					Insira aqui a designação da entidade jurídica registada							
Número do documento: P09S					Título do documento: **Política de Trabalho Remoto**							
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 6.1, 6.2, 8	
ISO/IEC 27002:2022	Controlo 6	
NIST SP 800-53 Rev.5	AC-17, AC-2	
Diretiva NIS2 da UE	Artigos 21(2)(b), 21(2)(h)	Diretiva NIS2 da UE
DORA da UE	Artigo 9	DORA da UE
COBIT 2019	DSS05, APO13	COBIT 2019
RGPD da UE	Artigo 32	RGPD da UE

1. Finalidade

1.1 Esta política estabelece os requisitos de segurança aplicáveis a trabalhadores e prestadores de serviços que exerçam funções em regime remoto, incluindo a partir de casa, de espaços de trabalho partilhados ou em deslocação.

1.2 Visa proteger a Confidencialidade, Integridade e Disponibilidade da informação da organização acedida fora de ambientes controlados pela empresa.

1.3 Esta política assegura o cumprimento de normas internacionais e reduz riscos como o acesso não autorizado, a perda de dados e a indisponibilidade de serviços.

2. Âmbito

2.1 Esta política aplica-se a todos os membros do pessoal (trabalhadores, prestadores de serviços, consultores e trabalhadores temporários) que acedam a sistemas, redes ou dados da empresa enquanto trabalham fora das instalações.

2.2 Abrange:

2.2.1 A utilização de dispositivos fornecidos pela empresa e de dispositivos pessoais

2.2.2 O acesso através de VPN, ambientes de trabalho remotos ou serviços na nuvem

2.2.3 O tratamento seguro da informação fora das instalações da empresa

2.2.4 A monitorização, o tratamento de exceções e a aplicação da política

2.3 Aplica-se tanto a regimes de trabalho remoto a tempo inteiro como a tempo parcial, incluindo acesso remoto ad hoc.

3. Objetivos

3.1 Prevenir o acesso não autorizado aos sistemas da empresa ou a dados sensíveis durante o trabalho remoto.

3.2 Assegurar que os dispositivos e as ligações de comunicação utilizados fora do escritório cumprem os requisitos mínimos de segurança.

3.3 Manter o controlo sobre os privilégios de acesso remoto e a respetiva monitorização.

3.4 Fornecer orientações claras a trabalhadores e gestores para práticas seguras de trabalho remoto.

3.5 Cumprir as expectativas da ISO, NIS2, RGPD, DORA e COBIT em matéria de trabalho remoto e móvel.

4. Papéis e responsabilidades

4.1 Diretor-Geral

4.1.1 Aprova os regimes de trabalho remoto e monitoriza o cumprimento.

4.1.2 Escalona incidentes de segurança ou incumprimentos reiterados.

4.1.3 Revê exceções e assegura o acompanhamento dos incidentes.

4.2 Apoio de TI ou prestadores externos de serviços de TI

4.2.1 Configura o acesso remoto seguro (por exemplo, VPN, MFA, gestão de dispositivos móveis).

4.2.2 Assegura a implementação de proteção de endpoints, cifragem e configurações seguras nos dispositivos.

4.2.3 Apoia os utilizadores e investiga quaisquer questões técnicas de segurança.

[... 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 Revisão anual da política

9.1.1 O Diretor-Geral e o Apoio de TI devem rever esta política anualmente para a alinhar com alterações tecnológicas, da força de trabalho e legais.

9.2 Fatores desencadeadores de atualização antecipada

9.2.1 É exigida uma revisão imediata após:

9.2.1.1 Incidente grave de segurança relacionado com trabalho remoto

9.2.1.2 Alterações aos requisitos da NIS2, do RGPD ou da DORA

9.2.1.3 Transição para nova tecnologia de acesso remoto (por exemplo, uma plataforma VPN diferente)

9.3 Controlo de versões e arquivo

9.3.1 Todas as versões desta política devem:

9.3.1.1 Ser datadas e aprovadas pelo Diretor-Geral

9.3.1.2 Ter um número de versão atribuído

9.3.1.3 Ser arquivadas durante, pelo menos, três anos

9.4 Comunicação ao pessoal

9.4.1 As atualizações da política devem ser comunicadas a todos os utilizadores remotos. É obrigatória a confirmação de receção para qualquer alteração significativa.

10. Políticas relacionadas e articulações

10.1 Esta política está articulada com as seguintes políticas e dá-lhes suporte:

10.1.1 P2S – Política de Papéis e Responsabilidades de Governação: define quem autoriza e supervisiona o acesso remoto

10.1.2 P4S – Política de Controlo de Acessos: estabelece a configuração segura do acesso remoto e os procedimentos de revogação

10.1.3 P6S – Política de Gestão de Riscos: acompanha e avalia os riscos relacionados com o acesso fora das instalações

10.1.4 P8S – Política de Sensibilização e Formação em Segurança da Informação: forma os utilizadores sobre os riscos do trabalho remoto e as melhores práticas

10.1.5 P30S – Política de Resposta a Incidentes: gere a resposta a incidentes de acesso remoto, como fuga de credenciais de autenticação ou perda de dispositivos

11. Normas e quadros de referência

11.1 ISO/IEC 27001

11.1.1 Cláusula 6.1 – Planeamento baseado no risco para cenários de acesso remoto

11.1.2 Cláusula 6.2 – Abrange responsabilidades de Recursos Humanos em contextos móveis/remotos

11.1.3 Cláusula 8.1 – Planeamento e controlo operacional de processos remotos

11.2 ISO/IEC 27002

11.2.1 Controlo 6.7 – Fornece orientações práticas sobre segurança para trabalho remoto e móvel

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-17 – Controlo do acesso remoto, proteções de sessão e monitorização de segurança

11.3.2 AC-2 – Gestão de contas para utilizadores fora das instalações

11.4 RGPD da UE

11.4.1 Artigo 32 – Exige a proteção de dados adequada, incluindo em contextos remotos

11.5 Diretiva NIS2 da UE

11.5.1 Artigo 21(2)(b) – Exige a utilização segura dos sistemas de rede e informação

11.5.2 Artigo 21(2)(h) – Prevê medidas de segurança relacionadas com Recursos Humanos, incluindo controlos fora das instalações

11.6 DORA da UE

11.6.1 Artigo 9 – Exige que as entidades financeiras mantenham a resiliência das TIC em todos os modos operacionais, incluindo o acesso remoto

11.7 COBIT 2019

11.7.1 DSS05 – Gerir Serviços de Segurança: inclui proteção de endpoints e práticas seguras de trabalho remoto

11.7.2 APO13 – Segurança Gerida: assegura o provisionamento seguro e a supervisão do risco do acesso móvel/remoto