					Insert Registered Legal Entity Name Here							
Document number: P10S					Document Title: **Clear Desk and Screen Lock 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

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clauses 7.2, 8	
ISO/IEC 27002:2022	Control 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	
EU GDPR	Article 32	

1. Purpose

1.1 This policy defines mandatory requirements for maintaining a secure working environment by ensuring that desks, workstations and display screens do not expose confidential information when unattended.

1.2 The primary purpose of this policy is to prevent unauthorized access to sensitive information through unattended printouts, unlocked screens or misplaced removable media in both office environments and remote working locations.

1.3 The clear desk and screen practices defined in this policy strengthen the organization's ability to meet ISO/IEC 27001 certification requirements by reducing avoidable exposure risks. These practices also demonstrate to customers, partners and auditors that information security is taken seriously, including in resource-constrained environments.

1.4 This policy supports a culture of accountability and awareness by 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, third-party service providers, interns and temporary workers using company-owned or personally assigned workstations, desks or mobile devices

2.1.2 All physical locations used for business activities, including dedicated offices, coworking environments and remote or 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 This policy also applies to any physical or digital asset that can display, contain or transmit sensitive information, including:

2.2.1 Printed records or handwritten 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, such as after-hours maintenance or emergency response activities.

3. Objectives

3.1 To enforce practical and consistent controls so that no sensitive information is left exposed on desks, screens or in shared spaces.

3.2 To minimize the risk of unauthorized access from both internal sources, such as unintended access by other employees, and external threats, such as visitors, cleaning personnel or contractors.

3.3 To support physical and logical access restrictions by requiring personnel to actively secure work materials and lock computers when unattended.

3.4 To strengthen security awareness of secure working practices and provide simple, enforceable rules for day-to-day operations regardless of work location.

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

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

4. Roles and Responsibilities

4.1 General Manager

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

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

4.1.3 Must perform, or delegate, regular checks at least quarterly to confirm that physical and digital workspaces meet the requirements of this policy.

4.2 Designated staff member, if assigned

4.2.1 May be assigned responsibility for implementing technical configurations, such as screen timeout settings, or distributing physical storage solutions, such as lockable drawers.

4.2.2 Supports the General Manager by reporting non-compliance, issuing workspace security reminders and tracking remediation actions when issues are identified.

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

[... Sections 4.3–8 are not included in this preview. Purchase the full document to access the complete policy content. ...]

9. Review and Update Requirements

9.1 The General Manager must review this policy at least annually and after any of the following events:

9.1.1 Introduction of new office spaces, devices or shared systems

9.1.2 Changes to applicable legal or certification requirements

9.1.3 Findings from audits, risk assessments or security incidents

9.2 Interim updates must be communicated to all employees by email, and acknowledgment is required.

9.3 Previous versions of this policy must be stored securely and remain auditable to demonstrate continued alignment with ISO/IEC 27001 and related frameworks.

10. Related Policies and Linkages

10.1 P2S – Governance Roles and Responsibilities Policy: Clarifies the authority of the General Manager to enforce and audit behaviour within physical and digital workspaces.

10.2 P4S – Access Control Policy: Supports the technical implementation of screen locking and secure workstation logon practices.

10.3 P8S – Information Security Awareness and Training Policy: Reinforces the behavioural training required for compliance with this policy.

10.4 P17S – Data Protection and Privacy Policy: Defines obligations for handling and protecting personal data and sensitive data in compliance with GDPR.

10.5 P30S – Incident Response Policy: Provides the escalation and response framework where a violation results in data exposure or a breach.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

11.1.1 Clause 7.2: Requires all personnel to be aware of their security responsibilities, including physical protection measures.

11.1.2 Clause 8.1: Requires operational controls to ensure appropriate physical and logical protection.

11.2 ISO/IEC 27002

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

11.3 NIST SP 800-53 Rev.5

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

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

11.4 EU GDPR

11.4.1 Article 32: Requires organizations to protect personal data through physical and technical safeguards, including protections for workstations and documents.

11.5 EU NIS2 Directive

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

11.6 EU DORA

11.6.1 Article 9(2)(f): Requires ICT security policies, including secure workspace practices, for financial sector entities and their supply chains.

11.7 COBIT 2019

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

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