Information Security Policy

PUBLIC
Public Release Authorized

Contents

1 Introduction

The Information Security Policy defines the requirements for creating and maintaining a strong information security position through the application of information security controls, information ownership and information protection. Implementation of this policy is intended to significantly reduce risk to the confidentiality, integrity and availability of Mimecast information systems and resources that enable achievement of Mimecast's strategic and operational business objectives.

2 Policy

Mimecast shall establish and maintain comprehensive protection and clear accountability for all Mimecast information assets and resources. This includes information assets that are proprietary to Mimecast, private to Mimecast customers and partners, and all other private and proprietary information and assets and resources that, if subject to inadvertent or unauthorized access or disclosure, would likely cause financial, legal, or reputational damage to Mimecast or Mimecast customers and partners.

3 Applicability

This Policy and associated standards, procedures and guidelines apply to all Mimecast employees, contractors, sub-contractors, and their respective facilities supporting Mimecast business operations, wherever Mimecast data is stored or processed, including any third-party contracted by Mimecast to handle, process, transmit, store, or dispose of Mimecast data.

4 Leadership and Commitment

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; 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"

5 Roles & Responsibilities

It is the responsibility of each Mimecast employee, consultant and contractor to read and understand this Policy as well as the associated procedures and documentation that will implement it. Management is accountable for implementing and supporting this Policy.

6 Data Classification

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.

7 Non-Compliance

In the absence of an approved exception, failure to comply may be considered a violation of the Code of Business Conduct and Ethics , and/or other related contracts or agreements (e.g. vendor, consultant, service provider, customer, business partner), and / or applicable laws / regulations. Failure to comply may result in disciplinary action as cited in those documents. Information systems and resources may be monitored to measure compliance.

8 Policy Approval, Communication and Review

This Policy is subject to review annually, or sooner in response to significant changes in Mimecast's business practices or law and regulations to ensure the Policy remains current with Mimecast's needs and business objectives.

This Policy is available on Mimecast's intranet and is required to be read and acknowledged, in the form of electronic sign-off, by all employees, consultants and contractors via the Mimecast eLearning Platform. Electronic sign-off evidences the policy is read, understood and agreement to comply.