§ 218 Dnr KS 2021/00122-1.3.2

Beslut - Policy för informationssäkerhet för Västerås stad

Beslut

Förslag till kommunfullmäktige:

1. Policy för informationssäkerhet för Västerås stad antas.

2. Policyn ersätter informationssäkerhetspolicy 2011, dnr KS 2011/00635 antagen av kommunfullmäktige den 1 december 2011.

Kommunstyrelsen för egen del:

3. Följande styrdokument upphävs:

Riktlinje för informationssäkerhet KS 2019/01627

Riktlinje för anskaffning av IT-stöd KS 2013/719-KS-004

Basnivå för informationssäkerhet KS 2014/1021-KS-004

Basnivå för IT-säkerhet KS 2015/321-KS-160

Instruktion – anskaffning, utveckling och underhåll av informationssystem KS 2014/1026-KS-004

Instruktion – Åtkomst till system och nätverk KS 2014/1022-KS-004

Instruktion – Logghantering och spårbarhet KS 2014/1023-KS-004

Instruktion – Hantering av skyddade personuppgifter KS 2016/169-KS-009

Ärendebeskrivning

Information är en av de viktigaste tillgångarna för Västerås stad. Det är via informationshantering i olika processer som Västerås stad styrs och utvecklas. Om informationen i processerna inte finns tillgänglig eller förändrats så att den blivit felaktig kan det få mycket allvarliga följder för Västerås stad. Stadens information behöver därför skyddas av tre skäl:

1. Information kan ha behov av åtkomstskydd som innebär att endast behöriga personer kan ta del av den (konfidentialitet).

2. Informationen ska vara korrekt så att vi kan lita på den. Den ska skyddas från manipulation och skadegörelse (riktighet).

3. Informationen ska alltid finnas tillgänglig när den behövs (tillgänglighet).

Skyddet behöver anpassas efter behov så att skyddet är tillräckligt i förhållande till riskbild och kostnader. Skyddet ska varken vara otillräckligt eller för omfattande. Det kan leda till onödiga kostnader. Därför måste informationsklassning och analyser göras av den information som vi använder och de system och tjänster som bär den. Bristande skydd kan leda till stora konsekvenser i verksamheterna för de tjänster som Västerås stad tillhandahåller.

Det övergripande målet med Västerås stads informationssäkerhet är att säkerställa ett tillräckligt skydd av de informationstillgångar som Västerås stad, dess bolag och kommunalförbund förvaltar och förfogar över. Rätt information ska vara tillgänglig för rätt person i rätt tid på ett spårbart sätt, såväl i fredstid som vid höjd beredskap.

En god informationssäkerhet ger förtroende för Västerås stads verksamheter, håller ner direkta och indirekta kostnader samt minskar risken för rättsliga processer. Informationssäkerhet innebär att systematiskt skydda stadens verksamheter mot avbrott och minimering av risken för att stadens information används på ett felaktigt sätt. Brister i informationen kan leda till ett försämrat förtroende för Västerås stads tjänster. Allvarliga eller upprepande störningar kan utvecklas till kriser.

Arbetet med informationssäkerhet ska vara en naturlig del av Västerås stad och dess verksamheter. Genom Policy för informationssäkerhet samt underliggande styrdokument fastställs ansvarsområden för nämnder och styrelser och helägda bolag.

Stadsledningskontoret har till kommunstyrelsen lämnat följande förslag till beslut:

Förslag till kommunfullmäktige:

1. Policy för informationssäkerhet för Västerås stad antas.

2. Policyn ersätter informationssäkerhetspolicy 2011, dnr KS 2011/00635 antagen av kommunfullmäktige den 1 december 2011.

Kommunstyrelsen för egen del:

3. Följande styrdokument upphävs:

Riktlinje för informationssäkerhet KS 2019/01627

Riktlinje för anskaffning av IT-stöd KS 2013/719-KS-004

Basnivå för informationssäkerhet KS 2014/1021-KS-004

Basnivå för IT-säkerhet KS 2015/321-KS-160

Instruktion – anskaffning, utveckling och underhåll av informationssystem KS 2014/1026-KS-004

Instruktion – Åtkomst till system och nätverk KS 2014/1022-KS-004

Instruktion – Logghantering och spårbarhet KS 2014/1023-KS-004

Instruktion – Hantering av skyddade personuppgifter KS 2016/169-KS-009

Proposition

Ordföranden finner att det enbart finns ett förslag till beslut, stadsledningskontorets förslag, och att kommunstyrelsen beslutar i enlighet med detta.

Kopia till

Samtliga nämnder, styrelser och kommunala bolag och förbund

Kommunstyrelsen
Andreas Weiborn
Epost: andreas.weiborn@vasteras.se

Kommunstyrelsen

Kopia till
Samtliga nämnder, styrelser och kommunala bolag och förbund

Tjänsteutlåtande - Policy för informationssäkerhet för Västerås stad

Förslag till beslut

Förslag till kommunfullmäktige:

1. Policy för informationssäkerhet för Västerås stad antas.

2. Policyn ersätter informationssäkerhetspolicy 2011, dnr KS 2011/00635 antagen av kommunfullmäktige den 1 december 2011.

Kommunstyrelsen för egen del:

3. Följande styrdokument upphävs:

Riktlinje för informationssäkerhet KS 2019/01627

Riktlinje för anskaffning av IT-stöd KS 2013/719-KS-004

Basnivå för informationssäkerhet KS 2014/1021-KS-004

Basnivå för IT-säkerhet KS 2015/321-KS-160

Instruktion – anskaffning, utveckling och underhåll av informationssystem KS 2014/1026-KS-004

Instruktion – Åtkomst till system och nätverk KS 2014/1022-KS-004

Instruktion – Logghantering och spårbarhet KS 2014/1023-KS-004

Instruktion – Hantering av skyddade personuppgifter KS 2016/169-KS-009

Ärendebeskrivning

Information är en av de viktigaste tillgångarna för Västerås stad. Det är via informationshantering i olika processer som Västerås stad styrs och utvecklas. Om informationen i processerna inte finns tillgänglig eller förändrats så att den blivit felaktig kan det få mycket allvarliga följder för Västerås stad. Stadens information behöver därför skyddas av tre skäl:

1. Information kan ha behov av åtkomstskydd som innebär att endast behöriga personer kan ta del av den (konfidentialitet).

2. Informationen ska vara korrekt så att vi kan lita på den. Den ska skyddas från manipulation och skadegörelse (riktighet).

3. Informationen ska alltid finnas tillgänglig när den behövs (tillgänglighet).

Skyddet behöver anpassas efter behov så att skyddet är tillräckligt i förhållande till riskbild och kostnader. Skyddet ska varken vara otillräckligt eller för omfattande. Det kan leda till onödiga kostnader. Därför måste informationsklassning och analyser göras av den information som vi

använder och de system och tjänster som bär den. Bristande skydd kan leda till stora konsekvenser i verksamheterna för de tjänster som Västerås stad tillhandahåller.

Det övergripande målet med Västerås stads informationssäkerhet är att säkerställa ett tillräckligt skydd av de informationstillgångar som Västerås stad, dess bolag och kommunalförbund förvaltar och förfogar över. Rätt information ska vara tillgänglig för rätt person i rätt tid på ett spårbart sätt, såväl i fredstid som vid höjd beredskap.

En god informationssäkerhet ger förtroende för Västerås stads verksamheter, håller ner direkta och indirekta kostnader samt minskar risken för rättsliga processer. Informationssäkerhet innebär att systematiskt skydda stadens verksamheter mot avbrott och minimering av risken för att stadens information används på ett felaktigt sätt. Brister i informationen kan leda till ett försämrat förtroende för Västerås stads tjänster. Allvarliga eller upprepande störningar kan utvecklas till kriser.

Arbetet med informationssäkerhet ska vara en naturlig del av Västerås stad och dess verksamheter. Genom Policy för informationssäkerhet samt underliggande styrdokument fastställs ansvarsområden för nämnder och styrelser och helägda bolag.

Stadsledningskontoret har till kommunstyrelsen lämnat följande förslag till beslut:

Förslag till kommunfullmäktige:

1. Policy för informationssäkerhet för Västerås stad antas.

2. Policyn ersätter informationssäkerhetspolicy 2011, dnr KS 2011/00635 antagen av kommunfullmäktige den 1 december 2011.

Kommunstyrelsen för egen del:

3. Följande styrdokument upphävs:

Riktlinje för informationssäkerhet KS 2019/01627

Riktlinje för anskaffning av IT-stöd KS 2013/719-KS-004

Basnivå för informationssäkerhet KS 2014/1021-KS-004

Basnivå för IT-säkerhet KS 2015/321-KS-160

Instruktion – anskaffning, utveckling och underhåll av informationssystem KS 2014/1026-KS-004

Instruktion – Åtkomst till system och nätverk KS 2014/1022-KS-004

Instruktion – Logghantering och spårbarhet KS 2014/1023-KS-004

Instruktion – Hantering av skyddade personuppgifter KS 2016/169-KS-009

Beslutsmotivering

Västerås stad har inom området för informationssäkerhet haft flertalet styrdokument över tid. Staden antog sin första informationssäkerhetspolicy år 2011. Därutöver har det funnits otaliga styrdokument inom området. Under de år som förflutit har Västerås stad blivit alltmer beroende av digitala arbetssätt och tillgång till korrekt och säker information.

Stadsledningskontorets intention är att göra ett omtag på området. Staden behöver nya styrdokument som ligger i linje med den digitalisering som pågår och som pekar ut bra förhållningssätt och metoder för att riskminimera.

Genom att förtydliga ansvar inom området informationssäkerhet bedömer stadsledningskontoret att det kommer att bidra till:

- Ökad kännedom om risker och hot mot nämndernas och bolagens informationssystem.
- Ökad medvetenhet hos den högsta ledningen i nämnder och bolag.
- Tydliga roller inom stadens arbete med informationssäkerhet, dataskydd och säkerhetsskydd.

Vidare föreslås det att kommunstyrelsen årligen ska följa upp arbetet med informationssäkerhet. Uppföljningen kommer att göras i samband med uppföljningen av stadens arbete med skydd och beredskap i enlighet med program för skydd och beredskap.

Program för digital förnyelse syftar till ökad digitalisering. Ökad digitalisering leder till en enklare vardag för medborgare, en öppnare förvaltning som stödjer innovation och delaktighet samt en högre kvalitet och effektivitet i verksamhetsprocesserna. Den ökade digitaliseringen i staden ska även leda till bättre utnyttjande av digital information vilket kräver en medveten hantering och användning där informations-säkerhetsrisker beaktas och i möjligaste mån elimineras.

Program för digital förnyelse följer regeringens vision om ett hållbart digitaliserat Sverige för att skapa mesta möjliga samhällsnytta. Det digitaliserade samhället ska inkludera alla. Fler ska kunna vara delaktiga genom att skapa och dra nytta av snabbare beslutsprocesser genom robotisering och molntjänster. Verksamhetsprocesserna blir billigare genom att de används av flera kommuner och genom sakernas Internet (IoT) som exempelvis bidrar med teknisk styrning av gatubelysning och information om lediga parkeringsplatser eller nära vård för vårdtagare i hemmet.

Den information/data som skapas i stadens processer behöver skyddas och övervakas på nya sätt eftersom informationen används på nya platser. Informationsutbytet mellan stadens nämnder och bolag förväntas öka under det kommande decenniet och kräver därför ny styrning för att risker inte ska uppstå eller att informationshanteringen suboptimeras. Därför behöver staden anta nya styrdokument i form av inledningsvis en förnyad policy för informationssäkerhet som i sin tur pekar ut underliggande styrdokument.

Juridisk bedömning

Kommunstyrelsen är behörig att fatta beslut i enlighet med kommunstyrelsens reglemente och kommunallagen.

Ekonomisk bedömning

Förslaget förväntas att medföra kostnader för styrelsen och nämnderna i form av informationssäkerhetsåtgärder. Samtidigt förväntas informationssäkerhetsåtgärderna medföra skydd av informationstillgångar och minimera risken för skador och hot. Därigenom kan oönskade

ekonomiska kostnader komma att undvikas eller reduceras. Kostnaderna förväntas dock att hanteras inom ramen för ordinarie budgetprocesser och systemobjektet i enlighet med ledningssystem för informationssäkerhet.

Hållbar utveckling

Arbetet med informationssäkerhet träffar flera områden enligt de globala hållbarhetsmålen. De mest centrala målen redovisas här nedan.

- Mål 9: Hållbar industri, innovationer och infrastruktur.
  - Delmål 9.1: Skapa hållbara, motståndskraftiga och inkluderande infrastrukturer.
- Mål 16: Fredliga och inkluderande samhällen.
  - Delmål 16.10: Säkerställa allmän tillgång till information och skydda de grundläggande friheterna.

Helene Öhrling	Carina Dahlström
Stadsdirektör	Tf Administrativ chef

Program
Policy
Handlingsplan
Riktlinje

Policy för informationssäkerhet för Västerås stad och helägda bolag

Antagen av kommunfullmäktige 2023-XX-XX

DNR: KS-2021/00122

VÄSTERÅS STAD

Innehållsförteckning

Program	uttrycker värdegrunder och förhållningssätt för arbetet med utvecklingen av Västerås som ort inklusive koncernen Västerås stad
Policy	uttrycker värdegrunder och förhållningssätt för arbetet i koncernen Västerås stad
Handlingsplan	anger strategier och konkreta åtgärder för att nå den politiska viljeinriktningen och fastställda mål på olika nivåer i organisationen
Riktlinje	säkerställer ett riktigt agerande och en god kvalitet i handläggning och utförande i koncernen Västerås stad

Inledning

Information är en av de viktigaste tillgångarna i koncernen Västerås stad. Information som används måste därför hanteras på ett säkert sätt och skyddas mot oavsiktlig spridning, såväl i fredstid som vid höjd beredskap. En god informationssäkerhet ger förtroende för Västerås stads verksamheter, håller ner direkta och indirekta kostnader samt minskar risken för rättsliga processer.

I regeringens nationella strategi för samhällets informations- och cybersäkerhet så är en av målsättningarna att ”Statliga myndigheter, kommuner, landsting, företag och andra organisationer ska ha kännedom om hot och risker, ta ansvar för sin informationssäkerhet och bedriva ett systematiskt informationssäkerhetsarbete”.

Genom att Västerås stad säkerställer en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet, ökar Västerås stads förmåga att förebygga, upptäcka och hantera cyberattacker och andra IT-incidenter, så att säkerheten i nätverk, produkter och system höjs.

FN:s globala mål

År 2015 antog FN Agenda 2030 – 17 globala mål för en ekonomiskt, socialt och miljömässigt hållbar utveckling. Genom antagandet har världens ledare förbundit sig att uppnå mål som att avskaffa extrem fattigdom, minska ojämlikheter och orättvisor samt hantera klimatkrisen.

Policy för informationssäkerhet förhåller sig till de mål i Agenda 2030 som Västerås stads program för skydd och beredskap pekar ut. De mål i Agenda 2030 som främst berör Västerås stads policy för informationssäkerhet är:

- Mål 9: HÅLLBAR INDUSTRI, INNOVATIONER OCH INFRASTRUKTUR
    - Delmål 9.1: Skapa hållbara, motståndskraftiga och inkluderande infrastrukturer
- Mål 16: FREDLIGA OCH INKLUDERANDE SAMHÄLLEN
    - Delmål 16.10: Säkerställa allmän tillgång till information och skydda de grundläggande friheterna

Allas gemensamma ansvar

Informations- och cybersäkerhet genomsyrar i princip all verksamhet som inbegriper informationsbehandling i Västerås stad. Alla som hanterar informationstillgångar har ett ansvar för att upprätthålla god informationssäkerhet.

Alla chefer har ett ansvar för att på alla nivåer aktivt verka för att deras medarbetare har god kännedom om risker kring informationssäkerhet och hur de ska hantera incidenter. Berörda medarbetare ska regelbundet få den utbildning de behöver för att kunna upprätthålla säkerheten.

Alla som använder Västerås stads informationstillgångar är skyldiga att känna till och arbeta i enlighet med Västerås stads policyer, riktlinjer och rutiner. Var och en ska vara uppmärksam på och rapportera händelser som kan påverka säkerheten i Västerås stads informationstillgångar.

Säkerhetskultur

Informationssäkerhet är en central del i Västerås stads säkerhetskultur. Den som använder Västerås stads informationstillgångar på ett sätt som strider mot denna policy och Västerås stads ledningssystem för informationssäkerhet kan bli föremål för arbetsrättsliga åtgärder.

Övergripande mål

Det övergripande målet med Västerås stads informationssäkerhet är att säkerställa ett tillräckligt skydd av de informationstillgångar som Västerås stad och helägda bolag förvaltar och förfogar över. Rätt information ska vara tillgänglig för rätt person i rätt tid på ett spårbart sätt, såväl i fredstid som vid höjd beredskap.

Policyn beskriver mål och inriktning för arbetet med informations- och cybersäkerhet för Västerås stad i fredstid och under höjd beredskap. Policyn ska tillsammans med underliggande styrdokument och instruktioner ge verksamheten stöd för det operativa arbetet.

Policyn gäller för:

- nämnder och styrelser inom Västerås stad
- Stadens helägda bolag

- Policyn ger vägledning till:
- Kommunalförbund, delägda bolag och i vissa fall externa aktörer, exempelvis Västerås stads upphandlade leverantörer

Strategiska mål för informationssäkerheten

Utifrån Västerås stads övergripande mål för informationssäkerhet gäller följande undermål:

- Skydda strategiskt viktiga tillgångar
- Hantera efterlevnad och skyldigheter i lagar och avtal
- Ge invånare och medarbetare en tilltro till att Västerås stads informationstillgångar är tillräckligt skyddade
- Säkerställa att Västerås stads medarbetare har tillräcklig kunskap om risker kring informationssäkerhet
- Förbättra Västerås stads återhämtningsförmåga vid incidenter
- Skapa förutsättningar för verksamhetsutveckling genom säker och stabil digitalisering
- Upprätta en stabil och robust miljö för Västerås stads informationsbehandling
- Reducera kostnader för säkerhetsåtgärder

Utgångspunkter

Styrdokument

Denna policy för informationssäkerhet utgår från Västerås stads Program för skydd och beredskap samt Program för digital utveckling. Policyn ska tillämpas såväl i fredstid som vid höjd beredskap.

Lagar & förordningar

Lagar styr olika verksamhetsområden och ställer krav på Västerås stads informationssäkerhet. Arbetet med informationssäkerhet utgår framför allt från lagkrav, förordningar och föreskrifter i dessa rättsligadokument:

- Tryckfrihetsförordningen (1949:105)
- Offentlighets- och Sekretesslagen (2009:400)
- Arkivlagen (1990:782)
- Dataskyddsförordningen (2016:679)
- Dataskyddslagen (2018:218)
- Kamerabevakningslagen (2018:1200)
- Säkerhet i samhällsviktiga funktioner (NIS-direktivet 2018:1174)
- Säkerhetsskyddslagen (2018:585)
- Skyddslagen (2010:305)
- Lag om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap (2006:544)

Standarder

Västerås stads arbete med informationssäkerhet ska huvudsakligen utgå från ISO 27000-serien.

Säkerhetsskydd

Begreppet informationssäkerhet har i denna policy en bredare ansats jämfört med samma begrepp enligt säkerhetsskyddslagen. Säkerhetsskydd är en del av Västerås stads arbete med informationssäkerhet. Kraven på säkerhetsskyddet fastställs genom säkerhetsskyddets egna styrdokument.

Centrala begrepp

Informationssäkerhet:

Informationssäkerheten omfattar Västerås stads informationstillgångar utan undantag. Med det menas all information, digital eller analog, och oavsett om den behandlas manuellt eller automatiserat.

Som informationstillgångar räknas exempelvis:

- Information i databaser, filer, bilder och filmer
- Program som IT-system eller operativsystem
- Tjänster som kan finnas i ”molnet” eller ”appar” i en telefon
- Fysiska tillgångar som datorer, telefoner, nätverkskomponenter eller papper i arkiv eller pärmar

Aktörer, roller och ansvar

Politisk organisation

KOMMUNSTYRELSEN

Kommunstyrelsen leder och samordnar Västerås stads övergripande arbete med informationssäkerhet, interna säkerhetsfrågor, cybersäkerhet och upphandlingsprocesser. Styrelsen leder och samordnar även Västerås stads övergripande digitaliseringsarbete och tillhandahåller nämndgemensam teknisk infrastruktur, som datakommunikation, telefoni, IT-infrastruktur och användarnära tjänster (datorer, telefoner och dylikt).

Inom området för informationssäkerhet finns delvis också dataskyddets hantering av personuppgifter enligt dataskyddsförordningen och dataskyddslagen. Kommunstyrelsen är personuppgiftsansvarig för de behandlingar av personuppgifter som sker i styrelsens verksamhet. Styrelsen utser dataskyddsombud för sin egen verksamhet samt för nämnder och övriga styrelser inom kommunen.

NÄMNDER/STYRELSER/BOLAG

Ytterst ansvarig för säkerheten för den information som används/behandlas inom Västerås stad är den nämnd/styrelse och därmed den verksamhetschef eller medarbetare som äger informationstillgången där informationen huvudsakligen skapas, bearbetas och lagras.

Nämnder, styrelser och bolag ansvarar för att:

- följa och arbeta enligt Västerås stads ledningssystem för informationssäkerhet
- årligen genomföra en riskanalys av de egna informationstillgångarna
- årligen rapportera informationssäkerhetsarbetet till kommunstyrelsen
- årligen fastställa en aktivitetsplan för informationssäkerhet
- informationstillgångar är förtecknade med ägare och dokumenterade i Västerås stads stödsystem för hantering av IT-system och IT-tjänster.
- varje informationstillgång är klassificerad enligt Västerås stads ledningssystem för informationssäkerhet

Förvaltningsorganisation

STADSDIREKTÖREN

Stadsdirektören är enligt Västerås stads program för skydd och beredskap övergripande ansvarig för Västerås stads samlade arbete med skydd och beredskap. Det innebär att stadsdirektören är övergripande ansvarig för Västerås stads arbete med informationssäkerhet. Stadsdirektören ansvarar för att Västerås stad har ett ledningssystem för informationssäkerhet.

STADSLEDNINGSKONTORET
Stadsledningskontoret ansvarar för att fastställa och utforma riktlinjer och instruktioner för att underlätta och stödja det systematiska arbetet med informationssäkerhet. Stadsledningskontoret ansvarar därigenom för ledningen av samt att fastställa Västerås stads ledningssystem för informationssäkerhet.

Stadsledningskontoret ansvarar också för att det finns stödverktyg för dokumentation av informationstillgångar. Informations- och utbildningsinsatser om informationssäkerhetsarbetet ska kunna erbjudas i samtliga förvaltningar och helägda bolag.

Uppföljning

Kommunstyrelsen är ansvarig för att årligen följa upp att nämnder och helägda bolag efterlever denna policy samt underliggande styrdokument.

Revidering
Denna policy ska revideras av kommunfullmäktige, en gång per mandatperiod.