

Physical Security Policy

Policy Owner: Diana Hussein

Effective Date: 07/12/22

Purpose

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

Scope

All Darwin Global LLC offices and locations. This Policy applies to all employees of Darwin Global LLC, and to all external parties with physical access to Darwin Global LLC owned or leased facilities.

Policy

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 Darwin Global LLC personnel; such as private offices, wiring closets, print and server rooms, and server racks.

Physical Entry Controls

Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. Where possible, Darwin Global LLC 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.

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 classified data and systems.

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, and alarms, 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.

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 Darwin Global LLC personnel. Darwin Global LLC 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 as needed. External party access to secure areas shall be confirmed with appropriate Darwin Global LLC personnel prior to being granted access. Darwin Global LLC 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. Visitors may be allowed to work unescorted provided that the Darwin Global LLC sponsoring party can ensure that they will not have unauthorized access to Darwin Global LLC information systems, networks, or data.

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.

Supplier, Vendor, and Third-Party Security

Suppliers, vendors, and third parties shall comply with Darwin Global LLC's physical security and environmental controls requirements. Darwin Global LLC shall assess the adequacy of third-party physical security controls as part of the vendor management process, in accordance with the Third-Party Management Policy.

Exceptions

Requests for an exception to this policy must be submitted to the Chief Software Architect and ISO for approval.

Violations & Enforcement

Any known violations of this policy should be reported to any member of management or operations. 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 up to and including termination of employment.

Version	Date	Description	Author	Approved by
1.0	07/12/2022	SOC2/2022	Diana Hussein	Diana Hussein