	Physical Security Policy

Overview

This document is for exclusive use by MSLA.

Version	Description [or description of changes]	Author	Creation date	Approved by	Date approval
2.0	Updated version	MSLA IT Department	07/22/2022	Luis Rios	08/08/2022

TABLE OF CONTENTS

Purpose

The purpose of the MSLA International Physical Security Policy is to establish the rules for the granting, control, monitoring, and removal of physical access to Information Resource facilities.

Audience

The MSLA International Physical Security Policy applies to all MSLA International individuals that install and support Information Resources, are charged with Information Resource security and data owners.

Contents

Policy

General

- Physical security systems must comply with all applicable regulations including but not limited to building codes and fire prevention codes.
- Physical access to all MSLA International restricted facilities must be documented and managed.
- All **Information Resource** facilities must be physically protected in proportion to the criticality or importance of their function at MSLA International.
- Access to **Information Resources** facilities must be granted only to MSLA International support personnel and contractors whose job responsibilities require access to that facility.
- All facility entrances, where unauthorized persons could enter the premises, must be controlled.
- Secure areas must be protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. This includes:
    - information processing facilities handling **confidential information** should be positioned carefully to reduce the risk of information being viewed by unauthorized persons during their use;
    - controls should be adopted to minimize the risk of potential physical and environmental threats;
    - environmental conditions, such as temperature and humidity, should be monitored for conditions which could adversely affect the operation of information processing facilities.
- Directories and internal telephone books identifying locations of confidential information processing facilities should not be readily accessible to anyone unauthorized.
- Equipment must be protected from power failures and other disruptions caused by failures in utilities.
- Restricted access rooms and locations must have no signage or evidence of the importance of the location.
- All **Information Resources** facilities that allow access to visitors will track visitor access with a sign in/out log.
- Card access records and visitor logs for **Information Resource** facilities must be kept for routine review based upon the criticality of the Information Resources being protected.
- Visitors in controlled areas of **Information Resource** facilities must be accompanied by authorized personnel at all times.

- Personnel responsible for **Information Resource** physical facility management must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.

Access Cards

- The process for granting card and/or key access to Information Resource facilities must include the approval of a member of the physical security committee.
- Each individual that is granted access rights to an **Information Resource** facility must sign the appropriate access and non-disclosure agreements.
- Access cards and/or keys must not be shared or loaned to others.
- Access cards and/or keys that are no longer required must be returned to personnel responsible for **Information Resource** physical facility management. Cards must not be reallocated to another individual, bypassing the return process.
- Lost or stolen access cards and/or keys must be reported to the person responsible for **Information Resource** physical facility management physical security committee as soon as possible.
- Physical security committee must remove the card and/or key access rights of individuals that change roles within MSLA International or are separated from their relationship with MSLA International.
- Physical security committee must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.

Waivers

Waivers from certain policy provisions may be sought following the MSLA International Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.