Third Party Information Security Risk Management

Overview

This document is for exclusive use by MSLA.

Version	Description [or description of changes]	Author	Creation date	Approved by	Date approval
1.1	Updated version	MSLA IT Department	11/07/2022	Luis Rios	11/21/2022

TABLE OF CONTENT

Purpose

MSLA International utilizes third-party products and services to support our mission and goals. Third-party relationships carry inherent and residual risks that must be considered as part of our due care and diligence. The Third-Party Information Security Risk Management Policy contains the requirements for how MSLA International will conduct our third-party information security due diligence.

Audience

This policy applies to all individuals who engage with a third-party on behalf of MSLA International.

Definitions

The following definitions apply only to aid the understanding of the reader of this policy:

- **Employee** – defined as a person who is a part-time or full-time hourly or salaried employee who is performing work for MSLA International as an employee, and not an independent contractor. Sometimes referred to as a "W2 employee".
- **Third-party or 3rd-party** – any person or organization who provides a service or product to MSLA International and is not an employee.
- **Information Resources** – any system involved in the creation, use, management, storage, and/or destruction of MSLA International information and the information itself.
- **Inherent information security risk** – the information security risk related to the nature of the 3rd-party relationship without accounting for any protections or controls. Inherent risk is sometimes referred to as "impact" and is used to classify third-party relationships as an indicator of what additional due diligence may be warranted.
- **Residual information security risk** – the information security risk remaining once all applicable protections and controls are accounted for.

Policy

The policy is organized into three sections; general, physical, and technical according to the precaution or requirement specified.

Assessments

- Every 3rd-party granted access to MSLA International Information Resources must sign the MSLA International Third-Party Non-Disclosure Agreement and Business Associate Agreement (if applicable).
- All 3rd-party relationships must be evaluated for inherent information security risk prior to any interaction with MSLA International Information Resources.
- Criteria for inherent risk classifications must be established; "High", "Medium", and "Low".

- All 3rd-party relationships must be re-evaluated for inherent information security risk bi-annually and any time there is a material change in how MSLA International utilizes the third-party product or service.
- 3rd-party relationships with significant inherent risk (classified as “High” or “Medium”) must be evaluated for residual risk using questionnaires, publicly available information, and/or technical tools.
- Residual information security risk assessments must account for administrative, physical, and technical controls.
- Residual information security risk thresholds must be established for 3rd-party relationships with significant inherent risk (classified as “High” or “Medium”).
- 3rd-party relationships that do not meet established residual information security risk thresholds:
    - Must be terminated,
    - Must be formally approved by executive management following an established waiver process, and/or;
    - Changed in a manner that reduces inherent and/or residual information security risk to meet MSLA International established thresholds.
- 3rd-party relationships concerning industry and/or regulatory requirements (i.e. PCI-DSS, HIPAA, etc.) must be reviewed on no less frequent than an annual basis.

Management

- 3rd-party agreements and contracts must specify:
    - The MSLA International information the vendor should have access to,
    - How MSLA International information is to be protected by the 3rd-party,
    - How MSLA International information is to be transferred between MSLA International and the 3rd-party,
    - Acceptable methods for the return, destruction or disposal of MSLA International information in the 3rd-party’s possession at the end of the relationship/contract,
    - Minimum information security requirements,
    - Information security incident response and notification requirements,
    - Right for MSLA International to audit 3rd-party information security protections and controls.
- If the 3rd-party subcontracts part of the information and communication technology service provided to MSLA International, the 3rd-party is required to ensure appropriate information security practices are followed throughout the supply chain,
- The 3rd-party must only use MSLA International Information Resources for the purpose of the business agreement and/or contract,
- Work outside of defined parameters in the contract must be approved in writing by the appropriate MSLA International point of contact.

- 3rd-party performance must be reviewed annually to ensure compliance with agreed upon contracts and/or service level agreements (SLAs). In the event of non-compliance with contracts or SLAs regular meetings will be conducted until performance requirements are met.
- The 3rd-party's major IT work activities must be entered into or captured in a log:
    - Made available to MSLA International IT management upon request, and
    - Must include events such as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.
- Any other MSLA International information acquired by the 3rd-party during the contract cannot be used for the 3rd-party's own purposes or divulged to others.
- 3rd-party personnel must report all security incidents directly to the appropriate MSLA International IT personnel.
- MSLA International IT will provide a technical point of contact for the 3rd-party. The point of contact will work with the 3rd-party to ensure compliance with this policy.
- 3rd-parties must provide MSLA International a list of key personnel working on the contract when requested.
- 3rd-parties must provide MSLA International with notification of key staff changes within 24 hours of change.
- Upon departure of a 3rd-party employee from a contract, for any reason, the 3rd-party will ensure all sensitive information is collected and returned to MSLA International or destroyed within 24 hours.
- Upon termination of contract, 3rd-parties must be reminded of confidentiality and non-disclosure requirements.
- Upon termination of contract or at the request of MSLA International, the 3rd-party must surrender all MSLA International badges, access cards, equipment and supplies immediately.
- Any equipment and/or supplies to be retained by the 3rd-party must be documented by authorized MSLA International IT management.

Waivers

Waivers from certain and specific policy provisions may be sought following the MSLA International Waiver Process. There are no exceptions to any provisions noted in this policy until and unless a waiver has been granted.

Enforcement

This Third-Party Information Security Risk Management Policy supplements and compliments all other related information security policies, it does not supersede any such policy or vice versa. Where there are any perceived or unintended conflicts between MSLA International policies, they must be brought to the attention of MSLA International for immediate reconciliation.

Personnel found to have violated any provision of this policy may be subject to sanctions up to and including removal of access rights, termination of employment, termination of contract(s), and/or related civil or criminal penalties.