Third Party Vendor Information Security Policy

Overview

This document establishes the policy governing security guidelines, requirements, and procedures that reduce risk and provide for the confidentiality, integrity, and availability of Boston Mutual Life Insurance Company's (BML) electronic information and assets, for all Third Party Vendors (the Vendor). The protection of information assets is mandatory for business, contractual, regulatory and legal reasons.

Scope

The Vendor is required to implement, test and continually monitor the administrative and technical controls outlined below to protect BML Sensitive Data (as defined below).

The Vendor will handle BML Sensitive Data in accordance with applicable laws, the terms of the applicable agreement between BML and the Vendor (including, without limitation, this Third Party Vendor Information Security Policy), and based on any additional instructions from BML and its authorized agents.

This Third Party Vendor Information Security Policy ("Policy") applies to all BML electronic information and assets, and vendors and agents operating on behalf of BML. Additional security and controls may be imposed as needed, but they are in addition to this Policy. BML reserves the right to amend or terminate this Policy at any time. BML has full and final discretionary authority for its interpretation and application. This Policy SUPERSEDES all other policies, procedures or information in direct conflict with it.

Definitions

"Breach" means any (a) unauthorized processing of BML Sensitive Data or (b) any act or omission that compromises or undermines the physical, technical, or administrative safeguards put in place by Vendor regarding processing BML Sensitive Data. For the avoidance of doubt, "unauthorized processing" includes, but is not limited to: misuse, loss, destruction, compromise, or unauthorized access or disclosure, collection, retention, storage, or transfer.

"Cybersecurity Event" means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.

"**Personal Identifiable Information**" **(PII)** means any information that can be used to uniquely identify, contact, or locate an individual, alone or in conjunction with other information.

"**Protected Health Information**" **(PHI)** means any or all individually identifiable health information relating to the physical or mental health condition of an individual, the provision of healthcare to an individual or payment for the provision of healthcare to an individual.

"**Sensitive Data**" means proprietary non-public information intended for use by BML's workforce, including but not limited to PII, PHI, financial data, customer lists, and employee data.

Policy

Information Security Policies

The Vendor must have and maintain a written policy or policies setting forth the Vendor's policies and procedures for the protection of its IT systems and nonpublic information stored on those IT systems. The Vendor must have a designated Chief Information Security Officer (or an equivalent designee) and employee training.

Acceptable Use Rules

The Vendor must document and implement rules for the acceptable use of assets of third parties, including without limitation, BML assets and data. These rules must require that third party assets are used in a professional, lawful, and ethical manner, and are not used for activities which have been identified as unacceptable conduct.

Access Control

The Vendor must:

- Ensure controls restrict other customers from accessing BML assets.
- Use authentication and authorization technologies for service, user and administrator level accounts.
- Ensure strong password criteria and standards exist on IT systems that access BML Sensitive Data.
- Utilize multi-factor authentication for any individual accessing the Vendor's internal networks from an external network, unless the Vendor has approved in writing the use of reasonable equivalent or more secure access controls.
- The Vendor must ensure procedures exist for prompt modification or termination of access or rights in response to organizational changes.
- The Vendor must periodically review the necessity of privileged access accounts.

Application Development and Maintenance

The Vendor must:

- Ensure infrastructure, network and application vulnerability assessments are periodically conducted and follow industry acceptable vulnerability management practices (e.g. process described in NIST & OWASP).
- Ensure firmware, software and application source code are validated and tested against vulnerabilities and weaknesses before deploying to production.

Electronic Data Destruction

The Vendor must maintain policies and procedures for the secure disposal on a periodic basis of any electronic BML Sensitive Data that is no longer necessary for business operations or for other legitimate business purposes, except where such information is otherwise required to be retained by law, regulation, or by contract, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

The Vendor must follow a process that securely wipes all data on all media using a method that will not allow data to be retrieved. At any time prior to reuse or repurposing of media used to store or process BML Sensitive Data, said media must be cleared or purged.

Data Security

The Vendor must:

- Use strong encryption key management practices to ensure the availability of encrypted authoritative information.
- Encrypt all BML data assets in transmission between the Vendor and BML as well as between the Vendor and all other third parties when transmitted data is BML data.
- Encrypt regulated information when it is "at rest" at all times, unless alternative controls are approved by BML in writing.
- Encryption must meet a minimal standard of AES-256-bit encryption.
- Not permit any third party, other than an authorized provider, to process BML Sensitive Data.
- Laptop computers used to review, store or transport any PII and/or PHI of a BML customer, or any information related in any way to BML business, which is not on encrypted software must be encrypted. PII or PHI of a BML customer may not be stored on a portable electronic devise unless it is protected to the level technically feasible.

Network Security

The Vendor must deploy Data Loss Prevention and/or intrusion monitoring services at perimeter points where BML Sensitive Data is used. The Vendor must ensure all unnecessary services, ports, and network traffic are disabled on all IT systems that access BML assets.

Operation Security

The Vendor must:

- Ensure that any changes to IT systems that are performing work on or for BML do not have any negative security implications.
- Follow documented change management practices and procedures.
- Not move or transfer BML Sensitive Data to any non-production environment or insecure location.

System Security

The Vendor must:

- Have a process for applying and managing security updates, patches, and fixes upgrades (collectively referred to as "Patches") on all IT systems.
- Ensure Malware, Virus, Trojan and Spyware protection is deployed, with up-to-date manufacturer's signatures, definition files, software and Patches, on all IT systems that access BML assets and data.
- Deploy methods to identify malicious activity, log information on such activity, attempt to block/stop the activity, and report such activity.

Incident Reporting

The Vendor must maintain a written incident response plan designed to promptly respond to, and recover from, any Breach or Cybersecurity Event materially affecting the confidentiality, integrity or availability of the Vendor's IT systems used in the course of servicing BML or processing BML Sensitive Data.

If at any time the Vendor has reason to believe that BML customer PII or PHI data in the Vendor's possession has been breached, the Vendor is required to report the breach in writing within one (1) business day of the discovery of the incident to the BML Chief Risk Officer. If a Vendor laptop or other electronic portable device containing BML customer PII or PHI data is ever stolen, the theft must be reported in writing within one (1) business day of the discovery of the incident to the BML Chief Risk Officer.