					Insira aqui a designação da entidade jurídica registada							
Número do documento: PII23					Título do documento: **Política de Subcontratante de PII na Nuvem**							
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 4.1; Clause 6.1.3	Processor	Supporting	Papel PIMS e aplicabilidade dos controlos
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Processor	Primary	Evidência documentada de subcontratante na nuvem e controlo operacional
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Processor	Supporting	Monitorização, não conformidade e ação corretiva
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.5; Annex A.2.2.6; Annex A.2.2.7	Processor	Primary	Acordos com clientes, instruções, apoio e registos
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Assistência ao cliente relativamente às obrigações perante os titulares dos dados
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Primary	Ficheiros temporários, devolução, transferência, eliminação e controlos de transmissão
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Supporting	Base e localizações das transferências
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Registos de divulgação e tratamento de pedidos de divulgação
ISO/IEC 27701:2025	Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9	Processor	Primary	Divulgação, contratação e aviso de alteração de subcontratantes subsequentes
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9; Annex A.3.14;	Processor	Supporting	Evidência de acesso, registos,

	Annex A.3.24; Annex A.3.25			cópias de segurança e logs
GDPR	Article 28	Processor	Primary	Subcontratante, subcontratante subsequente, assistência, auditoria, apagamento e devolução
GDPR	Article 30	Processor	Supporting	Registos do subcontratante
GDPR	Article 32; Article 33	Processor	Supporting	Segurança e notificação de violação ao responsável pelo tratamento
GDPR	Article 44	Conditional	Referenced	Encaminhamento de transferências internacionais
ISO/IEC 29100:2020	Clause 5.3; Clause 5.5; Clause 5.6	Processor	Supporting	Finalidade, minimização, utilização, retenção e limitação da divulgação
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Processor	Supporting	Responsabilização, segurança da informação e conformidade
ISO/IEC 29151:2022	Clause 15.1.2; Clause 15.2.2; Clause 15.2.3; Annex A.7; Annex A.7.2	Processor	Supporting	Avaliação, monitorização, alteração e controlos de retenção do subcontratante
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 5.19; 5.20; 5.21; 5.22; 5.23	Processor	Supporting	Aplicabilidade dos controlos, controlo operacional e controlos de fornecedores/nuvem
ISO/IEC 27002:2022	Control 5.19; Control 5.20; Control 5.21; Control 5.22; Control 5.23; Control 8.10; Control 8.15; Control 8.16	Processor	Supporting	Controlos de fornecedores, nuvem, eliminação, logging e monitorização

ISO/IEC 27018:2020	Annex A.2.1; Annex A.3.1	Processor	Primary	Assistência ao cliente por subcontratante na nuvem e limitação da finalidade
ISO/IEC 27018:2020	Annex A.6.1; Annex A.6.2; Annex A.8.1	Processor	Primary	Notificação de divulgação na nuvem, registos de divulgação e transparência sobre subcontratantes subsequentes
ISO/IEC 27018:2020	Annex A.10.1; Annex A.10.3; Annex A.11.11; Annex A.11.12; Annex A.12.1	Processor	Primary	Interface de violação na nuvem, saída, medidas contratuais, subcontratos e registos de localização
ISO/IEC 27036-2:2022	Clause 6.1.1; Clause 6.1.2	Processor	Supporting	Estratégia e governação da relação de fornecimento
ISO/IEC 27036-2:2022	Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5	Processor	Supporting	Planeamento, acordo, gestão, monitorização e cessação da relação com fornecedores
ISO/IEC 27555:2025	Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8	Processor	Supporting	Quadro de eliminação e documentação
ISO/IEC 27555:2025	Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7	Processor	Supporting	Implementação da eliminação e exceções

1. Âmbito

1.1 Esta política define requisitos obrigatórios de privacidade para serviços na nuvem em que a organização atua como subcontratante ou subcontratante subsequente de PII, incluindo serviços SaaS, PaaS, IaaS, aplicações alojadas, nuvem gerida, suporte na nuvem, armazenamento na nuvem, análise de dados na nuvem e serviços de infraestrutura na nuvem que tratam PII em nome de clientes.

1.2 Esta política aplica-se ao tratamento na nuvem realizado ao abrigo de acordos com clientes, instruções documentadas de clientes, instruções de subcontratantes a montante, acordos com subcontratantes subsequentes, configuração de regiões cloud, acesso para suporte na nuvem, administração de serviços, cópias de segurança, replicação, logging, monitorização, eliminação, devolução, apoio em caso de violação, apoio a auditorias e obrigações de assistência ao cliente.

1.3 Esta política abrange:

1.3.1 âmbito do tratamento de PII na nuvem e registos de instruções;

1.3.2 evidência de acordos com clientes e de responsabilidade partilhada;

1.3.3 evidência de isolamento entre tenants, acesso à nuvem, acesso administrativo e logging;

1.3.4 governação de subcontratantes subsequentes e da cadeia de fornecimento na nuvem;

1.3.5 localização, acesso remoto e encaminhamento de transferências internacionais;

1.3.6 evidência de devolução, transferência, eliminação, descarte e saída;

1.3.7 assistência ao cliente para direitos dos titulares dos dados, DPIA, auditorias e resposta a violações;

1.3.8 evidência de monitorização, exceções, aplicação e melhoria.

1.4 Esta política não cria um registo separado de contratos com clientes, registo de serviços na nuvem, registo de isolamento entre tenants, registo de acessos, registo de logs, registo de eliminação, registo de pedidos de suporte, registo de evidência de auditoria, registo de violações, registo de subcontratantes subsequentes ou comité de governação da nuvem.

1.5 Esta política não substitui:

1.5.1 PII03 para inventário de tratamento e titularidade do fundamento de licitude;

1.5.2 PII06 para o fluxo completo de direitos dos titulares dos dados;

1.5.3 PII07 para a metodologia de avaliação de riscos de privacidade e DPIA;

1.5.4 PII08 para gates de privacidade desde a conceção e por defeito;

1.5.5 PII09 para controlos gerais de recolha, utilização, divulgação e partilha;

1.5.6 PII10 para a metodologia de retenção, eliminação e descarte;

1.5.7 PII12 para a governação geral do ciclo de vida de subcontratantes, subcontratantes subsequentes e terceiros;

1.5.8 PII13 para a avaliação de mecanismos de transferência internacional;

1.5.9 PII14 para a arquitetura completa de segurança de PII e controlo de acesso;

1.5.10 PII15 para o fluxo de gestão de incidentes e violações;

1.5.11 PII17 para o controlo de informação documentada;

1.5.12 PII18 para a governação da monitorização, auditoria e melhoria do PIMS.

2. Finalidade

2.1 A finalidade desta política é assegurar que os serviços de subcontratante e subcontratante subsequente de PII na nuvem são operados com base em instruções documentadas do cliente, âmbito de tratamento claro, acordos controlados com subcontratantes subsequentes, responsabilidades adequadas de segurança na nuvem, localização e encaminhamento de

transferências documentados, obrigações de assistência ao cliente, apoio em caso de violação, capacidade de eliminação/devolução e evidência pronta para auditoria.

2.2 Esta política apoia a preparação para certificação PIMS segundo a ISO/IEC 27701:2025 para subcontratantes na nuvem e subcontratantes subsequentes na nuvem, mantendo a integração com o conjunto existente de políticas PIMS e com os objetos canónicos de evidência.

3. Objetivos

3.1 Os objetivos desta política são:

3.1.1 Definir o âmbito do tratamento de PII na nuvem antes da integração do cliente ou de uma alteração material.

3.1.2 Assegurar que as instruções do cliente são registadas, revistas e seguidas.

3.1.3 Manter evidência de subcontratantes e subcontratantes subsequentes na nuvem nos registos canónicos do PIMS.

3.1.4 Definir evidência de responsabilidade partilhada, isolamento entre tenants, acesso, logging e localização sem duplicar a política de segurança de PII.

3.1.5 Controlar a evidência de integração, alteração, obrigações em cadeia e monitorização de subcontratantes subsequentes.

3.1.6 Apoiar os clientes em direitos dos titulares dos dados, DPIA, pedidos de auditoria e resposta a violações.

3.1.7 Assegurar que a evidência de devolução, eliminação, transferência e descarte é retida na saída.

3.1.8 Monitorizar os controlos de subcontratante na nuvem e promover ações corretivas através de REG12.

4. Declarações da política

4.1 Âmbito do tratamento na nuvem e instruções do cliente

4.1.1 [Processor] Privacy Lead / PIMS Manager DEVE registar cada serviço de tratamento de PII na nuvem, papel de tratamento do cliente, fonte de instruções do cliente, categorias de PII, categorias de titulares dos dados, finalidade do serviço, localização do tratamento, dependência de subcontratante subsequente, dependência de eliminação e indicador de transferência em REG02 e REG08 antes da integração do cliente ou de alteração material do serviço.

4.1.2 [Processor] Process Owner / Business Owner DEVE registar as instruções documentadas do cliente para o tratamento de PII na nuvem em REG08 antes do início do tratamento.

4.1.3 [Subprocessor] Process Owner / Business Owner DEVE registar em REG08 as instruções do subcontratante a montante ou aprovadas pelo cliente antes de tratar PII como subcontratante subsequente na nuvem.

4.1.4 [Processor] Privacy Lead / PIMS Manager DEVE registar a aplicabilidade dos controlos de subcontratante na nuvem em REG03 antes de um novo serviço de tratamento de PII na nuvem ser lançado ou materialmente alterado.

4.1.5 [Processor] Data Protection Officer / Privacy Advisor DEVE rever em REG12 qualquer instrução do cliente que aparente ser inconsistente com obrigações documentadas do cliente, requisitos PIMS ou âmbito de serviço aprovado antes de a organização atuar com base nessa instrução.

4.1.6 [Processor] Process Owner / Business Owner DEVE registar em REG12 qualquer tratamento proposto de PII do cliente fora das instruções documentadas do cliente e obter aprovação de Privacy Lead / PIMS Manager antes de o tratamento ocorrer.

4.2 Configuração da nuvem, isolamento entre tenants, acesso e logging

4.2.1 [Processor] Information Security Lead DEVE registar em REG08 o limite de responsabilidade partilhada na nuvem para acesso a PII, administração, logging, cópias de segurança, cifragem, gestão de vulnerabilidades e eliminação antes da integração do cliente ou de alteração material do serviço.

4.2.2 [Processor] System Owner / Application Owner DEVE validar em REG12 os controlos de isolamento entre tenants ou de segregação de clientes antes da utilização em produção e após alteração material da arquitetura.

4.2.3 [Processor] System Owner / Application Owner DEVE conceder acesso administrativo na nuvem a PII do cliente apenas após a necessidade de negócio aprovada, o âmbito do acesso, a duração do acesso e a frequência de revisão estarem registados em REG12.

4.2.4 [Processor] Information Security Lead DEVE rever o acesso privilegiado na nuvem, o acesso para suporte, o acesso a PII do cliente e a cobertura de logging em REG12 pelo menos trimestralmente.

4.2.5 [Processor] System Owner / Application Owner DEVE validar a separação dos ambientes de produção, staging, teste e suporte para PII do cliente em REG12 antes da entrada em produção e após alteração material do ambiente.

4.2.6 [Processor] System Owner / Application Owner DEVE registar as localizações de cópias de segurança, replicação, armazenamento de logs e acesso para suporte para PII de clientes na nuvem em REG02, REG08 ou REG09 antes de ativar ou alterar essas localizações.

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

9. Exceções

9.1 [Processor] Process Owner / Business Owner DEVE solicitar uma exceção de subcontratante na nuvem em REG12 antes da integração, lançamento, renovação ou continuação da utilização quando a evidência exigida relativa a instruções do cliente, subcontratante subsequente, localização, acesso, logging, eliminação ou interface de incidentes estiver incompleta.

9.2 [Processor] Data Protection Officer / Privacy Advisor DEVE rever em REG12 os pedidos de exceção de subcontratante na nuvem significativos para a privacidade antes da aprovação quando a exceção afetar instruções do cliente, assistência a titulares dos dados, transferências, subcontratantes subsequentes, eliminação, apoio a violações ou PII de alto impacto.

9.3 [Processor] Top Management DEVE aprovar em REG12 exceções de subcontratante na nuvem de alto risco ou materiais antes de a exceção produzir efeitos.

9.4 [Processor] Privacy Lead / PIMS Manager DEVE atribuir em REG12 uma data de expiração, proprietário da remediação, data de revisão e nota de risco residual para cada exceção de subcontratante na nuvem aprovada antes da aprovação.

10. Aplicação

10.1 [Processor] Privacy Lead / PIMS Manager DEVE bloquear a integração de clientes, lançamento de serviços, renovação ou continuação do tratamento quando a evidência exigida em REG02, REG03, REG08, REG09, REG10 ou REG12 estiver em falta antes de o tratamento começar ou continuar.

10.2 [Processor] System Owner / Application Owner DEVE desativar acesso à nuvem não aprovado, utilização de região não aprovada, replicação não aprovada, acesso para suporte não aprovado ou fluxo de dados para subcontratante subsequente não aprovado no prazo de um dia útil após uma decisão de aplicação e registar a conclusão em REG08 ou REG12.

10.3 [Processor] Vendor / Procurement Owner DEVE suspender novo tratamento de PII por subcontratante subsequente na nuvem não aprovado ou não conforme até que a evidência de ação corretiva em REG08 esteja completa.

10.4 [Processor] Incident Response Coordinator DEVE escalar em REG10 e REG12 prazos de notificação de incidentes a clientes não cumpridos no prazo de um dia útil após a identificação.

10.5 [Processor] Internal Audit / Compliance Reviewer DEVE verificar a eficácia das ações corretivas para não conformidades maiores ou repetidas de subcontratante na nuvem em REG12 no prazo de 60 dias após o encerramento da ação corretiva.

11. Revisão e manutenção

11.1 [Processor] Privacy Lead / PIMS Manager DEVE rever esta política em REG12 anualmente e no prazo de 30 dias após uma alteração material às obrigações de subcontratante na nuvem, arquitetura na nuvem, governação de subcontratantes subsequentes, assistência ao cliente, capacidade de eliminação ou requisitos de certificação.

11.2 [Processor] Vendor / Procurement Owner DEVE rever os registos de subcontratantes subsequentes na nuvem e dependências de serviços na nuvem em REG08 pelo menos anualmente e antes da renovação.

11.3 [Processor] System Owner / Application Owner DEVE rever a evidência de isolamento entre tenants, acesso privilegiado, logging, cópias de segurança, replicação e eliminação em REG12 pelo menos anualmente e após alteração material da arquitetura.

11.4 [Processor] Privacy Lead / PIMS Manager DEVE rever os registos de localização na nuvem e encaminhamento de transferências em REG09 pelo menos anualmente e no prazo de 15 dias úteis após alteração material de localização, acesso para suporte, cópias de segurança ou subcontratante subsequente.

11.5 [Processor] Privacy Lead / PIMS Manager DEVE atualizar REG03 no prazo de 15 dias úteis após alterações aprovadas à política que afetem a aplicabilidade dos controlos de subcontratante na nuvem.

11.6 [All] Top Management DEVE aprovar revisões materiais desta política em REG12 antes da publicação.

12. Políticas relacionadas

12.1 Esta política é apoiada pelas seguintes políticas relacionadas:

12.2 PII01 - Política do Sistema de Gestão da Informação 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 PII06 - Política de Gestão de Direitos dos Titulares dos Dados

12.6 PII07 - Política de Avaliação de Riscos de Privacidade e DPIA

12.7 PII08 - Política de Privacidade desde a Conceção e por Defeito

12.8 PII09 - Política de Recolha, Utilização, Divulgação e Partilha de PII

12.9 PII10 - Política de Retenção, Eliminação e Descarte de PII

12.10 PII12 - Política de Gestão de Privacidade de Subcontratantes, Subcontratantes Subsequentes e Terceiros

12.11 PII13 - Política de Transferência Internacional de PII

12.12 PII14 - Política de Segurança de PII e Controlo de Acesso

12.13 PII15 - Política de Gestão de Incidentes e Violações de PII

12.14 PII17 - Política de Gestão de Informação Documentada e Evidência do PIMS

12.15 PII18 - Política de Monitorização, Auditoria e Melhoria do PIMS

12.16 PII20 - Política de Privacidade de Crianças

12.17 PII21 - Política de Privacidade para AI e Decisões Automatizadas

12.18 PII22 - Política de Privacidade de Marketing e Cookies

12.19 PII24 - Política de CCTV e Monitorização Física de Espaços

13. Normas e referenciais de referência

13.1 Esta política está mapeada para as seguintes normas e regulamentos. O mapeamento explica como a política apoia os requisitos citados e identifica as cláusulas internas que os implementam ou suportam.

13.2 ISO/IEC 27701:2025 - Clause 4.1; Clause 6.1.3. Addressed by clauses [4.1.1; 4.1.4; 5.2; 7.1; 11.5].

13.3 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.3.1; 4.4.1; 4.6.1; 4.7.1; 4.8.1; 7.1; 7.2; 7.3].

13.4 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.3.5; 4.6.6; 4.8.1; 4.8.2; 4.8.4; 6.1; 6.2; 8.1; 8.2; 8.3; 8.4; 8.5; 10.5; 11.1].

13.5 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.5; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.2; 4.1.3; 4.1.5; 4.1.6; 4.3.1; 4.7.5; 7.2].

13.6 ISO/IEC 27701:2025 - Annex A.2.3.2. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5].

13.7 ISO/IEC 27701:2025 - Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.8 ISO/IEC 27701:2025 - Annex A.2.5.2; Annex A.2.5.3. Addressed by clauses [4.2.6; 4.4.4; 4.5.1; 4.5.2; 7.5; 11.4].

13.9 ISO/IEC 27701:2025 - Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.5.3; 4.5.4; 4.7.2; 4.7.5].

13.10 ISO/IEC 27701:2025 - Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6].

13.11 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9; Annex A.3.14; Annex A.3.24; Annex A.3.25. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.7.3; 5.4; 5.6; 11.3].

13.12 GDPR - Article 28. Addressed by clauses [4.1.2; 4.1.3; 4.3.1; 4.3.2; 4.3.4; 4.4.2; 4.4.3; 4.4.5; 4.6.1; 4.6.3; 4.6.5; 4.7.2].

13.13 GDPR - Article 30. Addressed by clauses [4.1.1; 4.1.3; 4.4.1; 4.8.1; 7.1].

13.14 GDPR - Article 32; Article 33. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 7.6].

13.15 GDPR - Article 44. Addressed by clauses [4.2.6; 4.4.4; 4.5.1; 4.5.2; 7.5; 11.4].

13.16 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.1.6; 4.2.6; 4.5.1; 4.6.1; 4.6.3].

13.17 ISO/IEC 29100:2020 - Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.4; 4.3.5; 4.8.1; 4.8.4; 6.1; 8.5; 10.5].

13.18 ISO/IEC 29151:2022 - Clause 15.1.2; Clause 15.2.2; Clause 15.2.3; Annex A.7; Annex A.7.2. Addressed by clauses [4.4.1; 4.4.6; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.8.3].

13.19 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 5.19; 5.20; 5.21; 5.22; 5.23. Addressed by clauses [4.1.4; 4.2.1; 4.4.1; 4.4.3; 4.4.6; 4.8.1; 4.8.3; 6.1; 7.1; 11.5].

13.20 ISO/IEC 27002:2022 - Control 5.19; Control 5.20; Control 5.21; Control 5.22; Control 5.23; Control 8.10; Control 8.15; Control 8.16. Addressed by clauses [4.2.1; 4.2.4; 4.4.1; 4.4.3; 4.4.6; 4.6.1; 4.6.3; 4.7.3; 4.8.3; 11.3].

13.21 ISO/IEC 27018:2020 - Annex A.2.1; Annex A.3.1. Addressed by clauses [4.1.2; 4.1.6; 4.3.1; 4.3.2; 4.3.3; 4.3.5].

13.22 ISO/IEC 27018:2020 - Annex A.6.1; Annex A.6.2; Annex A.8.1. Addressed by clauses [4.4.1; 4.4.2; 4.4.5; 4.5.3; 4.5.4].

13.23 ISO/IEC 27018:2020 - Annex A.10.1; Annex A.10.3; Annex A.11.11; Annex A.11.12; Annex A.12.1. Addressed by clauses [4.2.6; 4.4.3; 4.4.4; 4.6.1; 4.6.3; 4.6.5; 4.7.1; 4.7.2; 4.7.5].

13.24 ISO/IEC 27036-2:2022 - Clause 6.1.1; Clause 6.1.2. Addressed by clauses [4.1.1; 4.2.1; 4.4.1; 4.4.6; 6.1; 7.2].

13.25 ISO/IEC 27036-2:2022 - Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.4.6; 4.8.2; 4.8.3; 10.3; 11.2].

13.26 ISO/IEC 27555:2025 - Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.27 ISO/IEC 27555:2025 - Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7. Addressed by clauses [4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6; 9.1; 9.4].