



Physical Security Policy

Policy Owner: Rohan Ganachari

Effective Date: July 17th, 2023

Purpose

To prevent unauthorized physical access or damage to the organization's information and information processing facilities. As a fully remote company, we prioritize the integrity, confidentiality, and availability of the company and client data, acknowledging that the security of information extends beyond digital boundaries to physical surroundings and environmental conditions.

Scope

All Finsweet locations. This Policy applies to all employees of Finsweet, and to all external parties who handle Finsweet's data, intellectual property, or client data.

Policy

Remote Work Security

Employees must ensure their remote workspace is secure from theft, misuse, environmental threats, unauthorized access, and other threats to the confidentiality, integrity, and availability of classified data and systems. This includes taking reasonable steps to ensure home offices or workspaces are private and protected from unauthorized view.

Environmental Hazards Protection

Employees should make reasonable efforts to ensure that devices are safe from environmental hazards such as water, heat, and dust.

Emergency Preparedness

Employees should have a basic understanding of their local emergency procedures in the event of a fire, natural disaster, or other emergency that could impact the physical security of their workspace.

Equipment Maintenance

Employees are responsible for maintaining their equipment in good working order. Any malfunctions or suspected issues that might compromise security must be reported to Finsweet Security Officer (FSO) immediately.

Visitor Control

In the rare case where visitors have access to devices used for Finsweet work, employees should monitor these visitors to ensure they do not access sensitive information.

Supplier, Vendor, and Third-Party Security

Suppliers, vendors, and third-parties shall comply with Finsweet physical security and environmental controls requirements. Finsweet 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.

Topics not applicable

Since Finsweet is a fully remote company with its entire workforce working from home, the following topics are not applicable to Finsweet.

- N/A. All entry and exit points monitored, logged and reviewed at least every 6 months
- N/A. CCTV monitors ingress/egress points of corporate facility/data centre and retention of logs for 90 days
- N/A. Visitors are escorted with access logging and monitoring
- N/A. Secure restricted zones have multi-layer controls such as biometrics, restrictive access cards, fingerprint sensors, etc. to access sensitive areas.
- N/A. Badge access to building is required
- N/A. Badge access is revoked within 24 hours of termination
- N/A. Signage needs to be displayed at the building entrance instructing users to properly display their badge.
- N/A. Permanent badges need to be deactivated when loaner badges are assigned or activated.
- N/A. All authorized personnel entering the Data Center/telco/MDF room must use dual-factor authentication of card swipe and PIN

Exceptions

Requests for an exception to this policy must be submitted to the FSO for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the FSO. 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	17-Jul-2023	Submit for approval	Rohan Ganachari	Joe Krug