Göteborgs Stad

Säkerhet & lokaler Gemensamt för staden
Säkerhetspolicy för Göteborgs Stad - Policy/riktlinjer/regler Handläggare: Peter Lönn
Fastställare: Kommunfullmäktige Gällande from 2013-11-15

Säkerhetspolicy för Göteborgs Stad

(H 2013:131, P 2013-09-05, § 21, Dnr 0540/14)

Bilaga 1

Göteborgs Stad

Dokumentansvarig: Chef Samhällsskydd och Beredskap Upprättad av: Samhällsskydd och Beredskap

Beslutad av: Kommunfullmäktige

Gäller för: Anställda och förtroendevalda i Göteborgs Stads förvaltningar, bolag, anknutna stiftelser och inhyrda entreprenörer.

Senast uppdaterad: 2013 - 08-05

Giltighetstid: Tills vidare

Säkerhetspolicy för Göteborgs Stad

Policy

- Säkerhet är en del av verksamhetens riskhantering[1] och kan beskrivas som förmågan att upprätthålla en definierad risknivå.

  Åtgärdsområden som ska inkluderas i säkerhetsarbetet är personsäkerhet, fysisk säkerhet, informationssäkerhet och krisberedskap.
- Säkerhetsarbetet ska vara långsiktigt och kontinuerligt och omfatta alla delar av stadens verksamheter.
- Nämnd och styrelse är ansvariga för säkerheten inom respektive verksamhet.
- Förvaltnings-/ Bolagsledning ska genom tydlig inriktning och fördelning av ansvar engagera sig i verksamhetens säkerhetsarbete samt minst årligen följa upp att säkerhetsnivån är acceptabel med återrapportering till Nämnd/Styrelse.
- Förvaltnings-/Bolagschef ska utse en säkerhetschef[2] med befogenhet att vara drivande och hålla ihop, initiera och genom stöd och uppföljning utveckla säkerhetsarbetet.
- Säkerhetsarbetet skall bedrivas med utgångspunkt från kontinuerliga riskanalyser och med tyngdpunkt på förebyggande aktiviteter.
- Varje verksamhet ska planera och öva för hur kritiska funktioner kan upprätthållas och fungera vid allvarliga störningar, så kallad krisberedskapsplanering.
- Organisation, delegation, beslut, planer och åtgärder beträffande säkerhetsarbetet ska dokumenteras.
- Alla medarbetare ska fortlöpande ges utbildning i förhållande till sitt ansvar och sina arbetsuppgifter för att förstå hur säkerhetsarbetet fungerar.
- Alla medarbetare ska aktivt arbeta för ökad säkerhet och ta ett ansvar för att säkerheten fungerar samt informera om upptäckta brister.
- Förvaltnings-/ Bolagsledning ska säkerställa att externa parter såsom entreprenörer, inhyrd personal, konsulter och leverantörer uppfyller och följer relevanta delar inom säkerhetsområdet.
- Policyn konkretiseras i underliggande riktlinjer och regler.

[1] Med riskhantering avses de samordnande aktiviteter som genomförs för identifiering, analys, utvärdering, behandling, övervakning och granskning av risker.
[2] Respektive förvaltning/bolag beslutar titel utifrån sin organisations struktur och tjänste nomenklatur.

Göteborgs Stad

Dokumentansvarig: Chef Samhällsskydd och Beredskap Upprättad av: Informationssäkerhetschef
Beslutad av: Kommunfullmäktige
Gäller för: Anställda och förtroendevalda i Göteborgs Stads förvaltningar, bolag, anknutna stiftelser och inhyrda entreprenörer.
Senast uppdaterad: 2013 - 08-05
Giltighetstid: Tills vidare

Riktlinje för informationssäkerhet

1 Inledning

Med informationssäkerhet avses att upprätthålla:

- Konfidentialitet, informationstillgångar är tillgängliga endast för behöriga
- Riktighet, informationstillgångar förändras eller påverkas inte oönskat eller utom kontroll
- Tillgänglighet, informationstillgångar kan nyttjas efter behov i förväntad utsträckning och inom önskad tid

Med informationstillgångar avses all information och informationshanterande resurser såsom manuella och IT-baserade informationssystem.

2 Syfte

Denna riktlinje syftar till att konkretisera säkerhetspolicyn avseende informationssäkerhetsområdet. Riktlinjen beskriver den grundsäkerhetsnivå som gäller för all informationshantering i Göteborgs Stad som blivit klassad i nivå 1 för ett eller flera av skyddsområdena konfidentialitet, riktighet eller tillgänglighet.

För informationshantering som har ett utökat skyddsbehov (nivå 2) ska kompletterande åtgärder införas. Dessa skyddsåtgärder utformas specifikt och tas ej upp i denna riktlinje.

För information som klassats i nivå 0 avseende alla de tre skyddsområdena konfidentialitet, riktighet eller tillgänglighet finns inga stadsövergripande krav på skyddsåtgärder.

3 Klassning av information

- Informationsklassning ska göras kontinuerligt av informationsägaren
- Informationslassningen ska ligga till grund för hur informationen ska hanteras i verksamheten
- Informationsklassningen skall utformas så att tillgången till information och öppenheten inom stadens verksamheter förblir så stor som möjligt för intressenter och allmänhet
- Tillämpliga lagar och andra giltiga styrdokument skall alltid uppfyllas och vägas in i informationsklassningen
- Nedanstående modell ska användas vid informationsklassningen

Kravnivå		Konfidentialitet	Riktighet	Tillgänglighet
Nivå 2	**Klassningsaspekt**	Känslig information som kan medföra **allvarlig skada** för egen eller annan organisations verksamhet eller för enskild person om den röjs för obehörig	Information som kan medföra **allvarlig skada** för egen eller annan organisations verksamhet eller för enskild person om den är felaktig.	Information som ingår i eller stöder kontinuerlig och kritisk verksamhet där avbrott innebär att man inte kan upprätthålla nödvändig tillgänglighet och servicenivå. Avbrott kan medföra **allvarlig skada** för egen eller annan organisations verksamhet eller för enskild person
Nivå 1 **GRUNDSÄKERHETSNIVÅ**	**Klassningsaspekt**	Information som kan medföra **skada** för egen eller annan organisations verksamhet eller för enskild person om den röjs för obehörig	Information som kan medföra **skada** för egen eller annan organisations verksamhet eller för enskild person om den är felaktig	Information som ingår i eller stöder kontinuerlig verksamhet där avbrott kan medföra **skada** för egen eller annan organisations verksamhet eller för enskild person
Nivå 0	**Klassningsaspekt**	Information som är öppen och avsedd för eller kan spridas till en obestämd krets mottagare utan risk för negativa konsekvenser. Spridning medför **ingen skada.**	Information som kan förändras utan risk för negativa konsekvenser Oriktig information medför försumbar eller **ingen skada**	Information med lågt verksamhetsberoende. Kan vara otillgänglig en längre tid utan risk för negativa konsekvenser. Brist på åtkomst medför försumbar eller **ingen skada.**

4 Hantering av informationstillgångar

- Samtliga informationssystem ska finnas förtecknade. I förteckningen beskrivs ändamål samt ansvarsfördelning såsom informationsägare, systemägare etc
- Tillämpliga regler, lagar, avtalsrättsliga åtaganden etc ska klart och tydligt definieras och dokumenteras för respektive informationssystem
- Informationsägaren ansvarar för informationsklassningen och att erforderligt skydd införs samt att säkerheten uppfyller ställda och rättsliga krav
- Alla som hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten

5 Personalresurser och säkerhet

- Kraven som ställs på personer som ska få tillgång till information och informationssystem ska vara definierade
- Det ska finnas användarinstruktion för respektive informationssystem
- Användarinstruktionen ska utformas på ett sådant sätt att en användares behov av att sätta sig in i detaljer kring gällande lagstiftning/regler för informationssystemet minimeras

6 Fysisk och miljörelaterad säkerhet

- Tillträde till lokaler som behöver skyddas mot obehörigt tillträde ska regleras och styras utifrån de krav som ställs av vederbörandes arbetssituation

-
- För säkerställande av centrala utrymmen med IT-baserade informationssystem, såsom datorhallar, ska
    - det fysiska skyddet ska vara entydigt definierat och dokumenterat där dokumentationen är skyddad från åtkomst av obehöriga
    - vara försett med ett skalskydd som är motståndskraftigt mot forcering och som är i nivå med skyddsklass 3 enligt Svenska Stöldskyddsföreningen
    - tillträde regleras restriktivt och strikt styras utifrån de krav som ställs av vederbörandes arbetssituation
    - det finnas dokumenterade besöksrutiner som inkluderar säkerställd besökslogg
    - besökare lätt kunna identifieras
    - besökare övervakas av behörig personal
    - larm med larmmottagare finnas för inbrott, brand, temperatur och fukt
    - systematiskt brandskyddsarbete enligt statens Räddningsverks allmänna råd bedrivas

7 Styrning av kommunikation och drift

- Det ska finnas en formellt beslutad driftdokumentation för IT-baserade informationssystem som minst omfattar återstarts- och återställningsrutiner, incidenthantering, ändringshantering samt hantering av logginformation. Ansvar gällande drift inkl system- och säkerhetsadministration ska också vara tydliggjort
- Loggning och skapande av spårbarhet för viktiga och säkerhetskritiska händelser ska ske. Loggning och loggarna ska skyddas för obehöriga samt vid behov analyseras och kunna nyttjas vid incidentutredningar
- Det ska för IT-baserade informationssystem finnas upptäckts- och skyddsåtgärder mot oönskad programkod och obehörigt nyttjande

8 Styrning av åtkomst

- Åtkomst och behörighet till informationstillgångar ska ges restriktivt och strikt styras utifrån de krav som ställs av vederbörandes arbetssituation
- Ansvarsfördelning och uppdelning av arbetsuppgifter ska tillämpas så att risken för missbruk begränsas
- För IT-baserade informationssystem ska endast ett fåtal personer erhålla privilegierade behörighet samt åtkomst till källprogramarkiv, operativsystem, systemhjälpmedel och revisionshjälpmedel
- Regelverk och rutin för registrering och avregistrering av behörigheter och åtkomst samt tilldelning av lösenord för IT-baserade informationssystem ska dokumenteras och finnas formellt beslutad
- Autentisering och åtkomstkontroll till IT-baserade informationssystem (gäller ej för öppen information) ska baseras på minst lösenord och bygga på unika användaridentiteter som är personliga och som ej får delas med andra
- Det ska finnas dokumenterade regler för vad som är tillåtet för anslutningar mellan IT-baserade informationssystem

9 Anskaffning, utveckling och underhåll

- Säkerhetsaspekter ska beaktas vid utveckling och anskaffning av informationssystem så att tillräckligt skydd uppnås. Att säkerhetsrutiner och regelverk efterlevs och motsvarar verksamhetens krav under informationssystemets hela livscykel inklusive avveckling och destruktion ska säkerställas och följas upp regelbundet
- System-/programutveckling och tester av modifierade IT-baserade informationssystem ska ske åtskilt från driftmiljön
- Det ska finnas formellt beslutade rutiner för ändringshantering för att inte åsidosätta befintliga skyddsåtgärder samt för att skapa ändringshistorik
- Det ska finnas regler för hur system- och programutveckling ska genomföras samt för installation av programvaror i IT-baserade informationssystem som är i drift
- Upphovsrättsliga frågor ska vara reglerade i avtal
- All systemdokumentation ska i rimlig omfattning och grad vara fullständig och aktuell samt uppdateras vid förändringar i informationssystem. Systemdokumentationen ska minst omfatta vad informationssystemets olika delar består av, en övergripande beskrivning av de olika delarnas uppgift samt en dokumentation över de funktioner som är relevanta för säkerheten
- IT-baserade informationssystem ska regelbundet analyseras för att identifiera sårbarheter eller problem som eventuellt kan orsaka incidenter

10 Hantering av incidenter

- Det ska finnas en formell fastlagd rutin för hur informationssystemets användare ska agera vid incidenter
- Det ska finnas rutiner för rapportering, loggning, åtgärdande, informationsspridning, eskalering, uppföljning och analys av incidenter

11 Kontinuitetsplanering i verksamheten

- Det ska finnas formella beslut gällande den längsta tid som information kan vara otillgänglig eller informationssystemet bedöms kunna vara ur funktion innan verksamheten påverkas i oacceptabel omfattning. Till grund för beslut ligger resultat från genomförda riskanalyser
- Grundat på verksamhetskraven ska det finnas en dokumenterad och formellt beslutad kontinuitetsplan. Övervägande om det finns behov av katastrofplanering ska ske
- Kontinuitetsplaner som inkluderar IT-baserade informationssystem ska omfatta återstarts- och reservrutiner för driftverksamheten som vidtas inom ramen för ordinarie drift så att återstart kan ske inom fastställd tid
- Återstarts- och reservrutiner för IT-baserade informationssystem såsom säkerhetskopiering och återläsning ska finnas och vara dokumenterade samt verifierade och anpassade för aktuell verksamhet
- Kontinuitetsplanen ska hållas aktuell och helt eller delvis testas årligen samt finnas tillgänglig för berörda i händelse av avbrott

12 Uppföljning av säkerhetsnivå

- Verksamhetens ledning ska kontinuerligt följa upp att säkerhetsnivån är acceptabel
- Uppföljning av informationssäkerhetsnivån i form av intern kontroll ska ske minst årligen. Resultatet rapporteras till nämnd/styrelse

13 Informationsspridning och uppföljning av efterlevnad

- Alla förtroendevalda och anställda inom Göteborgs Stad ska ha tillräckliga kunskaper om informationssäkerhet i förhållande till sina arbetsuppgifter

- Varje förvaltning, bolag och stiftelse där Göteborgs Stad är förvaltare eller utser majoriteten av styrelsen ansvarar för att denna riktlinje efterlevs

14 Definitioner

Nedan återfinns definitioner på begrepp som tillämpas i denna riktlinje.

Begrepp	Definition
Autentisering	Verifiering av uppgiven identitet.
Identitet	Unik beteckning för en viss individ eller ett visst föremål
Incident	Händelse som resulterat eller som kunnat resultera i en skada eller oönskade konsekvenser för verksamheten
Informationssystem	Rutiner, metoder, procedurer etc organiserade för behandling av information, såväl manuella som helt eller delvis IT-baserade
Informationssäkerhet	Säkerhet beträffande informationstillgångar rörande förmågan att bevara och upprätthålla konfidentialitet, riktighet och tillgänglighet.
Informationstillgång	All information och informationshanterande resurser såsom manuella och IT-baserade informationssystem
Informationsägare	Generellt den som bestämmer ändamålen med och medlen för behandling och hantering av informationen. Ansvaret för informationen och dess säkerhet följer med ansvaret för verksamheten.
Kontinuitetsplan	Beskriver hur verksamheten ska bedrivas när kritiska verksamhetsprocesser allvarligt påverkas under en längre tid.
Logg	Insamlad information om händelser som sker/utförs
Lösenord	Teckensträng som anges för att verifiera en identitet
Revisionshjälpmedel	System, program, funktioner etc som kan användas för att identifiera brister och/eller tydliggöra uppfyllelse av krav, regelverk, standarder etc
Skalskydd	Skyddet som finns för den omslutningsyta, såsom väggar, golv, tak, dörrar etc, som avgränsar en lokal från omvärlden
Skyddsåtgärd	Handling, procedur eller tekniskt arrangemang som, genom att minska sårbarheten möter identifierat hot.
Spårbarhet	Möjlighet att entydigt kunna härleda utförda aktiviteter i systemet till en identifierad användare.

Göteborgs Stad

Dokumentansvarig: Chef Samhällsskydd och Beredskap Upprättad av: Samhällsskydd och Beredskap
Beslutad av: Kommunfullmäktige
Gäller för: Anställda och förtroendevalda i Göteborgs Stads förvaltningar, bolag, anknutna stiftelser och inhyrda entreprenörer.
Senast uppdaterad: 2013 – 08-05
Giltighetstid: Tills vidare

Riktlinje för systematiskt brandskyddsarbetet – SBA

Denna riktlinje syftar till att konkretisera säkerhetspolicyn ur ett brandskyddsperspektiv

1 Inledning

Ett bra brandskydd är en vital del i skyddet för person, egendom och miljö. För att uppfylla lagens krav anser Göteborgs Stad att fastighetsägare och nyttjanderättshavare ska bedriva ett systematiskt brandskyddsarbete, fortsatt förkortat SBA. Syftet med att systematiskt arbeta med brandskydd är att skapa en allmän medvetenhet hos anställda och förtroendevalda om de risker och de skyddsanordningar som finns. Det handlar också om att skapa förståelse för helheten kring SBA och hur det fungerar.
Göteborgs stad, som ägare och nyttjare av fastigheter, måste systematiskt arbeta med brandskyddsfrågor för att förhindra att människor skadas, egendom förstörs och att miljön tar skada.
SBA handlar om alla former av brandskydd - från den enskildes och organisationens kunskap och kompetens till brandtekniska installationer.
Utgångspunkten för säkerhetsarbetet i Göteborgs Stad är stadens gemensamma säkerhetspolicy. Dessa riktlinjer utgör ett komplement och ett förtydligande inom området SBA. Brandskyddsansvaret följer linjeorganisationen.
Högst styrande för detta område ska Lagen om skydd mot olyckor med föreskrifter vara.

Följande regelverk ska stadens verksamheter beakta inom området SBA:

- Lag (2003:778) om skydd mot olyckor.
- Förordning (2003:789) om skydd mot olyckor.
- MSB:s allmänna råd SRVFS 2004:3, SRVFS 2004:4, SRVFS 2007:1
- Göteborgs Stads säkerhetspolicy.
- Försäkringskrav från aktuell försäkringsgivare.

2 Syfte

Det övergripande målet är att staden ska ha ett SBA som lägst motsvarar de krav som lagstiftaren ställer. Målet är att skapa en trygg miljö för alla, för allmänheten och för verksamma i kommunens lokaler, samt ett gott brandskyddsarbete som också ger en god helhetsbild kring stadens samlade SBA. För att detta ska vara möjligt finns denna riktlinje som klargör stadens intentioner när det gäller SBA utifrån lagstiftning och stadens säkerhetspolicy. Syftet är att:

- SBA i stadens förvaltningar och bolag ska ske enligt likformiga principer.
- Underlätta för förvaltningar och bolag att veta vad som ska beskrivas i deras olika verksamheter och fastigheters SBA.
- Säkerställa uppföljning och kontroll av SBA i staden.

Riktlinje

Alla de byggnader som staden äger, förvaltar eller bedriver verksamhet i ska ha ett dokumenterat SBA.

Det ska finnas en överenskommelse som reglerar ansvaret mellan ägare/förvaltare och nyttjanderättshavare för samtliga byggnader som staden äger, förvaltar eller bedriver verksamhet i.
Dessa aktörer ska ha en kontinuerlig samverkan kring brandskyddet.

SBA grundas på helhetsbilden av byggnadens utformning, verksamheten, organisationen, brandtekniska installationer och riskbilden för respektive byggnad eller verksamhet. Dokumentationen ska vara tillräckligt omfattande för att säkerställa att skäliga brandskyddsåtgärder vidtas och hålls funktionsdugliga.

Alla verksamheter eller byggnader kräver därför inte lika omfattande SBA. I en verksamhet med få anställda i en mindre byggnad, utan särskilda krav på tekniska eller organisatoriska brandskyddsåtgärder, kan sannolikt information och kunskap enkelt förmedlas. Då kan den skriftliga dokumentationen begränsas i omfattning.

Göteborgs Stad delar in omfattningen av SBA i tre nivåer. Under respektive nivå finns en generell förklaring till vilka verksamheter och byggnader som inkluderas.

Grundläggande nivå omfattar

Här ingår byggnader eller verksamheter med öppna ytor som går att överblicka, med låg riskbild. Lokalerna ska enkelt och snabbt kunna utrymmas vid fara.

Mellannivå omfattar

Här ingår byggnader eller verksamheter med lokaler och ytor som kan vara svåra att överblicka och utrymma. Verksamheten eller byggnadens brandskydd kräver speciellt underhåll. Personer som vistas i lokalerna kan ha dålig lokalkännedom och kan därför behöva hjälp att hitta vid en snabb utrymning.

Hög nivå omfattar

Här ingår större och mer komplexa byggnader och verksamheter som omfattar många personer. Här ingår också objekt som omfattas av krav på skriftlig redogörelse. Nivån omfattar även verksamheter med personer som sover och/eller har besökare som har dålig lokalkännedom. Personer som vistas i lokalerna kan behöva hjälp att utrymma. En ökad riskbild ökar kravet på djup och detaljer i byggnadsbeskrivning och organisation.

Uppgift som ska beskrivas i SBA-arbetet
Organisation
Varje verksamhet ska ha en brandskyddsorganisation som tydliggör ansvaret för verksamhetens brandskydd.
Personer i brandskyddsorganisation ska ha den kunskap som krävs för att fullgöra sina uppgifter.
Det ska finnas en utrymningsorganisation som beskriver roller, genomförande och återsamlingsplats.
Verksamhetens brandskydds- och utrymningsorganisation ska vara känd av samtliga anställda.
Verksamhetsbeskrivning
Verksamheten ska kortfattat beskriva vilken typ av verksamhet som bedrivs i byggnaderna. Här ska också anges antalet anställda, individer i verksamhet och besökare.
Riskanalys
Verksamheten ska ha kännedom om de brandrisker som finns
Verksamheten ska ha en dokumenterad riskanalys över verksamheten och i sin dokumentation beskriva: • De risker som kan orsaka brand • De risker som uppstår vid en brand • Vilka konsekvenser det medför för verksamheten • För varje identifierad risk, föreslå åtgärder för att minska sannolikhet och konsekvens
Utbildning och övning
Alla anställda ska ha tillräckliga kunskaper om det systematiska brandskyddsarbetet i förhållande till sina arbetsuppgifter.
Alla anställda ska ha kunskaper om vad de kan göra för att minimera risken för ett brandtillbud.
Alla anställda ska ha grundläggande kunskaper om hur de ska agera vid ett brandtillbud.
Övningar ska genomföras kontinuerligt i för verksamheten i skälig omfattning, efter fastställd plan.
En utbildningsplan ska upprättas som innehåller vilken typ av utbildning som ges, när och hur ofta utbildningarna sker.
Byggnads- och tekniskbeskrivning
Varje byggnad med brandtekniska installationer ska beskrivas när det gäller installationernas utförande och funktion, hur dessa används vid brandtillbud samt hur de kontrolleras.
Varje byggnad ska ha uppdaterade ritningar där brandcellsgränser och övrigt brandskydd är dokumenterat. Exempel på brandskydd är brandgasventilaion, utrymningsskyltar och släckutrustning. Vid förändring i byggnadens konstruktion eller utformning ska ritningar uppdateras och det ska säkerställas att brandcellsgränser är intakta.
Det ska finnas skriftlig redogörelse för de objekt där lagen så kräver. Se SFS 2003:789.
Egenkontroll och uppföljning
Verksamheterna ska skriftligen och kontinuerligt dokumentera sin egenkontroll. Dokumentationen ska visa vad som är kontrollerat, vad resultatet blev, när det kontrollerades samt när åtgärd vidtagits
Verksamheten ska följa upp att samtliga anställda har kännedom om SBA i den egna verksamheten.
Verksamheten ska en gång om året rapportera in egenkontrollen utifrån de ovan givna områdena till organisationens säkerhetschef eller motsvarande.

Förvaltning/bolag ska en gång om året göra en sammanställning av enheternas SBA och presentera för nämnd/styrelse.
Verksamheten ska årligen revidera sin riskanalys och åtgärda de eventuella brister som framkommer.

3 Informationsspridning och uppföljning

Alla förtroendevalda och anställda inom Göteborgs Stad ska ha kunskap om det systematiska brandskyddsarbetet i förhållande till sina arbetsuppgifter.

Denna riktlinje ska finnas tillgänglig i stadens *författningssamling.*

Varje förvaltning, bolag och anknuten stiftelse ansvarar för att riktlinjerna efterlevs och ska en gång om året rapportera status på det systematiska brandskyddsarbetet till nämnd/styrelse.

Ansvaret för arbetet och uppföljningen av säkerheten och säkerhetsarbetet beskrivs i Göteborgs Stads säkerhetspolicy som även inkluderar det systematiska brandskyddsarbetet.