Mailshake Risk Management Policy

Information Security Policies

Policy #	IS-02
Effective Date	June 30, 2019
Contact	josh@mailshake.com

This policy defines the risk management requirements for the identification of the appropriate control posture for all Mailshake computer and communications information system assets. This policy applies to all Mailshake computer systems and facilities, with a target audience of Mailshake executive management, information technology employees and our partners.

Security Personnel

Executive Team
Robert Senoff, Sujan Patel, Josh Sherman

Enterprise Security Team
Robert Senoff, Sujan Patel, Josh Sherman

Employee Security Team
Robert Senoff, Sujan Patel, Josh Sherman

Outsourcing Security Team
Robert Senoff, Sujan Patel, Josh Sherman

Chief Security Officer
Josh Sherman

Risk Management Process

Enterprise Security Risk Assessment
At least annually, the Enterprise Security Team conducts or manages an independent party who conducts an organization-wide information security risk assessment. The resulting analysis from this project must include a description of the information security risks currently facing the organization, and specific recommendations for preventing or mitigating these risks.

Employee Risk Assessment
At least annually, each employee of the company attends a security meeting to review security policies and ensure that they are ascribing to best practices and meet our policy requirements. The Employee Security Team is responsible for ensuring this compliance.

Outsourcing Risk Assessment
At least annually, the Outsourcing Security Team conducts a review of people or companies who perform outsourced work for the company and determines if continued outsourcing is appropriate, what security risks exist, and reevaluate the level of trust the company has with said individuals.

Risk Assessment Methodology
Assessing risk should be performed as necessary for the type of risk involved, but each assessment should minimally follow principles from frameworks similar to ISO 27002, ISO 27005, or NIST SP 800-30. Each risk should be listed in a risk register with a name, description, severity rating (high, medium, low), the likelihood of incidents, the impact on the company, a treatment categorization (avoid, transfer, mitigate, accept), a treatment plan, a treatment plan owner, and the date identified.

Third Party Disclosures

Prior to providing any non-public Mailshake information to an outsourcing firm, business partner, or any other non-governmental entity, the relevant Information Owner and the Executive Team, and/or the company's legal counsel must jointly perform a risk assessment. This team, or their delegates, must then collectively agree that the risks associated with this disclosure do not present an undue threat to Mailshake business interests.

Roles and Responsibilities

The following describes the key roles of the personnel who should support and participate in the risk management process (See NIST SP 800-30.)

Risk Assessment
The various risk assessment teams outlined above together define the specific scope of the risk assessment then identifies threats, assets, vulnerabilities, and risks to the company. Additionally, the team identifies risk mitigation by controls already in place. Remaining residual risks are categorized as either major or minor and are included in the analysis of the effectiveness of the security protection on the environment in the scope of the specific Risk Assessment.

Executive Management
The Executive Team, under the standard of due care and ultimate responsibility for mission accomplishment, must ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the mission. They must also assess and incorporate the results of the

risk assessment activity into the decision making process. An effective risk management program that assesses and mitigates IT-related mission risks requires the support and involvement of senior management.

The Executive Team is responsible for the enterprise's IT planning, budgeting, and performance including its information security components. Decisions made in these areas should be based on an effective risk management program.

Engineers

IT security practitioners (e.g., network, system, application, and database administrators; computer specialists; security analysts; security consultants) are responsible for proper implementation of security requirements in their respective IT systems. As changes occur in the existing IT system environment (e.g., expansion in network connectivity, changes to the existing infrastructure and organizational policies, and the introduction of new technologies), the IT security practitioners must support or use the risk management process to identify and assess new potential risks and implement new security controls as needed to safeguard their IT systems.

Vulnerability and Threat Analysis

Our Security Policy outlines the steps we take for vulnerability management and account security. This section of our risk policy asserts that these efforts are to be adhered to as policies central to risk management and are to be overseen by team managers, and ultimately, the Enterprise Security Team.

Threat analysis should be part of the Enterprise Security Risk Assessment and should cover which, if any, actors pose a threat to our security, in what ways might we be vulnerable to those threats, and what treatment plan we intend to pursue to address those threats

---

Approval and Ownership

	Name	Date	Signature
Policy Author	Josh Sherman		
Owner / Approved By	Robert Senoff		
Owner / Approved By	Sujan Patel		

Revision History

Version	Description	Approval Date	Approver Name

1.0	Initial document.	6/30/2019	Robert Senoff
1.1	Changed contact, policy author, and Chief Security Office to Dave Donaldson, also added Dave Donaldson to each of the security teams.	4/29/2020	Sujan Patel
1.2	Removed Colin Mathews from each of the security teams.	7/20/2022	Dave Donaldson
1.3	Changed contact, policy author, and Chief Security Office to Josh Sherman, also added Josh Sherman to each of the security teams.	6/28/2023	Josh Sherman
1.4	Removed Colin Mathews from approval and ownership section.	7/31/2023	Josh Sherman