					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: PII15-FS					Dokumenttitel: **Policy för hantering av PII-incidenter och personuppgiftsincidenter i finanssektorn**							
Version: 1.0		Ikraftträdandedatum: 01.01.2025			Dokumentägare:							
X	Policy		Standard		Rutin		Formulär		Register		Övrigt	

Revisionshistorik				
Revisionsnummer	**Revisionsdatum**	**Ändringar**	**Granskad av**	**Processägare**

Godkännanden			
Namn	**Titel**	**Datum**	**Underskrift**

Ansluten till standarder och regelverk

Standard / regelverk	Klausul / kontroll / artikel	Tillämplighet	Täckningstyp	Kommentar
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	PIMS-kommunikation och dokumenterat incidentunderlag
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Operativ styrning samt koppling till bedömning och behandling av integritetsrisker
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Övervakning, utvärdering, avvikelse, korrigerande åtgärd och förbättring
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Planering och förberedelse för incidenthantering vid behandling av PII
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Hantering av informationssäkerhetsincidenter som involverar PII
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Rättsliga, lagstadgade, regulatoriska och avtalsmässiga krav samt skydd av register
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Stöd för personuppgiftsbiträdets kundavtal och kundförpliktelser
GDPR	Article 5(2); Article 24	Controller	Supporting	Ansvarsskyldighet och den personuppgiftsansvariges ansvar
GDPR	Article 26	Joint Controller	Supporting	Samordning av incidentansvar mellan gemensamt personuppgiftsansvariga
GDPR	Article 28	Both	Supporting	Personuppgiftsbiträdets stöd och avtalsförpliktelser
GDPR	Article 32	Both	Supporting	Säkerhet i behandlingen och förmåga att upptäcka personuppgiftsincidenter
GDPR	Article 33	Both	Primary	Anmälan av personuppgiftsincidenter och dokumentation av personuppgiftsincidenter
GDPR	Article 34	Controller	Primary	Kommunikation av personuppgiftsincidenter till berörda registrerade

GDPR	Article 39	Conditional	Supporting	DPO-rådgivning, övervakning, samarbete och stöd som kontaktpunkt
DORA Regulation (EU) 2022/2554	Article 17	Conditional	Primary	Process för hantering av IKT-relaterade incidenter för finansiella entiteter som omfattas
DORA Regulation (EU) 2022/2554	Article 18	Conditional	Primary	Klassificeringskriterier för IKT-relaterade incidenter och betydande cyberhot
DORA Regulation (EU) 2022/2554	Article 19	Conditional	Primary	Rapportering av större IKT-relaterade incidenter och anmälan av betydande cyberhot
DORA Regulation (EU) 2022/2554	Article 20	Conditional	Supporting	Rapportinnehåll, tidsfrister, mallar och förfaranden
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Rapportering av betydande incidenter där det är tillämpligt
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Principer för informationssäkerhet och dataskyddsefterlevnad
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Ansvar för hantering av PII-incidenter och rapportering av händelser
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Incidentplanering, bedömning, åtgärder, erfarenhetsåterföring och insamling av underlag
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Livscykel för incidenthanteringsprocessen
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Incidentpolicy, plan, medvetenhet, testning och erfarenhetsåterföring
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Detektering, notifiering, triagering, analys, respons och rapportering i drift

ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Förväntningar på notifiering och register över personuppgiftsincidenter för publikt molnbaserat personuppgiftsbiträde

1. Omfattning

1.1 Denna policy anger krav för att identifiera, rapportera, triagera, klassificera, bedöma, begränsa, notifiera, dokumentera, stänga och förbättra arbetet utifrån PII-incidenter och personuppgiftsincidenter inom PIMS-omfattningar i finanssektorn.

1.2 **Information om införande:** Denna policy är en ersättande variant för finanssektorn av PII15. Den får inte tillämpas samtidigt med PII15 för samma PIMS-omfattning, verksamhetsenhet, produkt, kundmiljö, reglerade tjänst eller bevisgräns. Organisationer ska välja antingen PII15 eller PII15-FS för samma omfattning för att undvika dubbla incidenthanteringsskyldigheter, dubbla register och dubbelt arbete med revisionsunderlag.

1.3 Denna policy gäller för:

1.3.1 organisationen när den agerar som personuppgiftsansvarig i en finanssektorkontext;

1.3.2 organisationen när den agerar som gemensamt personuppgiftsansvarig där samordning av ansvar för incidenter eller personuppgiftsincidenter krävs;

1.3.3 organisationen när den agerar som personuppgiftsbiträde för kunder i finanssektorn;

1.3.4 organisationen när den agerar som underbiträde för kunder i finanssektorn eller överordnade personuppgiftsbiträden;

1.3.5 system, applikationer, tjänster, processer, leverantörer, personuppgiftsbiträden, underbiträden och tredje parter som behandlar, lagrar, överför, stödjer, har åtkomst till eller på annat sätt påverkar PII inom PIMS-omfattningen för finanssektorn.

1.4 Denna policy använder REG10 - PII Incident and Breach Register som primärt bevisobjekt för hantering av PII-incidenter och personuppgiftsincidenter i finanssektorn.

1.5 Denna policy använder stödjande bevisobjekt enligt följande:

1.5.1 REG01 för PIMS-omfattning och tillämplig kontext avseende intressenter, sektor, kunder, avtal och rapportering.

1.5.2 REG02 för berörda behandlingsaktiviteter, PII-kategorier, kategorier av registrerade, ändamål, system och tjänster.

1.5.3 REG03 för tillämpbarhetsförklaring och uppdateringar av kontrollernas tillämplighet, inklusive ersättning av PII15 med PII15-FS för samma omfattning.

1.5.4 REG04 för koppling till integritetsrisk, DPIA, kvarstående risk och riskbehandling.

1.5.5 REG08 för underlag om incidentgränssnitt mot personuppgiftsbiträden, underbiträden, kunder, leverantörer och tredje parter.

1.5.6 REG09 för koppling till internationella överföringar när en incident påverkar gränsöverskridande behandling.

1.5.7 REG11 för underlag om utbildning, medvetenhet och kompetens för incidenthantering.

1.5.8 REG12 för underlag om revision, avvikelse, korrigerande åtgärd, ledningens genomgång och förbättring.

1.6 Denna policy förlitar sig på relaterade PIMS-policyer för specialistkontroller:

1.6.1 PII03 styr behandlingsförteckning och register över rättslig grund.

1.6.2 PII04 styr integritetsmeddelanden och transparenskontroller utanför kommunikation som är specifik för personuppgiftsincidenter.

1.6.3 PII06 styr rättighetsbegäranden från registrerade som uppstår före, under eller efter en incident.

1.6.4 PII07 styr metodik för bedömning av integritetsrisker och DPIA.

1.6.5 PII08 styr integritetsskydd genom design och dataskydd som standard.

1.6.6 PII10 styr kontroller för bevarande, radering och bortskaffning.

1.6.7 PII12 styr integritetsrelaterade relationskontroller för personuppgiftsbiträden, underbiträden, leverantörer och tredje parter.

1.6.8 PII13 styr mekanismer för internationell överföring av PII och register över överföringsrisker.

1.6.9 PII14 styr förebyggande och upptäckande säkerhets- och åtkomstkontroller för PII.

1.6.10 PII16 styr integritetsutbildning, medvetenhet och kompetens.

1.6.11 PII17 styr dokumenterad information och hantering av underlag.

1.6.12 PII18 styr övervakning, internrevision, ledningens genomgång, avvikelse, korrigerande åtgärd och ständig förbättring.

1.6.13 PII23 styr kontroller för personuppgiftsbiträden i molnmiljö där skyldigheter för personuppgiftsbiträden i molnmiljö omfattas.

1.7 I denna policy gäller följande:

1.7.1 "PII-incident" avser en misstänkt eller bekräftad händelse som har påverkat, kan ha påverkat eller rimligen skulle kunna påverka konfidentialitet, riktighet, tillgänglighet, behandling med rättslig grund eller behörig hantering av PII.

1.7.2 "Personuppgiftsincident" avser en bekräftad PII-incident som innebär obehörig, olaglig, oavsiktlig eller oavsedd förstöring, förlust, ändring, röjande av, åtkomst till, otillgänglighet av eller kompromettering av PII.

1.7.3 "PII-incident i finanssektorn" avser en PII-incident som påverkar, kan påverka eller har rimlig koppling till reglerade finansiella tjänster, kunder i finanssektorn, finansiella motparter, finansiella transaktioner, finansiell verksamhet eller behandling av PII i finanssektorn.

1.7.4 "Större incident i finanssektorn" avser en PII-incident i finanssektorn eller relaterad IKT-incident som uppfyller dokumenterade väsentlighets- eller rapporteringskriterier i REG10.

1.7.5 "Betydande cyberhot" avser ett cyberhot som registreras i REG10 och som väsentligt skulle kunna påverka finansiella tjänster, PII-behandling, kunder, motparter eller verksamhet som omfattas.

1.7.6 "Bedömning av personuppgiftsincident" avser den dokumenterade utvärderingen av om en PII-incident är en personuppgiftsincident, vilka PII och registrerade som berörs, vilka risker som kan uppstå, vilka notifieringar eller kommunikationer som krävs och vilka avhjälpande åtgärder som behövs.

1.7.7 "Kännedom" avser den tidpunkt då organisationen har en rimlig grad av säkerhet om att en säkerhets- eller integritetsincident har inträffat och att PII har kompromitterats eller kan ha kompromitterats.

1.7.8 "PII-incident med hög påverkan i finanssektorn" avser en PII-incident som involverar högriskbehandling, särskilda kategorier av PII eller mycket känslig PII, storskalig PII, sårbara personer, reglerade kunder, väsentlig tjänstestörning, finansiella motparter, finansiella transaktioner, påverkan i flera jurisdiktioner, kompromettering av privilegierad åtkomst, offentlig exponering, ransomware, otillgänglighet för tjänst eller betydande operativ, kundrelaterad, finansiell eller anseenderelaterad påverkan.

1.7.9 "Väsentlig incidentförändring" avser ny eller ändrad information som påverkar incidentens omfattning, allvarlighetsgrad, PII-kategorier, påverkan på registrerade, tjänstepåverkan, klassificering i finanssektorn, notifieringsbeslut, kundpåverkan, rotorsak, begränsning, återhämtning, korrigerande åtgärd eller externa rapporteringsskyldigheter.

2. Syfte

2.1 Syftet med denna policy är att säkerställa att PII-incidenter och personuppgiftsincidenter i finanssektorkontexter hanteras konsekvent, skyndsamt, lagenligt, säkert och med underlag som är redo för revision.

2.2 Denna policy stödjer ansvarsskyldighet genom att kräva att PII-incidenter och personuppgiftsincidenter i finanssektorn registreras i REG10 och kopplas till berörda behandlingsregister, integritetsrisker, relationer med personuppgiftsbiträden och underbiträden, överföringsregister, korrigerande åtgärder, utbildningsregister, rapporteringsbeslut för finanssektorn och underlag för ledningens genomgång när detta utlöses.

2.3 Denna policy säkerställer att skyldigheter för personuppgiftsansvarig, gemensamt personuppgiftsansvarig, personuppgiftsbiträde och underbiträde hanteras genom separata tillämplighetsregler, samtidigt som en integrerad modell för underlag om incidenter och personuppgiftsincidenter i finanssektorn upprätthålls.

3. Mål

3.1 Målen med denna policy är att:

3.1.1 säkerställa att misstänkta PII-incidenter i finanssektorn rapporteras och registreras skyndsamt;

3.1.2 säkerställa att PII-incidenter i finanssektorn triageras och klassificeras med enhetliga integritets-, säkerhets-, operativa och sektoriella kriterier;

3.1.3 säkerställa att bedömningar av personuppgiftsincidenter beaktar berörda PII, registrerade, system, tjänster, behandlingsaktiviteter, personuppgiftsbiträden, underbiträden, överföringar, risker, kunder, motparter och avhjälpande åtgärder;

3.1.4 säkerställa att beslut om notifiering från personuppgiftsansvarig och kommunikation till registrerade dokumenteras;

3.1.5 säkerställa att personuppgiftsbiträdens och underbiträdens notifieringar om personuppgiftsincidenter till kunder eller överordnade parter görs utan onödigt dröjsmål och i enlighet med tillämpliga avtal;

3.1.6 säkerställa att rapporteringsutlösare för finanssektorn utvärderas, dokumenteras och följs upp där det är tillämpligt;

3.1.7 säkerställa att underlag bevaras och skyddas under incidenthantering;

3.1.8 säkerställa att begränsning, eliminering, återhämtning och validering följs upp genom REG10;

3.1.9 säkerställa att betydande cyberhot och större incidenter i finanssektorn dirigeras till lämpliga besluts- och rapporteringsarbetsflöden;

3.1.10 säkerställa att erfarenhetsåterföring från incidenter leder till korrigerande åtgärder, utbildning, kontrollförbättring och ledningens genomgång;

3.1.11 säkerställa att incident- och personuppgiftsincidentregister finns tillgängliga för revision, ledningens genomgång, kundförsäkran och regulatorisk översyn där det är tillämpligt;

3.1.12 säkerställa att PII15-FS ersätter PII15 för samma finanssektoromfattning och inte dubblerar underlagsarbetet för PII15.

4. Policyuttalanden

4.1 Aktivering av variant, beredskap och mottagning

4.1.1 [Conditional] Privacy Lead / PIMS Manager MUST dokumentera aktivering av PII15-FS i REG01 och REG03 innan denna policy används för en PIMS-omfattning i finanssektorn.

4.1.2 [Conditional] Privacy Lead / PIMS Manager MUST dokumentera i REG03 och REG12 att PII15 inte tillämpas samtidigt för samma PIMS-omfattning i finanssektorn innan PII15-FS godkänns.

4.1.3 [All] Incident Response Coordinator MUST registrera varje rapporterad eller upptäckt misstänkt PII-incident i finanssektorn i REG10 inom en arbetsdag från mottagande, eller tidigare om en tillämplig notifierings-, kund- eller rapporteringstidslinje kan utlösas.

4.1.4 [Conditional] Privacy Lead / PIMS Manager MUST upprätthålla kriterier för hantering av PII-incidenter och personuppgiftsincidenter i finanssektorn i REG10 minst årligen och efter varje väsentlig ändring av PIMS-omfattning, rättslig kontext, kundförpliktelser, avtalsförpliktelser, sektoriell rapporteringskontext eller högriskbehandling.

4.1.5 [Both] Information Security Lead MUST bekräfta krav på bevarande av incidentunderlag i REG10 inom 24 timmar efter att en misstänkt incident påverkar ett system, en tjänst eller en applikation som behandlar PII.

4.1.6 [Conditional] Vendor / Procurement Owner MUST upprätthålla krav på incidentkontakter och underlagsdirigering för tredje parter i finanssektorn i REG08 före onboarding och minst årligen för personuppgiftsbiträden, underbiträden, leverantörer och outsourcade rapporteringsleverantörer som omfattas.

4.2 Klassificering och bedömning av personuppgiftsincident

4.2.1 [All] Incident Response Coordinator MUST klassificera varje REG10-post inom 24 timmar från mottagning som händelse utan PII, misstänkt PII-incident, bekräftad PII-incident, bekräftad personuppgiftsincident, PII-incident i finanssektorn, större incident i finanssektorn, betydande cyberhot eller post som inväntar klassificering.

4.2.2 [Conditional] Information Security Lead MUST bedöma berörda tjänster, klienter, motparter, transaktioner, tjänsteavbrott, geografisk spridning, dataförlust, tjänstekritikalitet och ekonomisk påverkan i REG10 när en PII-incident kan påverka finansiella tjänster eller finansiell verksamhet.

4.2.3 [Both] Privacy Lead / PIMS Manager MUST identifiera berörd behandlingsaktivitet, PII-kategorier, kategorier av registrerade, system, personuppgiftsbiträden, underbiträden, överföringsplatser och integritetsrisker i REG02, REG04, REG08, REG09 och REG10 innan beslutet om anmälan av personuppgiftsincident färdigställs.

4.2.4 [Controller] Data Protection Officer / Privacy Advisor MUST bedöma risken för berörda registrerade för varje bekräftad eller rimligen misstänkt personuppgiftsincident och registrera notifieringsrekommendation, riskmotivering och rådgivning i REG10 innan beslut om extern notifiering fattas.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager MUST registrera ansvarsfördelning för incidenter mellan gemensamt personuppgiftsansvariga i REG08 och REG10 inom 24 timmar efter att delat ansvar för en misstänkt eller bekräftad personuppgiftsincident har identifierats.

4.2.6 [Processor] Privacy Lead / PIMS Manager MUST bedöma kundinstruktioner, avtalsmässiga notifieringsskyldigheter och samarbetsskyldigheter i REG08 och REG10 inom 24 timmar efter att en misstänkt eller bekräftad personuppgiftsincident påverkar behandling som utförs som personuppgiftsbiträde.

4.2.7 [Subprocessor] Vendor / Procurement Owner MUST identifiera den överordnade notifieringskedjan och erforderlig underlagsdirigering i REG08 och REG10 inom 24 timmar efter att en misstänkt eller bekräftad PII-incident påverkar behandling som utförs som underbiträde.

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Undantag

9.1.1 [All] Privacy Lead / PIMS Manager MUST registrera varje undantag från denna policy i REG12 före genomförande, eller inom 24 timmar efter akut åtgärd där förhandsgodkännande inte var möjligt.

9.1.2 [Conditional] Top Management MUST godkänna varje undantag som väsentligt påverkar tidpunkt för anmälan av personuppgiftsincident, tidpunkt för rapportering i finanssektorn, offentlig kommunikation, kundåtagande, bevarande av underlag eller risk för registrerade innan incidenten stängs, med godkännandeunderlag bevarat i REG10 och REG12.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor MUST dokumentera rådgivning för varje försenad notifiering, beslut om utebliven notifiering, rapporteringsundantag eller avvikande kommunikationsansats före incidentstängning, med rådgivningen bevarad i REG10.

9.1.4 [Both] Vendor / Procurement Owner MUST registrera undantag hos leverantörer, personuppgiftsbiträden, underbiträden, kunder eller outsourcade leverantörer som påverkar incidenthantering i finanssektorn i REG08 och REG12 inom fem arbetsdagar efter att undantaget identifierats.

9.1.5 [All] Privacy Lead / PIMS Manager MUST granska öppna undantag från denna policy minst månadsvis fram till stängning, med granskningsstatus bevarad i REG12.

10. Efterlevnad och tillämpning

10.1.1 [All] Process Owner / Business Owner MUST eskalera underlåtenhet att rapportera en misstänkt PII-incident i finanssektorn, bevara underlag, följa tilldelade åtgärder eller samarbeta vid bedömning av personuppgiftsincident till Privacy Lead / PIMS Manager inom två arbetsdagar efter upptäckt, med underlag bevarat i REG12.

10.1.2 [Both] Incident Response Coordinator MUST eskalera sen rapportering, missad klassificering, saknat underlag, missad eskalering eller försenad begränsningsåtgärd till Privacy Lead / PIMS Manager inom en arbetsdag efter att problemet identifierats, med underlag bevarat i REG10 och REG12.

10.1.3 [Both] Privacy Lead / PIMS Manager MUST registrera en REG12-avvikelse när ett brott mot denna policy påverkar incidentmottagning, triage, begränsning, notifiering, rapportering, underlagsintegritet, kommunikation eller korrigerande åtgärd.

10.1.4 [Both] Vendor / Procurement Owner MUST initiera åtgärdande hos leverantör, personuppgiftsbiträde, underbiträde eller outsourcad leverantör genom REG08 och REG12 inom fem arbetsdagar när en tredje part inte uppfyller överenskomna incident-, personuppgiftsincident-, underlags- eller rapporteringsskyldigheter.

10.1.5 [Conditional] Top Management MUST granska väsentliga eller återkommande PII15-FS-avvikelser vid nästa planerade ledningsgenomgång, med beslut och erforderliga åtgärder bevarade i REG12.

10.1.6 [All] Privacy Lead / PIMS Manager MUST utlösa avhjälpande utbildning i REG11 inom 30 kalenderdagar när en policyavvikelse avser rollmedvetenhet, sen rapportering, eskaleringsfel, fel i hantering av underlag eller kommunikationsfel.

11. Granskning och underhåll

11.1.1 [Conditional] Privacy Lead / PIMS Manager MUST granska denna policy minst årligen och registrera granskningsresultat, erforderliga ändringar och godkännandestatus i REG12.

11.1.2 [Conditional] Incident Response Coordinator MUST utlösa en efterincidentgranskning av denna policy inom 30 kalenderdagar efter stängning av varje PII-incident med hög påverkan i finanssektorn, bekräftad personuppgiftsincident, större incident i finanssektorn eller betydande cyberhot, med granskningsunderlag bevarat i REG10 och REG12.

11.1.3 [Conditional] Privacy Lead / PIMS Manager MUST granska denna policy inom 30 kalenderdagar efter att ha fått kännedom om en väsentlig ändring av rättsliga, sektoriella, kundrelaterade, avtalsmässiga, personuppgiftsbiträdesrelaterade, underbiträdesrelaterade, rapporteringsmallsrelaterade, rapporteringstidslinjerelaterade eller överföringsrelaterade krav på incidentrapportering, med granskningsunderlag bevarat i REG01, REG08, REG09 och REG12.

11.1.4 [Both] Internal Audit / Compliance Reviewer MUST granska genomförandet av denna policy minst årligen genom det interna PIMS-revisionsprogrammet, med revisionsiakttagelser och korrigerande åtgärder bevarade i REG12.

11.1.5 [Conditional] Top Management MUST granska incidenttrender, betydande personuppgiftsincidenter, rapporteringsprestanda, försenade korrigerande åtgärder och policyns effektivitet under planerad ledningsgenomgång, med resultat bevarade i REG12.

11.1.6 [Conditional] Privacy Lead / PIMS Manager MUST granska ersättningsrelationen mellan PII15-FS och PII15 minst årligen och efter varje ändring av PIMS-omfattning för att verifiera att båda policyerna inte tillämpas för samma finanssektoromfattning, med granskningsunderlag bevarat i REG03 och REG12.

12. Relaterade policyer

12.1 Denna policy bör läsas tillsammans med:

12.2 PII01 - Policy för ledningssystem för hantering av integritetsinformation

12.3 PII02 - Policy för integritetsroller, ansvar och ansvarsskyldighet

12.4 PII03 - Policy för behandlingsförteckning och rättslig grund för PII

12.5 PII04 - Policy för integritetsmeddelande och transparens

12.6 PII06 - Policy för hantering av rättigheter för registrerade

12.7 PII07 - Policy för bedömning av integritetsrisker och DPIA

12.8 PII08 - Policy för integritetsskydd genom design och dataskydd som standard

12.9 PII10 - Policy för bevarande, radering och bortskaffning av PII

12.10 PII12 - Policy för integritetshantering av personuppgiftsbiträden, underbiträden och tredje parter

12.11 PII13 - Policy för internationell överföring av PII

12.12 PII14 - Policy för PII-säkerhet och åtkomstkontroll

12.13 PII16 - Policy för integritetsutbildning, medvetenhet och kompetens

12.14 PII17 - Policy för dokumenterad PIMS-information och hantering av underlag

12.15 PII18 - Policy för PIMS-övervakning, revision och förbättring

12.16 PII23 - Policy för personuppgiftsbiträde i molnmiljö, där skyldigheter för personuppgiftsbiträden i molnmiljö i finanssektorn omfattas

12.17 PII15 - Policy för hantering av PII-incidenter och personuppgiftsincidenter är den grundläggande policyn för incidenter och personuppgiftsincidenter. PII15-FS är en ersättande variant för finanssektorn av PII15. PII15 och PII15-FS får inte tillämpas samtidigt för samma PIMS-omfattning, verksamhetsenhet, produkt, kundmiljö, reglerade tjänst eller bevisgräns.

13. Referensstandarder och ramverk

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.8; 4.5.1; 4.5.4; 4.5.5; 5.2.2; 7.1.1; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.1.3; 4.2.3; 4.3.1; 4.3.4; 4.3.5; 4.7.3; 6.1.4; 7.1.4].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.7.1; 4.7.2; 4.7.6; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 9.1.1; 10.1.1; 11.1.4; 11.1.5].

13.4 ISO/IEC 27701:2025 - Annex A.3.11. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 5.1.1; 6.1.1; 7.1.2; 7.1.6; 7.1.7].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.6.1; 4.6.2].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 4.5.7; 9.1.2; 11.1.3].

13.7 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.6. Addressed by clauses [4.2.6; 4.2.7; 4.3.6; 4.4.4; 4.4.5; 4.4.10; 4.5.6; 5.7.1; 7.1.3; 8.1.5; 10.1.4].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.5.1; 4.7.2; 5.2.1; 6.1.1; 8.1.2; 11.1.6].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.6; 4.5.1].

13.10 GDPR - Article 28. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3; 10.1.4].

13.11 GDPR - Article 32. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.2; 4.7.3; 7.1.4].

13.12 GDPR - Article 33. Addressed by clauses [4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.5.4; 8.1.2].

13.13 GDPR - Article 34. Addressed by clauses [4.4.3; 4.5.4].

13.14 GDPR - Article 39. Addressed by clauses [4.2.4; 4.4.3; 5.3.1; 6.1.4; 9.1.3].

13.15 DORA Regulation (EU) 2022/2554 - Article 17. Addressed by clauses [4.1.3; 4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.3; 4.3.4; 4.3.6; 4.4.7; 4.5.1; 4.7.1; 5.4.1; 6.1.2; 7.1.7].

13.16 DORA Regulation (EU) 2022/2554 - Article 18. Addressed by clauses [4.2.1; 4.2.2; 4.6.1; 4.6.2; 4.6.3; 8.1.3].

13.17 DORA Regulation (EU) 2022/2554 - Article 19. Addressed by clauses [4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.5; 8.1.3].

13.18 DORA Regulation (EU) 2022/2554 - Article 20. Addressed by clauses [4.4.8; 4.5.5; 6.1.4; 7.1.2; 8.1.3; 11.1.3].

13.19 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.4.7; 4.4.8; 4.5.5; 6.1.4; 8.1.3; 11.1.3].

13.20 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.4.3; 4.5.1; 4.5.3; 4.7.2; 5.2.1; 8.1.2].

13.21 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.7.1].

13.22 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.4; 4.3.6; 4.5.2; 4.7.1; 4.7.2; 7.1.7; 10.1.2].

13.23 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.4; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1.7].

13.24 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.4; 4.1.6; 4.7.1; 4.7.5; 7.1.6; 7.1.7; 10.1.6].

13.25 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.1; 4.7.1].

13.26 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3].