					Insira aqui a designação da entidade jurídica registada							
Número do documento: P11S					Título do documento: **Política de Gestão de Contas de Utilizador e Privilégios**							
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 5.3, 8	Papéis, responsabilidades e planeamento/controlo operacional para a gestão de acessos de utilizadores
ISO/IEC 27002:2022	Controlo 8	Controlos para atribuição, revisão e remoção de privilégios elevados
NIST SP 800-53 Rev.5	AC-2, AC-5, AC-6	Criação de contas, monitorização, princípio do menor privilégio e segregação de funções
Diretiva NIS2 da UE	Artigo 21(2)(d)	Gestão de acessos de utilizadores para entidades essenciais e importantes
DORA da UE	Artigo 9(2)(b)	Controlo de acessos privilegiados em entidades financeiras
COBIT 2019	DSS05.03, DSS05.04	provisionamento e desprovisionamento de acessos, e revisão periódica dos acessos dos utilizadores
RGPD da UE	Artigo 32	Controlos de acesso adequados para a proteção de dados pessoais

1. Finalidade

1.1 Esta política estabelece regras para gerir contas de utilizador e direitos de acesso de forma segura, consistente e rastreável. Garante que apenas utilizadores autorizados acedem a sistemas e dados e que esse acesso é adequado à respetiva função e responsabilidades.

1.2 A gestão eficaz de contas e privilégios é essencial para prevenir acessos não autorizados, minimizar ameaças internas e assegurar a conformidade com a ISO/IEC 27001, o RGPD da UE e outros requisitos regulamentares.

1.3 Esta política permite à organização atribuir titularidade e responsabilidade pela utilização de contas, monitorizar e auditar elevações de privilégios e desativar ou revogar acessos de forma segura quando deixem de ser necessários.

1.4 Protege ainda as operações de negócio contra erros operacionais ou utilizações indevidas causadas por acessos excessivos ou não monitorizados e ajuda a reduzir o risco de fuga acidental de dados, uso indevido de privilégios ou incumprimento regulamentar.

2. Âmbito

2.1 Esta política aplica-se a:

2.1.1 Todos os trabalhadores, estagiários, contratados e terceiros com acesso aos sistemas de TI da organização

2.1.2 Todos os sistemas, dispositivos, serviços e plataformas geridos pela organização ou em seu nome, incluindo plataformas na nuvem, infraestrutura local e ferramentas de terceiros

2.2 Abrange todos os tipos de contas de utilizador, incluindo:

2.2.1 Contas nominativas de utilizador (por exemplo, contas de correio eletrónico e autenticação de sistemas)

2.2.2 Contas de administrador e contas de sistema

2.2.3 Credenciais de acesso temporárias, de convidado ou de terceiros

2.2.4 Contas de serviço utilizadas por aplicações ou sistemas de automatização

2.3 A política aplica-se a todo o ciclo de vida das contas, desde a criação e aprovação até à alteração, monitorização e desativação. Isto inclui o provisionamento inicial de acessos durante o processo de integração, as revisões de acesso durante alterações de função e a revogação aquando da cessação.

3. Objetivos

3.1 Atribuir identidades de utilizador únicas e rastreáveis a todos os utilizadores dos sistemas, assegurando a responsabilização e eliminando a dependência de credenciais partilhadas.

3.2 Aplicar o princípio do menor privilégio, garantindo que a cada utilizador é concedido apenas o nível mínimo de acesso necessário para desempenhar as suas funções.

3.3 Prevenir acessos não autorizados a sistemas ou dados sensíveis através de processos de aprovação e revisão claramente documentados.

3.4 Assegurar a desativação atempada das contas de utilizador quando deixem de ser necessárias, por exemplo, em caso de cessação, conclusão de contrato ou alteração de função.

3.5 Manter um ambiente seguro e auditável, documentando todas as alterações a contas, aprovações e revisões periódicas, de modo a permitir a demonstração de conformidade.

3.6 Assegurar que a elevação de privilégios é estritamente controlada, aprovada de forma independente e registada, e que o acesso elevado é revogado prontamente quando deixar de ser necessário.

4. Papéis e responsabilidades

4.1 Diretor-Geral (GM)

4.1.1 Detém a responsabilidade global pela aplicação desta política.

4.1.2 Assegura que as práticas de gestão de contas estão alinhadas com os requisitos de certificação ISO/IEC 27001 e com as obrigações legais aplicáveis (por exemplo, o RGPD da UE).

4.1.3 Deve ser informado imediatamente de qualquer acesso não autorizado, incidente de segurança ou violação da política relacionada com contas de utilizador.

4.1.4 Supervisiona as revisões da política, as auditorias e as medidas de aplicação.

4.2 Responsável de TI ou prestadores externos de serviços de TI

4.2.1 É responsável pela implementação técnica dos controlos de contas e privilégios nos sistemas utilizados pela organização.

4.2.2 Deve provisionar, alterar e desativar contas de utilizador apenas com base em aprovações documentadas.

4.2.3 Deve aplicar requisitos de complexidade de palavras-passe, tempo limite de bloqueio de ecrã, autenticação multifator (se disponível) e registo de eventos nos sistemas.

4.2.4 Deve manter registos seguros de todas as aprovações de acesso, titularidade de contas, elevações de privilégios e revogações.

4.2.5 Deve monitorizar contas não autorizadas ou contas sem proprietário identificado e comunicar discrepâncias 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 Esta política deve ser revista pelo menos anualmente pelo Diretor-Geral (GM) e pelo Responsável de TI para assegurar a conformidade com:

9.1.1 Os controlos e orientações em vigor da ISO/IEC 27001:2022

9.1.2 As atualizações regulamentares aplicáveis (por exemplo, RGPD da UE, DORA da UE, Diretiva NIS2 da UE)

9.1.3 As alterações nos sistemas, serviços ou estrutura do negócio

9.2 Devem também ser realizadas revisões após:

9.2.1 Incidentes de segurança significativos ou constatações de auditoria

9.2.2 Alterações relevantes nos sistemas de TI ou na arquitetura de contas

9.2.3 Introdução de novas plataformas que exijam integração com o controlo de acesso

9.3 Todas as alterações devem ser aprovadas pelo Diretor-Geral (GM) e comunicadas de forma clara ao pessoal afetado.

10. Políticas relacionadas e ligações

10.1 P2S – Política de Papéis e Responsabilidades de Governação: Estabelece a responsabilização e a autoridade de decisão para aprovações de acesso e supervisão.

10.2 P4S – Política de Controlo de Acesso: Regula a aplicação do controlo de acesso em toda a organização e os métodos de autenticação.

10.3 P7S – Política de Admissão e Cessação: Assegura que a criação e remoção de contas estão integradas nas alterações de pessoal geridas por Recursos Humanos.

10.4 P8S – Política de Sensibilização e Formação em Segurança da Informação: Forma os utilizadores sobre práticas seguras de utilização de contas e expectativas de utilização.

10.5 P30S – Política de Resposta a Incidentes (P30): Define as ações a adotar se o uso indevido de uma conta resultar numa violação de segurança ou divulgação não autorizada.

11. Normas e quadros de referência

11.1 ISO/IEC 27001

11.1.1 Cláusula 5.3: Exige que os papéis e responsabilidades em segurança da informação sejam claramente atribuídos e aplicados.

11.1.2 Cláusula 8.1: O planeamento e controlo operacional devem incluir a gestão de acessos de utilizadores.

11.2 ISO/IEC 27002

11.2.1 Controlo 8.2: Detalha os controlos técnicos e processuais para atribuição, revisão e remoção de privilégios elevados.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-2: Exige a criação, monitorização e revogação de contas com base em funções e processos definidos.

11.3.2 AC-5: Trata da segregação de funções para prevenir conflitos ou abuso de privilégios.

11.3.3 AC-6: Determina a aplicação do princípio do menor privilégio a todos os direitos de acesso.

11.4 RGPD da UE

11.4.1 Artigo 32: Exige controlos de acesso adequados para proteger os dados pessoais contra acesso ou alteração não autorizados.

11.5 Diretiva NIS2 da UE

11.5.1 Artigo 21(2)(d): Determina a gestão de acessos de utilizadores como parte dos controlos de segurança essenciais para entidades essenciais e importantes.

11.6 DORA da UE

11.6.1 Artigo 9(2)(b): Exige que as entidades financeiras implementem controlos de acesso que restrinjam e monitorizem privilégios de acesso.

11.7 COBIT 2019

11.7.1 DSS05.03: Especifica o provisionamento e o desprovisionamento de acessos dos utilizadores como parte da governação de TI.

11.7.2 DSS05.04: Exige a revisão contínua e o alinhamento dos acessos dos utilizadores com as funções organizacionais.