (73 Pa. Cons. Stat. §§ 2301 to 2329, 2005). Pennsylvania does not have specific laws restricting employer monitoring of workplace email beyond federal standards.

Non-profit Considerations: The Pennsylvania Solicitation of Funds for Charitable Purposes Act imposes record-keeping requirements on charitable organizations (10 P.S. §§ 162.1-162.24, 1990).

In *Commonwealth v. Citizens Alliance for Better Neighborhoods*, 983 A.2d 1274 (Pa. Commw. Ct. 2009), the court addressed issues of non-profit governance and transparency that affect communication practices.

Rhode Island

Rhode Island's Identity Theft Protection Act requires businesses to implement reasonable security procedures and notify individuals of data breaches (R.I. Gen. Laws §§ 11-49.3-1 to 11-49.3-6, 2015). Rhode Island does not have specific laws restricting employer monitoring of workplace email beyond federal standards.

Non-profit Considerations: Rhode Island non-profits must comply with the Rhode Island Nonprofit Corporation Act, which establishes record-keeping requirements (R.I. Gen. Laws §§ 7-6-1 to 7-6-94, 1984).

South Carolina

South Carolina's Financial Identity Fraud and Identity Theft Protection Act requires notification of security breaches involving personal information (S.C. Code Ann. §§ 37-20-110 to 37-20-200, 2008). South Carolina does not have specific laws restricting employer monitoring of workplace email beyond federal standards.

Non-profit Considerations: South Carolina non-profits must comply with the South Carolina Nonprofit Corporation Act, which establishes record-keeping requirements (S.C. Code Ann. §§ 33-31-101 to 33-31-1708, 1994).

South Dakota

South Dakota's data breach notification law requires notification of security breaches involving personal information (S.D. Codified Laws §§ 22-40-19 to 22-40-26, 2018).

South Dakota follows federal guidelines for workplace monitoring and does not impose additional restrictions on employer email monitoring.

Non-profit Considerations: South Dakota non-profits must comply with the South Dakota Nonprofit Corporation Act, which establishes record-keeping requirements (S.D. Codified Laws §§ 47-22-1 to 47-22-78, 1965).

Tennessee

Tennessee's Identity Theft Deterrence Act requires notification of security breaches involving personal information (Tenn. Code Ann. §§ 47-18-2107, 2005). Tennessee does not have specific laws restricting employer monitoring of workplace email beyond federal standards.

Non-profit Considerations: Tennessee non-profits must comply with the Tennessee Nonprofit Corporation Act, which establishes record-keeping requirements (Tenn. Code Ann. §§ 48-51-101 to 48-68-105, 1987).

Texas

Texas's data breach notification law requires notification of security breaches involving personal information (Tex. Bus. & Com. Code Ann. §§ 521.002, 521.053, 2009). Texas follows federal guidelines for workplace monitoring and does not impose additional restrictions on employer email monitoring.

Non-profit Considerations: The Texas Non-Profit Corporation Act addresses record-keeping requirements for non-profit corporations (Tex. Bus. Orgs. Code § 22.001 et seq., 2006).

In *Gearhart Industries, Inc. v. Smith International, Inc.*, 741 F.2d 707 (5th Cir. 1984), the court established fiduciary duty standards that affect board communications in non-profit contexts.

Utah

Utah's Protection of Personal Information Act requires notification of security breaches involving personal information (Utah Code Ann. §§ 13-44-101 to 13-44-301, 2006). The Utah Consumer Privacy Act, effective December 31, 2023, establishes consumer rights regarding personal data (Utah Code Ann. §§ 13-61-101 to 13-61-404, 2022).

Non-profit Considerations: Utah non-profits must comply with the Utah Revised Nonprofit Corporation Act, which establishes record-keeping requirements (Utah Code Ann. §§ 16-6a-101 to 16-6a-1705, 2000).

Vermont

Vermont's Security Breach Notice Act requires notification of security breaches involving personal information (Vt. Stat. Ann. tit. 9, §§ 2430 to 2435, 2006). Vermont does not have specific laws restricting employer monitoring of workplace email beyond federal standards.

Non-profit Considerations: Vermont non-profits must comply with the Vermont Nonprofit Corporation Act, which establishes record-keeping requirements (Vt. Stat. Ann. tit. 11B, §§ 1.01 to 17.05, 1996).

Virginia

Virginia enacted the Consumer Data Protection Act (CDPA), effective January 1, 2023, which establishes consumer rights regarding personal data (Va. Code Ann. §§ 59.1-575 to 59.1-585, 2021). Virginia's data breach notification law requires notification of security breaches involving personal information (Va. Code Ann. § 18.2-186.6, 2008).

Non-profit Considerations: The Virginia Solicitation of Contributions Law imposes record-keeping requirements on charitable organizations (Va. Code Ann. §§ 57-48 to 57-69, 1974).

In *Williams v. Dominion Technology Partners, L.L.C.*, 265 Va. 280 (2003), the court addressed electronic discovery issues relevant to organizational record-keeping.

Washington

Washington's data breach notification law requires notification of security breaches involving personal information (Wash. Rev. Code §§ 19.255.010 to 19.255.900, 2005). The Washington Privacy Act establishes consumer rights regarding personal data (Wash. Rev. Code §§ 19.375.010 to 19.375.900, 2023).

Non-profit Considerations: The Charitable Solicitations Act imposes record-keeping requirements on charitable organizations (Wash. Rev. Code §§ 19.09.010-19.09.915, 1973).

In *State v. Breast Cancer Prevention Fund*, 151 Wn. App. 861 (2009), the court addressed issues of charitable solicitation that affect email communications with donors.

West Virginia

West Virginia's data breach notification law requires notification of security breaches involving personal information (W. Va. Code §§ 46A-2A-101 to 46A-2A-105, 2008). West Virginia does not have specific laws restricting employer monitoring of workplace email beyond federal standards.

Non-profit Considerations: West Virginia non-profits must comply with the West Virginia Nonprofit Corporation Act, which establishes record-keeping requirements (W. Va. Code §§ 31E-1-101 to 31E-16-1603, 2002).

Wisconsin

Wisconsin's data breach notification law requires notification of security breaches involving personal information (Wis. Stat. § 134.98, 2006). Wisconsin does not have specific laws restricting employer monitoring of workplace email beyond federal standards.

Non-profit Considerations: Wisconsin non-profits must comply with the Wisconsin Nonstock Corporation Law, which establishes record-keeping requirements (Wis. Stat. §§ 181.0103 to 181.1703, 1997).

Wyoming

Wyoming's data breach notification law requires notification of security breaches involving personal information (Wyo. Stat. Ann. §§ 40-12-501).