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 apply 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; and (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").

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)

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

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

D. Educate and train employees regarding information security and require their compliance with the 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) to those personnel who require such access to perform their job duties

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

F. *Storage* – Store Company information in a manner that protects the information based on its classification

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. Prohibiting use of default passwords;
4. Limitations on password guessing attempts; and
5. Expirations for passwords

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* – Ensure that Company computer systems have robust malware protection software correctly installed, configured and updated

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

E. *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

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

G. *Logging* – Log (and monitor logs of) significant computer and network security events, including password guessing attempts, hacking and virus incidents and modifications to system software

H. *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

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

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

K. *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)

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. Where appropriate, conduct risk assessments of prospective third-party service providers' abilities to protect Company information and require them to do so by contract
3. Where appropriate, may conduct periodic audits to ensure that third-party service providers are appropriately protecting Company information

B. *Customers*

1. 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
2. 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) and appropriately limiting the nature, size and scope of customers' personnel access to the Company's network
3. Enforce regular password change intervals if possible as dictated by a strong password policy
4. Make training available to customers regarding the authentication of *all* of their outbound email

VI. Incident Response

A. Require Company personnel to report suspected and actual information security incidents immediately

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 and determining whether to trigger a broader incident response

D. For any incident where the core response team convenes a broader incident response team, investigate, respond to and 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. Assigning appropriate personnel to remediate ongoing incidents;
3. Engaging third-party resources, where appropriate, such as outside legal counsel, third-party investigators and law enforcement;
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