					[Insert Registered Legal Entity Name Here]							
Document number: P10S					Document Title: **Clear Desk and Screen Policy**							
Version: 1.0		Effective Date: 01.01.2025			Document Owner:							
X	Policy		Standard		Procedure		Form		Register		Other	

Revision history				
Revision number	**Revision Date**	**Changes**	**Reviewed by**	**Process owner**

Approvals			
Name	**Title**	**Date**	**Signature**

Aligned with standards and regulations where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	Clauses 7.2, 8.1	
ISO/IEC 27002:2022	Control 7.7	
NIST SP 800-53 Rev.5	PE-2, AC-11	
EU NIS2	Article 21(2)(d)	
EU DORA	Article 9(2)(f)	
COBIT 2019	DSS01.06, DSS05.02	
EU GDPR	Article 32	

					[Insert Registered Legal Entity Name Here]								
Document number: P10S					Document Title: **Clear Desk and Screen Policy**								
Version: 1.0		Effective Date: 01.01.2025			Document Owner:								
X	Policy		Standard		Procedure		Form		Register		Other		

1. **Purpose**
   1.1. This policy establishes enforceable guidelines for maintaining a secure working environment by ensuring that desks, workstations, and display screens are kept free of visible confidential information when unattended.
   1.2. Its main purpose is to prevent unauthorized access to sensitive information through unattended printouts, unlocked screens, or misplaced removable media in both physical office environments and remote work locations.
   1.3. The clear desk and screen practices defined in this policy strengthen our organization's ability to meet ISO/IEC 27001 certification requirements by minimizing preventable exposure risks. These practices also reassure customers, partners, and auditors that we take information security seriously, even in resource-constrained environments.
   1.4. This policy supports a culture of accountability and awareness, ensuring that all personnel-regardless of role or technical expertise-understand their responsibility to protect company and customer information from visual exposure, theft, or loss.
2. **Scope**
   2.1. This policy applies to:
      2.1.1. All employees, contractors, interns, and temporary staff using company-owned or personally assigned workstations, desks, or mobile devices
      2.1.2. All physical locations used for business activity, including dedicated offices, coworking environments, and remote/home-based workspaces
      2.1.3. All digital devices with display capabilities, including desktops, laptops, tablets, and external monitors used for business purposes
   2.2. The policy extends to any physical or digital asset that can display, contain, or transmit sensitive information, including:
      2.2.1. Printed records or hand-written notes
      2.2.2. USB drives, CDs, and external hard drives
      2.2.3. Mobile phones used for business messaging or email
      2.2.4. Computer monitors and projectors connected to work systems
   2.3. This policy remains applicable outside regular working hours and during non-standard operations (e.g., after-hours maintenance or emergency response work).
3. **Objectives**
   3.1. To enforce practical, consistent controls that ensure no sensitive information is left exposed on desks, screens, or communal spaces.
   3.2. To minimize the risk of unauthorized access, both from internal sources (e.g., unintentional access by other employees) and external threats (e.g., visitors, cleaning staff, or contractors).
   3.3. To support physical and logical access restrictions by requiring staff to actively secure work materials and lock computers when unattended.
   3.4. To build staff awareness of secure working practices and provide simple, enforceable rules applicable in day-to-day operations, regardless of the working location.

3.5. To ensure alignment with ISO/IEC 27001 Annex A Control 7.7 and its implementation guidance under ISO/IEC 27002 for clear desk and screen requirements.

3.6. To ensure organization can demonstrate due diligence and readiness for audits without requiring enterprise-grade infrastructure.

4. Roles and Responsibilities

4.1. **General Manager (GM)**

4.1.1. Owns this policy and ensures it is properly communicated, understood, and followed by all employees and contractors.

4.1.2. Is responsible for approving any exceptions, responding to violations, and overseeing training related to secure work practices.

4.1.3. Must perform or delegate regular checks (at least quarterly) to confirm that physical and digital workspaces meet the policy's expectations.

4.2. **Designated Staff Member (if assigned)**

4.2.1. May be assigned responsibility for implementing technical configurations (e.g., screen timeout settings) or distributing physical storage materials (e.g., locking drawers).

4.2.2. Supports the GM by reporting non-compliance, handling workspace security reminders, and tracking remediation steps when issues are identified.

4.2.3. Helps ensure that all employees have access to appropriate locking mechanisms or secure storage spaces where feasible.

4.3. **All Employees and Contractors**

4.3.1. Must follow all practical safeguards defined in this policy, including locking screens and securing documents when stepping away from their desk.

4.3.2. Are required to avoid leaving confidential materials in meeting rooms, shared printers, or unattended workstations.

4.3.3. Must not rely solely on digital controls-digital controls (e.g., session timeouts) are necessary but insufficient; physical safeguards like locked cabinets or drawers are also required.

4.3.4. Must report any workspace risks or violations observed, even if not directly responsible for the asset in question.

5. Governance Requirements

5.1. The GM must ensure the policy is embedded in the employee onboarding and induction process. This includes briefing new hires on:

5.1.1. How to manually lock their device

5.1.2. How to securely store confidential documents

5.1.3. What qualifies as a policy violation

5.2. Screen timeout configurations (e.g., auto-lock after 5 minutes of inactivity) must be enforced where technically feasible, either by external IT providers or locally installed settings.

5.3. All company workspaces-whether permanent or shared-must have access to physical storage options for securing documents and portable media.

5.4. Where secure storage is not feasible, personnel must carry materials with them when temporarily leaving the space or seek supervisor authorization for alternate arrangements.

5.5. The GM must document and retain records of any compliance checks or training events related to clear desk and screen practices. These records may be reviewed during internal audits or certification assessments.

6. Policy Implementation Requirements

6.1. **Clear Desk Enforcement**

6.1.1. All staff must ensure that at the end of the working day, or whenever leaving their desk for a prolonged period, no sensitive material remains exposed.

[……..]

Reference Standards and Frameworks

ISO/IEC 27001:2022

Clause 7.2: Requires all staff to be aware of security responsibilities, including physical safeguarding.
Clause 8.1: Operational controls must ensure appropriate physical and logical protections.

ISO/IEC 27002:2022

Control 7.7: Provides detailed guidance on establishing, communicating, and enforcing clear desk and screen requirements.

NIST SP 800-53 Rev.5

PE-2: Establishes physical access control expectations, including personnel behavior within secure environments.

AC-11: Mandates session lock functionality for workstations to prevent unauthorized viewing or interaction.

EU GDPR

Article 32: Requires organizations to protect personal data using physical and technical safeguards, including workstations and documents.

EU NIS2 Directive

Article 21(2)(d*)*: Requires organizations to implement risk-based physical and logical access policies.

EU DORA

Article 9(2)(f): Mandates ICT security policies, including secure workspace hygiene, for financial sector operators and their supply chains.

COBIT 2019

DSS01.06: Requires asset protection practices, including physical controls over workspaces and media.

DSS05.02: Supports enforcement of end-user security practices across operating environments.