Virksomhedens informationssikkerheds-politik

Indholdsfortegnelse

Kontrol af dokumenter

Indholdsfortegnelse

Kontrol af dokumenter

Dokumentets navn	Virksomhedens informationssikkerhedspolitik
Klassificering	INTERNT
Revisionsnummer	3.5
Revisionsdato	05/12/2024
Forvalter	Enterprise Security Manager
Godkendelse	Indsigt IS Forum
Revision	Årligt: Enterprise Security Manager
Næste anmeldelse	December 2025

1. Overblik

Denne politik er baseret på ISO 27001:2022, den anerkendte internationale standard for informationssikkerhed. Denne standard sikrer, at Insights overholder følgende sikkerhedsprincipper:

Fortrolighed Alle følsomme oplysninger beskyttes mod uautoriseret adgang eller offentliggørelse.

Integritet Alle oplysninger vil blive beskyttet mod utilsigtet, ondsindet og svigagtig ændring eller ødelæggelse.

Tilgængelighed Informationstjenesterne vil være tilgængelige på de tidspunkter, der er aftalt med brugerne, og være beskyttet mod utilsigtet eller ondsindet beskadigelse eller afvisning af tjenester.

2. Formål

Formålet med denne politik er at demonstrere det engagement og forpligtelse, som Insights Learning and Development har i forhold til sikkerheden af de data, de er ansvarlige for. Ydermere, illustrerer politikken de kontroller og ansvarsområder, der er på plads for at understøtte informationssikkerhedsledelsessystemet, ISMS, som har ISO 27001:2022 som sin vigtigste ramme.

3. Omfang

Omfanget af denne politik dækker alle interne og eksterne parter og understøtter Insights' fortsatte engagement i ISO 27001:2022.

4. Politik

4.1 Ledelsens ansvarsområder

Insights' ledelse er forpligtet til at opfylde alle gældende krav i denne politik og til løbende at forbedre informationssikkerhedsledelsessystemet (ISMS), og har derfor etableret denne informationssikkerhedspolitik, så:

- den er passende til Insights formål;
- Den indeholder mål for informationssikkerhed og giver rammerne for at fastsætte løbende mål for informationssikkerhed.

Denne informationssikkerhedspolitik skal være tilgængelig som dokumenteret information; kommunikeres inden for Insights; og være tilgængelig for interesserede parter, hvis det er relevant.

Overholdelse af denne politik og alle andre sikkerhedspolitikker og -procedurer er obligatorisk for alle medarbejdere.

Den administrerende direktør godkender denne politik. Information Security Forum (ISF) har ansvaret for at sikre, at politikken implementeres og overholdes i hele virksomheden, som er omfattet af ISMS.

4.2 Lederskab og engagement

Ledelsen vil udvise deres ledelse og fortsatte engagement med hensyn til ISMS ved at:

- at sikre, at informationssikkerhedspolitikken og informationssikkerhedsmålene er fastlagt og er

forenelige med Insights' strategiske virksomhedsretning;
- at sikre integration af ISMS-kravene i Insights' processer;
- sikre, at de nødvendige ressourcer til ISMS er til rådighed;
- at kommunikere vigtigheden af effektiv informationssikkerhedsstyring og af at overholde ISMS-kravene;
- at sikre, at ISMS opnår det eller de tilsigtede resultater;
- lede og støtte personer, der skal bidrage til effektiviteten af ISMS;
- Fremme de løbende forbedringer og støtte til andre relevante ledelsesroller, således de kan udvise lederskab inden for deres ansvarsområder.

4.3 Målsætninger for informationssikkerhed

Der er fastlagt mål for informationssikkerhed, som er forenelige med Insights' strategiske retning, og hovedmålet er at arbejde i overensstemmelse med afsnittene i standarden for bedste praksis ISO 27001:2022, som er beskrevet nedenfor.
Desuden vil sikkerhedsmålætninger blive fastsat af Information Security Forum (ISF) som en løbende opgave og på ISMS Management Review Meetings.

4.4 Kontinuerlig forbedring af ISMS-rammen

Insights vil løbende søge at forbedre ledelsessystemet for informationssikkerhed i overensstemmelse med en PLAN-DO-CHECK-ACT-tilgang til at forbedre processer, der er indlejret i ISMS.

Vigtigheden, der tillægges informationssikkerhed, fremgår af eksistensen af Information Security Forum (ISF); ISF's funktion er skitseret nedenfor;

- gennemgang og udvikling af strategiske sikkerhedsspørgsmål;
- etablere relationer uden for Insights med andre sikkerhedsrådgivere;
- at vurdere virkningen af nye lovmæssige eller regulatoriske krav, der pålægges os;
- overvågning af ISMS's effektivitet, f.eks. ud fra resultaterne af interne revisionsrapporter og rapporter om sikkerhedshændelser;
- anbefale/godkende ændringer til ISMS.

Information Security Forum mødes regelmæssigt for at tage fat på ovenstående aktiviteter med henblik på at sikre den fortsatte effektivitet af Insights' ISMS. Gennemgangsprocessen er defineret i "Information Security Forum Management Review Policy".

Denne politik for informationssikkerhed bekræfter Insights' forpligtelse til løbende forbedringer og fremhæver de vigtigste områder (kaldet "temaer") for effektivt at sikre sine oplysninger, nemlig

- Organisatoriske kontroller
- Kontrol af personale
- Fysiske kontroller
- Teknologiske kontroller

4.5 Organisatoriske kontroller

Organisatoriske kontroller er Information Security Forums ansvar og omhandler følgende områder:
- Strategiske informationssikkerhedspolitikker - som dækker denne politik, politikken for sikkerhedsmål og kommunikationspolitikken.
- Roller og ansvarsområder - Enterprise Security Manager er formand for Information Security Forum.
- Identitets- og adgangsstyring - Enterprise Security Manager/teamlederne er ansvarlige for både at etablere og vedligeholde robuste logiske adgangskontroller. En passende politik er på plads og skal overholdes af alle medarbejdere og eksterne parter.
- Asset Management – Insights' oplysninger skal klassificeres i henhold til deres følsomhed, og der skal udpeges en informationsejer. Enterprise Security Manager vedligeholder en fortegnelse over informationsaktiver, som opdateres med jævne mellemrum i henhold til risikoprofilen og beskyttes i overensstemmelse hermed.
- Relationer - Krav til informationssikkerhed for at mindske risikoen i forbindelse med leverandørens adgang til Insights-aktiver skal aftales med leverandøren og dokumenteres.
- Aftaler med cloud-leverandører skal etableres, dokumenteres og løbende gennemgås.

- Hændelsesstyring - Registreringer af sikkerhedshændelser skal vedligeholdes centralt, opdateres og overvåges løbende. Alle medarbejdere skal være klar over, hvad der udgør en faktisk eller potentiel sikkerhedshændelse, hvordan hændelsen skal rapporteres, og hvem den skal rapporteres til. Ansvaret for tilsynet med alle sikkerhedsbrud ligger hos Enterprise Security Manager.
- Business Continuity Management - Insights skal sikre en konsekvent og effektiv tilgang til håndtering af større informationssikkerhedshændelser, herunder kommunikation om sikkerhedshændelser og -svagheder og konsekvenserne for business continuity management.

- Overholdelse - Insights skal undgå at overtræde juridiske, lovbestemte, regulatoriske eller kontraktlige forpligtelser i forbindelse med informationssikkerhed og eventuelle sikkerhedskrav. Insights skal træffe tekniske og organisatoriske foranstaltninger for at beskytte personoplysninger mod hændelig eller ulovlig tilintetgørelse, hændeligt tab eller ændring samt uautoriseret videregivelse eller adgang. Insights skal især træffe foranstaltninger, der har til formål at sikre, at:

    - Alle, der administrerer og håndterer persondata, forstår, at de er kontraktligt ansvarlige for at følge god praksis for databeskyttelse.
    - Alle, der administrerer og håndterer persondata, er tilstrækkeligt uddannet til at gøre det; og
    - Alle, der administrerer og håndterer persondata, er under passende opsyn.

4.6. Kontrol af personale

Kontrol af personale er HR-teamets ansvar og omhandler følgende områder:

- Alle medarbejdere skal underskrive medarbejderhåndbogen, som kræver, at de arbejder i overensstemmelse med alle politikker og procedurer, herunder specifikke krav til informationssikkerhed.
- En sikkerhedspolitik for personlige oplysninger sikrer, at medarbejderne bliver gjort opmærksomme på, at de er forpligtet til at følge bedste praksis med hensyn til informationssikkerhed.
- Der er også en procedure for alle medarbejdere, der forlader Insights (herunder midlertidigt ansatte og kontraktansatte), for at deaktivere deres netværkskonto og få alle ejendele tilbage.
- Alle nye medarbejdere (faste, midlertidige og underleverandører) skal uddannes i procedurer på de områder, der er beskrevet ovenfor, som en del af deres introduktionsprogram. Løbende uddannelse skal leveres i form af et program med regelmæssige opdateringer og uddannelsessessioner af informationssikkerhedsforummet.

4.7 Fysiske kontroller

Fysisk kontrol er facilitetsteamets ansvar og omhandler følgende områder:

- Medarbejderne skal være opmærksomme på og følge det detaljerede sæt af foranstaltninger, kontroller og procedurer, der findes for at sikre tilstrækkelig kontrol med den fysiske sikkerhed. Disse omfatter:

    - Bygningsalarm og CCTV-systemer
    - begrænset adgang til bygningen og yderligere begrænset adgang inde i bygningen
    - sikre skabe, skuffer, pengeskabe og opbevaring, brandsikker opbevaring
    - sikker offsite-backup og -arkivering
    - ryddeligt skrivebord og ryddelig skærm
    - procedurer for udstedelse af alle type medier
    - behovet for løbende overvågning af alle fysiske sikkerhedsforanstaltninger

4.8. Teknologiske kontroller

Teknologiske kontroller er Enterprise Technology & Security Teams ansvar og omhandler følgende områder:

- Alle endpoint-enheder skal være tilstrækkeligt beskyttede og krypterede, hvor det er relevant.
- Identitets- og adgangsstyring - IT-systemadministratorer (privilegerede brugere) sikrer, at de aftalte adgangskontroller og -procedurer administreres i overensstemmelse med den fastlagte politik.
- Kryptografi - Hvor Insights anvender kryptografiske kontroller, er der udviklet og implementeret en

politik for brug af kryptografiske kontroller til beskyttelse af oplysninger.

- IT-driftssikkerhed - Insights vil sikre korrekt og sikker drift af informationsbehandlingsfaciliteter. Enterprise Technology & Security Team foretager løbende overvågning af alle IT-driftsaktiviteter.
- IT-kommunikationssikkerhed - medarbejderne skal være opmærksomme på, at brugen af teknologi og kommunikation etableres, kontrolleres og styres af Enterprise Security Manager. Han er ansvarlig for at sikre, at de rette sikkerhedsforanstaltninger og -processer er på plads. Insights vil sikre, at sikkerheden omkring netværket, endpoint og fjernarbejde er tilstrækkeligt beskyttet.
- Sikkerhed i forbindelse med udvikling af IT-systemer - Enterprise Security Manager sikrer, at de relevante informationssikkerhedsprocesser indgår i alle projekter. En sikker udviklingstilgang, herunder politik, procedurer, miljø og test, er på plads.

4.9. Periode for gennemgang af politik

Information Security Forum vil gennemgå denne politik mindst en gang om året.

5. Overholdelse af politik

Måling af **overholdelse**: Sikkerhedsteamet og/eller Information Security Forum vil verificere overholdelse af denne politik gennem forskellige metoder, herunder, men ikke begrænset til, periodiske gennemgange, videoovervågning,
rapporter om forretningsværktøjer, interne og eksterne revisioner og feedback til policeejeren.

Undtagelser: Alle undtagelser fra denne politik skal godkendes af den ansvarlige for politikken og den, der godkender den. I deres
fravær, som f.eks. ved årlig ferie, vil dette falde ind under disse medarbejderes ledere
eller Information Security Forum.

Manglende overholdelse: En medarbejder, der har overtrådt denne politik, og som negativt påvirker Insights Learning & Developments omdømme, eller den bredere Insights Group kan risikere disciplinære foranstaltninger, og i visse tilfælde en opsigelse af deres ansættelse.

6. Relaterede standarder, politikker og processer

Vare	Int eller Ext	Dokumentets titel
1	Internt	ISMS-dokumentstyringssystem
2		
3		
4		
5		
6		

7. Definitioner og termer

Ikke anvendelig

8. Revisionshistorik

Revision	Dato	Ændret af	Beskrivelse
2.0	09/01/2020	Graham Watson	Politik godkendt af CEO
2.1	24/09/2021	Kevin McAuley	Mindre ændringer baseret på ændringer i roller og struktur
3.0	30/11/2021	Kevin McAuley	Politik godkendt af direktionen
3.1	13/02/2023	Dave McClure	Opdatering af politik med tilføjelse af nye politikker
3.2	06/03/2023	Dave McClure	Roller og ansvar flyttet til ny politik
3.3	05/04/2023	Ian Gowen	Tilføjet intern ref-tabel
3.4	28/04/2023	Ian Gowen	Ændret rækkefølgen af interne referencer
3.5	05/12/2024	Andy Moore	Årlig gennemgang og godkendelse af CEO

Underskrevet: Dato: 5th december 2024

Fiona Logan
Administrerende direktør