Getinge-policy

Global IT-policy

Dokument-ID: POL-0128 rev1
Godkänd av styrelsen den 23 april 2019

1. Sammanfattning

Getinge är förpliktigat att skydda både människor och information samtidigt som man minskar den övergripande IT-risken. Denna policy definierar Getinges ståndpunkter inom IT-området och klargör det beteende vi förväntar oss från användare, systemadministratörer, ledning och IT-säkerhetspersonal. Den sätter också säkerhetsstandarderna för vårt IT-system och våra applikationer. Denna policy gäller alla medarbetare och affärsrelationer som agerar å Getinges vägnar.

2. Definitioner

CFO – Chief Finance Officer

CIO – Chief Information Office

CISO – Chief Information Security Officer

GDPR – General Data Protection Regulation (EU:s dataskyddsförordning för skydd av personuppgifter)

BYOD – Bring Your Own Device – en användares personliga dator, surfplatta eller mobiltelefon

ITIL – Information Technology Infrastructure Library. En uppsättning detaljerade rutiner för IT-servicehantering som fokuserar på att anpassa IT-tjänsterna efter verksamhetens behov.

3. Omfattning och syfte

Denna policy gäller alla Getinge-företag, dess dotterbolag och konsortier (benämns gemensamt ”Getinge”) och omfattar alla våra medarbetare samt konsulter och inhyrd personal som arbetar på Getinges anläggningar eller under Getinges ledning (samtliga benämns ”medarbetare” i denna policy).

Syftet med denna policy är att erbjuda vägledning och stöd i samband med IT-beslut inom Getinge. Det beskriver standarder och procedurer som återspeglar en säker och godtagbar praxis baserad på vedertagen och aktuell kunskap, riktlinjer och sedvanor.

4. Principer

Åtaganden och förväntningar

Getinges IT-struktur tillför värde genom att erbjuda företaget bästa möjliga service där risker och fördelar balanseras mot IT-investeringens avkastning.

Getinge är förpliktigat att skydda både människor och information samtidigt som man minskar den övergripande IT-risken. Vi styr och kontrollerar våra IT-funktioner genom strukturerad ledning, en konsekvent process och genom att bygga upp starka relationer till verksamheten.

Målet med denna policy är att:

- skydda människor och information
- definiera reglerna för det beteende som förväntas av användare, systemadministratörer, ledning och IT-säkerhetspersonal
- sätta standarderna för IT-system och applikationer
- minska den övergripande IT-risken.

Vi förväntar oss att alla medarbetare och underentreprenörer som använder Getinges IT-system eller maskinvara ska följa denna policy och på ett konsekvent sätt tillämpa dess höga standarder. Mer information finns i de underliggande direktiven och instruktionerna.

Direktivet om informationssäkerhet

Informationssäkerhet handlar om att skydda information från obehörig åtkomst, användning, offentliggörande, störning, modifiering, granskning, kontroll, inspelning eller förstörelse.

Getinges direktiv om informationssäkerhet definierar hur vi hanterar risker för Getinges informationssäkerhet och etablerar de säkerhetsåtgärder som krävs för att skydda Getinges informationstillgångar oavsett vilken form dessa data har (t.ex. elektroniska eller fysiska säkerhetskopior).

Syftet med detta direktiv om informationssäkerhet är att erbjuda riktlinjer om hur – ur säkerhetssynpunkt – vi ska säkerställa att:

- vår information är konfidentiell
- våra system är åtkomliga och tillgängliga

- vår dataintegritet är fullgod.

Direktivet om informationssäkerhet gäller alla datoriserade informationssystem som understödjer Getinges affärsprocesser. Detta omfattar applikationsinfrastruktur (inklusive nätverk och kommunikation), tillhandahållna IT-tjänster, stationära och bärbara datorer, mobila enheter (inklusive telefoner, surfplattor, bärbara tillbehör) och personliga enheter som t.ex. BYOD:ar som används för Getinge-relaterade aktiviteter.

Alla frågor om informationssäkerhet ska ställas till Getinges CISO.

Mer information finns i: *Direktivet om informationssäkerhet*

Klassificering av information

Syftet med direktivet om klassificering av information är att säkerställa att Getinges information skyddas i lämplig omfattning med utgångspunkt från hur viktig och känslig informationen är och de system där den används, vilket ska minska risken för att Getinges information avslöjas, går förlorad eller kommer till skada.

All lagring, användning, överföring och radering av data måste utföras i enlighet med informationens klassificering. Om användningen av data måste förändras anger detta direktiv vilka begränsningar, ansvar och åtgärder som gäller. Alla nya datatyper måste klassificeras. Vi undersöker alltid nya regelverk som påverkar datasäkerheten och/eller integriteten och genomför lämpliga uppdateringar.

Mer information finns i: *Direktivet om informationssäkerhet*

Direktiv om acceptabel IT-användning

Detta direktiv definierar acceptabel användning av Getinges IT-resurser i syfte att på ett effektivt sätt hantera och säkra användningen av all IT-egendom. Detta omfattar inte bara datorer och mobiltelefoner, utan även användningen av elektroniska informationssystem (t.ex. programvaror och delade filsystem), Getinges nätverk, internetåtkomst och e-postsystemet.

Dessa system används för affärsändamål under vår normala verksamhet i syfte att främja företagets och dess kunders intressen. All användning måste följa tillämplig lagstiftning, förordningar och regler och där så är lämpligt även branschstandarder och samförståndsbaserade standarder.

Mer information finns i: *Direktiv om acceptabel IT-användning*

Direktivet om IT-moln

Datormoln är ett sätt att leverera databehandlingstjänster – servrar, lagring, databaser, nätverk, programvara, analyser m.m. – via Internet (”molnet”).

Detta direktiv beskriver vilka överväganden som krävs vid val, införande och drift av molnlösningar eller molntjänster:

- Tydliggöra viktiga egenskaper vid användning av datormoln, servicemodeller och installationsmodeller.
- Nödvändigheter, bästa praxis och vad som är förbjudet när det gäller IT-moln.
- Rekommendationer och förklaringar som beskriver varför IT måste delta i processerna för inköp av molntjänster i ett så tidigt skede som möjligt.

Mer information finns i: Direktivet om IT-moln

5. Vid överträdelser – säg till

Tveka inte att ta upp ett problem. Alla Getinge-medarbetare som misstänker brott mot denna policy förväntas säga till och informera sin linjechef, Ethics & Compliance Office eller använda Getinge Ethics Line. Information om visselblåsarfunktionen finns på Getinges interna och externa webbsidor.

Getinge accepterar inga former av repressalier mot någon som gör sin röst hörd eller ger uttryck för oro eller åsikter.

Se även: Global instruktion för visselblåsare och förbud mot repressalier

6. Roller och ansvar

Alla Getinge-medarbetare ansvarar personligen för att läsa, förstå och följa denna policy. Varje enskild medarbetare är ansvarig för att agera i enlighet med denna policy.

Varje enskild linjechef ansvarar för att säkerställa att samtliga teammedlemmar har tillgång till denna policy och relaterade direktiv, instruktioner och riktlinjer.

Alla chefer ansvarar för att med stöd från IT-avdelningen dagligen uppmärksamma IT-frågor, informera och utbilda i ämnet och följa upp efterlevnaden.

Överträdelser av policyn kan leda till disciplinära åtgärder, vilket även kan innebära uppsägning.

7. Undantag från IT-policyn och direktiven

Om det finns skäl till att inte följa någon del av IT-policyn eller IT-direktiven (t.ex. vad gäller juridik, regelverk, ekonomi eller teknik) måste en undantagsförfrågan fyllas i och skickas till Getinges CISO (Chief Information Security Officer).

Undantag från IT-policyn får endast godkännas av Getinge Security Board, och beroende på risknivå kan ytterligare godkännanden bli nödvändiga.

Godkännanden av undantag måste vara begränsade både vad gäller tid och omfattning.

Mer information finns i https://intranet.getinge.com/en/our-company/it/it-security/security-exceptions/

8. Ramverk

Denna policy ingår i Getinges ramverk för styrning, där också följande ingår:

- Uppförandekod, Våra kulturella kärnvärden, Strategiskt ramverk, policyer som godkänts av styrelsen, direktiv som godkänts av koncernchefen eller direktrapporter till koncernchefen samt lokala instruktioner.
- Beslut fattade av koncernchefen eller på uppdrag av denne.
- Ethics & Compliance Office ansvarar för att säkerställa att den senaste versionen av denna policy publiceras på Getinges intranät och är tillgänglig för alla medarbetare.
- Denna policy kommer att granskas vartannat år eller vid behov.
- Policyn är ursprungligen skriven på engelska.

9. Stöd och vägledning

Denna policy och flera direktiv och instruktioner är avsedda att fungera som stöd och vägledning för hur vi ska uppträda i relation till Getinges ställningstaganden avseende IT-frågor. Om du har frågor om denna policy eller är osäker på vilka regler som gäller, kontakta Ethics & Compliance Office.

Praktiska länkar:

Direktivet om informationssäkerhet

Direktiv om acceptabel IT-användning

Direktivet om IT-moln

Process för begäran om undantag från IT-säkerhet