					Insira aqui a designação da entidade jurídica registada							
Número do documento: P10S					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	Cláusulas 7.2, 8	
ISO/IEC 27002:2022	Controlo 7	
NIST SP 800-53 Rev.5	PE-2, AC-11	
Diretiva NIS2 da UE	Artigo 21(2)(d)	
DORA da UE	Artigo 9(2)(f)	
COBIT 2019	DSS01.06, DSS05	
RGPD da UE	Artigo 32	

1. Finalidade

1.1 Esta política estabelece diretrizes obrigatórias para manter um ambiente de trabalho seguro, assegurando que secretárias, postos de trabalho e ecrãs permanecem sem informação confidencial visível quando não estão sob vigilância.

1.2 A sua principal finalidade é prevenir o acesso não autorizado a informação sensível através de impressões deixadas sem vigilância, ecrãs desbloqueados ou suportes amovíveis incorretamente acondicionados, tanto em ambientes físicos de escritório como em contextos de trabalho remoto.

1.3 As práticas de mesa limpa e ecrã limpo definidas nesta política reforçam a capacidade da organização para cumprir os requisitos de certificação ISO/IEC 27001, minimizando riscos de exposição evitáveis. Estas práticas demonstram também a clientes, parceiros e auditores que a organização trata a Segurança da Informação com o devido rigor, mesmo em contextos com recursos limitados.

1.4 Esta política promove uma cultura de responsabilização e sensibilização, assegurando que todo o pessoal, independentemente da função ou do nível de conhecimento técnico, compreende a sua responsabilidade na proteção da informação da empresa e dos clientes contra exposição visual, furto ou perda.

2. Âmbito

2.1 Esta política aplica-se a:

2.1.1 Todos os trabalhadores, prestadores de serviços, estagiários e trabalhadores temporários que utilizem postos de trabalho, secretárias ou dispositivos móveis detidos pela empresa ou atribuídos individualmente

2.1.2 Todos os locais físicos utilizados para atividade empresarial, incluindo escritórios dedicados, espaços de coworking e locais de trabalho remotos/domésticos

2.1.3 Todos os dispositivos digitais com capacidade de visualização, incluindo computadores de secretária, computadores portáteis, tablets e monitores externos utilizados para fins profissionais

2.2 A política abrange qualquer ativo físico ou digital que possa apresentar, conter ou transmitir informação sensível, incluindo:

2.2.1 Registos impressos ou notas manuscritas

2.2.2 Unidades USB, CDs e discos rígidos externos

2.2.3 Telemóveis utilizados para mensagens profissionais ou correio eletrónico

2.2.4 Monitores de computador e projetores ligados a sistemas de trabalho

2.3 Esta política mantém-se aplicável fora do horário normal de trabalho e durante operações não habituais (por exemplo, manutenção fora de horas ou atividades de resposta a emergências).

3. Objetivos

3.1 Implementar controlos práticos e consistentes que assegurem que nenhuma informação sensível fica exposta em secretárias, ecrãs ou espaços comuns.

3.2 Minimizar o risco de acesso não autorizado, tanto por fontes internas (por exemplo, acesso não intencional por outros trabalhadores) como por ameaças externas (por exemplo, visitantes, pessoal de limpeza ou prestadores de serviços).

3.3 Reforçar as restrições de acesso físico e lógico, exigindo que o pessoal proteja ativamente os materiais de trabalho e bloqueie os computadores quando não estiver presente.

3.4 Reforçar a sensibilização do pessoal para práticas de trabalho seguras e estabelecer regras simples e aplicáveis no dia a dia, independentemente do local de trabalho.

3.5 Assegurar o alinhamento com o Controlo 7.7 do Anexo A da ISO/IEC 27001 e com as orientações de implementação da ISO/IEC 27002 relativas aos requisitos de mesa limpa e ecrã limpo.

3.6 Assegurar que a organização consegue demonstrar diligência devida e evidenciar conformidade em auditoria sem exigir infraestrutura de nível empresarial.

4. Papéis e responsabilidades

4.1 Diretor-Geral (DG)

4.1.1 É responsável por esta política e por assegurar que a mesma é devidamente comunicada, compreendida e cumprida por todos os trabalhadores e prestadores de serviços.

4.1.2 É responsável por aprovar quaisquer exceções, responder a violações e supervisionar a formação relacionada com práticas de trabalho seguras.

4.1.3 Deve realizar ou delegar verificações regulares (pelo menos trimestrais) para confirmar que os espaços de trabalho físicos e digitais cumprem os requisitos da política.

4.2 Membro do pessoal designado (se aplicável)

4.2.1 Pode ser-lhe atribuída a responsabilidade de implementar configurações técnicas (por exemplo, definições de tempo limite de ecrã) ou distribuir meios físicos de armazenamento (por exemplo, gavetas com fechadura).

4.2.2 Apoia o DG através da comunicação de incumprimentos, da emissão de lembretes sobre segurança do espaço de trabalho e do acompanhamento das ações corretivas quando sejam identificados problemas.

4.2.3 Ajuda a assegurar que todos os trabalhadores dispõem, sempre que viável, de mecanismos de fecho adequados ou de espaços de armazenamento seguro.

[... 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 O DG deve rever esta política pelo menos uma vez por ano e após qualquer um dos seguintes eventos:

9.1.1 Introdução de novos espaços de escritório, dispositivos ou sistemas partilhados

9.1.2 Alterações aos requisitos legais ou de certificação aplicáveis

9.1.3 Constatações de auditorias, avaliações de risco ou incidentes de segurança

9.2 As atualizações intercalares devem ser comunicadas a todos os trabalhadores por correio eletrónico, sendo obrigatória a respetiva confirmação.

9.3 As versões anteriores desta política devem ser armazenadas em segurança e estar disponíveis para auditoria, de modo a demonstrar o alinhamento contínuo com a ISO/IEC 27001 e os referenciais relacionados.

10. Políticas relacionadas e ligações

10.1 P2S – Política de Papéis e Responsabilidades de Governação: Clarifica a autoridade do DG para aplicar a política e auditar o comportamento em espaços de trabalho físicos e digitais.

10.2 P4S – Política de controlo de acessos: Apoia a implementação técnica das práticas de bloqueio de ecrã e autenticação segura em postos de trabalho.

10.3 P8S – Política de sensibilização e formação em segurança da informação: Reforça a formação comportamental necessária para o cumprimento da política.

10.4 P17S – Política de proteção de dados e privacidade: Define obrigações para o tratamento e proteção de dados pessoais e sensíveis em conformidade com o RGPD da UE.

10.5 P30S – Política de Resposta a Incidentes: Estabelece o quadro de escalonamento e resposta caso uma violação resulte em exposição de dados ou numa violação de dados pessoais.

11. Normas e quadros de referência

11.1 ISO/IEC 27001

11.1.1 Cláusula 7.2: Exige que todo o pessoal esteja sensibilizado para as responsabilidades de segurança, incluindo a proteção física.

11.1.2 Cláusula 8.1: Os controlos operacionais devem assegurar salvaguardas físicas e lógicas adequadas.

11.2 ISO/IEC 27002

11.2.1 Controlo 7.7: Fornece orientações detalhadas sobre o estabelecimento, comunicação e aplicação de requisitos de mesa limpa e ecrã limpo.

11.3 NIST SP 800-53 Rev.5

11.3.1 PE-2: Estabelece expectativas de controlo de acesso físico, incluindo o comportamento do pessoal em ambientes seguros.

11.3.2 AC-11: Exige funcionalidade de bloqueio de sessão para postos de trabalho, de modo a impedir visualização ou interação não autorizada.

11.4 RGPD da UE

11.4.1 Artigo 32: Exige que as organizações protejam dados pessoais através de salvaguardas físicas e técnicas, incluindo postos de trabalho e documentos.

11.5 Diretiva NIS2 da UE

11.5.1 Artigo 21(2)(d): Exige que as organizações implementem políticas de acesso físico e lógico baseadas no risco.

11.6 DORA da UE

11.6.1 Artigo 9(2)(f): Exige políticas de segurança das TIC, incluindo práticas seguras de higiene do espaço de trabalho, para operadores do setor financeiro e respetivas cadeias de fornecimento.

11.7 COBIT 2019

11.7.1 DSS01.06: Exige práticas de proteção de ativos, incluindo controlos físicos sobre espaços de trabalho e suportes.

11.7.2 DSS05.02: Apoia a aplicação de práticas de segurança do utilizador final em todos os ambientes operacionais.