Namn	Version	Ersätter	Org. plats	Sida # (av #)
Policy för information och data	1.4	1.3	N/A	1(4)

Ägare	Ändrad av	Senast ändrad	Dokumenttyp
CFO	Tova Boustedt	2025-04-22	Policy

Fastställd av	Fastställd datum	Status	Ersatt av
Styrelsen	2025-05-06	Fastställd	N/A

Policy för information och data

Bakgrund

Vad omfattar denna policy?

Denna policy beskriver Hemnet Group AB (publ) och dess dotterbolags ("Bolaget", "Koncernen") tillvägagångssätt för att hantera och skydda dess informations- och datatillgångar. Policyn säkerställer att Hemnet upprätthåller integritet, konfidentialitet och tillgänglighet för sina informationstillgångar samtidigt som den följer lagkrav och bästa praxis. Policyn hanterar också de risker som är förknippade med informationssäkerhet och dataintegritet, och fastställer tydliga riktlinjer för ansvarsfull datahantering, åtkomstkontroll och incidenthantering.

Vem berörs av denna policy?

Denna policy gäller för samtliga medarbetare anställda på Bolaget som på något sätt har anförtrotts och fått tillgång till Hemnets data- och informationstillgångar.

Varför har vi skapat denna policy?

De centrala målen med denna policy är att säkerställa att data samlas in, hanteras och skyddas i enlighet med tillämpliga dataskyddslagar samtidigt som Hemnet skyddar integriteten, sekretessen och tillgängligheten för dess informationstillgångar. Den syftar till att skydda Hemnets verksamhet, rykte och individens rätt till personlig integritet genom att implementera riskbaserade säkerhetsåtgärder. Policyn säkerställer även efterlevnad av GDPR, ansvarsfull datahantering samt tydliga rutiner för åtkomstkontroll och incidenthantering.

Information

Hemnets övergripande mål för information och data

Data är en viktig tillgång i Bolagets verksamhet. Användandet av Hemnets data ska ligga till grund för att utveckla Bolagets affär och verksamhet. Användningen ska alltid följa gällande lagar och regler och ska ske med hänsyn till berörda individers intresse av personlig integritet.

Hemnet ska med tillämpning av ett riskbaserat angreppssätt använda relevanta säkerhetsåtgärder för att skydda verksamheten från alla former av hot mot informationssystem eller data som kan störa eller få negativ påverkan på Bolagets verksamhet, renommé eller för individers rätt till personlig integritet. Detta innefattar risker som kan påverka Bolagets informationssystem och dess datas integritet, konfidentialitet och tillgänglighet.

Fokus

- Hemnet ska använda alla rimliga åtgärder för att skydda och hantera Bolagets data på ett sätt som följer av tillämplig dataskyddslagstiftning och Bolagets intressenters krav och skäliga förväntningar. Skyddsåtgärder ska utformas så att de omfattar, men inte begränsas till, tillgänglighet, sekretess och integritet.

- Skyddsåtgärder ska där möjligt baseras på god praxis (t. ex. ISO 27001/27701). Vid val och implementering av skyddsåtgärder ska hänsyn tas till påverkan på Bolagets medarbetare och besökare.
- Säkerheten av fysiska informationstillgångar skall säkras med lämpliga åtgärder. Fysiska informationstillgångar inkluderar, men är inte begränsade till, bolagets kontor, datorer, nätverksutrustning, och lagringsenheter.
- Hemnet ska kontinuerligt och systematiskt arbeta med att analysera och utvärdera de krav, förväntningar och risker som finns när det gäller Bolagets information och data för att säkerställa att de åtgärder som vidtas är relevanta och effektiva. Utvärderingen ska ske enligt de riktlinjer som finns fastställda av Hemnets ledningsgrupp.
- Det ska finnas relevanta riktlinjer och rutiner för skydd av personuppgifter som säkerställer att Hemnet efterlever tillämplig dataskyddslagstiftning.
- Hemnet ska, från insamling till radering, säkerställa att Bolagets data är korrekt och trovärdig.
- Alla informations- och datatillgångar ska finnas dokumenterade och samtliga tillgångar ska tilldelas en klassificering för att säkerställa att de hanteras korrekt.
- I allt utvecklingsarbete och upphandling ska alltid skydd av personuppgifter och informationssäkerhet finnas med som en del av kraven.
- Alla medarbetare som hanterar incidenter relaterade till information och data ska ha tillräcklig kunskap för att avgöra om incidenten inkluderar personuppgifter.
- Alla medarbetare som hanterar personuppgifter ska ha tillräcklig kunskap om de regelverk som styr personuppgiftsbehandling.
- Hemnet ska ha relevanta rutiner för att hantera alla typer av incidenter som kommer av de identifierade riskerna.
- För viktiga informations- och datatillgångar ska det finnas en kontinuitetsplan som säkerställer att verksamheten kan fortgå vid allvarliga störningar i tillgängligheten.
- Hemnet ska endast tilldela åtkomst till information och IT-resurser i den utsträckning som krävs för att möjliggöra utförandet av arbetsuppgifter, i enlighet med principen om minsta möjliga behörighet.
- Alla personer som tilldelas behörigheter, t.ex. i form av kontouppgifter, ska vara medvetna om att tilldelningen är personlig och ej får göras tillgänglig för annan part oavsett dennes relation till Hemnet eller på något sätt överlåtas utan godkännande från den som tilldelade behörigheten.
- Hemnet ska eftersträva en kultur av hög medvetenhet om informationssäkerhet och skydd av personuppgifter. Alla Hemnets medarbetare, oavsett anställningsform, ska vara medvetna om de regler och riktlinjer som gäller för data och informationssystem samt förstå vikten av en ansvarsfull användning av Hemnets data och informationsresurser.

Styrning

Roller och ansvar

Denna policy ägs av CFO, och eventuella uppdateringar eller ändringar kräver godkännande av styrelsen. Ledningen och styrelsen ansvarar för att säkerställa att dataskydd och

informationssäkerhet upprätthålls i enlighet med denna policy. För att säkerställa att bolagets användning av information, informationssystem och data är i linje med affärsmålen ska ledningen även ansvara för att upprätthålla en tydlig styrning av Hemnets strategiska beslut och investeringar. Detta inkluderar att säkerställa att roller, ansvar och befogenheter är tydligt dokumenterade i enlighet med riktlinjerna för IT-styrning. Alla individer med tillgång till Hemnets resurser måste följa denna policy och rapportera eventuella överträdelser.

Tredjepartsstandarder

Hemnet bedriver sin verksamhet i linje med interna principer, strategiska prioriteringar och viktiga lagstadgade krav (t.ex. GDPR).

Uppföljning och efterlevnad

Övervakning och granskning

Denna policy genomgår en årlig granskning i enlighet med Riktlinjer för Hemnets styrdokument och Policy för bolagsstyrning, för att säkerställa att den implementeras på rätt sätt och är fortsatt relevant för Hemnets operativa behov. Under granskningen utvärderas dess effektivitet när det gäller att hantera aktuella risker och krav på efterlevnad.

Granskningsprocessen utförs av HOIS, i enlighet med Hemnets policy för bolagsstyrning. HOIS säkerställer att policyn förblir i linje med förändringar i lagstiftningen, utvecklande affärsbehov och säkerställer efterlevnad genom lämpliga stöddokument och utbildning. Resultatet av granskningsprocessen, inklusive eventuella nödvändiga uppdateringar, rapporteras till styrelsen för slutligt godkännande.

Tillgänglighet till policyn

Denna policy är tillgänglig för alla anställda och relevanta intressenter via interna kommunikationsplattformar och Hemnets webbplats på https://www.hemnetgroup.se/. Utbildning och utbildningsmaterial tillhandahålls för att säkerställa en omfattande förståelse och efterlevnad av policyn.

Rapporteringskanaler för brister i efterlevnad

Av Hemnets *uppförandekod* framgår vilka rapporteringskanaler som ska användas av medarbetare som upptäcker brister i efterlevnad av styrdokument. Varje medarbetare uppmanas att i första hand där möjligt ta upp frågan med den person som ärendet berör. Om det inte är lämpligt eller möjligt, kontaktas ansvarig chef. Om det inte heller är lämpligt eller möjligt uppmanas medarbetaren att kontakta sin chefs chef, Hemnets Chief People & Culture Officer eller Hemnets chefsjurist. Vidare finns möjlighet till anonym rapportering för allvarliga oegentligheter genom Bolagets visselblåsarfunktion som nås via https://report.whistleb.com/sv/hemnet

Överträdelse av denna policy

Överträdelser av denna policy kommer alltid att tas på största allvar och kan leda till disciplinära åtgärder, inklusive uppsägning. Därutöver kan brott mot relevanta lagar innebära att du (och/eller Bolaget) blir föremål för rättsliga påföljder.

Relaterade dokument

- Riktlinjer för Dataskydd
- Riktlinjer för informationssäkerhet
- Riktlinje för informationsklassificering
- Riktlinjer för ansvarsfullt användande
- Riktlinje för ansvar & befogenheter IT
- Riktlinjer för val av leverantörer
- Riktlinjer för styrande dokument.
- Uppförandekod