Physical Security Policy

Version number	1.4
Last Approved	Mar 4, 2024
Classification	PUBLIC

Overview

The Physical Security Policy defines The Company's security controls for offices and data centers and aligns these controls to the principle of least access for all persons visiting our locations. The policy also defines tracking and documentation requirements for all facility access.

Applicability

The applicability of this statement falls under purview of the Global Policy Applicability Statement.

Purpose

Physical security is the first and most important line of defence in the protection and privacy of employees and company assets.

Physical security is the responsibility of every employee of The Company. Security measures have been put in place to ensure that The Company's security stance is maintained at the highest degree possible at all times.

Scope

This policy applies to all employees, contractors, visitors and LTG offices, including facilities containing critical IT resources or sensitive information.

Physical Security Perimeter Policy

Objectives

1. To prevent unauthorised physical access, damage and interference to the organisation’s facilities.

Responsibilities

2. The Facilities team is responsible for managing access to secure areas.

3. All employees should immediately notify security personnel if they encounter unescorted visitors and immediately report any suspicious activity for follow-up investigation.

4. All employees should ensure any Health and Safety issues have been identified and addressed.

Office Security

5. All sites must have alarms fitted, which are tested and maintained regularly.

6. All contractors and third parties are required to wear an identification badge return it at the end of their visit.

7. Access to secure areas where confidential or restricted information is processed or stored is restricted to authorised persons. Authorisation is provided by Facilities or approved by a senior manager onsite.

8. Access to critical IT systems is limited to authorised personnel only and requires PIN, a swipe/contact proximity card, or a security code for entrance". Mechanical locks can be used as well, assuming CCTV is in place for monitoring.

9. Access to a delivery and loading area from outside of the building should be restricted to identified and authorised personnel.

10. Only authorised maintenance personnel should carry out repairs and service equipment.

11. Critical IT equipment should not be taken off-site without prior authorisation.

12. Visitors must be accompanied by a responsible employee at all times.

13. “Coat tailing” (i.e., allowing another person to access office spaces without badging in) is strictly prohibited.

Data center security

14. We require increased stringency in security at data centers. The requirements apply universally to any data center that may hold client data irrespective of implementation, such as cloud, on premise or colocation.

15. We require data centers to be protected by the following security measures:
    a. **Perimeter security:** Perimeter fencing, entry points, video surveillance
    b. **Access control:** Multi-layered authentication is required, such as an RFID badge, PIN code, and biometric scanning. Entry systems to prevent tailgating and visitor management procedures must be in place as well as access logs

c. **Internal security:** Physical separation between high and lower security areas, server room access requires at least two levels of authentication for entry. High security areas should be covered by video surveillance
d. **Environmental controls:** Fire suppression systems, climate control and backup power and/or uninterruptable power supply
e. **Resilience and compliance:** Emergency response and disaster recovery plans must be in place along with appropriate security standards such as ISO 27001, and SOC 2. Auditing, penetration testing and BC/DR plan testing should be implemented.
f. **Security personnel:** Appropriately background checked and trained, on duty 24/7
g. **Assets and hardware:** Acquisition and transport of assets is controlled.
h. **Storage media:** Secure media disposal and destruction must be in place and aligned to industry standards.

Document control

This policy is only controlled in its live, digital format. Any other format or export of this policy is an uncontrolled version of this document

Document Owner	@Paul Gordon	
Author(s)	@Paul Gordon	
Required Approver(s) and Approval Date	@Paul Gordon - QHSE Coordinator	Dec 4, 2023
	@Emma Burton - Operations Manager	Mar 4, 2024
Review cycle	ANNUAL	
Next review date	Dec 3, 2024	

Version History

Date	Author(s)	Version	Changes
Nov 18, 2024	@Paul Gordon @angelina.kilmer	1.4	Updated formatting & Classification from Confidential to Public
Nov 11, 2024	@Paul Gordon	1.3	Policy expanded to differentiate between office and data center security
Mar 28, 2024	@Paul Gordon	1.2	Update to elaborate on security measures
Dec 4, 2023	@Paul Gordon	1.1	Updated following change in how we utilise our office space, for example hotdesking

Mar 1, 2018	@Aleksandr Zaldak	1.0	Original