					Insira aqui a designação da entidade jurídica registada							
Número do documento: P03					Título do documento: **Política de Utilização Aceitável**							
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	Estabelece normas comportamentais e requisitos para a Política de Utilização Aceitável
ISO/IEC 27002:2022	Controlos 6.1, 6.2, 8.1, 8.12	Orienta as responsabilidades de segurança da informação, a sensibilização e a governação de dispositivos e dados
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Controlos de acesso e de sensibilização/comportamentais relevantes para a utilização de ativos de TIC
RGPD da UE	Artigos 5(1)(f), 32; Considerando 39	Impõe a confidencialidade e a integridade, exige controlos técnicos e organizativos e fundamentos jurídicos para a utilização adequada
Diretiva NIS2 da UE	Artigo 21(2)(a–d)	Exige políticas operacionais e formação para uma utilização segura
DORA da UE	Artigo 5	Apoia a gestão do risco das TIC ao regular o comportamento dos utilizadores
COBIT 2019	APO07, BAI05, DSS05, MEA01	Recursos humanos, gestão da mudança, serviços de segurança geridos e monitorização da conformidade/desempenho

1. Finalidade

1.1 Esta política define a utilização aceitável e inaceitável dos sistemas de informação, recursos informáticos, ferramentas de comunicação e práticas de tratamento de dados da organização.

1.2 Assegura que todos os utilizadores compreendem as suas responsabilidades na utilização de ativos de TIC corporativos e que as suas ações apoiam a Confidencialidade, Integridade e Disponibilidade, bem como o tratamento lícito da informação.

1.3 A política cumpre a Cláusula 5.10 da ISO/IEC 27001:2022 ao estabelecer regras de comportamento para a utilização dos sistemas e aplicar salvaguardas técnicas e processuais para minimizar o risco de uso indevido, negligência ou abuso.

1.4 A política apoia igualmente as atividades de investigação e de aplicação, incluindo a resposta a incidentes e a adoção de medidas disciplinares em caso de violação.

2. Âmbito

2.1 Esta política aplica-se a todas as pessoas singulares e entidades às quais seja concedido acesso aos sistemas de informação e ativos da organização, incluindo, entre outros:

2.1.1 trabalhadores, prestadores de serviços, consultores, estagiários e trabalhadores temporários

2.1.2 terceiros fornecedores com acesso a sistemas ou funções administrativas delegadas

2.1.3 convidados ou parceiros que utilizem infraestrutura de TIC pertencente à organização ou por esta autorizada

2.2 O âmbito inclui todos os ativos tecnológicos e de dados da organização, incluindo:

2.2.1 postos de trabalho, computadores portáteis, dispositivos móveis e servidores

2.2.2 infraestrutura de rede e serviços alojados na nuvem

2.2.3 correio eletrónico, mensagens, armazenamento de ficheiros, plataformas de colaboração e VPN

2.2.4 dados em repouso, em trânsito ou em processamento, independentemente do formato ou da localização

2.2.5 qualquer dispositivo pessoal utilizado ao abrigo de um regime Bring Your Own Device (BYOD) que se ligue aos sistemas da organização

2.3 Esta política aplica-se a todos os ambientes de trabalho, incluindo:

2.3.1 escritórios corporativos e instalações de produção

2.3.2 locais de trabalho remoto ou modelos híbridos

2.3.3 operações no terreno ou instalações geridas por terceiros

2.4 Todos os utilizadores devem reconhecer e cumprir esta política como condição de acesso aos sistemas da organização ou de tratamento de dados corporativos.

3. Objetivos

3.1 Definir e aplicar regras para a utilização autorizada dos recursos informáticos da organização.

3.2 Prevenir acessos não autorizados, fuga de dados ou danos resultantes de utilização negligente ou maliciosa.

3.3 Proteger as redes, os ativos e os dados da organização contra ameaças introduzidas pelo comportamento dos utilizadores.

3.4 Apoiar obrigações legais e contratuais através da demonstração de diligência devida na governação dos recursos de TIC.

3.5 Assegurar consistência e clareza na aplicação de medidas disciplinares e processos de tratamento de exceções.

3.6 Promover uma cultura de utilização ética, segura e responsável dos recursos informáticos digitais e físicos.

4. Papéis e responsabilidades

4.1 Alta Direção

4.1.1 Aprova a Política de Utilização Aceitável e assegura o seu alinhamento com os objetivos do negócio, os requisitos regulamentares e os valores organizacionais.

4.1.2 Afeta recursos para a aplicação, formação, monitorização e revisão da política.

4.1.3 Revê o estado de conformidade e as medidas disciplinares associadas a violações da política no âmbito da governação do SGSI.

4.2 Equipas de TI e de Segurança da Informação

4.2.1 Implementam salvaguardas técnicas para aplicar esta política, incluindo:

4.2.2 filtragem de conteúdos, proteção contra malware, segurança de endpoints e ferramentas de monitorização de rede

4.2.3 configurações de segurança do correio eletrónico e soluções de prevenção de perda de dados (DLP)

4.2.4 listas de bloqueio e listas de permissões para software, hardware e websites

4.2.5 Mantêm um inventário de software, dispositivos e serviços aprovados e proibidos.

4.2.6 Investigam suspeitas de violações da Política de Utilização Aceitável, recolhem evidência forense e apoiam ações disciplinares ou legais, quando aplicável.

4.2.7 Colaboram com Recursos Humanos e Jurídico no tratamento de incidentes, escalonamento e cumprimento das obrigações de notificação.

[... 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 Desencadeadores de revisão e frequência

9.1.1 Esta política deve ser revista:

9.1.1.1 pelo menos anualmente

9.1.1.2 na sequência de alterações significativas na tecnologia ou na infraestrutura

9.1.1.3 após incidentes ou constatações de auditoria que evidenciem lacunas na aplicação

9.1.1.4 em resposta a alterações na legislação aplicável ou nos contratos

9.2 Propriedade e aprovação

9.2.1 O Diretor de Segurança da Informação ou o Gestor do SGSI designado é responsável pelo processo de revisão.

9.2.2 As atualizações devem ser aprovadas pela Alta Direção e comunicadas a toda a organização.

9.2.3 A aceitação dos termos atualizados deve ser novamente recolhida aquando da reemissão da política.

9.3 Gestão documental

9.3.1 A política deve incluir os seguintes metadados e elementos de versionamento:

9.3.1.1 título, ID e nível de classificação

9.3.1.2 proprietário da política e responsável pela gestão documental

9.3.1.3 histórico de alterações e fundamentação das atualizações

9.3.1.4 datas de revisão e da próxima atualização planeada

9.3.1.5 referências ao registo de distribuição e de aceitação

9.3.2 A cópia mestre deve ser mantida no repositório documental do SGSI, sujeita a controlo de versões.

10. Políticas relacionadas e articulações

10.1 Esta política deve ser interpretada em conjunto com as seguintes:

10.1.1 P1 – Política de Segurança da Informação: Estabelece as expectativas comportamentais fundamentais e o compromisso da liderança de topo com a utilização aceitável.

10.1.2 P4 – Política de controlo de acesso: Define as permissões e os direitos associados ao acesso de utilizadores, sistemas e dados, aplicando diretamente os limites da utilização aceitável.

10.1.3 P6 – Política de Gestão de Riscos: Trata os riscos relacionados com o comportamento e apoia atividades de monitorização e tratamento associadas a ameaças originadas por utilizadores.

10.1.4 P7 – Política de Admissão e Cessação: Assegura que os termos de utilização aceitável são aceites na entrada e revogados na saída.

10.1.5 P9 – Política de trabalho remoto: Estende as disposições de utilização aceitável aos ambientes de trabalho remoto e híbrido.

10.2 Estas políticas relacionadas constituem um modelo de defesa em profundidade para a governação comportamental, técnica e contratual.

11. Normas e quadros de referência

11.1 Esta Política de Utilização Aceitável está alinhada com normas reconhecidas internacionalmente e quadros jurídicos aplicáveis, para assegurar controlos comportamentais aplicáveis, auditáveis e baseados no risco em toda a utilização de sistemas de informação digitais e físicos.

11.2 ISO/IEC 27001:2022

11.2.1 Cláusula 5.10 – Utilização aceitável da informação e de outros ativos associados: Esta política cumpre diretamente o requisito de definir, comunicar e aplicar regras que regem a utilização adequada dos recursos de TIC.

11.2.2 Anexo A Controlo 6.1 – Responsabilidade pela Segurança da Informação: Atribui responsabilidades claras pelo comportamento dos utilizadores e pela supervisão do cumprimento.

11.2.3 Anexo A Controlo 6.2 – Sensibilização, educação e formação em segurança da informação: Os processos de formação integrada e de aceitação da política fazem parte da aplicação da Política de Utilização Aceitável.

11.2.4 Anexo A Controlo 8.1 – Dispositivos endpoint do utilizador e 8.12 – Prevenção da perda de dados: Trata o comportamento aceitável nos dispositivos dos utilizadores e rege atividades que possam conduzir à exposição ou fuga de dados.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-19 (Controlo de acesso para dispositivos móveis) e AC-20 (Utilização de sistemas de informação externos): Esta política define obrigações e restrições dos utilizadores para BYOD e acesso a sistemas de terceiros.

11.3.2 PL-4 (Regras de comportamento): Estabelece requisitos detalhados de utilização aceitável consistentes com esta política.

11.3.3 AT-2 (Formação de sensibilização em segurança): Suportado através da formação dos utilizadores e da aceitação documentada da política.

11.3.4 AU-2 (Eventos de auditoria) e AU-12 (Geração de auditoria): A aplicação assenta na monitorização das ações dos utilizadores e na geração de alertas sobre violações.

11.4 RGPD da UE (2016/679):

11.4.1 Artigo 5(1)(f): Impõe a segurança e a integridade dos dados pessoais; esta política mitiga os riscos introduzidos pelo comportamento humano e pela utilização não autorizada.

11.4.2 Artigo 32: Exige medidas técnicas e organizativas, como controlos comportamentais e restrições de utilização, para proteger dados pessoais.

11.4.3 Considerando 39: Destaca a necessidade de assegurar apenas o acesso necessário e a utilização lícita dos dados por pessoas autorizadas.

11.5 Diretiva NIS2 da UE (2022/2555):

11.5.1 Artigo 21(2)(a–d): Exige políticas operacionais e formação para a utilização segura dos sistemas, o que esta Política de Utilização Aceitável assegura através da definição de comportamentos, monitorização e processos de aplicação.

11.6 DORA da UE (2022/2554):

11.6.1 Artigo 5: Esta política apoia o quadro de gestão do risco das TIC ao definir regras para a interação entre pessoas e sistemas e ao minimizar a exposição ao risco cibernético baseado no comportamento.

11.7 COBIT 2019:

11.7.1 APO07 – Gerir recursos humanos: Aplica responsabilidades e sensibilização dos utilizadores ao longo do ciclo de vida do trabalhador.

11.7.2 BAI05 – Gestão da mudança organizacional: Incorpora a governação da utilização aceitável nos processos de mudança que afetam o comportamento dos utilizadores.

11.7.3 DSS05 – Gerir serviços de segurança: Apoia a monitorização da atividade dos utilizadores, alertas comportamentais e mecanismos de resposta automatizados.

11.7.4 MEA01 – Monitorizar, avaliar e analisar o desempenho e a conformidade: A política define métricas e mecanismos para validar o cumprimento, pelos utilizadores, das expectativas comportamentais.