iMocha	**PHYSICAL SECURITY POLICY**

Version Control

Current Version	**1.2**
Released on:	**1-Sep-2025**
Classification	**Internal Use**

Version Number	**Date of Release**	**Nature / Description of Change**	**Prepared / Changed By**	**Approved By**
1.0	1-Sep-2022	Initial version	Wasim Shaikh	Sujit Karpe
1.1	1-Sep-2023	Second version	Nishant Thool	Sujit Karpe
1.2	1-Sep-2024	Third version	Nishant Thool	Sujit Karpe
1.3	1-Sept-2025	Fourth version	Nishant Thool	Sujit Karpe

iMocha	**PHYSICAL SECURITY POLICY**

Purpose and Scope

The Physical Security Policy specifies the requirements for physically protecting assets and their data via physical controls and safeguards. Physical security is the first line of defense in information security, and without physical protections, virtual protections offer minimal security for assets and data. iMocha maintains reasonable steps to ensure that its facilities, information systems, and data are accessed only by authorized personnel or authorized third party visitors to prevent unauthorized access, damage, theft, and interference. All physical security requirements are applicable to both remote and in-office work. Key aspects of physical security include: perimeter and border security, entry controls, visitor management, restricted areas, equipment protection and maintenance, awareness and training, and risk management.

Perimeter and Border Security

iMocha facilities should be secured via external locked doors. iMocha facilities should be monitored via personnel, security cameras, and/or other mechanisms to detect potential security threats and respond to alerts.

Entry Controls

iMocha requires employees and applicable contractors to utilize access cards/keys to unlock external doors throughout all business hours. For facilities that have a security desk at the point of initial external access, external doors can be left unlocked as long as 1) employees and/or contractors authenticate prior to internal access via key/badge and 2) visitors are required to sign-in at the security desk prior to internal admittance.

Visitor Management

All visitors must sign-in with security prior to being allowed in internal office areas. Upon sign-in, the following visitor-specific information should be collected:

- Visitor name
- Visitor organization name (if applicable)
- Government-issued identification card information

Upon exit, the badge/nametag and should be collected and the hr/min/sec timestamp for visitor exit should be captured. Visitor logs should be stored for at least 90 days via securely stored paper or digital records. Visitors that are unescorted should not have the ability to logically access restricted areas unless pre-authorization has been given by the approving manager. Visitors should receive a temporary badge or nametag - badge/nametag should be marked in a way that identifies them as a visitor. Any non-escorted or unauthorized visitors should be reported to the security team immediately.

iMocha	**PHYSICAL SECURITY POLICY**

Restricted Areas

Only authorized personnel shall be allowed entry into restricted areas. Restricted areas may include:

- Personal, confined offices
- Network closets
- Power & utilities closets
- Server rooms (as applicable)

Restricted areas must be secured via access badges/keys or security personnel.

Equipment

The following types of protection and monitoring equipment should be maintained at all times:

- Power utilities (e.g. generators, UPS)
- HVAC systems, including environmental sensors (thermometers and humidity sensors)
- Fire suppression systems
- Network, power, and telecommunications cabling
- On-premise servers and desktops (as applicable)
- Physical data backups

iMocha must securely store/protect the aforementioned equipment/assets from physical threats via proper access controls.

iMocha should maintain awareness of necessary maintenance schedules for the aforementioned equipment/assets. Maintenance should occur accordingly to prevent the failure of any of the aforementioned assets. Any third party/maintenance company that has access to a iMocha facility (e.g. night cleaning company) must receive security clearance from management and must follow all applicable parts of the security policies. Maintenance to and external movement of physical security components should be documented and tracked accordingly.

Risk Management

iMocha includes physical security within annual risk assessment scope.

Exceptions

iMocha business needs, local situations, laws and regulations may occasionally call for an exception to this policy or any other iMocha policy. If an exception is needed, iMocha management will determine an acceptable alternative approach.

Enforcement

Any violation of this policy or any other iMocha policy or procedure may result in disciplinary action, up to and including termination of employment. iMocha reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. iMocha does not consider conduct in violation of this policy to be within an employee's or contractor's course and scope of work.

Any personnel who is requested to undertake an activity that he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager or any other manager of iMocha as soon as possible.

The disciplinary process should also be used as a deterrent to prevent employees and contractors from violating organizational security policies and procedures, and any other security breaches.

Responsibility, Review, and Audit

iMocha reviews and updates its security policies and plans to maintain organizational security objectives and meet regulatory requirements at least annually. The results are shared with appropriate parties internally and findings are tracked to resolution. Any changes are communicated across the organization.

This document is maintained by Sujit Karpe.

This document was last updated on 01/09/2025.