					Insira aqui a designação da entidade jurídica registada							
Número do documento: P34S					Título do documento: **Política de Dispositivos Móveis e Traga o Seu Próprio Dispositivo (BYOD)**							
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**

Alinhada com normas e regulamentos

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusulas 5.1, 5.2, 6.1, 6.2, 8	Requisitos gerais do SGSI e controlos aplicáveis a dispositivos móveis/BYOD
ISO/IEC 27002:2022	Controlos 5.10–5.13	Controlos detalhados para dispositivos móveis/BYOD e acesso remoto
NIST SP 800-53 Rev.5	AC-19, AC-20, CM-6, MP-7	Controlos federais aplicáveis a dispositivos, suportes e configuração
RGPD da UE	Artigo 5.º, n.º 1, alínea f)	Proteção de dados pessoais em terminais móveis
Diretiva NIS2 da UE	Artigo 21.º, n.º 2, alínea d)	Proteção de dispositivos críticos para o negócio, incluindo BYOD
DORA da UE	Artigos 9.º, 10.º	Gestão do risco das TIC e continuidade aplicadas a terminais móveis
COBIT 2019	APO13, DSS01, DSS05	Governação de TI, operações e controlos dos serviços de segurança

1. Finalidade

1.1. Esta política define os requisitos de segurança obrigatórios para a utilização de dispositivos móveis, incluindo smartphones, tablets e computadores portáteis, no acesso a informação, sistemas ou serviços da empresa.

1.2. Esta política regula igualmente a utilização de Traga o Seu Próprio Dispositivo (BYOD), de modo a assegurar a proteção dos dados dos clientes e do negócio, independentemente da titularidade do dispositivo.

1.3. A política estabelece proteções consistentes para o acesso móvel, apoia o cumprimento dos objetivos de certificação ISO/IEC 27001 e previne a perda de dados ou o comprometimento decorrente de terminais móveis perdidos, furtados ou utilizados indevidamente.

1.4. A política assegura que são aplicadas salvaguardas técnicas e processuais à utilização móvel em PME sem equipas de TI dedicadas, incluindo ambientes de trabalho remoto e serviços baseados na nuvem.

2. Âmbito

2.1. Esta política aplica-se a todos os trabalhadores, contratados, estagiários e prestadores de serviços que:

2.1.1. Utilizem um dispositivo móvel para aceder, tratar ou armazenar dados ou sistemas da empresa.

2.1.2. Se liguem a serviços da empresa, incluindo correio eletrónico, pastas partilhadas, aplicações na nuvem ou sistemas internos através de VPN.

2.2. Esta política abrange:

2.2.1. Todos os dispositivos móveis: smartphones, tablets e computadores portáteis, fornecidos pela empresa ou pessoais em regime BYOD.

2.2.2. Todos os sistemas operativos, incluindo iOS, Android, Windows e macOS.

2.2.3. Todos os locais de utilização, incluindo escritório, domicílio, trabalho remoto e espaços públicos.

2.3. A política aplica-se a todos os ambientes de trabalho e deve ser cumprida independentemente da titularidade do dispositivo.

3. Objetivos

3.1. Prevenir a perda de dados: assegurar que a utilização de dispositivos móveis não expõe dados sensíveis da empresa ou dos clientes a acessos não autorizados, furto ou utilização indevida.

3.2. Definir regras claras para BYOD: estabelecer condições vinculativas para a utilização de dispositivos pessoais para fins profissionais, assegurando salvaguardas jurídicas e técnicas.

3.3. Apoiar o cumprimento regulatório: cumprir os requisitos da ISO/IEC 27001, do RGPD da UE, da Diretiva NIS2 da UE e de outras obrigações legais através de práticas de segurança móvel aplicáveis.

3.4. Minimizar o risco operacional: reduzir a probabilidade de perturbação operacional causada por utilização indevida, comprometimento ou falha de dispositivos móveis.

3.5. Manter a confiança dos clientes: demonstrar a clientes e parceiros que os seus dados permanecem protegidos mesmo quando acedidos em dispositivos móveis ou pessoais.

4. Papéis e responsabilidades

4.1. Diretor-Geral (GM):

4.1.1. Mantém a responsabilidade por esta política.

4.1.2. Aprova toda a utilização de acesso móvel e BYOD aos sistemas da empresa.

4.1.3. Assegura que os acordos de BYOD são assinados, arquivados e monitorizados.

4.1.4. Verifica que os prestadores externos de serviços de TI aplicam as proteções móveis exigidas.

4.2. Colaborador designado ou suporte de TI:

4.2.1. Apoia a configuração inicial, o registo e a parametrização dos dispositivos móveis utilizados para trabalho.

4.2.2. Aplica controlos de acesso, restrições de aplicações e regras de monitorização relacionadas com dispositivos móveis.

4.2.3. Apoia a resposta a incidentes relacionados com dispositivos móveis, incluindo dispositivos perdidos, furtados ou comprometidos.

[... 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

9.1.1. O Diretor-Geral (GM) deve rever esta política pelo menos uma vez a cada 12 meses.

9.1.2. A revisão deve verificar a manutenção do alinhamento com os requisitos da ISO/IEC 27001, a evolução das tecnologias móveis e as alterações nas operações do negócio.

9.1.3. As atualizações devem também considerar incidentes recentes, resultados de auditoria ou desenvolvimentos regulatórios, como o RGPD da UE, a Diretiva NIS2 da UE e o DORA da UE.

9.2. Eventos desencadeadores de revisão intercalar

9.2.1. Esta política deve ser atualizada imediatamente se ocorrer qualquer uma das seguintes situações:

9.2.1.1. Incidente grave de segurança móvel, como uma violação através de um dispositivo perdido ou comprometido.

9.2.1.2. Alteração nas plataformas suportadas ou nas ferramentas de gestão móvel.

9.2.1.3. Alteração legal ou regulatória que afete a utilização de dispositivos pessoais ou a proteção de dados.

9.2.1.4. Introdução de novas aplicações, serviços ou ferramentas de terceiros utilizadas em dispositivos móveis.

9.3. Documentação das alterações

9.3.1. Todas as revisões e atualizações devem ser documentadas, incluindo a data da revisão, as alterações efetuadas e a aprovação do Diretor-Geral (GM).

9.3.2. Deve ser mantido um histórico de controlo de versões para fins de auditoria.

9.4. Comunicação e acesso

9.4.1. O Diretor-Geral (GM) deve assegurar que todos os utilizadores, incluindo trabalhadores, contratados e terceiros, são informados das alterações.

9.4.2. As versões atualizadas devem estar facilmente acessíveis, por exemplo em pastas partilhadas ou plataformas internas.

10. Políticas relacionadas e articulações

10.1. Esta política integra o conjunto global de políticas de segurança da informação para PME e deve ser implementada em articulação com as seguintes:

10.1.1. P4S – Política de controlo de acesso: define os requisitos para a gestão do acesso seguro aos sistemas, incluindo os acedidos através de dispositivos móveis. Impõe a higiene das palavras-passe e controlos de sessão.

10.1.2. P8S – Política de sensibilização e formação em segurança da informação: assegura que os utilizadores recebem formação de sensibilização em segurança sobre utilização segura de dispositivos móveis, notificação de incidentes e condições de BYOD.

10.1.3. P17S – Política de proteção de dados e privacidade: estabelece o tratamento de dados pessoais e dados da empresa em plataformas móveis em conformidade com o RGPD da UE, especialmente quando são utilizados dispositivos pessoais para trabalho.

10.1.4. P9S – Política de trabalho remoto: está alinhada com as expectativas de utilização móvel em trabalho fora das instalações ou a partir de casa, incluindo o tratamento de dispositivos e as salvaguardas de acesso à rede.

10.1.5. P30S – Política de resposta a incidentes: fornece o enquadramento de resposta para incidentes relacionados com dispositivos móveis, incluindo dispositivos comprometidos ou perdidos.

10.2. Estas políticas relacionadas funcionam em conjunto para formar um conjunto completo de controlos de segurança dos dispositivos móveis em PME sem pessoal de TI dedicado, assegurando aplicabilidade, transparência e preparação para certificação.

11. Normas e referenciais de referência

11.1. Esta política suporta o alinhamento integral com as seguintes normas e referenciais de segurança e conformidade:

11.2. ISO/IEC 27001:

11.2.1. Cláusula 5.1 – Liderança e compromisso: assegura a supervisão da gestão e a responsabilização pelo acesso móvel e BYOD.

11.2.2. Cláusula 6.1 – Ações para tratar riscos: exige que os riscos de segurança móvel sejam avaliados e tratados.

11.2.3. Cláusula 8.1 – Planeamento e controlo operacional: exige procedimentos consistentes de acesso móvel para proteger os dados do negócio.

11.3. ISO/IEC 27002:

11.3.1. Controlos 5.10 (utilização de dispositivos móveis), 5.11 (teletrabalho), 5.12 (acesso remoto) e 5.13 (BYOD): fornecem orientações de implementação para gerir riscos associados a dispositivos num contexto de pequena empresa.

11.4. NIST SP 800-53 Rev.5:

11.4.1. AC-19 – controlo de acesso para dispositivos móveis: exige definições de segurança para utilização móvel autorizada.

11.4.2. AC-20 – utilização de sistemas externos: rege os riscos de BYOD e de acesso remoto.

11.4.3. CM-6 – definições de configuração: impõe definições seguras por defeito e personalizadas em plataformas móveis.

11.4.4. MP-7 – utilização de suportes: trata da utilização correta e das restrições aplicáveis ao armazenamento móvel e ao acesso a dados.

11.5. RGPD da UE (2016/679):

11.5.1. Artigo 5.º, n.º 1, alínea f) – Integridade e confidencialidade: exige a proteção dos dados através de segurança adequada dos dados pessoais, em especial em plataformas móveis.

11.5.2. Artigo 32.º – Segurança do tratamento: obriga à utilização de medidas técnicas e organizativas adequadas (TOMs) para proteger os dados acedidos ou armazenados em dispositivos móveis.

11.6. Diretiva NIS2 da UE (2022/2555):

11.6.1. Artigo 21.º, n.º 2, alínea d) – medidas de segurança dos dispositivos: exige controlos de segurança para hardware e software utilizados no acesso a sistemas críticos para o negócio, incluindo dispositivos pessoais.

11.7. DORA da UE (2022/2554):

11.7.1. Artigo 9.º – Quadro de gestão do risco das TIC: exige a proteção de terminais móveis utilizados em comunicações críticas do negócio e serviços na nuvem.

11.7.2. Artigo 10.º – continuidade do negócio das TIC: exige a manutenção de acesso seguro aos sistemas do negócio mesmo durante interrupções ou trabalho remoto.

11.8. COBIT 2019:

11.8.1. APO13 – Gerir Segurança: exige que a organização aplique políticas de dispositivos móveis e BYOD alinhadas com o risco empresarial.

11.8.2. DSS01 – Gerir Operações: assegura a implementação técnica de mecanismos de acesso seguro.

11.8.3. DSS05 – Gerir Serviços de Segurança: rege o envolvimento de terceiros na manutenção de ambientes móveis seguros e na coordenação da resposta a incidentes.