Getinges globala policy

IT global policy

Dokumentägare	Agneta Palmér
Version	V3
Antagen av styrelsen	18 december 2023

1. Sammanfattning

Getinge Group har åtagit sig att skydda människor och information, samtidigt som den övergripande IT-risken minskar. Denna koncernpolicy definierar Getinges ståndpunkter inom IT-området, och förtydligar 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 för alla medarbetare och affärsrelationer som agerar på uppdrag av Getinge Group.

2. Definitioner

I denna globala policy har följande termer följande betydelse:

CIO	Informationschef
CISO	Chief Information Security Officer
GDPR	Allmän dataskyddsförordning (EU-förordning om skydd av personuppgifter)
BYOD	Bring Your Own Device – en användares personliga PC, surfplatta eller mobiltelefon

3. Omfattning

Denna globala policy gäller för alla Getinge-företag, dess dotterbolag och gemensamma verksamheter (gemensamt "Getinge") och gäller alla våra anställda och styrelseledamöter, samt konsulter och byråpersonal som arbetar i Getinges lokaler eller under ledning av Getinge (alla hänvisas till i denna globala policy som "anställda").

Syftet med denna policy är att ge vägledning och stöd för IT-beslut inom Getinge. Den beskriver standarder och procedurer som återspeglar säker och acceptabel praxis baserad på accepterad och aktuell kunskap, riktlinjer och vanlig praxis.

4. Principer

Engagemang och förväntningar

Getinges IT-struktur tillför värde genom att tillhandahålla IT-tjänster till företaget, balansera risk och belöning med avkastning på IT-investeringar.

Getinge har åtagit sig att skydda människor och information samtidigt som den övergripande IT-risken minskar. Vi styr och kontrollerar våra IT-funktioner genom strukturerad ledning, en konsekvent process och genom att bygga starka relationer med verksamheten.

Syftet med denna policy är att:

- Skydda data och information;
- Ange regler för förväntat beteende av användare, systemadministratörer, ledning och IT-säkerhetspersonal;
- Sätt standarderna för IT-systemet och applikationerna;
- Minska den övergripande IT-risken.

Vi förväntar oss att alla anställda och entreprenörer som använder Getinges IT-system eller hårdvara följer denna policy och konsekvent tillämpar dess höga standarder.

5. Acceptabel användning av IT-resurser

Auktoriserad användning: IT-resurser som tillhandahålls av Getinge är avsedda för affärsändamål i enlighet med tillämpliga lagar, förordningar och branschstandarder. Personligt bruk är acceptabelt så länge som det inte stör arbetsansvaret eller bryter mot någon annan policy.

Förbjudna aktiviteter: Följande aktiviteter är strängt förbjudna:

- Obehörig åtkomst till IT-system eller data.
- Distribution, innehav eller användning av olaglig eller obehörig programvara.
- Användning av IT-resurser för alla olagliga eller oetiska aktiviteter.
- Otillåten ändring, förstörelse eller avslöjande av data.
- Trakasserier, diskriminering eller brott mot organisationens uppförandekod med hjälp av IT-resurser.
- All aktivitet som äventyrar nätverks- eller datasäkerhet.

För ytterligare vägledning, se: *IT-direktivet för acceptabel användning*

6. Informationssäkerhet

Cybersäkerhet

Definierar hur vi hanterar cybersäkerhet och upprättar de säkerhetskontroller som krävs för att skydda Getinges digitala tillgångar och data från hot:

- Följ etablerade cybersäkerhetsdirektiv och förfaranden, som definierar regler och bästa praxis för att skydda data- och teknikresurser.
- Utvärdera och identifiera regelbundet cybersäkerhetsrisker som kan påverka organisationens informationssystem och data.
- Bedöma och hantera cybersäkerhetsrisker förknippade med tredjepartsleverantörer och tjänsteleverantörer.
- Övervaka regelbundet system för misstänkta aktiviteter, utföra säkerhetsrevisioner och följa revisionskrav.

Alla frågor om cybersäkerhet ska ställas till Getinges CISO.

För ytterligare vägledning, se: *Cybersäkerhetsdirektivet*

Datahantering

- Anställda måste skydda konfidentiell och känslig information. Data ska klassificeras och hanteras enligt Getinges dataklassificeringsdirektiv.

För ytterligare vägledning, se: *Data Management Directive*

Rapportering av säkerhetsincidenter

- Alla anställda måste omedelbart rapportera alla säkerhetsincidenter eller misstänkta säkerhetsintrång till IT-avdelningen eller utsedd IT-personal.

För ytterligare vägledning, se: *Cybersecurity Incident Direktiv*

Direktiv om identitets- och åtkomsthantering

- Säkerställer att åtkomst till känsliga system och data begränsas till endast auktoriserad personal, med hjälp av starka autentiserings- och auktoriseringsmekanismer.

För ytterligare vägledning, se: *Identity and Access Management Direktiv*

Fjärråtkomst och mobila enheter

- Fjärråtkomst till Getinges nätverk tillåts endast genom säkra och auktoriserade metoder.

Utbildning och medvetenhet

- Anställda kommer att få utbildning om IT-säkerhetspraxis, och regelbundna påminnelser kommer att skickas för att upprätthålla medvetenheten.

7. IT-utrustning och programvara

IT-drift

Etablerar en baslinje för IT-drift för att leverera stabila och effektiva IT-tjänster.

Täcker områden som nätverkssäkerhetshantering, patch- och sårbarhetshantering, skydd mot skadlig kod, loggning och övervakning samt hantering av persondatorer och mobila enheter:

- Skydd mot skadlig programvara: Alla enheter som är anslutna till Getinges nätverk måste ha uppdaterade antivirus- och anti-malware-program.
- E-postsäkerhet: Använd endast IT-godkända e-posttjänster som säkerställer att integrerade system följer Getinges säkerhetsstandarder.
- Utrustning: IT-utrustning som tillhandahålls av Getinge är för affärsbruk. All annan utrustning som är ansluten till Getinges nätverk måste uppfylla säkerhetsstandarder.
- Mjukvaruinstallation: Installation av programvara på Getinges enheter bör auktoriseras av IT-avdelningen. Använd endast licensierad programvara.
- Konfigurera system, enheter och applikationer säkert för att minska attackytan och minimera säkerhetsrisker.

För ytterligare vägledning, se: *IT-driftdirektivet*

Säkerhetskopiering av data

Se till att det finns planer för att upprätthålla nödvändig verksamhet.

- All kritisk data måste säkerhetskopieras regelbundet för att förhindra dataförlust. Anställda ansvarar för att viktig data ingår i IT-backupprocessen.

För ytterligare vägledning, se *: IT-säkerhetskopierings- och återställningsdirektivet*

IT-styrning

För att säkerställa effektiv och säker leverans av IT-projekt och tjänster, samt att upprätthålla global licensefterlevnad och upprätthålla goda inköpsmetoder för IT-utrustning och tjänster:

- Alla IT-projekt måste följa Project Portfolio Management-processen och få lämpliga godkännanden.
- Praxis för IT-licenshantering måste följas för att upprätthålla överensstämmelse med programvarulicensavtal.
- IT-inköpshanteringsprocedurer bör följas för all IT-relaterade upphandlingsverksamhet.

För ytterligare vägledning, se: *IT-styrningsdirektivet*

IT-molnhantering

Beskriver vad du bör tänka på innan du väljer, implementerar och använder molnlösningar eller molntjänster:

- IT måste involveras i molnköpprocesser (så tidigt som möjligt).

För ytterligare vägledning, se: *IT-molndirektivet*

Applikationssäkerhet

Säkerställer att säkerheten är integrerad i tidiga skeden av IT-systemutveckling eller anskaffning.

För ytterligare vägledning, se: *Application Security Directive*

8. Roller och ansvar

Alla Getinge-anställda är individuellt ansvariga för att läsa, förstå och följa denna policy. Varje anställd är ansvarig för att agera i enlighet med denna policy,

Varje linjechef är ansvarig för att se till att varje teammedlem har tillgång till denna policy och relaterade direktiv, instruktioner och riktlinjer.

Dag-till-dag förstärkning, inklusive regelbunden information och utbildning inom IT-området, samt efterlevnadsuppföljning, är en del av varje chefs ansvar, med stöd av IT-avdelningen

Brott mot koncernpolicyn kan leda till disciplinära åtgärder, upp till och inklusive uppsägning.

9. Brott mot den globala policyn – Säg upp

Tveka inte att ta upp en oro. Alla Getinge-anställda som misstänker brott mot denna globala policy förväntas ta upp frågan och ta upp frågan till sin linjechef, till Etik- och efterlevnadskontoret eller använda Getinges Speak Up Line. Getinge Speak Up Line är tillgänglig på Getinges interna och externa webbsidor. På Getinge accepterar vi inte någon form av vedergällning mot någon som uttalar sig, uttrycker oro eller åsikter.

Se vidare: Global Speak Up and Non-Retaliation Directive

10. Vägledning och assistans

Om det finns en anledning till att inte följa någon del av IT-policyn eller IT-direktiven (t.ex. juridiska, regulatoriska, finansiella eller tekniska) måste en begäran om undantag fyllas i och skickas till Getinges Chief Information Security Officer och beroende på risknivån ytterligare godkännanden kan behövas.

Om du har frågor om denna globala policy, vänligen kontakta Pelle Nilsson, CIO.

Relaterade dokument

- Cybersäkerhetsdirektivet
- Direktivet om cybersäkerhetsincidenter
- Direktivet om godtagbar användning av IT
- IT-styrningsdirektivet
- IT-driftdirektivet
- Direktivet för IT-säkerhetskopiering och återställning
- IT-molndirektivet
- Datahanteringsdirektivet
- Direktiv om identitets- och åtkomsthantering
- Applikationssäkerhetsdirektivet
- Begäran om undantag för IT-säkerhet