					Insira aqui a designação da entidade jurídica registada							
Número do documento: P04S					Título do documento: **Política de Controlo de Acessos**							
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 5	
ISO/IEC 27002:2022	Controlos: 5.15, 5.16, 5	
NIST SP 800-53 Rev. 5	AC-1 a AC-5	
RGPD da UE	Artigo 32	
Diretiva NIS2 da UE	Artigo 21(2)(b)	
DORA da UE	Artigo 9	
COBIT 2019	APO07 Gerir Recursos Humanos, DSS	

1. Finalidade

1.1. Esta política define a forma como a organização gere o acesso a sistemas, dados e instalações, de modo a assegurar que apenas indivíduos autorizados podem aceder à informação com base na necessidade de negócio.

1.2. Estabelece regras claras para o provisionamento, alteração, monitorização e remoção de acessos de utilizadores, de forma a minimizar o risco de acesso não autorizado e apoiar o cumprimento das leis e normas aplicáveis.

1.3. A política aplica o princípio do menor privilégio, exigindo que o acesso seja limitado ao mínimo necessário para o exercício das funções profissionais.

2. Âmbito

2.1. Esta política aplica-se a todos os indivíduos que utilizem ou gerem o acesso aos sistemas informáticos, redes, dados ou instalações da organização, incluindo:

2.1.1. Trabalhadores

2.1.2. Contratados

2.1.3. Trabalhadores temporários

2.1.4. Prestadores externos de serviços de TI

2.2. Abrange o acesso a:

2.2.1. Aplicações empresariais, partilhas de ficheiros e bases de dados

2.2.2. Correio eletrónico, VPN e sistemas de acesso remoto

2.2.3. Serviços na cloud utilizados para fins empresariais

2.2.4. Acesso físico a instalações seguras, como escritórios ou salas de servidores

2.3. Esta política é aplicável a todos os dispositivos (fornecidos pela organização ou aprovados ao abrigo do regime Traga o Seu Próprio Dispositivo (BYOD)), plataformas e localizações.

3. Objetivos

3.1. Assegurar que os direitos de acesso são concedidos apenas após aprovação formal, com base na função e na justificação de negócio.

3.2. Prevenir acessos não autorizados ou excessivos a dados sensíveis, sistemas ou infraestrutura.

3.3. Definir procedimentos claros para o provisionamento, alteração e revogação do acesso de utilizadores.

3.4. Exigir revisões regulares de acessos e registo automatizado ou manual para suporte a auditorias.

3.5. Apoiar a aplicação técnica das restrições de acesso através da configuração e monitorização.

4. Papéis e responsabilidades

4.1. Diretor-Geral (GM)

4.1.1. Aprova esta política e assegura a disponibilidade dos recursos necessários para implementar controlos de acesso eficazes.

4.1.2. Aprova exceções e analisa as auditorias anuais de acessos.

4.2. Responsável de TI / Prestador externo de serviços de TI

4.2.1. Assegura o provisionamento, a alteração e a revogação de contas de utilizador.

4.2.2. Mantém um Registo de Controlo de Acessos com todas as atividades relevantes (criações, alterações e remoções).

4.2.3. Implementa o controlo de acessos baseado em funções (RBAC) e aplica autenticação forte (por exemplo, MFA).

4.2.4. Revê os registos de acesso para identificar atividade suspeita e comunica quaisquer incidentes ao Diretor-Geral (GM).

[... 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 Responsável de TI deve rever esta política anualmente. Qualquer alteração do contexto jurídico, técnico ou organizacional deve desencadear uma atualização imediata.

9.2. Fatores desencadeadores da revisão

9.2.1. A política deve também ser revista caso ocorra qualquer uma das seguintes situações:

9.2.2. Alterações significativas a sistemas ou migrações para a cloud

9.2.3. Alterações de funções ou da estrutura organizacional

9.2.4. Um incidente de segurança que envolva acesso não autorizado

9.2.5. Alterações regulamentares (por exemplo, atualizações ao RGPD, à NIS2 ou à DORA)

9.3. Documentação e comunicação das alterações

9.3.1. As revisões devem ser registadas com histórico de versões, aprovação pelo Diretor-Geral (GM) e comunicação a todo o pessoal afetado.

9.4. Acessibilidade e formação

9.4.1. Esta política deve ser disponibilizada a todo o pessoal, devendo ser ministrada formação relevante no âmbito do processo de integração e, posteriormente, com periodicidade anual.

10. Políticas relacionadas e ligações

10.1. Esta política deve ser aplicada em articulação com as seguintes políticas SME, para assegurar a aplicação integral de práticas seguras de acesso:

10.1.1. P3S – Política de Utilização Aceitável: assegura que os utilizadores compreendem o comportamento aceitável no âmbito dos acessos concedidos.

10.1.2. P5S – Política de Gestão de Alterações: assegura que os direitos de acesso estão alinhados com alterações de sistema aprovadas.

10.1.3. P7S – Política de Admissão e Cessação: define os pontos de desencadeamento para o provisionamento e desprovisionamento de acessos de utilizadores.

10.1.4. P17S – Política de Proteção de Dados e Privacidade: assegura que os controlos de acesso estão alinhados com as salvaguardas aplicáveis aos dados pessoais.

10.1.5. P30S – Política de Resposta a Incidentes: define a forma como os incidentes relacionados com acessos (por exemplo, utilização indevida ou violações) são geridos e investigados.

11. Normas e referenciais de referência

11.1. ISO/IEC 27001

11.1.1. Cláusula 5.15 – Exige políticas e processos formalizados de controlo de acessos.

11.2. ISO/IEC 27002

11.2.1. Controlos 5.15–5.17 – Especificam orientações detalhadas sobre controlo de acessos baseado em funções, gestão do ciclo de vida dos acessos de utilizadores e tratamento de acessos privilegiados.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AC-1 a AC-5 – Exigem políticas estruturadas para a gestão de acessos, incluindo autorização de contas, revisão e monitorização.

11.4. RGPD da UE

11.4.1. Artigo 32 – Exige controlos técnicos e organizativos (tais como a gestão de acessos) para assegurar a segurança e a confidencialidade dos dados.

11.5. Diretiva NIS2 da UE

11.5.1. Artigo 21(2)(b) – Impõe controlos operacionais de acesso e sistemas de gestão de identidades para prevenir acessos não autorizados a sistemas.

11.6. DORA da UE

11.6.1. Artigo 9 – Salienta a gestão segura dos riscos de TIC, incluindo um controlo de acessos robusto para entidades financeiras.

11.7. COBIT 2019

11.7.1. APO07 Gerir Recursos Humanos – Requer responsabilidades de acesso definidas e aplicadas.

11.7.2. DSS01 – Gerir Operações: inclui procedimentos para gerir o acesso lógico e manter ambientes operacionais seguros.