The ultimate email compliance checklist for IT professionals

Are your email systems meeting compliance standards?

Email compliance is an essential aspect of data privacy and security. As an IT professional, you play a crucial role in ensuring that your organization's email systems comply with various regulations. Compliance not only protects sensitive information but also helps to prevent costly legal issues.

Maintain email compliance effortlessly with this practical, IT-approved checklist.

Exclaimer

exclaimer.com

01 Assessing email compliance requirements

Risk assessment:

□ Conduct a risk assessment to identify vulnerabilities in email practices.

□ Map data flows to understand storage, transmission, and processing locations.

□ Collaborate with legal teams to determine relevant compliance laws.

□ Establish data retention periods based on applicable regulations.

Regulatory compliance:

□ Identify and stay updated on applicable industry and location-specific regulations.

□ Ensure compliance with regulatory standards:

- **North America:** CAN-SPAM, GLBA, HIPAA, SOX, CASL, FRCP
- **Europe:** GDPR, PECR
- **Global:** PCI DSS

□ Maintain documented compliance guidelines and communicate them to employees.

□ Appoint a Compliance/Data Protection Officer (DPO) responsible for oversight.

02 Vendor & third-party compliance

Vendor security compliance:

□ Ensure third-party email service providers adhere to compliance standards.

□ Include data protection clauses in vendor contracts and conduct regular audits.

□ Require compliance documentation (e.g., SOC 2 Type II reports).

Risk assessment & auditing:

□ Evaluate risks posed by third-party vendors and update assessments regularly.

□ Establish monitoring systems to track vendor security practices.

□ Review service level agreements (SLAs) for security and compliance obligations.

03 Implementing email security measures

Server & access security:

□ Configure secure email servers with encryption for incoming/outgoing emails.

□ Require strong passwords, regular updates, and two-factor authentication (2FA).

□ Limit access to sensitive data with strict role-based controls.

Threat prevention:

□ Deploy Secure Email Gateways (SEGs) to filter malicious emails.

□ Encrypt sensitive emails and implement secure file-sharing policies.

□ Conduct regular audits on admin privileges and account security.

04 Data protection & privacy

Transparency & consent:

□ Create an acceptable use policy and set rules for email and data handling.

□ Clearly disclose data collection, usage, and retention policies.

□ Obtain necessary consent with opt-in/out options.

□ Maintain a secure and compliant email list.

Security measures:

□ Encrypt emails containing personal or sensitive data.

□ Enforce TLS encryption and regularly update security protocols.

□ Use Data Loss Prevention (DLP) tools to prevent data leaks.

User rights & compliance:

□ Implement a process for Data Subject Access Requests (DSARs).

□ Allow users to request data deletion or anonymization as per compliance laws.

□ Regularly clean CRM databases to remove outdated records.

05 Data retention & archiving practices

Retention & backup policies:

- □ Define retention periods for different email data categories.
- □ Implement automatic email archiving and ensure data accessibility for audits.
- □ Conduct regular encrypted backups, stored securely off-site.

Monitoring & compliance:

- □ Monitor email traffic for compliance violations (e.g., unauthorized data sharing).
- □ Ensure policies dictate what data should be archived, retained, or deleted.

06 Email filtering & threat protection

Anti-phishing & anti-malware:

- □ Configure DKIM, SPF, and DMARC to authenticate email sources.
- □ Implement real-time spam and phishing detection with regular updates.
- □ Scan all incoming emails and attachments for malware.
- □ Enable advanced malware protection by using sandboxing for attachments and URLs.
- □ Block risky attachments and quarantine potential threats.

Incident management:

- □ Enable alerts for suspicious activity (e.g., multiple failed logins, data exfiltration).
- □ Detect unauthorized logins and automatically lock accounts after multiple failed attempts.
- □ Establish protocols for reporting and investigating email security incidents.

07 User awareness & training

Employee security training:

□ Conduct regular training on email security, phishing awareness, and compliance.

□ Implement simulated phishing campaigns to test employee responses.

□ Enforce strong password management practices, including MFA usage.

Incident response preparedness:

□ Train employees on reporting security breaches and suspicious emails.

□ Establish clear incident response procedures and escalation pathways.

08 Email monitoring, logging, & auditing

Email activity tracking:

□ Log and monitor email activities, including sending, receiving, and deletion.

□ Implement real-time alerts for unusual email behaviors.

□ Use monitoring tools to detect compliance violations or security threats.

Regular audits & reviews:

□ Conduct periodic internal compliance reviews and security audits.

□ Maintain documentation for compliance verification and regulatory reporting.

09 Business continuity & disaster recovery

Backup & recovery plans:

□ Ensure robust email backup and recovery solutions are in place.
□ Regularly test backup restorations and disaster recovery plans.
□ Review third-party email providers' disaster recovery protocols.

Emergency communication plans:

□ Develop alternative communication channels in case of email system failure.
□ Regularly evaluate risks and update contingency strategies.

10 Legal hold & eDiscovery

Retention for legal purposes:

□ Ensure emails are retrievable for legal investigations.
□ Define processes for responding to legal requests.

Recommended security solutions

- **Anti-spam & anti-phishing tools:** Implement DKIM, SPF, and DMARC.
- **Advanced malware protection:** Scan emails and attachments for threats.
- **Attachment management tools:** Block and quarantine malicious files.
- **Data Loss Prevention (DLP) systems:** Prevent unauthorized data sharing.
- **Email encryption tools:** Secure sensitive communications.
- **Email archiving software:** Ensure retention compliance.
- **Email signature management:** Standardize email signatures.

Get a demo of Exclaimer
and see how it can help
your email compliance.