					Insira aqui a designação da entidade jurídica registada							
Número do documento: P03S					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	Relevante para o âmbito global da política e para a sua implementação
ISO/IEC 27002:2022	5.10, 5.11, 5	Fornece orientações sobre requisitos e controlos de utilização aceitável
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Abrange a utilização de sistemas e dispositivos, a monitorização e a formação dos utilizadores
RGPD da UE	Artigos 5(1)(f), 32	Integridade e confidencialidade dos dados e medidas de segurança
Diretiva NIS2 da UE	Artigo 21(2)(b)	Exige políticas de segurança e de utilização aceitável adequadas
DORA da UE	Artigo 9	Política de gestão do risco das TIC, controlos e aplicação
COBIT 2019	DSS05, BAI08	Serviços de segurança e gestão do conhecimento

1. Finalidade

1.1. Esta política define a utilização aceitável, responsável e segura dos sistemas, dispositivos, acesso à Internet, correio eletrónico, serviços na nuvem e quaisquer dispositivos pessoais utilizados para fins profissionais, disponibilizados ou autorizados pela empresa.

1.2. Assegura que os utilizadores compreendem as suas obrigações na utilização dos recursos informáticos da organização, protegendo a integridade dos dados, a privacidade e a continuidade operacional.

1.3. Esta política apoia a conformidade com a ISO/IEC 27001:2022, ao estabelecer normas claras de comportamento dos utilizadores, alinhadas com requisitos legais, contratuais e regulamentares.

2. Âmbito

2.1. Esta política aplica-se a todos os indivíduos que acedam, administrem ou interajam com sistemas ou dados da empresa, incluindo:

2.1.1. trabalhadores e prestadores de serviços

2.1.2. trabalhadores temporários ou estagiários

2.1.3. prestadores externos de serviços de TI

2.2. Abrange:

2.2.1. computadores, telemóveis e tablets propriedade da empresa

2.2.2. dispositivos pessoais (BYOD) aprovados para uso profissional

2.2.3. redes da empresa, plataformas na nuvem e serviços de software

2.2.4. acesso à Internet, sistemas de correio eletrónico, armazenamento partilhado e aplicações empresariais

2.3. Esta política aplica-se a todos os ambientes de trabalho — presencial, remoto e híbrido — e durante todo o período de atividade da empresa.

3. Objetivos

3.1. Definir o que constitui utilização aceitável e utilização não aceitável dos sistemas de TI.

3.1.1. Reduzir os riscos de segurança decorrentes de utilização indevida, acesso não autorizado ou introdução de malware.

3.1.2. Proteger os dados do negócio, a informação dos clientes e a reputação da empresa.

3.1.3. Estabelecer regras aplicáveis e assegurar a responsabilização de todos os utilizadores.

3.1.4. Apoiar a monitorização e a conformidade, para detetar violações atempadamente e adotar ações corretivas.

4. Funções e responsabilidades

4.1. Diretor-Geral (GM)

4.1.1. Aprova esta política e é responsável por assegurar a disponibilidade dos recursos e da autoridade necessários à sua aplicação.

4.1.2. Revê e autoriza quaisquer exceções a esta política.

4.2. Gestor de TI ou Prestador Externo de Serviços de TI

4.2.1. Mantém inventários de software e hardware aprovados.

4.2.2. Configura os dispositivos para aplicar as regras de utilização aceitável (por exemplo, filtragem de conteúdos, registo de acessos).

4.2.3. Monitoriza a utilização para identificar potenciais violações e investiga incidentes.

4.2.4. Assegura que os dispositivos pessoais utilizados para fins profissionais (BYOD) estão autorizados e configurados de forma segura.

[... 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. Esta política deve ser revista anualmente pelo Gestor de TI, com aprovação final do Diretor-Geral (GM), para assegurar que permanece alinhada com os padrões de utilização da tecnologia, os riscos emergentes e as obrigações de conformidade.

9.2. Fatores de revisão intercalar

9.2.1. As revisões devem também ser realizadas em resposta a:

9.2.2. novos sistemas ou tecnologias (por exemplo, novo serviço na nuvem ou nova plataforma de endpoint)

9.2.3. violações significativas da política

9.2.4. atualizações legislativas ou de termos contratuais que afetem a utilização de TI

9.3. Documentação de alterações

9.3.1. Todas as atualizações devem ser registadas num registo de versões que inclua:

9.3.1.1. número da versão

9.3.1.2. data da revisão

9.3.1.3. resumo das alterações

9.3.1.4. autoridade de aprovação

9.4. Comunicação da política

9.4.1. As versões revistas desta política devem ser comunicadas a todos os utilizadores afetados. Os trabalhadores devem confirmar a receção e a compreensão no âmbito das suas obrigações de sensibilização para a segurança.

10. Políticas relacionadas e articulações

10.1. Esta política funciona em conjunto com várias outras políticas SME para assegurar uma cobertura abrangente das responsabilidades de segurança:

10.1.1. P4S – Política de controlo de acesso: define a aplicação técnica e processual da utilização permitida e das restrições de conta.

10.1.2. P8S – Política de sensibilização e formação em segurança da informação: proporciona formação aos utilizadores sobre os limites de utilização aceitável e as obrigações de comunicação.

10.1.3. P9S – Política de trabalho remoto: regula a utilização dos sistemas da empresa em ambientes externos ou domésticos.

10.1.4. P17S – Política de Proteção de Dados e Privacidade: aplica regras de tratamento de dados pessoais que se articulam com a monitorização da utilização aceitável e com dispositivos pessoais (BYOD).

10.1.5. P30S – Política de Resposta a Incidentes (P30): define os procedimentos de investigação e resposta a utilizações indevidas ou violações dos termos de utilização aceitável.

11. Normas e referenciais

11.1. ISO/IEC 27001

11.1.1. Cláusula 5.10 – Exige que as organizações definam e apliquem regras de utilização aceitável dos ativos de informação.

11.2. ISO/IEC 27002

11.2.1. Controlo 5.10 – Fornece orientações para a utilização aceitável dos sistemas, incluindo comportamentos permitidos e proibidos.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-19 – Trata o controlo da utilização de sistemas, incluindo dispositivos pessoais.

11.3.2. AC-20 – Exige autorização e monitorização de sistemas externos.

11.3.3. AT-2 – Salienta a importância de formar os utilizadores sobre práticas de utilização aceitável.

11.4. RGPD da UE

11.4.1. Artigo 5(1)(f) – Exige a integridade e a confidencialidade dos dados pessoais, que podem ser comprometidas por utilização indevida por parte dos utilizadores.

11.4.2. Artigo 32 – Exige a implementação de medidas técnicas e organizativas para proteger sistemas e dados.

11.5. Diretiva NIS2 da UE

11.5.1. Artigo 21(2)(b) – Exige políticas de segurança adequadas, incluindo regras de utilização aceitável, para mitigar ciberameaças.

11.6. DORA da UE

11.6.1. Artigo 9 – Exige políticas de gestão do risco das TIC, incluindo controlos de utilização e mecanismos de aplicação.

11.7. COBIT 2019

11.7.1. DSS05 – Gerir Serviços de Segurança: salienta o controlo do comportamento dos utilizadores com base em políticas.

11.7.2. BAI08 – Gerir o Conhecimento: aborda a sensibilização para as responsabilidades decorrentes das políticas e a formação em utilização aceitável.