



Physical Security Policy

August 2019

| | |
|--|---|
| PUBLICATION NOTE | 2 |
| DOCUMENT MANAGEMENT | 2 |
| DOCUMENT APPROVAL AND ACCEPTANCE | 2 |
| | |
| 1. PURPOSE | 3 |
| 2. SCOPE | 3 |
| 3. POLICY | 3 |
| 1. PHYSICAL SECURITY PERIMETER | 3 |
| 2. PHYSICAL ENTRY CONTROLS | 3 |
| 3. SECURING OFFICES, ROOMS & FACILITIES | 3 |
| 4. PROTECTING AGAINST EXTERNAL & ENVIRONMENTAL THREATS | 3 |
| 5. WORKING IN SECURE AREAS / VISITOR MANAGEMENT | 4 |
| 6. DELIVERY & LOADING AREAS | 4 |
| 7. SUPPLIER, VENDOR & THIRD-PARTY SECURITY | 4 |
| 4. AMENDMENT/TERMINATION OF THIS POLICY | 4 |
| 5. EXCEPTIONS | 4 |
| 6. VIOLATIONS/ENFORCEMENT | 4 |



Publication Note

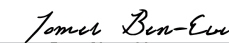


This policy is the property of Mursion and is exclusively for the use of Mursion employees, authorized agents, and affiliated companies. It contains Mursion confidential and proprietary information, and under no circumstances is it to be delivered or disclosed to any person not employed by Mursion, its authorized agents, or affiliated companies, without the express written authorization of an officer of Mursion.

Document Management

Version History

| Revision | Release Date | Updated by | Remarks/Comments |
|----------|--------------|------------|------------------|
| O.1 | 5/6/19 | M. Cooper | Initial draft |
| O.2 | 5/18/2019 | T.Ben-Evi | Second draft |

Document Approval and Acceptance

| Name | Signature | Date |
|---------------|--|-------------------------|
| Tomer Ben-Evi |  DocuSigned by: | 8/5/2019 10:16 AM PDT |
| Tomer BenEvi |  A1112A21C6D546F... | 7/14/2020 |
| Tomer Ben-Evi |  A1112A21C6D546F... | 7/26/2021 |





1. Purpose

To prevent unauthorized physical access or damage to the organization's information and information processing facilities.

2. Scope

The scope of this policy effects all Mursion offices, locations and information systems that are business critical and/or process, store, or transmit confidential data. This policy applies to all employees of Mursion, Mursion facilities, and to all external parties, including but not limited to Mursion consultants, contractors, business partners, vendors, suppliers, outsourced service providers, and other third-party entities who provide and/or access Mursion IT networks and system resources.

3. Policy

1. Physical Security Perimeter

Physical offices and processing facilities shall meet all local building codes for construction materials for walls, windows, doors, and access control mechanisms. Some interior zones may be identified as secure areas where physical access is further restricted to a subset of Mursion personnel; such as private offices, wiring closets, print and server rooms, and server racks.

2. Physical Entry Controls

Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. Where possible, Mursion access control systems shall be tied to a centralized system that provides granular access control for individual personnel. Access events shall be appropriately logged and reviewed as needed according to risk. Cameras and intrusion detection systems shall be used at facilities that store or process production data.

3. Securing Offices, Rooms & Facilities

Physical security for offices, rooms and facilities shall be designed and applied to protect from theft, misuse, environmental threats, unauthorized access, and other threats to the confidentiality, integrity, and availability of confidential or restricted information.

4. Protecting Against External & Environmental Threats

Physical protection against natural disasters, malicious attack or accidents shall be designed and applied. Secure areas shall be monitored through the use of intrusion detection systems, alarms, and/or video surveillance systems where feasible. Visitor and third-party access to secure areas shall be restricted to reduce the risk of information loss and theft.

Production processing facilities shall be equipped with appropriate environmental and business continuity controls including fire-suppression systems, climate control and monitoring systems, and emergency backup power systems. Physical information system hardware and supporting infrastructure shall be regularly serviced and maintained in accordance with the manufacturer's recommendations.



5. Working In Secure Areas / Visitor Management

Visitors, delivery personnel, outside support technicians, and other external agents shall not be permitted access to secure areas without escort and/or appropriate oversight. Third-parties in secure areas shall be escorted or monitored by Mursion personnel. Mursion personnel observing unescorted visitors should approach the visitor, confirm their status, and ensure they return to approved areas, or report the observation to the responsible authority. External party access to secure areas shall be confirmed with appropriate Mursion personnel prior to being granted access. Mursion personnel providing access to external parties into secure areas are responsible for ensuring that the third-party personnel adhere to all security requirements and are accountable for all actions taken by outsiders they provide with access. Long-term visitors may be issued a visitor badge identifying them as authorized visitors. Badged visitors may be allowed to work unescorted provided that the Mursion sponsoring party can ensure that they will not have unauthorized access to Mursion information systems, networks, or data.

6. Delivery & Loading Areas

Access points such as delivery and loading areas and other points where unauthorized persons could enter secure areas shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

7. Supplier, Vendor & Third-Party Security

Suppliers, vendors and third-parties shall comply with Mursion physical security and environmental controls requirements. Mursion shall assess the adequacy of third-party physical security controls as part of the vendor management process. Mursion shall interview third-party personnel and review third-party certifications, attestations, audits, audit reports, and questionnaire responses as needed, and ensure that third-parties have made adequate commitments through contracts, service level agreements, or other mechanisms as determined by Mursion. The physical security controls of suppliers, vendors and third-parties shall be assessed and managed in accordance with the Mursion Vendor Security Policy.

4. Amendment/Termination Of This Policy

Mursion reserves the right to modify, amend or terminate this policy at any time. This policy does not constitute a contract between the company and its employees, partners, agents and contractors.

5. Exceptions

Requests for an exception to this Policy must be submitted to authorized personnel for approval. All exception requests will be handled in accordance with the Information Security Exception Policy and Standard.

6. Violations/Enforcement

Any known violations of this policy should be reported to the company's IT department. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with Company procedures. Mursion may advise law enforcement agencies when a criminal offense may have been committed.