SVENSKA HANDELSFASTIGHETER
ERFARENHET • LÅNGSIKTIGHET • SAMVERKAN

IT- och informationssäkerhetspolicy

Introduktion

Svenska Handelsfastigheter ska kännetecknas av hög säkerhet, både vad gäller den fysiska säkerheten för våra medarbetare och intressenter samt informationssäkerhetsmässigt. Vi ska arbeta enligt ställda krav med stort fokus på hållbara lösningar. Vår IT- och informationssäkerhetspolicy är grundläggande i vårt arbete för att ständigt förbättra vår och våra hyresgästers och samarbetspartners säkerhet.

Syftet med denna policy är att beskriva styrande principer för IT- och informationssäkerhetsarbetet samt informera om vårt förhållningssätt avseende användande av Svenska Handelsfastigheters-koncernens IT-resurser. Den ska även bidra till att säkerställa att resurser, data, samt personuppgifter hanteras på ett tillbörligt och lagligt sätt. Modern IT möjliggör hög tillgänglighet till information, men om hanteringen inte sker på ett korrekt sätt kan det leda till både materiella och immateriella skador och förluster för Svenska Handelsfastigheter. Arbetet med IT- och informationssäkerhet sker därför strukturerat utifrån det ansvar som beskrivs nedan.

En förutsättning för att information ska vara skyddad är att en god säkerhetskultur genomsyrar hela verksamheten. Med det avses att alla som hanterar Svenska Handelsfastigheters information har god kunskap om vilka regler som gäller vid informationshantering. Alla som hanterar information ska känna till vad det egna ansvaret omfattar och ha god kunskap om vilka säkerhetsregler som gäller.

Vad är IT?

Med IT avses utrustning, media, tjänst, system, infrastrukturtjänst, anslutning eller liknande som innehåller information eller som kan överföra eller tillgängliggöra information. Exempel på informationstillgångar som finns i Svenska Handelsfastigheter-koncernen är personuppgifter, fysiska och elektroniska dokument, filer och mappar, mjukvarulicenser, system, datorer, surfplattor, nätverk, servrar, hårdvara, mjukvara, telefonutrustning, teknisk utrustning, databaser, teknologi, skrivare, internet och e-post.

IT-säkerhet, risker, förhållningssätt och laglighet

Våra konkurrenter har ett stort intresse av att ta del av det sammanlagda informationsinnehållet i våra servrar och datorer. Det innebär att det finns ett starkt behov av att skydda koncernens information så den inte hamnar i orätta händer. Alla medarbetare ska ha ett ifrågasättande förhållningssätt mot obehöriga som ber om åtkomst. Medarbetare ska även tänka på hur information hanteras på offentliga platser, exempelvis genom att tillse att obehöriga inte kan se datorskärmen samt genom att överväga vilken information som kan behandlas i ett telefonsamtal.

Principer för system och resurser

Endast godkända system och programvaror får användas. Datorer, telefoner, surfplattor och motsvarande ska vara ägda av Svenska Handelsfastigheter och de ska vara konfigurerade av bolagets

IT-ansvarige. Om användare behöver ytterligare programvaror eller utrustning ska detta godkännas av IT-ansvarig. Syftet är att säkerställa att utrustningen uppfyller våra krav på säkerhet vad gäller virusskydd, behörigheter samt att programvaror med så kallade Malware (skräpprogram) inte installeras.

All IT-utrustning ska hanteras varsamt. Användare ska iaktta försiktighet så att stöldrisk och dataförlust minimeras. Datorn får inte lånas ut till obehöriga utan kontinuerlig övervakning. När datorn inte används ska denna alltid låsas och om det är möjligt ska utloggning ske från system.

Mobila enheter ska alltid förses med pinkod eller biometriskt lås. Åtkomst till Svenska Handelsfastigheters system genom mobila enheter ska skyddas. Applikationer på mobila enheter ska installeras med försiktighet.

Hantering av data

All data tillhör Svenska Handelsfastigheter. Data ska lagras på koncernens server och i avsedd filstruktur enligt gällande riktlinjer. Data som lagras tillfälligt på lokal disk ska så snart det är möjligt flyttas till servern för att säkerställa att informationen blir säkerhetskopierad via koncernens backup-system.

Externa lagringslösningar, såsom Dropbox och Sharepoint, ska inte användas då de inte uppfyller Svenska Handelsfastigheters krav på informationssäkerhet. Detta gäller inte Google Drive som uppfyller säkerhetskraven och som används av Svenska Handelsfastigheter.

All skyddsvärd information ska sorteras in i relevant mapp i serverstrukturen. Den användare som lagrar datan ansvarar för att klassificera informationen och ställa de säkerhetskrav som krävs för att informationen har ett fullgott skydd. Som utgångspunkt ska data inte delas med fler användare än vad som erfordras för att arbetsuppgifter ska kunna utföras ändamålsenligt.

Som data räknas även utskriven information. Det innebär att skrivbord ska hållas rena samt att skyddsvärd information ska förvaras inlåst och, vid behov, i brandsäkra skåp. Vidare ska skyddsvärd information destrueras genom strimling eller genom att slängas i avsett låst sopkärl för dokumentåtervinning. Utskrifter av dokument ska hanteras på ett säkert sätt där dokument inte lämnas oövervakat.

Lösenordshantering

För att kunna identifiera medarbetare samt minimera risken för dataintrång har varje medarbetare ett eget användarnamn och lösenord. Den anställde uppmanas att byta lösenord regelbundet. Lösenord ska hanteras som en skyddsvärd tillgång och får inte skrivas ut, distribueras eller lagras i system.

Nätverk

Interna trådbundna nätverk ska i första hand användas vid kontorsarbete. Vid nyttjande av arbetsgivarens IT-system från en extern plats, såsom hemarbetsplats, publik eller extern arbetsplats, är det den anställdes ansvar att upprätthålla en tillräckligt hög nivå av informationssäkerhet för att skydda koncernens information och kommunikation.

Vid uppkoppling till publika trådlösa nätverk ska endast kända nätverkspunkter användas. Kan inte accesspunkten verifieras, det vill säga uppkopplingspunkten för WIFI, ska mobila uppkopplingen via telefonen användas.

Sociala medier

Utgångspunkten är att Svenska Handelsfastigheter ser positivt på att anställda deltar på olika sätt i sociala medier. Vårt engagemang i sociala medier sprider våra budskap och stärker vårt varumärke. Det stärker också bilden av organisationen som öppen och tillgänglig. Du som person är alltid närvarande som en enskild individ, men din medverkan i sociala medier påverkar inte bara bilden av dig utan också bilden av Svenska Handelsfastigheter. Det är mycket viktigt att varje medarbetare skiljer på när deltagande i sociala medier faller inom ramen för anställningen och när deltagande faller inom ramen för det privata. Varje medarbetare är alltid personligt ansvarig för material publicerat på eget bevåg, oavsett om publiceringen skett i egenskap av arbetstagare eller privatperson. Uppgifter som är till skada för Svenska Handelsfastigheter kan utgöra brott mot lojalitetsplikten i anställningsförhållandet.

E-post och användande av Svenska Handelsfastigheters namn och varumärke

Medarbetaren representerar Svenska Handelsfastigheter bland annat via sin e-post-adress. E-postadresser är konstruerad enligt modellen ”fornamn.efternamn@handelsfastigheter.se”.

Användning av e-post för privat bruk är tillåtet i begränsad omfattning. Vid privat användning ska beaktas att den e-post som skickas från Svenska Handelsfastigheters e-postkonto kan uppfattas av mottagaren som företagspost. Det är inte tillåtet att använda koncernens IT-resurser för privat kommersiell verksamhet, till exempel försäljning, reklam, publicitet och liknande.

E-posthantering med personuppgifter

E-post innehåller nästan alltid personuppgifter innebärande att dataskyddsförordningen gäller för e-post. Det betyder att det ska finnas en rättslig grund för behandlingen av personuppgifter och att en bedömning avseende behandlingen behöver göras. För att minimera risk för förlust eller felhantering av personuppgifter i e-post, ska följande principer följas:

- Begränsa användningen av personuppgifter i e-post till vad som är nödvändigt för att uppfylla ändamålet (uppgiftsminimeringsprincipen).
- Överväg vilka som behöver ta del av den e-post som innehåller personuppgifter. Som huvudregel ska endast personer som har behov av tillgång till personuppgifter för att kunna utföra sitt arbete ha tillgång till dessa.
- Lagra bara e-post om det är ändamålsenligt och radera övrig e-post. Personuppgifter får bara behandlas så länge de behövs för att uppfylla ändamålen med behandlingen.
- Om personuppgifter i e-post ska sparas, exempelvis kontaktuppgifter till en hyresgäst, skriv in dessa i rätt dokumentation och radera e-posten. Huvudprincipen är alltid att flytta uppgifterna till det system/lista de hör till för att därefter radera e-posten.

Fysisk säkerhet

Den primära fysiska säkerheten upprättas genom traditionella säkerhetsanordningar såsom dörrlås, portkoder, larmsystem, passerkort, brandskydd, m.m. Om sådan utrustning eller skydd åsidosätts genom att en anställd släpper in gäster i arbetsgivarens lokaler, ansvarar den anställde för dessa gäster till dess att de lämnar arbetsgivarens lokaler. Passerkort, nycklar och motsvarande får aldrig överlämnas till externa.

Övriga IT-och informationssäkerhetsrelaterade regler

I tillägg till vad som i övrigt anges i denna policy ska följande regler följas av alla medarbetare:

- Utskickade säkerhetsuppdateringar ska installeras och inga ändringar av fördefinierade säkerhetsinställningar får genomföras.
- Det är inte tillåtet att skriva ut information för att ta med utanför Svenska Handelsfastigheters lokaler annat än då det behövs för att ”utföra sitt arbete”.
- Det är inte tillåtet att kopiera data till externt minne, till exempel i form av hårddisk eller USB-minne, om det inte krävs för att ”utföra sitt arbete”.
- Koncernens IT-resurser får inte användas för att på ett otillbörligt sätt sprida, förvara eller förmedla information i strid mot gällande lagstiftning, t.ex. hets mot folkgrupp, barnpornografibrott, diskriminering, olaga våldsskildring, förtal, dataintrång eller upphovsrättsbrott.
- IT-verktyg är ett arbetsverktyg och får för privat bruk användas bara i sådan omfattning att det inte inkräktar på arbetet eller medför onödiga kostnader för arbetsgivaren. Privat surfing är tillåten i begränsad omfattning och med gott omdöme. Det är inte tillåtet att surfa till sidor som innehåller eller erbjuder olagligt material.
- Vid längre frånvaro eller ledighet ska det finnas ett system för hantering av inkommande e-post. Den anställde ska se till att ett automatisk meddelande svarar på inkommande e-post och hänvisar till en kollega som finns på plats.

Rapporteringsskyldighet

Vid upptäckande av fel och brister avseende säkerhetsrutiner och system är alla medarbetare skyldiga att rapportera upptäckten till IT-ansvarig. Exempel på brister, fel och incidenter som ska anmälas är om utrustning förloras eller om det finns information eller misstanke om dataintrång eller virussmitta.

Målgrupp

Denna policy gäller LSTH Svenska Handelsfastigheter AB och samtliga dotterbolag i koncernen. Den gäller för samtliga anställda och alla som hanterar information för bolaget och dess dotterbolag.

Ansvar

Bolagets styrelse fastställer IT- och informationssäkerhetspolicyn och VD är ytterst ansvarig för att det som fastställs i policyn integreras i verksamheten. Policyn omfattar samtliga medarbetare som ansvarar för att agera i linje med denna policy. Varje chef har ansvar för att tillse att IT- och informationssäkerhetspolicyn iakttas inom dennes ansvarsområde.