					Insira aqui a designação da entidade jurídica registada							
Número do documento: PII14					Título do documento: **Política de segurança e controlo de acesso a PII**							
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 / Controlo / Artigo	Aplicabilidade	Tipo de cobertura	Comentário
ISO/IEC 27701:2025	Clause 6.1.3; Clause 8.1	Both	Primary	Planeamento e operação de controlos de segurança de PII
ISO/IEC 27701:2025	Clause 7.5; Clause 9.1; Clause 10.2	Both	Supporting	Evidência, monitorização e ações corretivas
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9	Both	Primary	Identidade e direitos de acesso para o tratamento de PII
ISO/IEC 27701:2025	Annex A.3.22; Annex A.3.23	Both	Primary	Proteção de endpoint e autenticação segura
ISO/IEC 27701:2025	Annex A.3.25; Annex A.3.26	Both	Primary	Registo e proteção criptográfica
ISO/IEC 27701:2025	Annex A.3.28; Annex A.3.29	Both	Supporting	Segurança das aplicações e arquitetura segura
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.15; Annex A.3.16	Both	Supporting	Proteção e revisão de registos
GDPR	Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32	Both	Primary	Segurança, responsabilização e controlos de subcontratantes
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Integração de controlos do ISMS
ISO/IEC 27002:2022	Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Orientações para implementação de controlos de segurança
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Princípios de segurança da informação e conformidade em privacidade

ISO/IEC 29151:2022	Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	Controlos de segurança para proteção de PII

1. Âmbito

1.1 Esta política define requisitos específicos de segurança e controlo de acesso a PII para sistemas, aplicações, serviços, dispositivos, ambientes de nuvem e processos operacionais que armazenem, transmitam, tratem, acedam, administrem ou protejam PII.

1.2 Esta política aplica-se a contextos de responsável pelo tratamento, responsável conjunto pelo tratamento, subcontratante e subcontratante subsequente em que a organização determine, opere, suporte ou dependa de controlos de segurança para o tratamento de PII.

1.3 Esta política abrange os seguintes domínios de controlos de segurança de PII:

1.3.1 linha de base de segurança de PII e integração com as políticas de segurança da informação existentes;

1.3.2 controlo de acesso;

1.3.3 autenticação;

1.3.4 acesso privilegiado;

1.3.5 cifragem e armazenamento seguro;

1.3.6 registo e monitorização;

1.3.7 configuração segura e gestão de vulnerabilidades;

1.3.8 controlos de acesso de endpoint e de nuvem;

1.3.9 ligação de evidência através de REG02, REG08, REG10 e REG12.

1.4 Esta política não substitui um sistema completo de gestão de segurança da informação, uma política de segurança de redes, uma política de desenvolvimento seguro, uma política de cópias de segurança, uma política de endpoint, uma política de segurança da nuvem, uma norma criptográfica, um procedimento de gestão de vulnerabilidades ou um procedimento de resposta a incidentes. Quando essas políticas já existam, esta política define as ligações e os requisitos de evidência específicos de PII necessários para a garantia do PIMS.

1.5 Esta política não duplica:

1.5.1 a titularidade do inventário de tratamento de PII e do fundamento de licitude em PII03;

1.5.2 a metodologia de avaliação de riscos de privacidade e de DPIA em PII07;

1.5.3 os gates de privacidade desde a conceção em PII08;

1.5.4 as regras de recolha, utilização, divulgação e partilha em PII09;

1.5.5 a execução da retenção, eliminação e destruição em PII10;

1.5.6 a governação do ciclo de vida de subcontratantes em PII12;

1.5.7 os controlos dos mecanismos de transferência internacional em PII13;

1.5.8 o fluxo de trabalho de incidentes e violações em PII15;

1.5.9 a governação da informação documentada em PII17;

1.5.10 a governação da monitorização, auditoria e melhoria do PIMS em PII18.

1.6 Para efeitos desta política, os logs operacionais, as saídas de ferramentas de segurança, as exportações de revisões de acessos, os relatórios de vulnerabilidades e a evidência de configuração são fontes de evidência anexadas, resumidas ou referenciadas pelos objetos de evidência canónicos. Não constituem registos PIMS separados.

2. Finalidade

2.1 A finalidade desta política é assegurar que a PII é protegida por controlos de segurança e de acesso adequados, alinhados com o risco e auditáveis ao longo de todo o tratamento.

2.2 Esta política permite à organização demonstrar que os controlos de segurança de PII são planeados, implementados, revistos, monitorizados e melhorados através de REG02, REG08,

REG10 e REG12, sem criar registos de segurança duplicados nem substituir políticas de segurança da informação existentes.

3. Objetivos

3.1 Os objetivos desta política são:

3.1.1 definir uma linha de base de controlo de acesso a PII para sistemas e atividades de tratamento;

3.1.2 assegurar que os controlos de autenticação são adequados à sensibilidade da PII e ao contexto de acesso;

3.1.3 definir requisitos de revisão para o acesso privilegiado e ordinário a PII;

3.1.4 definir expectativas de cifragem e armazenamento seguro para PII em repouso, em trânsito e em contextos relevantes de nuvem ou endpoint;

3.1.5 definir expectativas de registo e monitorização para o acesso a PII, alterações a PII e administração de PII;

3.1.6 definir requisitos de evidência de configuração segura e de vulnerabilidades para sistemas que tratam PII;

3.1.7 definir expectativas de acesso de endpoint e de nuvem sem criar uma política completa de endpoint ou de segurança da nuvem;

3.1.8 ligar incidentes de segurança de PII suspeitos a REG10 sem duplicar o fluxo de trabalho de incidentes;

3.1.9 integrar com políticas de segurança da informação existentes, quando disponíveis;

3.1.10 manter evidência preparada para auditoria utilizando apenas REG02, REG08, REG10 e REG12.

4. Declarações da política

4.1 Linha de base de segurança de PII e integração com o ISMS

4.1.1 [Both] The Information Security Lead MUST definir a linha de base de segurança de PII para cada sistema ou serviço que trate PII em REG12 antes de o sistema ou serviço entrar em produção ou sofrer uma alteração material.

4.1.2 [Both] The System Owner / Application Owner MUST registar em REG12 a localização da evidência dos controlos de segurança de PII implementados antes de se apoiar num controlo de segurança da informação existente para garantia do PIMS.

4.1.3 [Controller] The Process Owner / Business Owner MUST identificar a sensibilidade da PII, o contexto do tratamento e a necessidade de acesso em REG02 antes de solicitar acesso novo ou materialmente alterado a PII.

4.1.4 [Processor] The Vendor / Procurement Owner MUST registar as instruções de segurança do cliente, os limites de responsabilidade do cliente e os compromissos de segurança do subcontratante em REG08 antes de o acesso do subcontratante à PII do cliente começar ou sofrer alteração material.

4.1.5 [Both] The Privacy Lead / PIMS Manager MUST verificar que a evidência de segurança de PII está ligada a REG02, REG08, REG10 ou REG12 antes de aceitar a atividade de tratamento como auditável no PIMS.

4.2 Linha de base de controlo de acesso

4.2.1 [Both] The System Owner / Application Owner MUST restringir o acesso a PII a funções aprovadas e utilizadores autorizados registados ou rastreáveis em REG02 ou REG12 antes de o acesso ser ativado.

4.2.2 [Both] The Process Owner / Business Owner MUST aprovar a finalidade de negócio do acesso a PII em REG02 ou REG12 antes de The System Owner / Application Owner provisionar o acesso.

4.2.3 [Both] The System Owner / Application Owner MUST rever o acesso de utilizadores a sistemas que tratem PII de alto impacto ou sensível pelo menos trimestralmente e registar o resultado da revisão em REG12.

4.2.4 [Both] The System Owner / Application Owner MUST rever o acesso de utilizadores a outros sistemas que tratem PII pelo menos anualmente e registar o resultado da revisão em REG12.

4.2.5 [Both] The System Owner / Application Owner MUST remover ou alterar o acesso a PII em REG12 no prazo de um dia útil após mudança de função, cessação, conclusão de contrato ou quando o acesso deixar de ser necessário.

4.2.6 [Processor] The Vendor / Procurement Owner MUST confirmar em REG08 que o acesso do subcontratante à PII do cliente está limitado às instruções documentadas do cliente antes de o acesso ser ativado ou alterado.

4.2.7 [Subprocessor] The Vendor / Procurement Owner MUST confirmar em REG08 que o acesso do subcontratante subsequente a PII está limitado às atividades de subcontratação autorizadas antes de o acesso do subcontratante subsequente ser ativado ou alterado.

[... As secções 4.3–8 não estão incluídas nesta pré-visualização. Adquira o documento completo para aceder ao conteúdo integral. ...]

9. Exceções

9.1.1 [Both] The Information Security Lead MUST registar cada exceção a um requisito de segurança de PII ou de controlo de acesso em REG12 antes de a exceção ser ativada.

9.1.2 [Both] The Data Protection Officer / Privacy Advisor MUST aconselhar sobre exceções de segurança de PII de maior risco em REG12 antes da aprovação.

9.1.3 [Both] Top Management MUST aprovar exceções de segurança de PII em REG12 antes da ativação quando a exceção afetar PII de alto impacto, PII sensível, acesso privilegiado, cifragem, registo ou vulnerabilidades de alto risco não resolvidas.

9.1.4 [Both] The Information Security Lead MUST definir em REG12 a expiração da exceção, o controlo compensatório e a data de revisão antes da aprovação da exceção.

9.1.5 [Both] The System Owner / Application Owner MUST remediar, renovar ou encerrar exceções de segurança de PII expiradas em REG12 no prazo de cinco dias úteis após a expiração.

9.1.6 [Processor] The Vendor / Procurement Owner MUST registar em REG08 e REG12 exceções de segurança de subcontratantes ou subcontratantes subsequentes que afetem PII do cliente antes da aceitação.

10. Aplicação

10.1.1 [Both] The Privacy Lead / PIMS Manager MUST registar não conformidades por evidência de segurança de PII ausente ou incompleta em REG12 no prazo de cinco dias úteis após a identificação.

10.1.2 [Both] The Information Security Lead MUST atribuir a titularidade da remediação de falhas de controlos de segurança de PII em REG12 no prazo de cinco dias úteis após a validação.

10.1.3 [Both] The System Owner / Application Owner MUST desativar ou restringir acesso a PII não autorizado, excessivo ou não suportado no prazo de um dia útil após a validação e registar a ação em REG12.

10.1.4 [Conditional] The Incident Response Coordinator MUST ligar ações de aplicação a REG10 no prazo de um dia útil quando a matéria de aplicação envolver um incidente de PII suspeito ou confirmado.

10.1.5 [Both] Top Management MUST rever não conformidades de segurança de PII repetidas ou de alto risco em REG12 antes da revisão pela gestão.

11. Revisão e manutenção

11.1.1 [All] The Privacy Lead / PIMS Manager MUST rever esta política com The Information Security Lead pelo menos anualmente e registar o resultado da revisão em REG12.

11.1.2 [Both] The Information Security Lead MUST rever a linha de base de segurança de PII em REG12 no prazo de 30 dias após uma alteração material tecnológica, de ameaça, auditoria, incidente ou regulamentar que afete a segurança de PII.

11.1.3 [Both] The System Owner / Application Owner MUST atualizar em REG12 a evidência de segurança de PII ao nível do sistema no prazo de 30 dias após alteração material de arquitetura, acesso, configuração, vulnerabilidade ou registo.

11.1.4 [Processor] The Vendor / Procurement Owner MUST rever a evidência de responsabilidades de segurança de PII de subcontratantes e subcontratantes subsequentes em REG08 no prazo de 30 dias após alteração material de serviço, instrução do cliente ou subcontratante subsequente.

11.1.5 [All] The Internal Audit / Compliance Reviewer MUST verificar a evidência de revisão da política e evidência selecionada de controlos de segurança de PII em REG12 de acordo com o plano de auditoria aprovado.

12. Políticas relacionadas

12.1 Esta política deve ser lida em conjunto com:

12.2 PII01 - Política do sistema de gestão de informações de privacidade;

12.3 PII02 - Política de papéis, responsabilidades e responsabilização em privacidade;

12.4 PII03 - Política de inventário de tratamento de PII e fundamento de licitude;

12.5 PII07 - Política de avaliação de riscos de privacidade e DPIA;

12.6 PII08 - Política de privacidade desde a conceção e por defeito;

12.7 PII09 - Política de recolha, utilização, divulgação e partilha de PII;

12.8 PII10 - Política de retenção, eliminação e destruição de PII;

12.9 PII12 - Política de gestão de privacidade de subcontratantes, subcontratantes subsequentes e terceiros;

12.10 PII13 - Política de transferência internacional de PII;

12.11 PII15 - Política de gestão de incidentes e violações de PII;

12.12 PII16 - Política de formação, sensibilização e competência em privacidade;

12.13 PII17 - Política de informação documentada e gestão de evidência do PIMS;

12.14 PII18 - Política de monitorização, auditoria e melhoria do PIMS.

13. Normas e referenciais de referência

13.1 ISO/IEC 27701:2025 - Clause 6.1.3; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.7; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5; 5.1.4; 5.1.6; 6.1.2; 7.1.1; 7.1.2].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.5.5; 4.6.3; 4.6.4; 4.7.5; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 7.1.3; 7.1.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.2; 11.1.1; 11.1.5].

13.3 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 10.1.3].

13.4 ISO/IEC 27701:2025 - Annex A.3.22; Annex A.3.23. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5].

13.5 ISO/IEC 27701:2025 - Annex A.3.25; Annex A.3.26. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.6 ISO/IEC 27701:2025 - Annex A.3.28; Annex A.3.29. Addressed by clauses [4.1.1; 4.1.2; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 7.1.1; 7.1.2].

13.7 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.15; Annex A.3.16. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.6.2; 4.6.3; 4.6.4; 4.7.2; 4.7.3; 5.1.9; 6.1.6; 8.1.4; 10.1.1; 11.1.5].

13.8 GDPR - Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.5; 4.2.6; 4.2.7; 4.3.2; 4.4.4; 4.5.1; 4.5.2; 4.6.1; 4.6.6; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 4.8.5; 5.1.1; 5.1.7; 6.1.4; 7.1.4; 9.1.3; 10.1.4].

13.9 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.10 ISO/IEC 27002:2022 - Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.11 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.1; 4.5.1; 4.6.2; 4.6.6; 4.7.6; 5.1.2; 6.1.1; 8.1.4; 10.1.1; 11.1.1].

13.12 ISO/IEC 29151:2022 - Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.7.1; 4.7.2; 4.7.4; 4.8.1; 4.8.2; 6.1.6; 11.1.5].