mimecast

Information Security Policy

Introduction

This Information Security Policy defines how Information Security is set up, managed, measured, reported on and developed within Mimecast in order to protect the confidentiality, integrity and availability of business information.

ISO 27001

In 2012, an independent ISO registration body validated that the effective adoption of security best practices had been appropriately implemented at Mimecast as an Information Security Management System (ISMS) and Mimecast was awarded certification to the ISO 27001 standard. Mimecast has maintained this certification, conducting external and independent bi-annual ISO 27001 audits.

Taking into account the importance of our service to customer privacy and continuity and the impact we can have to customer day to day operations, the ISMS scope is all encompassing and applies to all regions Mimecast operates within:

The service platform, products, infrastructure, support, operational services, and facilities

Security Framework

Aligning our information security efforts with ISO 27001 gives Mimecast an internationally recognised framework for building an information security and privacy program. Customers and prospects must be able to evaluate our security program against a well-known set of physical, technical, administrative controls as well as their own specific needs; this is key to good customer experience. ISO 27001 is also the baseline framework to which we map our regional specific legal and contractual requirements.

Mimecast's other key requirement is to protect our own confidential information. This is achieved through education, awareness of our staff and suppliers; risk evaluation, testing and assessments; internal audit and review and our classification and handling policies.

Policy

Leadership and Commitment Policy

Mimecast's Security Steering Committee is committed to promoting information security and privacy objectives globally. This commitment is demonstrated through their support of the ISMS operations and ISO27001 certification process; encouraging a culture of security vigilance; their provisioning of the appropriate resources required to develop and maintain the ISMS, as well as their support of legal, contractual and customer experience endeavors.

Mimecast's Security Steering Committee is involved in the establishment and ongoing maintenance of Information Security and data protection at Mimecast. The committee understands that Mimecast must:

"secure our technologies and facilities in order that Mimecast provides an easy to use and safe experience for Mimecast's customers, partners and staff that meets and exceeds the level of acceptable risk appropriate to a business data storage service provider" This is echoed in Mimecast's vision, to be "The safest and most useful place for business data"

Various Information Security specific roles have been created at Mimecast in order to implement, maintain, evaluate and report on the effectiveness of the ISMS and security practices:

- **Executive Security Champions (Chief Finance Officer and Chief Executive Officer):** Instilling a security culture within the Executive management and delivering strategic direction in both compliance and delivery of information security. Accountable for information security and data protection.

- **Chief Information Security Officer:** Implementation and authorization of security policies, controls and procedures, strategic direction, training and awareness. Responsible for Information Security and data protection.

- **Senior Operational Risk and Compliance Manager:** Implementation, maintenance and continual improvement of ISO 27001 certification and global privacy regulation requirements, business continuity and internal audit.

- **Technical Security Architects:** Design, review and testing of security related functionality of all products and services.

- **Risk Improvement Project Manager:** Co-ordination of corrective and preventive actions, and project management of cross departmental/ regional continual improvement projects.

- **Internal Auditors**: Volunteer auditors from across the business operating under instruction from the Senior Operational Risk and Compliance Manager on an ad-hoc basis.

Security Goals and Strategy

Mimecast is committed to safeguarding the confidentiality, integrity and availability of all physical and electronic information assets of our customers as well as those of the business. Information Security goals are supported through the management of policies and controls contained within the ISMS. The goals are tied to general business goals, customer experience requirements, contractual and legal requirements and ISO certification requirements. Mimecast has assigned a strategy and when possible a measurement for meeting our Security goals.

Goals
Keeping information security and data privacy at the top of Mimecast business ethos
Meeting the security and privacy needs of our customers and partners
Maintaining a clean Mimecast ISO 27001 certification and audit
Fulfilling Mimecast legal and contractual obligations
Keeping information confidential and in line with our classification and handling policies
Maintaining the integrity of customer information (Integrity)
Providing customer access to their information when needed (Availability), even in the event of a major security incident
Continual identification and reduction of risk to below the agreed acceptable level
The needs and safety of our staff
The continual education and motivation of our staff in order that they consider security in all their actions and thereby minimize the risk of a security incident
Ensuring staff are able to access and support systems where and when required, while maintaining an acceptable level of risk

Mimecast uses an annual cycle to set and review success against the objectives for Information security and privacy.

Continual Improvement Policy

As a key component to any security program, Mimecast aims to continually improve our effectiveness in reducing risk and meeting our security and privacy objectives. This is achieved by driving improvement through:

1. Identifying best practice in terms of our model and market place
2. Maintaining our proactive focus with regard to our Information Security program
3. Making information security endeavors more measurable
4. Reviewing and acting upon metrics, results of audits, risk assessments, vulnerability scan and penetration testing
5. Holding a security committee on a monthly basis to track and discuss high priority security projects
6. Maintaining a security awareness program to educate users on Mimecast's security policies and review understanding and contribution.

Ideas for improvement may come from many sources, for example customers, partners, staff, suppliers, risk assessments, vulnerability scans and penetration testing. When evaluating improvement proposals, the following criteria will be considered:

1. Benefit to the business and stakeholders
2. The level of risk to not implementing the proposal
3. The timescale required to implement the proposal
4. The resources required to implement the proposal
5. Cost and value for money

Data Classification Policy

Mimecast classifies information within the scope of our ISMS by the level of sensitivity. That way we can appropriately allocate resources for the protection of each type of asset or media through a range of controls, policies, processes, procedures, organizational structures, training, software, hardware and network functionality and design. Mimecast has four levels of data classification as described on the following page (version 2 Classification Table). Customer data is given the highest level of classification:

Classification	Description/ Examples	Disclosure Guidelines	Handling Guidelines
RESTRICTED: CUSTOMER DATA	**RESTRICTED: CUSTOMER DATA** includes customer email and files, entered, stored and processed in the Mimecast Service Platform and via ingestion services	Access to systems and hardware containing encrypted email and file data classified as Restricted: Customer Data is limited to a role based subset of Mimecast staff and thereafter on a need to know basis.	**Labeling:** Yes **Storage:** Encrypted at rest and in transit. Locked in secure areas when stored or in use. Even if the media is no longer functional.
RESTRICTED	**RESTRICTED** information is limited to a sub-set of Mimecast staff on a need-to-know basis, or by team e.g. Human Resources.	NB. Unauthorized disclosure of **RESTRICTED** information inside the organization may cause significant impact on Mimecast' s reputation or may result in legislative or regulatory prosecution. Distribution and access of information classified as **RESTRICTED** must stay within the group intended.	**Labeling:** Yes In which case the **RESTRICTED** can be listed followed with the group e.g. **RESTRICTED: HUMAN RESOURCES** **Storage:** Encryption on storage devices and media. Hardcopy to be locked away when not in use. **Printing:** Permitted **Disposal:** Paper records shredded. Physical assets containing data to be securely wiped on termination of access.

COMPANY CONFIDENTIAL	**COMPANY CONFIDENTIAL** information is freely available to Mimecast employees regardless of role.	**COMPANY CONFIDENTIAL** is subject to distribution to third parties where applicable and where confidentiality terms exist. NB. If information is not labelled with any other classification it must be handled in line **COMPANY CONFIDENTIAL** guidelines	**Labeling:** Yes **Storage:** Laptops to be encrypted. Hardcopy company confidential information to be locked away when not in use **Printing:** Permitted **Disposal:** Paper records shredded. Physical assets containing data must be securely wiped on termination of access.
PUBLIC	Information is freely available for all Mimecast employees, third- parties and the public. Examples include, the corporate website and marketing brochures.	There is no impact on Mimecast of disclosure of Public information.	**Labeling:** Yes **Storage:** no restrictions but please follow good document management processes. **Printing:** Permitted **Disposal:** General waste or shredded

Policy Approval, Communication and Review

The Mimecast Information Security Policy is subject to review at the Mimecast Information Security Steering Committee Meetings, or in response to significant changes in Mimecast's business practices, infrastructure or ISMS scope. This policy is approved by the Information Security Steering Committee.

This Information Security Policy is available on our intranet and website and is communicated to employees, partners, suppliers and customers.

Additional Information

Please contact security@mimecast.com for further information on our ISMS or ISO 27001 Certification