					Insert Registered Legal Entity Name Here							
Document number: P10					Document Title: **Clean Desk Policy and Clear 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

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 6.1.3, Clause 8	Risk treatment planning, operational planning, and controls for secure workspaces
ISO/IEC 27002:2022	Control 7	Behavioral and environmental controls to protect unattended physical information
NIST SP 800-53 Rev.5	PE-2, PS-7, MP-6, AC-11, CM-6, IA-5	Physical access, external personnel security, media sanitization, session lock, configuration, and authenticator controls
EU GDPR	Articles 5(1)(f), 32; Recital 39	Data integrity, confidentiality, and physical safeguards for personal data
EU NIS2	Articles 21(2)(d), 21(3)	Policies for physical security, user behavior, and data leakage prevention
EU DORA	Articles 5, 8, 9	Internal governance, ICT risk management, and incident management involving physical security
COBIT 2019	DSS01, DSS05, MEA	Managed operations, security services, and compliance monitoring

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 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 resulting from unattended or visible information.

1.3 This policy strengthens physical and information security in day-to-day 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 workers

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 environments (e.g., hot-desking) and public-facing settings where there is a risk of shoulder surfing or unattended data exposure.

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 controls, 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 clear screen practices into the 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 Top Management

4.1.1 Approves this policy and promotes a security-aware culture across all business units.

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

4.2 CISO / ISMS Manager

4.2.1 Owns this policy and ensures alignment with ISO/IEC 27001:2022, audit requirements, and risk treatment strategies.

4.2.2 Develops awareness programs and controls to ensure consistent implementation across facilities and hybrid environments.

4.2.3 Coordinates with Facilities and IT to ensure appropriate physical safeguards are in place.

[... 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 Policy Review Schedule

9.1.1 This policy shall be reviewed:

9.1.1.1 At least annually

9.1.1.2 After any audit nonconformity related to workspace or screen exposure

9.1.1.3 Following any physical or environmental incident (e.g., device theft, tailgating, surveillance)

9.1.1.4 Upon implementation of new office layouts, facility policies, or workspace models (e.g., hot-desking, remote hubs)

9.2 Responsible Owners

9.2.1 The policy owner is the CISO or the appointed ISMS Manager.

9.2.2 The review process shall involve:

9.2.2.1 Facilities and Corporate Security teams

9.2.2.2 IT and IT infrastructure teams for device-related enforcement

9.2.2.3 Human Resources (HR) and Legal and Compliance for behavioral enforcement and disciplinary alignment

9.2.3 All policy updates must be version controlled, approved by the ISMS Steering Committee, and redistributed with re-acknowledgment where required.

9.3 Change Communication

9.3.1 Users shall be notified of material updates through:

9.3.1.1 The intranet policy center or portal

9.3.1.2 Targeted email communications

9.3.1.3 Onboarding refreshers and quarterly briefings

9.3.1.4 Mandatory acknowledgment prompts for any new critical enforcement clauses

10. Related Policies and Linkages

10.1 This policy aligns with and supports the following:

10.1.1 P1 – Information Security Policy: Establishes user behavior and physical security expectations that underpin this policy.

10.1.2 P3 – Acceptable Use Policy: Addresses user accountability for protecting data and systems, including in physical environments.

10.1.3 P6 – Risk Management Policy: Incorporates physical workspace risks into enterprise-wide information risk analysis.

10.1.4 P12 – Asset Management Policy: Supports the tracking and secure handling of devices and media left at desks.

10.1.5 P13 – Data Classification and Labeling Policy: Links to clean desk enforcement for physical documents labeled Confidential or Internal.

10.1.6 P14 – Data Retention and Disposal Policy: Provides guidance on physical document retention, shredding, and secure disposal bin handling.

10.1.7 P22 – Logging and Monitoring Policy: May be used to monitor workstation lock status, idle time, or workspace camera feeds where permitted.

10.2 These related policies establish an integrated security culture that combines user awareness, physical controls, and accountability to support resilient workspaces.

11. Reference Standards and Frameworks

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

11.2 ISO/IEC 27001

11.2.1 Clause 6.1.3 – Risk Treatment Plan: Supports the implementation of controls to mitigate physical and environmental risks, including those associated with user behavior in open workspaces.

11.2.2 Clause 8.1 – Operational Planning and Control: Establishes operational safeguards for the management of secure workspaces and equipment use.

11.3 ISO/IEC 27002:2022 – Control 7

11.3.1 This control requires behavioral and environmental protections to prevent unauthorized access to information through unattended media, screens, or printed materials. This policy enforces physical workspace discipline, screen locking, and the secure disposal of sensitive documents.

11.4 NIST SP 800-53 Rev.5

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

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

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

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

11.5 EU GDPR (2016/679)

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

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

11.5.3 Recital 39: Requires access to personal data to be limited to authorized individuals, including securing such data in physical form when unattended.

11.6 EU NIS2 Directive (2022/2555)

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

11.6.2 Article 21(3): Promotes a security culture incorporating appropriate user behavior, awareness, and prevention of unintentional data leakage, supported by the behavioral controls in this policy.

11.7 EU DORA (2022/2554)

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

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

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

11.8 COBIT 2019

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

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

11.8.3 MEA03 – Monitor, Evaluate, and Assess Compliance: Promotes the auditing of physical safeguards and policy adoption in day-to-day business practices.