					Insira aqui a designação da entidade jurídica registada							
Número do documento: P10					Título do documento: **Política de Mesa Limpa e Ecrã Limpo**							
Versão: 1.0		Data de entrada em vigor: 01.01.2025			Proprietário do documento:							
X	Política		Norma		Procedimento		Formulário		Registo		Outro	

Histórico de revisões				
Número da revisão	**Data da revisão**	**Alterações**	**Revisto por**	**Proprietário do processo**

Aprovações			
Nome	**Cargo**	**Data**	**Assinatura**

Alinhamento com normas e regulamentos

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusula 6.1.3, Cláusula 8	plano de tratamento de riscos, planeamento e controlo operacional e controlo de espaços de trabalho seguros
ISO/IEC 27002:2022	Controlo 7	controlos comportamentais e ambientais para proteger informação física deixada sem vigilância
NIST SP 800-53 Rev.5	PE-2, PS-7, MP-6, AC-11, CM-6, IA-5	acesso físico, segurança de pessoal externo, eliminação de suportes, bloqueio de sessão e controlos de configuração e autenticação
RGPD da UE	Artigos 5(1)(f), 32; Considerando 39	integridade dos dados, confidencialidade e salvaguardas físicas dos dados
Diretiva NIS2 da UE	Artigos 21(2)(d), 21(3)	políticas de segurança física, comportamento dos utilizadores e prevenção de fuga de dados
DORA da UE	Artigos 5, 8, 9	governação interna, TIC e gestão de incidentes relacionados com segurança física
COBIT 2019	DSS01, DSS05, MEA	operações geridas, serviços de segurança e monitorização do cumprimento

1. Finalidade

1.1 Esta política estabelece controlos obrigatórios para proteger informação sensível, exigindo o tratamento seguro de documentos físicos, postos de trabalho, ecrãs e suportes amovíveis, tanto em ambientes de escritório como em espaços de trabalho partilhados.

1.2 Esta política suporta o Controlo 7.7 do Anexo A da ISO/IEC 27001, impondo práticas comportamentais e técnicas que mitigam o risco de divulgação não autorizada, furto ou perda de dados decorrentes de informação deixada sem vigilância ou visível.

1.3 Esta política reforça a segurança física e da informação nas operações diárias e apoia o cumprimento das obrigações legais, contratuais e regulamentares aplicáveis.

2. Âmbito

2.1 Esta política aplica-se a todo o pessoal que opere em espaços de trabalho físicos ou a eles aceda, incluindo:

2.1.1 Trabalhadores permanentes e temporários

2.1.2 Contratados, consultores, fornecedores e estagiários

2.1.3 Prestadores de serviços terceiros e visitantes com acesso no local a informação sensível

2.2 Os requisitos aplicam-se em:

2.2.1 Escritórios individuais, cubículos e espaços de trabalho em open space

2.2.2 Salas de reunião e áreas colaborativas partilhadas

2.2.3 Áreas de impressão, balcões de receção e salas de cópias

2.2.4 Áreas onde sejam utilizados postos de trabalho remotos ou quiosques partilhados

2.3 Esta política aplica-se igualmente a ambientes de trabalho temporários ou híbridos (por exemplo, hot-desking) e a contextos expostos ao público em que exista risco de observação indevida do ecrã ou de dados deixados sem vigilância.

3. Objetivos

3.1 Prevenir o acesso não autorizado a informação confidencial, sensível ou regulada deixada exposta em formato físico ou digital.

3.2 Promover uma postura de segurança consistente em todos os ambientes de trabalho através da utilização de salvaguardas físicas, da configuração dos postos de trabalho e do comportamento do utilizador final.

3.3 Reduzir o risco de violações de privacidade, perda de propriedade intelectual e exfiltração de dados causadas por negligência ou falta de diligência.

3.4 Integrar comportamentos de mesa limpa e ecrã limpo na cultura organizacional, promovendo disciplina operacional, auditabilidade e robustez regulamentar.

3.5 Apoiar o cumprimento da ISO/IEC 27001, do Artigo 32 do RGPD da UE, do Artigo 15 da Diretiva NIS2 da UE e de outros requisitos relevantes de segurança física aplicáveis a dados críticos ou pessoais.

4. Papéis e responsabilidades

4.1 Alta Direção

4.1.1 Aprova esta política e promove uma cultura de sensibilização para a segurança em todas as unidades de negócio.

4.1.2 Afeta recursos adequados para a implementação da política, campanhas de sensibilização e mecanismos de controlo físico.

4.2 Diretor de Segurança da Informação / Gestor do SGSI

4.2.1 É responsável por esta política e assegura o seu alinhamento com a ISO/IEC 27001:2022, os requisitos de auditoria e as estratégias de tratamento de riscos.

4.2.2 Desenvolve programas de sensibilização e controlos para assegurar uma implementação consistente nas instalações e em contextos de trabalho híbrido.

4.2.3 Coordena com as áreas de gestão de instalações e de ativos e com as equipas de TI e de Segurança da Informação para assegurar a existência de salvaguardas físicas adequadas.

[... As secções 4.3–8 não estão incluídas nesta pré-visualização. Adquira o documento completo para aceder ao conteúdo integral. ...]

9. Requisitos de revisão e atualização

9.1 Calendário de revisão da política

9.1.1 Esta política deve ser revista:

9.1.1.1 Pelo menos anualmente

9.1.1.2 Após qualquer não conformidade de auditoria relacionada com exposição de espaços de trabalho ou de ecrãs

9.1.1.3 Na sequência de um incidente físico ou ambiental (por exemplo, furto de dispositivo, tailgating, vigilância)

9.1.1.4 Aquando da implementação de novos layouts de escritório, políticas de instalações ou modelos de espaço de trabalho (por exemplo, hot-desking, hubs remotos)

9.2 Responsáveis designados

9.2.1 O responsável por esta política é o Diretor de Segurança da Informação ou o Gestor do SGSI designado.

9.2.2 O processo de revisão deve envolver:

9.2.2.1 Equipas de instalações e de segurança corporativa

9.2.2.2 TI e Infraestruturas para implementação de controlos relacionados com dispositivos

9.2.2.3 Recursos Humanos e Jurídico para alinhamento comportamental e disciplinar

9.2.3 Todas as atualizações à política devem estar sujeitas a controlo de versões, ser aprovadas pelo Comité de Direção do SGSI e ser redistribuídas com nova aceitação, quando aplicável.

9.3 Comunicação de alterações

9.3.1 Os utilizadores devem ser notificados de alterações materiais através de:

9.3.1.1 Centro ou portal de políticas na intranet

9.3.1.2 Comunicações direcionadas por correio eletrónico

9.3.1.3 Sessões de reciclagem na integração e briefings trimestrais

9.3.1.4 Pedidos obrigatórios de aceitação para quaisquer novas cláusulas críticas de aplicação

10. Políticas relacionadas e ligações

10.1 Esta política está alinhada com e apoia o seguinte:

10.1.1 P1 – Política de Segurança da Informação: estabelece expectativas de comportamento dos utilizadores e de segurança física que servem de base a esta política.

10.1.2 P3 – Política de Utilização Aceitável: trata da responsabilização dos utilizadores na proteção de dados e sistemas, incluindo em ambientes físicos.

10.1.3 P6 – Política de Gestão de Riscos: incorpora riscos associados a espaços de trabalho físicos no âmbito da análise de riscos de informação à escala da organização.

10.1.4 P12 – Política de Gestão de Ativos: apoia o rastreio e o tratamento seguro de dispositivos e suportes deixados em secretárias.

10.1.5 P13 – Política de Classificação e Rotulagem de Dados: estabelece a ligação com a aplicação da mesa limpa a documentos físicos classificados como Confidencial ou Interno.

10.1.6 P14 – Política de Retenção e Eliminação de Dados: orienta as práticas de retenção de documentos físicos, trituração e gestão de recipientes de eliminação.

10.1.7 P22 – Política de Registo e Monitorização: pode ser utilizada para monitorizar o estado de bloqueio de postos de trabalho, o tempo de inatividade ou imagens de câmaras em espaços de trabalho, quando permitido.

10.2 Estas políticas relacionadas estabelecem uma cultura de segurança integrada, combinando sensibilização dos utilizadores, salvaguardas físicas e responsabilização para assegurar espaços de trabalho resilientes.

11. Normas e quadros de referência

11.1 Esta política está alinhada com normas internacionalmente reconhecidas e requisitos legais que determinam a proteção de informação sensível em ambientes físicos e através do comportamento dos utilizadores.

11.2 ISO/IEC 27001

11.2.1 Cláusula 6.1.3 – plano de tratamento de riscos: apoia a implementação de controlos para mitigação de riscos físicos e ambientais, incluindo os associados ao comportamento dos utilizadores em espaços de trabalho abertos.

11.2.2 Cláusula 8.1 – planeamento e controlo operacional: estabelece salvaguardas operacionais para gerir espaços de trabalho seguros e a utilização de equipamentos.

11.3 ISO/IEC 27002:2022 – Controlo 7

11.3.1 Este controlo exige proteções comportamentais e ambientais para prevenir o acesso não autorizado à informação através de suportes, ecrãs ou materiais impressos deixados sem vigilância. A política impõe disciplina no espaço de trabalho físico, utilização de bloqueio de ecrã e eliminação de documentos sensíveis.

11.4 NIST SP 800-53 Rev.5

11.4.1 PE-2 (Autorizações de acesso físico): relacionado com restrições de acesso ao espaço de trabalho e imposição de armazenamento com fechadura em ambientes de alto risco.

11.4.2 PS-7 (Segurança de pessoal externo): aplicado através de requisitos de mesa limpa e ecrã limpo estendidos a contratados e utilizadores terceiros.

11.4.3 MP-6 (sanitização de suportes) e AC-11 (bloqueio de sessão): implementados através de procedimentos de eliminação segura e temporizadores obrigatórios de bloqueio de ecrã.

11.4.4 CM-6 (parâmetros de configuração) e IA-5 (gestão de autenticadores): suportam a aplicação técnica do bloqueio de ecrã e do controlo de sessão nos endpoints.

11.5 RGPD da UE (2016/679)

11.5.1 Artigo 5(1)(f): impõe a integridade e confidencialidade dos dados pessoais, incluindo proteções contra exposição física ou visualização por pessoas não autorizadas.

11.5.2 Artigo 32 – Segurança do Tratamento: exige medidas físicas e organizativas adequadas para proteger os dados pessoais contra destruição acidental ou ilícita, perda ou divulgação não autorizada, objetivo alcançado através dos controlos de mesa limpa e ecrã limpo.

11.5.3 Considerando 39: exige a limitação do acesso aos dados pessoais a indivíduos autorizados, incluindo a sua proteção em formato físico quando deixados sem vigilância.

11.6 Diretiva NIS2 da UE (2022/2555)

11.6.1 Artigo 21(2)(d): exige políticas e procedimentos relacionados com a segurança física e ambiental, incluindo proteções de segurança da informação ao nível do local de trabalho.

11.6.2 Artigo 21(3): incentiva uma cultura de segurança que incorpore comportamentos adequados dos utilizadores, sensibilização e prevenção de fugas de dados não intencionais, suportada pelos controlos comportamentais desta política.

11.7 DORA da UE (2022/2554)

11.7.1 Artigo 5 – Governação interna e controlo: exige que todos os riscos relacionados com TIC, incluindo ameaças humanas e ambientais, sejam geridos através de políticas aplicáveis.

11.7.2 Artigo 8 – Gestão do risco das TIC: impõe salvaguardas em contextos digitais e físicos, assegurando que utilizadores remotos, em sucursais e em infraestrutura on-premises não criam exposição não gerida.

11.7.3 Artigo 9 – Gestão de incidentes: exige que falhas ambientais ou comportamentais que resultem em exposição de dados sejam registadas, classificadas e tratadas com ações corretivas adequadas.

11.8 COBIT 2019

11.8.1 DSS01 – Operações geridas: assegura disciplina operacional na proteção de espaços de trabalho físicos e sistemas através de controlos repetíveis.

11.8.2 DSS05 – Serviços de segurança geridos: apoia a proteção de dados, dispositivos e endpoints de acesso através de mecanismos de aplicação baseados no comportamento, como as práticas de mesa limpa.

11.8.3 MEA03 – Monitorizar, Avaliar e Analisar o cumprimento: incentiva a auditoria de salvaguardas físicas e da adoção da política nas práticas diárias da organização.