ESPC
Email Sender & Provider Coalition

ESPC Information Security Best Practices

ESPC Member Companies (“Members” or “Companies”) believe that strong information security practices are essential to maintain trust in, and the viability of, the email ecosystem. ESPC Members understand that their customers, employees, and consumers expect that Member Companies will handle information received from or about them in an accurate manner, protected against errors, secured from theft and protected against unauthorized access and disclosure.

These Best Practices describe the information security principles that ESPC Members believe are appropriate for companies in the email service provider industry. Members understand that information security is not static, and expect that these Best Practices will evolve over time, as warranted. It is also understood that some Member Companies’ practices are subject to legal regimes, such as GLBA, HIPAA and the FTC Act, that some Member Companies are subject to self-regulatory codes of conduct, and that Member Companies are often subject to contractual provisions regarding information security. Similarly, it is understood that different legal regimes impose different obligations with respect to different types of information and, in some instances, applicable law may impose obligations beyond those described in these Best Practices with respect to certain types of information. These Best Practices are not intended to conflict with those existing obligations. Rather, they are intended to serve as a baseline to make sure that all Member Companies have an appropriate set of Best Practices underlying their email service provider operations. Moreover, it is assumed that Member Companies will comply with all applicable law.

In addition to these Best Practices, ESPC Members are encouraged to engage in an ongoing dialog regarding emerging information security threats and potential controls to address those threats, consistent with legal and confidentiality obligations.

The Best Practices apply to Members in the context of their email service provider businesses. Specifically, these best practices are only intended to apply to a Member’s email service provider business “environment,” including: (1) all employees, contractors, consultants, temporaries, and other workers that perform work in connection with such business; (2) all equipment and facilities that are owned or leased by the Member and that are used in connection with such business; (3) all data, in paper and electronic form, that is owned, licensed, stored or maintained by the Member in connection with such business, including any data over which its customers have granted the Member custody (this information is referred to herein as “Company Information”); and (4) all content and information transmitted by or through the Member on behalf of a customer (“Transmitted Information”).

The Best Practices are broken down into six broad categories:

Administrative;
Information classification;
Information management;
Technical controls;
Third parties; and
Incident response.

I. Administrative

A. Develop, implement, maintain and monitor a comprehensive, written information security program that contains administrative, technical and physical safeguards to protect the security, confidentiality and integrity of Company Information (in all forms) and ensure the security of Transmitted Information.

B. Conduct periodic risk assessments to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality and integrity of Company Information or the security of Transmitted Information and, where necessary, upgrade or implement safeguards to limit any identified risks.

C. Establish a process for receiving and addressing vulnerability reports from third parties that identify risks to the security, confidentiality and integrity of Company Information or the security of Transmitted Information, and use such information to update the Company's written information security program.

D. Designate one or more employees to be responsible for maintaining and monitoring the information security program to ensure that it is operating as intended.

E. Educate and train employees regarding information security and require their compliance with the Company's written information security program.

II. Information Classification

A. Periodically identify the types of information that the Company collects, handles, maintains or otherwise has access to and identify the types of paper, electronic and other records and information systems that the Company commonly uses to handle this information (and where such records and information systems reside).

B. Develop an information classification scheme for this information (*e.g.*, Confidential Information, Personal Information, Internal Information and Public Information).

C. Identify the information classifications that require heightened protections (*e.g.*, customer data and data subject to information security laws) and what heightened protections are appropriate.

III. Information Management

A. *Data Minimization* – Limit the collection of information (particularly personal information) on behalf of the Member's Customers to that which is reasonably necessary, as determined by the Member's Customers, to accomplish defined business purposes.

B. *Retention* – Develop and implement a retention policy for Company Information that limits the retention of information to a time period reasonably necessary to accomplish defined business purposes.

C. *Access* – Limit access to Company Information (and information systems) and Transmitted Information to those personnel who require such access to perform their job duties, restrict administrator access as appropriate, promptly remove access permissions when no longer necessary, and establish a procedure to periodically review user permissions and accounts.

D. *Use* – Limit the use of Company Information to the performance of job duties in furtherance of defined business objectives.

E. *Communication* – Communicate Company Information in a manner that protects the information based on its classification, including authenticating and securing the connections used to transmit Company Information and encrypting Company Information where appropriate.

F. *Storage* – Store Company Information in a manner that protects the information based on its classification including, where appropriate, encrypting Company Information.

G. *Disposal* – Dispose of information in paper, electronic and other forms when it is no longer to be retained in a secure manner based on its classification.

IV. Technical Controls

A. *Passwords* – Implement a password policy requiring strong passwords to access Company Information systems, including:

1. Requirements for character type and length;
2. Limitations on similarity to previous passwords;
3. Prohibitions on the use of default passwords;
4. Prohibitions on the use of common passwords;
5. Limitations on password guessing attempts;
6. Expirations for passwords; and
7. Prohibitions on the storage of passwords in plain text.

B. *Log-Ins* – At a minimum, require a unique Company-issued user ID and user-selected password (or other authentication technology) to gain access to Company Information systems and ensure that access rights for each user ID are appropriate, including administrator accounts.

C. *Malware Protection (Company systems)* – Ensure that Company computer systems have robust antivirus, malware protection, and intrusion detection software correctly installed, configured and updated regularly.

D. *Segmentation of Networks* – Implement appropriate segmentation of Company networks.

E. *Network Access* – Configure Company networks to restrict access to unauthorized users.

F. *Remote Access* – Only permit remote access connections to the Company network through Company-approved remote access technologies that adhere to the Company's malware protection, patch management and other security policies, and consider dual-factor authentication for all access to the Company network, including remote access.

G. *Internet* – Implement procedures to secure the Company's internet use and connection.

H. *Logging* – Log (and monitor logs of) significant computer and network security events, including password guessing attempts, hacking and virus incidents, modifications to system software, and flows of data into and out of the Company network.

I. *Monitor Network Activity* – Monitor and evaluate large batches of data leaving the Company network and, if possible, scan the data (if not possible, scan a random sample of the data) to ensure transmission and encryption of data is proper and in line with standard company practices, with the goal being to detect unauthorized exfiltration of Company Information.

J. *Patch Management* – Ensure that Company assets that connect to the Company's internal network have the latest security patches and updates appropriately installed, provided however that Company may engage in appropriate security and compatibility testing prior to installing such patches or updates.

K. *Software Development* – Implement security throughout the software development life cycle.

L. *Facilities* – Implement physical security measures to prevent unauthorized access to Company facilities and the information and information systems contained in such facilities.

M. *Devices and Removable Media* – Implement password requirements and other reasonable security measures on devices that store Company Information or access Company networks, restrict the use of removable media on the Company network, and encrypt Company Information stored on removable media.

N. *Email Authentication Inbound Requirements* – Require email authentication on inbound corporate email systems and drop or reject emails that do not pass authentication checks (*e.g.*, SPF, SID, DKIM).

O. *Content Scanning* – Scan content and hyperlinks contained in Transmitted Information for malware immediately prior to initiating transmission using industry-standard scanning technologies and tools, which may be updated or altered from time to time.

V. Third Parties

A. *Service Providers*

1. Take reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect Company Information, and ensure that contracts with them contain appropriate information security provisions, including those that are consistent with these Best Practices.
2. Restrict third-party service providers' access to Company Information, systems and networks except as necessary to provide defined services to the Company.
3. Where appropriate, conduct risk assessments of prospective third-party service providers' abilities to protect Company Information and require them to do so by contract.
4. Where appropriate, may conduct periodic audits to ensure that third-party service providers are appropriately protecting Company Information.

B. *Customers*

1. Take reasonable steps to authenticate new and existing customers and, where appropriate, conduct risk assessments of prospective customers' likelihood of distributing malware through Transmitted Information or using Company services.
2. Restrict customers' access to Company Information, systems and networks except as necessary to access the Company's services.
3. Require customers to maintain the security of Company's information (*e.g.*, log-in information), systems and networks they use to access the Company's services.
4. Prohibit customers by contract from distributing or allowing the distribution of malware through Transmitted Information or using Company services.
5. Provide customers with periodic training or guidance on how to protect the security of the Company's services, including maintaining the security of log-in information (including frequently changing this information), appropriately limiting the nature, size and scope of customers' personnel access to the Company's network, and ensuring the security of Transmitted Information.
6. Enforce regular password change intervals if possible as dictated by a strong password policy.

7. Make training available to customers regarding the authentication of *all* of their outbound email.

VI. Incident Response

A. Require Company personnel to immediately report to a person designated pursuant to VI.C. suspected and actual information security incidents involving the compromise of Company Information or the distribution of malware through Transmitted Information.

B. Implement a written response plan that is designed to manage the Company's response to potential incidents.

C. Implement a core response team that will be responsible for receiving reports of potential information security incidents involving the compromise of Company Information or the distribution of malware through Transmitted Information and determining whether to trigger a broader incident response based on written criteria.

D. For any incident where the core response team convenes a broader incident response team, investigate, respond to, and if necessary, remediate the incident, including:

1. Investigating the cause and circumstances of the incident (the who, what, where, when, why and how) and documenting the chronology of the incident;
2. If necessary, assign appropriate personnel to remediate ongoing incidents;
3. Engaging third-party resources, where appropriate, such as outside legal counsel, third-party investigators and law enforcement (consult counsel prior to doing so);
4. Managing communications related to the incident, including communications to consumers, customers, regulators, law enforcement and the media; and
5. Following resolution of an incident, determine any appropriate remedial measures to prevent recurrence of the incident or similar incidents.