					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P10S					Dokumenttitel: **Richtlinie für 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 Vorschriften

Standard/Vorschrift	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klauseln 7.2, 8	
ISO/IEC 27002:2022	Maßnahme 7	
NIST SP 800-53 Rev.5	PE-2, AC-11	
EU-NIS2-Richtlinie	Artikel 21(2)(d)	
EU DORA	Artikel 9(2)(f)	
COBIT 2019	DSS01.06, DSS05	
DSGVO	Artikel 32	

1. Zweck

1.1 Diese Richtlinie legt verbindliche Vorgaben für die Aufrechterhaltung einer sicheren Arbeitsumgebung fest, indem sichergestellt wird, dass Schreibtische, Arbeitsplätze und Bildschirme bei Abwesenheit keine offen einsehbaren vertraulichen Informationen enthalten.

1.2 Hauptzweck ist die Verhinderung unbefugten Zugriffs auf sensible Informationen durch unbeaufsichtigte Ausdrucke, entsperrte Bildschirme oder falsch abgelegte Wechseldatenträger sowohl in physischen Büroumgebungen als auch an Remote-Arbeitsplätzen.

1.3 Die in dieser Richtlinie festgelegten Clean-Desk- und Clear-Screen-Praktiken stärken die Fähigkeit unserer Organisation, die Anforderungen an eine Zertifizierung nach ISO/IEC 27001 zu erfüllen, indem vermeidbare Offenlegungsrisiken minimiert werden. Diese Praktiken geben zudem Kunden, Partnern und Auditoren die Gewissheit, dass wir Informationssicherheit auch in ressourcenbegrenzten Umgebungen ernst nehmen.

1.4 Diese Richtlinie unterstützt eine Kultur der Rechenschaftspflicht und Sensibilisierung und stellt sicher, dass sämtliches Personal – unabhängig von Rolle oder technischem Fachwissen – seine Verantwortung zum Schutz von Unternehmens- und Kundeninformationen vor Einsichtnahme, Diebstahl oder Verlust versteht.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für:

2.1.1 alle Mitarbeiter, Auftragnehmer, Praktikanten und Zeitarbeitskräfte, die unternehmenseigene oder persönlich zugewiesene Arbeitsplätze, Schreibtische oder mobile Geräte nutzen

2.1.2 alle physischen Orte, die für geschäftliche Tätigkeiten genutzt werden, einschließlich fester Büros, Coworking-Umgebungen sowie Remote-Arbeitsplätze und Homeoffice-Arbeitsplätze

2.1.3 alle digitalen Geräte mit Anzeigefunktion, einschließlich Desktop-Computern, Laptops, Tablets und externen Monitoren, die für geschäftliche Zwecke verwendet werden

2.2 Die Richtlinie erstreckt sich auf sämtliche physischen oder digitalen Assets, die sensible Informationen anzeigen, enthalten oder übertragen können, einschließlich:

2.2.1 gedruckter Unterlagen oder handschriftlicher Notizen

2.2.2 USB-Laufwerken, CDs und externen Festplatten

2.2.3 Mobiltelefonen, die für geschäftliche Nachrichten oder E-Mails genutzt werden

2.2.4 Computermonitoren und Projektoren, die mit Arbeitssystemen verbunden sind

2.3 Diese Richtlinie gilt auch außerhalb der regulären Arbeitszeiten sowie bei nicht standardmäßigen Betriebsabläufen, z. B. Wartungsarbeiten außerhalb der Geschäftszeiten oder Notfallmaßnahmen.

3. Ziele

3.1 Durchsetzung praktikabler, konsistenter Kontrollen, die sicherstellen, dass keine sensiblen Informationen offen auf Schreibtischen, Bildschirmen oder in gemeinsam genutzten Bereichen zurückgelassen werden.

3.2 Minimierung des Risikos unbefugten Zugriffs sowohl durch interne Quellen, z. B. unbeabsichtigten Zugriff durch andere Mitarbeiter, als auch durch externe Bedrohungen, z. B. Besucher, Reinigungspersonal oder Auftragnehmer.

3.3 Unterstützung von Beschränkungen des physischen und logischen Zugriffs durch die Anforderung an das Personal, Arbeitsunterlagen aktiv zu sichern und Computer bei Abwesenheit zu sperren.

3.4 Förderung des Sicherheitsbewusstseins der Mitarbeiter für sichere Arbeitspraktiken und Bereitstellung einfacher, durchsetzbarer Regeln für den Tagesbetrieb unabhängig vom Arbeitsort.

3.5 Sicherstellung der Ausrichtung an ISO/IEC 27001 Anhang A Maßnahme 7.7 und den Umsetzungshinweisen der ISO/IEC 27002 zu Clean-Desk- und Clear-Screen-Anforderungen.

3.6 Sicherstellung, dass die Organisation gebotene Sorgfalt und Auditbereitschaft nachweisen kann, ohne eine Infrastruktur auf Unternehmensebene vorauszusetzen.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsführung (GM)

4.1.1 ist Eigentümerin dieser Richtlinie und stellt sicher, dass sie allen Mitarbeitern und Auftragnehmern angemessen kommuniziert wird, verstanden wird und eingehalten wird.

4.1.2 ist verantwortlich für die Genehmigung etwaiger Ausnahmen, die Reaktion auf Verstöße und die Aufsicht über Schulungen zu sicheren Arbeitspraktiken.

4.1.3 muss regelmäßige Überprüfungen durchführen oder delegieren, mindestens vierteljährlich, um zu bestätigen, dass physische und digitale Arbeitsbereiche die Anforderungen dieser Richtlinie erfüllen.

4.2 Benanntes Personalmitglied, falls bestimmt

4.2.1 kann mit der Verantwortung für die Umsetzung technischer Konfigurationen, z. B. Zeitüberschreitungen für Bildschirmsperren, oder die Bereitstellung physischer Aufbewahrungsmittel, z. B. abschließbarer Schubladen, betraut werden.

4.2.2 unterstützt die GM durch Meldung von Nichteinhaltung, Hinweise zur Arbeitsplatzsicherheit und Nachverfolgung von Abhilfemaßnahmen, wenn Probleme festgestellt werden.

4.2.3 unterstützt dabei, sicherzustellen, dass alle Mitarbeiter, soweit praktikabel, Zugang zu geeigneten Schließmechanismen oder sicheren Aufbewahrungsbereichen haben.

[... 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 Die GM muss diese Richtlinie mindestens einmal jährlich sowie nach jedem der folgenden Ereignisse überprüfen:

9.1.1 Einführung neuer Büroräume, Geräte oder gemeinsam genutzter Systeme

9.1.2 Änderungen an anwendbaren gesetzlichen oder Zertifizierungsanforderungen

9.1.3 Feststellungen aus Audits, Risikobewertungen oder Informationssicherheitsvorfällen

9.2 Zwischenzeitliche Aktualisierungen müssen allen Mitarbeitern per E-Mail mitgeteilt werden; eine Bestätigung ist erforderlich.

9.3 Frühere Versionen dieser Richtlinie müssen sicher aufbewahrt und auditierbar sein, um die fortlaufende Ausrichtung an ISO/IEC 27001 und verwandten Rahmenwerken nachzuweisen.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 P2S – Richtlinie zu Rollen und Verantwortlichkeiten in der Governance: Präzisiert die Befugnis der GM zur Durchsetzung und Überprüfung des Verhaltens in physischen und digitalen Arbeitsbereichen.

10.2 P4S – Richtlinie zur Zugriffskontrolle: Unterstützt die technische Umsetzung sicherer Bildschirmsperren und sicherer Anmeldepraktiken an Arbeitsplätzen.

10.3 P8S – Richtlinie zur Sensibilisierung und Schulung in der Informationssicherheit: Verstärkt die für die Einhaltung dieser Richtlinie erforderliche verhaltensorientierte Schulung.

10.4 P17S – Richtlinie zu Datenschutz und Privatsphäre: Definiert Verpflichtungen für den Umgang mit und den Schutz personenbezogener und sensibler Daten im Einklang mit der DSGVO.

10.5 P30S – Incident-Response-Richtlinie (P30): Stellt das Eskalations- und Reaktionsrahmenwerk bereit, falls ein Verstoß zu Datenexposition oder einer Sicherheitsverletzung führt.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Klausel 7.2: Verlangt, dass sämtliches Personal sich der Sicherheitsverantwortlichkeiten einschließlich physischer Schutzmaßnahmen bewusst ist.

11.1.2 Klausel 8.1: Operative Kontrollen müssen angemessene physische und logische Schutzmaßnahmen sicherstellen.

11.2 ISO/IEC 27002

11.2.1 Maßnahme 7.7: Gibt detaillierte Hinweise zur Festlegung, Kommunikation und Durchsetzung von Clean-Desk- und Clear-Screen-Anforderungen.

11.3 NIST SP 800-53 Rev.5

11.3.1 PE-2: Legt Anforderungen an die physische Zugriffskontrolle fest, einschließlich des Verhaltens von Personal in sicheren Umgebungen.

11.3.2 AC-11: Schreibt die Funktion zur Sitzungssperre für Arbeitsplätze vor, um unbefugte Einsichtnahme oder Interaktion zu verhindern.

11.4 DSGVO

11.4.1 Artikel 32: Verlangt von Organisationen den Schutz personenbezogener Daten durch physische und technische Schutzmaßnahmen, einschließlich Arbeitsplätzen und Dokumenten.

11.5 EU-NIS2-Richtlinie

11.5.1 Artikel 21(2)(d): Verlangt von Organisationen die Umsetzung risikobasierter Richtlinien für physischen und logischen Zugriff.

11.6 EU DORA

11.6.1 Artikel 9(2)(f): Schreibt IKT-Sicherheitsrichtlinien einschließlich sicherer Arbeitsplatzhygiene für Unternehmen des Finanzsektors und deren Lieferketten vor.

11.7 COBIT 2019

11.7.1 DSS01.06: Verlangt Praktiken zum Schutz von Assets, einschließlich physischer Kontrollen für Arbeitsbereiche und Medien.

11.7.2 DSS05.02: Unterstützt die Durchsetzung von Sicherheitspraktiken für Endbenutzer in unterschiedlichen Betriebsumgebungen.