					[Insert Registered Legal Entity Name Here]								
Document number: P10					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	Clause 6.1.3, Clause 8.1	
ISO/IEC 27002:2022	Control 7.7	
NIST SP 800-53 Rev.5	PE-2, PS-7	
EU GDPR	Articles 5(1)(f), 32; Recital 39	
EU NIS2	Articles 21(2)(d), 21(3)	
EU DORA	Articles 5, 8, 9	
COBIT 2019	DSS01, DSS05, MEA03	

<table>
<tr><td colspan="3"></td><td colspan="9">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="3">Document number:
P10</td><td colspan="9">Document Title:
Clear Desk and Screen Policy</td></tr>
<tr><td colspan="2">Version:
1.0</td><td colspan="2">Effective Date:
01.01.2025</td><td colspan="9">Document Owner:</td></tr>
<tr><td>X</td><td>Policy</td><td></td><td>Standard</td><td></td><td>Procedure</td><td></td><td>Form</td><td></td><td>Register</td><td></td><td>Other</td></tr>
</table>

1. Purpose

1.1 This policy establishes mandatory controls to protect sensitive information by requiring the secure handling of physical documents, workstations, screens, and removable media in both office and shared workspace environments.

1.2 It supports ISO/IEC 27001 Annex A Control 7.7 by enforcing behavioral and technical practices that mitigate the risk of unauthorized disclosure, theft, or loss of data due to unattended or visible information.

1.3 This policy reinforces physical and information security in daily operations and supports compliance with applicable legal, contractual, and regulatory obligations.

2. Scope

2.1 This policy applies to all personnel operating in or accessing physical workspaces, including:

2.1.1 Permanent and temporary employees

2.1.2 Contractors, consultants, vendors, and interns

2.1.3 Third-party service providers and on-site visitors with access to sensitive information

2.2 The requirements apply in:

2.2.1 Individual offices, cubicles, and open-plan workspaces

2.2.2 Meeting rooms and shared collaboration areas

2.2.3 Printer stations, reception desks, and copy rooms

2.2.4 Areas where remote workstations or shared kiosks are used

2.3 This policy also applies to temporary or hybrid work environments (e.g., hot-desking) and public-facing settings where risk of shoulder surfing or unattended data exists.

3. Objectives

3.1 To prevent unauthorized access to confidential, sensitive, or regulated information left exposed in physical or digital form.

3.2 To promote a standardized security posture across all work environments through the use of physical safeguards, workstation configuration, and end-user behavior.

3.3 To reduce the risk of privacy breaches, intellectual property loss, and data exfiltration caused by negligence or oversight.

3.4 To embed clean desk and screen behavior into organizational culture, supporting operational discipline, auditability, and legal defensibility.

3.5 To support compliance with ISO/IEC 27001, GDPR Article 32, NIS2 Article 15, and other physical security requirements relevant to critical or personal data.

4. Roles and Responsibilities

4.1 **Executive Management**

4.1.1 Endorses this policy and promotes a security-aware culture throughout all business units.

4.1.2 Allocates appropriate resources for policy enforcement, awareness campaigns, and physical control mechanisms.

4.2 **CISO / ISMS Manager**

[……]

11. Reference Standards and Frameworks

This policy is aligned with globally recognized standards and legal requirements that mandate the safeguarding of sensitive information in physical environments and through user behavior.

ISO/IEC 27001:2022

Clause 6.1.3 – Risk Treatment Plan: Supports control implementation for mitigating physical and environmental risks, including those tied to user behavior in open workspaces.

Clause 8.1 – Operational Planning and Control: Establishes operational safeguards to manage secure workspaces and equipment usage.

ISO/IEC 27002:2022 – Control 7.7

This control mandates behavioral and environmental protections to prevent unauthorized access to information via unattended media, screens, or printed materials. The policy enforces physical workspace hygiene, lock screen use, and disposal of sensitive documents.

NIST SP 800-53 Rev.5

PE-2 (Physical Access Authorizations): Linked through workspace restrictions and locked storage enforcement in high-risk environments.

PS-7 (External Personnel Security): Applied through clean desk and screen requirements extended to contractors and third-party users.

MP-6 (Media Sanitization) and **AC-11 (Session Lock)**: Implemented through secure disposal procedures and mandatory screen lock timers.

CM-6 (Configuration Settings) and **IA-5 (Authenticator Management)**: Support technical enforcement of screen locking and session control on endpoints.

EU GDPR (2016/679)

Article 5(1)(f): Enforces integrity and confidentiality of personal data, including protections against physical exposure or viewing by unauthorized persons.

Article 32 – Security of Processing: Requires appropriate physical and organizational measures to protect personal data from accidental or unlawful destruction, loss, or unauthorized disclosure—achieved through desk and screen controls.

Recital 39: Requires limiting access to personal data to authorized individuals—this includes securing it in physical form when unattended.

EU NIS2 Directive (2022/2555)

Article 21(2)(d): Requires policies and procedures related to physical and environmental security, including workplace-level information security protections.

Article 21(3): Encourages a security culture that incorporates good user behavior, awareness, and prevention of unintentional data leaks—supported by this policy's behavioral controls.

EU DORA (2022/2554)

Article 5 – Internal Governance and Control: Requires that all ICT-related risks, including human and environmental threats, are governed through enforceable policies.

Article 8 – ICT Risk Management: Enforces safeguards in both digital and physical contexts, ensuring that remote, branch, and on-premises users do not create unmanaged exposure.

Article 9 – Incident Management: Requires that environmental or behavioral lapses resulting in data exposure be logged, classified, and addressed with appropriate corrective actions.

COBIT 2019

DSS01 – Managed Operations: Ensures operational discipline in protecting physical workspaces and systems through repeatable controls.

DSS05 – Managed Security Services: Supports the protection of data, devices, and access endpoints through behavior-based enforcement like clean desk practices.

MEA03 – Monitor, Evaluate, and Assess Compliance: Encourages auditing of physical safeguards and policy adoption in daily business practices.