					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P10					Dokumenttitel: **Richtlinie zu Clean Desk und Clear Screen**							
Version: 1.0		Datum des Inkrafttretens: 01.01.2025			Dokumentenverantwortlicher:							
X	Richtlinie		Standard		Verfahren		Formular		Register		Sonstiges	

Änderungshistorie				
Änderungsnummer	**Änderungsdatum**	**Änderungen**	**Geprüft von**	**Prozessverantwortlicher**

Genehmigungen			
Name	**Position**	**Datum**	**Unterschrift**

Ausgerichtet an Standards und regulatorischen Anforderungen

Standard/Vorschrift	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klausel 6.1.3, Klausel 8	Risikobehandlungsplan, operative Planung und Kontrollen für sichere Arbeitsbereiche
ISO/IEC 27002:2022	Maßnahme 7	Verhaltensbezogene und umgebungsbezogene Kontrollen zum Schutz unbeaufsichtigter physischer Informationen
NIST SP 800-53 Rev.5	PE-2, PS-7, MP-6, AC-11, CM-6, IA-5	Physischer Zutritt, Sicherheit von Auftragnehmern, Entsorgung von Datenträgern, Sitzungssperre sowie Konfigurations- und Authentifikatorenkontrollen
DSGVO	Artikel 5(1)(f), 32; Erwägungsgrund 39	Datenintegrität, Vertraulichkeit und physische Schutzmaßnahmen für Daten
NIS2	Artikel 21(2)(d), 21(3)	Richtlinien für physische Sicherheit, Benutzerverhalten und Verhinderung von Datenabfluss
DORA	Artikel 5, 8, 9	Interne Governance, IKT und Vorfallmanagement unter Einbeziehung physischer Sicherheit
COBIT 2019	DSS01, DSS05, MEA	Gesteuerter Betrieb, Sicherheitsdienste und Überwachung der Einhaltung

1. Zweck

1.1 Diese Richtlinie legt verbindliche Kontrollen zum Schutz sensibler Informationen fest, indem sie den sicheren Umgang mit physischen Dokumenten, Arbeitsplätzen, Bildschirmen und Wechselmedien sowohl in Büroumgebungen als auch in gemeinsam genutzten Arbeitsbereichen vorschreibt.

1.2 Sie unterstützt ISO/IEC 27001 Anhang A Maßnahme 7.7, indem sie verhaltensbezogene und technische Praktiken verbindlich festlegt, die das Risiko unbefugter Offenlegung, Diebstahls oder Datenverlusts aufgrund unbeaufsichtigter oder sichtbar ausliegender Informationen mindern.

1.3 Diese Richtlinie stärkt die physische Sicherheit und die Informationssicherheit im Tagesgeschäft und unterstützt die Einhaltung geltender gesetzlicher, vertraglicher und regulatorischer Verpflichtungen.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für sämtliches Personal, das in physischen Arbeitsbereichen tätig ist oder auf diese zugreift, einschließlich:

2.1.1 festangestellter und befristet beschäftigter Mitarbeiter

2.1.2 Auftragnehmern, Beratern, Lieferanten und Praktikanten

2.1.3 Drittanbieter-Dienstleistern und Besuchern vor Ort mit Zugriff auf sensible Informationen

2.2 Die Anforderungen gelten in:

2.2.1 Einzelbüros, Büroarbeitsplätzen und Großraumbüros

2.2.2 Besprechungsräumen und gemeinsam genutzten Kollaborationsbereichen

2.2.3 Druckerbereichen, Empfangstheken und Kopierräumen

2.2.4 Bereichen, in denen Remote-Arbeitsplätze oder gemeinsam genutzte Kiosksysteme genutzt werden

2.3 Diese Richtlinie gilt auch für temporäre oder hybride Arbeitsumgebungen (z. B. Desk Sharing) sowie für öffentlich zugängliche Umgebungen, in denen das Risiko des Mitlesens über die Schulter oder unbeaufsichtigter Daten besteht.

3. Ziele

3.1 Verhinderung des unbefugten Zugriffs auf vertrauliche, sensible oder regulierte Informationen, die in physischer oder digitaler Form offen einsehbar sind.

3.2 Förderung eines einheitlichen Informationssicherheitsniveaus in allen Arbeitsumgebungen durch physische Schutzmaßnahmen, Arbeitsplatzkonfigurationen und Benutzerverhalten.

3.3 Verringerung des Risikos von Datenschutzverletzungen, des Verlusts geistigen Eigentums und der Datenexfiltration infolge von Fahrlässigkeit oder Unachtsamkeit.

3.4 Verankerung eines Clean-Desk- und Clear-Screen-Verhaltens in der Unternehmenskultur zur Unterstützung operativer Disziplin, Auditierbarkeit und regulatorischer Resilienz.

3.5 Unterstützung der Einhaltung von ISO/IEC 27001, Artikel 32 DSGVO, Artikel 15 NIS2 und weiteren Anforderungen an die physische Sicherheit im Zusammenhang mit kritischen oder personenbezogenen Daten.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsleitung

4.1.1 Genehmigt diese Richtlinie und fördert in allen Geschäftsbereichen eine sicherheitsbewusste Unternehmenskultur.

4.1.2 Stellt angemessene Ressourcen für die Durchsetzung der Richtlinie, Sensibilisierungskampagnen und physische Kontrollmechanismen bereit.

4.2 CISO / ISMS-Manager

4.2.1 Ist für diese Richtlinie verantwortlich und stellt ihre Ausrichtung an ISO/IEC 27001:2022, Audit-Anforderungen und Risikobehandlungsstrategien sicher.

4.2.2 Entwickelt Sensibilisierungsprogramme und Kontrollen, um eine konsistente Umsetzung über Standorte und hybride Arbeitsumgebungen hinweg sicherzustellen.

4.2.3 Stimmt sich mit dem Facility Management und der IT ab, um sicherzustellen, dass angemessene physische Schutzmaßnahmen vorhanden sind.

[... Abschnitte 4.3–8 sind in dieser Vorschau nicht enthalten. Erwerben Sie das vollständige Dokument, um auf den gesamten Inhalt zuzugreifen. ...]

9. Anforderungen an Überprüfung und Aktualisierung

9.1 Zeitplan für die Richtlinienüberprüfung

9.1.1 Diese Richtlinie ist zu überprüfen:

9.1.1.1 mindestens jährlich

9.1.1.2 nach jeder Audit-Nichtkonformität im Zusammenhang mit Arbeitsplatz- oder Bildschirmexposition

9.1.1.3 nach einem physischen oder umgebungsbezogenen Vorfall (z. B. Gerätediebstahl, Tailgating, Überwachung)

9.1.1.4 bei Einführung neuer Bürokonzepte, Standortregelungen oder Arbeitsplatzmodelle (z. B. Desk Sharing, Remote-Hubs)

9.2 Verantwortliche

9.2.1 Der Richtlinienverantwortliche ist der CISO oder ein benannter ISMS-Manager.

9.2.2 Am Überprüfungsprozess sind zu beteiligen:

9.2.2.1 Teams aus Facility Management und Corporate Security

9.2.2.2 IT und Infrastruktur für die technische Durchsetzung auf Endgeräten

9.2.2.3 HR und Rechtsabteilung für Verhaltensdurchsetzung und die Abstimmung disziplinarischer Maßnahmen

9.2.3 Alle Aktualisierungen dieser Richtlinie müssen versionskontrolliert, durch den Informationssicherheitslenkungsausschuss genehmigt und bei Bedarf mit erneuter Bestätigung verteilt werden.

9.3 Kommunikation von Änderungen

9.3.1 Benutzer sind über wesentliche Aktualisierungen zu informieren über:

9.3.1.1 das Richtlinienportal oder Policy Center im Intranet

9.3.1.2 gezielte E-Mail-Kommunikation

9.3.1.3 Auffrischungen im Onboarding und vierteljährliche Briefings

9.3.1.4 verpflichtende Bestätigungsaufforderungen für neue kritische Durchsetzungsklauseln

10. Zugehörige Richtlinien und Verknüpfungen

10.1 Diese Richtlinie ist mit den folgenden Richtlinien abgestimmt und unterstützt diese:

10.1.1 P1 – Informationssicherheitsrichtlinie: Legt Verhaltenserwartungen an Benutzer und Anforderungen an die physische Sicherheit fest, die dieser Richtlinie zugrunde liegen.

10.1.2 P3 – Richtlinie zur zulässigen Nutzung: Behandelt die Verantwortung der Benutzer für den Schutz von Daten und Systemen, einschließlich physischer Umgebungen.

10.1.3 P6 – Risikomanagement-Richtlinie: Bezieht Risiken physischer Arbeitsbereiche in die unternehmensweite Analyse von Informationsrisiken ein.

10.1.4 P12 – Richtlinie zum Asset Management: Unterstützt die Nachverfolgung und den sicheren Umgang mit Geräten und Datenträgern, die auf Schreibtischen zurückgelassen werden.

10.1.5 P13 – Richtlinie zur Datenklassifizierung und Kennzeichnung: Verknüpft die Durchsetzung von Clean Desk mit physischen Dokumenten, die als vertraulich oder intern gekennzeichnet sind.

10.1.6 P14 – Richtlinie zur Datenaufbewahrung und Entsorgung: Regelt die Aufbewahrung physischer Dokumente, das Schreddern und den Umgang mit Entsorgungsbehältern.

10.1.7 P22 – Richtlinie zur Protokollierung und Überwachung: Kann zur Überwachung des Sperrstatus von Arbeitsplatzsystemen, der Leerlaufzeit oder von Kameraaufzeichnungen in Arbeitsbereichen eingesetzt werden, soweit zulässig.

10.2 Diese zugehörigen Richtlinien schaffen eine integrierte Sicherheitskultur, die Benutzerbewusstsein, physische Schutzmaßnahmen und Rechenschaftspflicht verbindet, um resiliente Arbeitsbereiche sicherzustellen.

11. Referenzstandards und Rahmenwerke

11.1 Diese Richtlinie ist an weltweit anerkannten Standards und gesetzlichen Anforderungen ausgerichtet, die den Schutz sensibler Informationen in physischen Umgebungen und durch angemessenes Benutzerverhalten vorschreiben.

11.2 ISO/IEC 27001

11.2.1 Klausel 6.1.3 – Risikobehandlungsplan: Unterstützt die Umsetzung von Kontrollen zur Minderung physischer und umgebungsbezogener Risiken, einschließlich solcher, die mit Benutzerverhalten in offenen Arbeitsumgebungen verbunden sind.

11.2.2 Klausel 8.1 – Operative Planung und Steuerung: Legt operative Schutzmaßnahmen zur Verwaltung sicherer Arbeitsbereiche und der Nutzung von Geräten fest.

11.3 ISO/IEC 27002:2022 – Maßnahme 7

11.3.1 Diese Maßnahme verlangt verhaltensbezogene und umgebungsbezogene Schutzmaßnahmen, um den unbefugten Zugriff auf Informationen über unbeaufsichtigte Datenträger, Bildschirme oder gedruckte Unterlagen zu verhindern. Die Richtlinie setzt physische Arbeitsplatzhygiene, die Verwendung von Bildschirmsperren und die Entsorgung sensibler Dokumente verbindlich fest.

11.4 NIST SP 800-53 Rev.5

11.4.1 PE-2 (Genehmigungen für physischen Zutritt): Umgesetzt durch Arbeitsplatzbeschränkungen und die Durchsetzung verschlossener Aufbewahrung in Hochrisikoumgebungen.

11.4.2 PS-7 (Sicherheit externer Mitarbeiter): Umgesetzt durch Clean-Desk- und Clear-Screen-Anforderungen, die auch auf Auftragnehmer und Benutzer Dritter ausgeweitet werden.

11.4.3 MP-6 (Bereinigung von Medien) und AC-11 (Sitzungssperre): Umgesetzt durch Verfahren zur sicheren Entsorgung und verpflichtende Zeitgeber für Bildschirmsperren.

11.4.4 CM-6 (Konfigurationseinstellungen) und IA-5 (Verwaltung von Authentifikatoren): Unterstützen die technische Durchsetzung von Bildschirmsperre und Sitzungssteuerung auf Endgeräten.

11.5 DSGVO (2016/679)

11.5.1 Artikel 5(1)(f): Erzwingt die Integrität und Vertraulichkeit personenbezogener Daten, einschließlich des Schutzes vor physischer Offenlegung oder Einsichtnahme durch unbefugte Personen.

11.5.2 Artikel 32 – Sicherheit der Verarbeitung: Verlangt geeignete physische und organisatorische Maßnahmen zum Schutz personenbezogener Daten vor unbeabsichtigter oder unrechtmäßiger Zerstörung, Verlust oder unbefugter Offenlegung – umgesetzt durch Schreibtisch- und Bildschirmkontrollen.

11.5.3 Erwägungsgrund 39: Verlangt die Beschränkung des Zugriffs auf personenbezogene Daten auf berechtigte Personen – dies umfasst auch deren Schutz in physischer Form bei unbeaufsichtigtem Zustand.

11.6 NIS2-Richtlinie (2022/2555)

11.6.1 Artikel 21(2)(d): Verlangt Richtlinien und Verfahren im Zusammenhang mit physischer und umgebungsbezogener Sicherheit, einschließlich informationssicherheitsbezogener Schutzmaßnahmen auf Arbeitsplatzebene.

11.6.2 Artikel 21(3): Fördert eine Sicherheitskultur, die gutes Benutzerverhalten, Sensibilisierung und die Verhinderung unbeabsichtigter Datenabflüsse einschließt – unterstützt durch die verhaltensbezogenen Kontrollen dieser Richtlinie.

11.7 DORA (2022/2554)

11.7.1 Artikel 5 – Interne Governance und Kontrolle: Verlangt, dass alle IKT-bezogenen Risiken, einschließlich menschlicher und umgebungsbezogener Bedrohungen, durch durchsetzbare Richtlinien gesteuert werden.

11.7.2 Artikel 8 – IKT-Risikomanagement: Erzwingt Schutzmaßnahmen sowohl in digitalen als auch in physischen Kontexten und stellt sicher, dass Remote-, Niederlassungs- und Vor-Ort-Benutzer keine unkontrollierte Angriffsfläche schaffen.

11.7.3 Artikel 9 – Vorfallmanagement: Verlangt, dass umgebungsbezogene oder verhaltensbezogene Versäumnisse, die zu einer Datenexposition führen, protokolliert, klassifiziert und mit geeigneten Korrekturmaßnahmen behandelt werden.

11.8 COBIT 2019

11.8.1 DSS01 – Gesteuerter Betrieb: Stellt operative Disziplin beim Schutz physischer Arbeitsbereiche und Systeme durch wiederholbare Kontrollen sicher.

11.8.2 DSS05 – Sicherheitsdienste verwalten: Unterstützt den Schutz von Daten, Geräten und Zugriffsendpunkten durch verhaltensbasierte Durchsetzung wie Clean-Desk-Praktiken.

11.8.3 MEA03 – Überwachen, Evaluieren und Beurteilen der Einhaltung: Fördert die Auditierung physischer Schutzmaßnahmen und der Umsetzung von Richtlinien in den täglichen Geschäftsabläufen.