Policy för informationssäkerhet och dataskydd

Beslutad av Grant Thorntons styrelse 2024-12-10

Giltig fr.o.m. 2025-01-01

Policyägare: Chief Information Officer

Informationsklassning: Öppen

1. Introduktion och syfte

Grant Thornton Sweden AB:s (”Grant Thorntons”) policy för informationssäkerhet och dataskydd ska, tillsammans med uppförandekoden, våra framgångsfaktorer och övriga styrande dokument, bidra till att företaget är framgångsrikt och når sina mål. Policyn syftar till att öka kvalitet, uppfylla lagkrav och stödja företagets strategi och vision genom att etablera principer för informationssäkerhet och dataskydd. Policyn är en viktig del av företagets kvalitets-, risk-, regelefterlevnads-, och hållbarhetsarbete.

Grant Thornton hanterar stora mängder information, både inom ramen för kundverksamheten och internt. Externa och interna regler för revision, yrkesetik och dataskydd ställer höga krav på säkerhet vid hantering av såväl verksamhetsinformation som personuppgifter.

2. Tillämplighet

Policyn gäller för alla personer som arbetar på eller för Grant Thornton, däribland anställda, praktikanter och (i tillämpliga fall) externa konsulter, vilka i styrande dokument benämns medarbetare. För leverantörer och andra samarbetspartners gäller ”Uppförandekod för leverantörer”. Roller och ansvar beskrivs på ett övergripande sätt i Grant Thorntons governance-ramverk.

Fokusområden i denna policy

- Roller och ansvar avseende informationssäkerhet
- Roller och ansvar avseende dataskydd
- Lämpligt skydd för information och personuppgifter
- Intern rapportering av olika typer av incidenter avseende informationssäkerhet och dataskydd

3. Allmän regelefterlevnad

Grant Thornton ska följa all tillämplig lagstiftning i de länder och jurisdiktioner där bolaget verkar liksom, i tillämplig omfattning, standarder respektive internationella riktlinjer avseende de områden som täcks i denna policy inklusive standarder utfärdade av Grant Thornton International Limited (”GTIL”).

4. Utbildning, vägledning och medvetenhetshöjande insatser

Grant Thornton ska agera för medvetenhet om policyns innehåll hos medarbetare. Utbildning, vägledning och kommunikationsinsatser ska vara relevanta och anpassade utifrån roll och verksamhetstillhörighet. Effektiviteten i aktiviteterna ska följas upp.

5. Informationssäkerhets- och dataskyddsarbete inom Grant Thornton

Grant Thorntons riskbaserade arbete med informationssäkerhet och dataskydd grundar sig på såväl tillämplig dataskyddslagstiftning som internationella standarder och riktlinjer för informationssäkerhet. Syftet är att vi som företag ska säkerställa regelefterlevnad och ett lämpligt skydd för den information, och de personuppgifter, som hanteras i verksamheten samt att en god informationssäkerhetskultur respektive dataskyddskultur ska uppnås.

Grundläggande för informationssäkerhets- och dataskyddsarbetet är att det ska finnas tydliga roller och ansvar inom respektive område, ett lämpligt skydd för information och personuppgifter ska säkerställas, samt att olika typer av incidenter avseende informationssäkerhet och dataskydd internt ska rapporteras och hanteras.

Grant Thornton ska bedriva ett aktivt informationssäkerhetsarbete i syfte att skydda Grant Thorntons informationstillgångar på ett lämpligt sätt, reducera risk för felaktig användning av verksamhetsinformation samt förebygga IT-relaterade störningar som kan påverka verksamheten på ett negativt sätt. Skyddet ska vara anpassat med hänsyn till art, omfattning och risk samt med beaktande av såväl externa som interna krav enligt lagar, regler och interna styrande dokument.

Grant Thornton ska bedriva ett aktivt dataskyddsarbete och därigenom ha en god efterlevnad av tillämplig dataskyddslagstiftning och att upprätthålla ett lämpligt skydd, både organisatoriskt och tekniskt, för behandlade personuppgifter. En god dataskyddskultur är en viktig del av en övergripande informationssäkerhetskultur.

5.1. Roller och ansvar avseende informationssäkerhet

Alla medarbetare har ett ansvar att upprätthålla en god informationssäkerhet i det dagliga arbetet. Inom Grant Thornton är det vd som är ytterst ansvarig för informationssäkerheten och efterlevnaden av informationssäkerhetskraven inom Grant Thornton. Det operativa ansvaret för informationssäkerheten och informationsägarskapet ligger på respektive Business Leader och Corporate Functions. Därtill ska bland annat en informationssäkerhetsansvarig (Chief Information Security Officer, CISO) och systemägare utses och/eller definieras.

5.1.1. En god informationssäkerhetskultur

En god informationssäkerhetskultur innebär att alla medarbetare ska veta vad det egna ansvaret för informationssäkerhet innefattar, vilka regler som gäller samt ha förmågan att upptäcka händelser som kan påverka informationssäkerheten negativt. Genom utbildning och information ska alla medarbetare göras medvetna om informationssäkerhetsfrågor vilket främjar regelefterlevnad och en god informationssäkerhetskultur.

5.2. Roller och ansvar avseende dataskydd

Alla medarbetare har ett ansvar att upprätthålla en lämplig nivå av skydd för behandlade personuppgifter i det dagliga arbetet. Inom Grant Thornton är det styrelsen som har det yttersta ansvaret för att personuppgifter behandlas i enlighet med tillämplig dataskyddslagstiftning. Det operativa ansvaret för efterlevnad av dataskyddsregler följer informationsägarskapet, det vill säga respektive chefs ansvar. Grant Thornton ska utse ett dataskyddsombud, vars ställning och grundläggande uppgifter framgår av tillämplig dataskyddslagstiftning. Dataskyddsombudet ansvarar inte för att tillämplig dataskyddslagstiftning efterlevs, det ansvaret ligger alltid på den personuppgiftsansvarige.

5.2.1. En god dataskyddskultur

Grant Thornton ska bedriva ett aktivt dataskyddsarbete för att säkerställa regelefterlevnad avseende dataskydd när personuppgifter behandlas i Grant Thorntons verksamhet. Det är viktigt att de grundläggande principerna för behandling av personuppgifter efterlevs. Dataskyddsarbetet ska vara integrerat i den dagliga verksamheten. Genom utbildning och information ska alla medarbetare göras medvetna om dataskyddsfrågor vilket främjar ett högt skydd för behandlade personuppgifter och en god dataskyddskultur.

5.3. Lämpligt skydd för information och personuppgifter

All information som hanteras i verksamheten ska klassificeras (fyra kategorier: öppen, intern, konfidentiell och hemlig) och personuppgiftsbehandlingar ska riskanalyseras i syfte att säkerställa en lämplig skyddsnivå för såväl information som personuppgifter. Ett lämpligt skydd ska säkerställas under hela livscykeln, dvs. från kravställning inför inköp, vid införande, under användning/behandling, vid utveckling samt vid avveckling av informationssystem/IT-stöd. Lämpliga skyddsåtgärder ska även innefatta riskbaserade bakgrundskontroller. Företaget ska ha full insikt i och kontroll över den digitala leverantörskedjan för att säkerställa att alla parter uppfyller säkerhets- och dataskyddskraven.

5.4. Intern rapportering av olika typer av incidenter avseende informationssäkerhet och dataskydd

Incidenthantering är en del av ett regelbundet och systematiskt informationssäkerhets- och dataskyddsarbete. Grant Thornton ska hantera alla incidenter som inträffar, åtgärda eventuella brister samt regelbundet följa upp incidenter för att säkerställa ett högt skydd för både verksamhetsinformation och personuppgifter. En viktig del i detta arbete är att få kännedom om de incidenter som inträffar i den dagliga verksamheten, vilket förutsätter kunskap och upptäcktsförmåga hos samtliga medarbetare. Det ska finnas en process för intern rapportering av säkerhetsincidenter och personuppgiftsincidenter.

6. Efterlevnad och uppföljning

Policyägaren har det övergripande ansvaret för policyn, vilket innefattar att:

- Utveckla och regelbundet uppdatera mer detaljerade regler avseende policyns innehåll, i enlighet med syftet och ändamålet med denna policy.
- Agera för att policyn och underliggande styrande dokument kommuniceras och är välkända för medarbetare.

- Följa upp graden av efterlevnaden av policyn.
- I tillämpliga fall av oegentligheter eller allvarliga avvikelser från policyn, tillse eller bistå i att rättsliga eller disciplinära åtgärder vidtas.
- Tillse att ytterligare åtgärder vidtas, inklusive korrigerande åtgärder och rapportering, nödvändiga för att uppfylla syftet med policyn.

Business Leaders är ansvariga för att skapa kännedom om policyn och säkerställa efterlevnad i respektive Business Line. Respektive chef för Corporate Functions har motsvarande ansvar. Medarbetare förväntas rapportera materiella avvikelser från policyn till sin närmaste chef eller till policyägare.

7. Referenser

Policyn kompletteras av underliggande instruktioner som innehåller med detaljerade regler gällande informationssäkerhet och dataskydd.

8. Versionshistorik

Version	Datum	Kommentar
1.0	2024-01-15	Första version av Policyn.
1.1	2024-11-22	Årlig översyn och mindre uppdateringar.