STYRDOKUMENT
I BOTKYRKA KOMMUN

Riktlinje för informations-säkerhet

Strategi
Program
Plan
Policy
Riktlinje
Regel

BOTKYRKA KOMMUN

Diarienummer: KS/2022:00464
Dokumentet är beslutat av: Kommunstyrelsen
Dokumentet beslutades den: 3 oktober 2022
Dokumentet gäller för: Samtliga nämnder och förvaltningar
Dokumentet gäller till den: Tills vidare

Dokumentansvarig är: Informationssäkerhetsansvarig
För revidering av dokumentet ansvarar: Informationssäkerhetsansvarig
För uppföljning av dokumentet ansvarar: Informationssäkerhetsansvarig
Relaterade dokument: Policy för informationssäkerhet

Innehåll

1. Inledning

Denna riktlinje syftar till att konkretisera policyn för informationssäkerhet.

Botkyrka kommun är beroende av att behandla information för att kunna utföra sitt uppdrag. En effektiv och säker behandling av information är en förutsättning både för verksamheten och för förtroendet från medborgare, medarbetare, leverantörer samt externa parter.
Information är ett omfattande begrepp som inkluderar allt från kunskap och information som enskilda medarbetare besitter till information som lagras och behandlas i olika informationssystem.
Informationssäkerhetsarbetet ska vara en integrerad del av verksamheten och informationsbehandlingen.
I arbetet med informationssäkerhet ska följande förutsättningar och krav säkerställas:

• **Konfidentialitet** – åtkomst till informationen ska begränsas utifrån behov.
• **Riktighet** - informationen ska vara tillförlitlig, korrekt och fullständig.
• **Tillgänglighet** - informationen ska kunna användas, efter behov, av rätt person med behörighet.

Samtliga anställda, interna och externa aktörer på Botkyrka kommun ska ha kännedom om relevanta regelverk kring informationssäkerhet samt följa dessa.
All information ska ha ett tilldelat ägandeskap och alla som hanterar informationstillgångar ansvarar för att informationssäkerheten upprätthålls enligt informationsägarens kravställning.
Var och en ska vara uppmärksam på och rapportera händelser som kan påverka säkerheten för våra informationstillgångar.

Denna riktlinje beskriver den grundsäkerhetsnivå som gäller för all informationsbehandling i Botkyrka kommun som blivit klassad i nivå 1 till 3 för ett eller flera av skyddsområdena konfidentialitet, riktighet eller tillgänglighet.
För information klassad i nivå 4, och därmed har ett utökat skyddsbehov, ska styrdokument för Säkerhetsskydd i stället gälla.

1.1 Efterlevnad

Kommunen ska säkerställa att överträdelser av lagar, författningar eller avtalsförpliktelser, samt andra säkerhetskrav inte sker.
Informationssäkerhetsansvarig inom kommunen ska följa upp att alla säkerhetsrutiner inom respektive ansvarsområde utförs korrekt för att uppnå efterlevnad av kommunens informationssäkerhetsregelverk.
System och delar i IT-miljö, nätverk och tillhörande infrastruktur ska regelbundet kontrolleras så att informationens konfidentialitet, riktighet och tillgänglighet upprätthålls. Alla åtgärder ska dokumenteras.

1.2 Ledningssystem

Botkyrka kommuns ledningssystem för informationssäkerhet består av:

- Policy för informationssäkerhet
- Riktlinje för informationssäkerhet
- Regler
- Rutiner, instruktioner, processer, handböcker, etc.

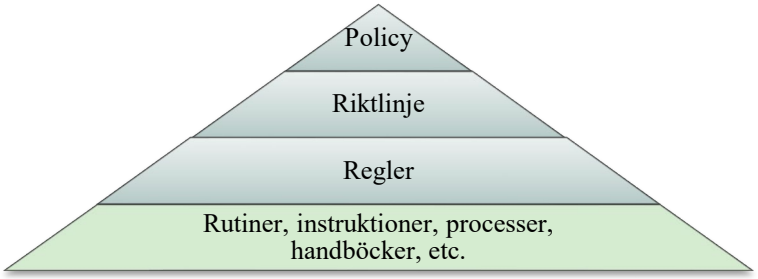

Bild 1: Botkyrka kommuns ledningssystem för informationssäkerhet (LIS)

1.4 Dokumentets struktur

Detta dokument är utformat enligt *Riktlinjer för styrdokument i Botkyrka kommun*. Riktlinjer vägleder och ger konkret stöd kring hur arbetsuppgifter bör utföras inom ett visst område. De kan rekommendera tillvägagångssätt och är därför mer detaljerade än en policy men inte lika detaljerade som en regel. Dokumentet följer också i stora delar samma struktur som ISO 27001, Riktlinjer för informationssäkerhetsåtgärder och har skapats med hjälp av MSB:s [1]metodstöd för ledningssystem för informationssäkerhet (LIS).

2. Informationssäkerhet

Informationssäkerhet omfattar skydd av Botkyrka kommuns informationstillgångar med syftet att säkerställa informationens konfidentialitet, riktighet och tillgänglighet. All information Botkyrka kommun behandlar ska informationssäkerhetsklassificeras.
Informationssäkerhet uppnås genom införande och efterlevnad av relevanta policyer, riktlinjer, regler samt tekniska säkerhetslösningar i de verksamhetsprocesser och informationssystem där informationstillgångarna hanteras.
Med informationssäkerhet avses såväl administrativ säkerhet som teknisk säkerhet. Administrativ säkerhet avser införande av skyddsåtgärder av organisatorisk och administrativ natur. i form av utbildning, processer och rutiner. Med teknisk säkerhet avses införande av tekniska och logiska skyddsåtgärder.

[1] Myndigheten för Samhällsskydd och beredskap

3. Definitioner

Begrepp	Förklaring
Andra externa parter	Andra kommuner och myndigheter
Arkivering	Bevarande av information på lång sikt och för andra syften än det ursprungliga bevarandet.
Autentisering	Kontroll (verifiering) av uppgiven identitet.
Behandling	All form av hantering, användning och manipulation av information oberoende om det utförs automatiserat eller ej.
Digitala verktyg	Hjälpmedel som möjliggör medarbetares behandling av information exempelvis mobiltelefon, arbetsdator etc.
Extern leverantör	Privat leverantör som tillhandahåller produkter eller tjänster på uppdrag av Botkyrka kommun.
Information	Kunskap, data och källkod som har ett värde för Botkyrka kommun oavsett i vilken form som informationen behandlas.
Informationssystem	IT-tjänst, IT-system och annan teknisk utrustning som stödjer behandling av information. Definitionen av informationssystem omfattar exempelvis serversystem, arbetsdatorer, mobiltelefoner, nätverksutrustning, molntjänster, etc.
Informationstillgång	Avser all information oavsett om den behandlas manuellt eller automatiserat och oberoende av dess form eller miljön den förekommer i.
Intern leverantör	Förvaltningar, stiftelser och bolag inom Botkyrka kommuns verksamhet.
ISO 27000	Internationell standard framtagen för ledning och styrning av informationssäkerhetsarbete.
Kritisk	Informationstillgångar och informationssystem som är kritiska för Botkyrka kommuns verksamhet baserat på en riskbaserad bedömning.
Känslig	Information med åtkomst endast för en viss krets inom Botkyrka kommun och, i tillämpliga fall, även till behörig leverantör eller annan extern part.
Ledningssystem för informationssäkerhet (LIS)	Ett stöd för hur informationssäkerhetsarbetet genomförs i kommunens verksamhet.
Multifaktorautentisering (MFA)	Autentisering (identitetskontroll) med minst två former av information, exempelvis en kombination av lösenord, smartkort, och biometrisk.
Processer	Beskrivning av vilka resurser, aktiviteter och leverabler som krävs för att en uppgift ska anses vara fullföljd.
Riskbaserat arbetssätt	Förutsätter en dokumenterad riskbedömning med ett dokumenterat riskägarskap.
Sekretess	Förbud mot att röja sekretessinformation vare sig det sker muntligt, genom utlämnande av allmän handling eller på annat sätt.
Styrande dokument	Upprättande och underhåll av styrande dokument sker i enlighet med dokumentet “Riktlinjer för styrdokument i Botkyrka kommun”.
Systemutvecklare	Tar fram och utvecklar data/IT-system eller delar av system.

4. Omfattning

Detta dokument omfattar all behandling av information, inklusive verktyg och processer, som tillhör Botkyrka kommun oavsett format och fysisk form. Riktlinjen omfattar alla förvaltningar och nämnder. I de fall informationen hanteras elektroniskt omfattas samtliga IT-miljöer. Om Botkyrka kommuns information behandlas i en extern miljö ska behandlingen vara reglerad i avtal i enlighet med denna riktlinje.

4.1 Hantering av undantag

Eventuella undantag ska riskbedömas, dokumenteras och godkännas av informationsägaren.

Säkerhetsåtgärder

Ett godkännande gällande undantag kan göras om ett behov av undantag föreligger. Ett godkännande av undantag förutsätter följande:
a) Om behov av undantag föreligger ska ett riskbaserat angreppssätt, i enlighet med avsnitt 5 i denna riktlinje, styra eventuellt godkännande av undantag. Undantag är aldrig permanenta, utan har en begränsad giltighetstid på som längst ett år.
b) Om behov av undantaget kvarstår efter ett år ska en ny riskbedömning genomföras.

5. Identifiering och hantering av risk

Riskarbetet ska säkerställa att informationssäkerhetsrisker i Botkyrka kommun identifieras, analyseras, bedöms, dokumenteras, rapporteras och hanteras.

5.1 Identifiering av informationssäkerhetsrisker

Informationssäkerhetsrisker som har betydelse för informationssäkerheten inom Botkyrka kommuns verksamhet ska identifieras och dokumenteras.

Säkerhetsåtgärder

a) Botkyrka kommun ska identifiera och analysera informationssäkerhetsrisker årligen samt vid förändringar som har betydelse för informationssäkerheten.
b) Vid identifiering av risker som rör Botkyrka kommuns information ska olika källor användas som underlag, exempelvis:

- Inträffade incidenter.
- Noteringar av brister i informationssäkerhetsskyddet.
- Omvärldsbevakning (generella hotbildstrender).
- I samband med anskaffning, utveckling och förändring av verktyg, processer, Informationssystem och IT-infrastruktur.

- Vid uppföljning gällande efterlevnad av Botkyrka kommuns styrande dokument.
- Hantering av undantag från Botkyrka kommuns riktlinjer för informationssäkerhet.
- Säkerhetstester.
- Externa revisioner av informationssäkerhet.

5.2 Hantering av informationssäkerhetsrisker

Risker som har betydelse för Botkyrka kommuns informationssäkerhet ska hanteras och dokumenteras enligt en fastställd process.

6. Organisation och ansvar

Botkyrka kommun ska ha en ändamålsenlig organisation med tydliga roller och tillhörande ansvar. Organisationen ska tillgodose att varje verksamhet inom Botkyrka kommun kan upprätthålla ett strukturerat informationssäkerhetsarbete där all information ska ha ett tilldelat ägandeskap och vara klassad.

6.1 Informationssäkerhetsforum

För att samordning och uppföljning av informationssäkerhetsarbetet ska kunna bedrivas effektivt ska det finnas ett kommunövergripande informationssäkerhetsforum. Forumet leds av informationssäkerhetsansvarig och består av informationssäkerhetsrepresentanter från varje förvaltning.
Forumet ska agera stödjande till Botkyrka kommun och främja erfarenhets- och kunskapsutbyte, bevaka vilket behov av stöd som finns i verksamheterna och föreslå förbättringar samt förankra och samordna informationssäkerhetsaktiviteter.

6.2 Roller och ansvar

Nedan följer de roller som ingår i informationssäkerhetsorganisationen samt rollernas ansvar.

Roll	**Ansvar**
Kommunfullmäktige	Fastställer kommunens informationssäkerhetspolicy och har det yttersta ansvaret för kommunens informationssäkerhet.
Kommunstyrelse	Fastställer kommunövergripande riktlinjer och regler.
Nämnder	Fastställer nämndövergripande styrdokument. Är personuppgiftsansvarig och bestämmer för vilka ändamål och hur uppgifter ska behandlas.
Kommundirektör	Säkerställer att kommunen efterlever gällande styrdokument samt de externa och interna kraven för informationssäkerhet.

Informationssäkerhetsansvarig	Ansvarar för ledningssystemet för informationssäkerhet och för kommunövergripande uppföljning av de externa och interna kraven. Leder informationssäkerhetsforum för informationssäkerhetssamordnarna. Rapporterar till kommundirektören.
Förvaltningsdirektör	Fastställer förvaltningsspecifika styrdokument och informationssäkerhetsåtgärder.
Processägare	Ansvarar för att all informationsbehandling inom processen finns beskriven i enlighet med interna och externa krav och fastställda styrdokument.
Verksamhetsansvarig	Ansvarar för att all informationsbehandling inom egna verksamheten sker i enlighet med interna och externa krav och fastställda styrdokument.
Informationsägare	Informationsägaren ansvarar för informationstillgångar, inklusive personuppgifter, och är riskägaren för informationen och ska därför genomföra riskanalys. Ansvarar för att informationen informationssäkerhetsklassificeras. Informationsägaren ansvarar för informationens riktighet, tillgänglighet samt på vilket sätt informationen sprids i enlighet med klassificering, interna och externa krav.
Förvaltningsledare	Förvaltar informationen/informationssystemet på uppdrag av informationsägaren.
Informationssäkerhetssamordnare	Bör finnas en per förvaltning. Rapporterar till förvaltningarnas respektive Förvaltningsdirektör. Deltar i förvaltningsöverskridande informationssäkerhetsforum. Agerar stödfunktion för förvaltningen inom informationssäkerhetsfrågor. Ansvarar för förvaltningens riskregister.
Dataskyddsombud	Definition i enlighet med dataskyddsförordningen. Företräder de registrerades rättigheter inom förvaltningen. Granskar förvaltningens kapacitet att efterleva regelverket och är kontaktperson mot IMY.
Objektägare	Säkerställer att tekniska förutsättningar finns för att uppfylla krav och hantera risker.
Alla anställda, uppdragstagare och utomstående användare inom Botkyrka kommun	Ansvarar för att efterleva gällande regler för informationssäkerhet.

7. Personalresurser och säkerhet

Alla anställda, uppdragstagare och utomstående användare ska vara bedömt lämpliga samt förstå sitt ansvar inom informationssäkerhet. Det ska också säkerställas att de är medvetna om hot och problem som rör

informationssäkerhet, samt är rustade för att följa kommunens regelverk för informationssäkerhet när de utför sitt arbete för att minska risken för mänskliga fel.

7.1 Före och vid anställning

Lämplighet samt ansvar och skyldigheter gällande informationssäkerhet ska tydliggöras före och i samband med anställning eller kontraktering av en medarbetare eller uppdragstagare.

Säkerhetsåtgärder

a) Vid rekrytering till en tjänst som medför åtkomst till känslig, kritisk eller konfidentiell information ska en fastslagen process finnas som innefattar beslut om bakrundkontroll och/eller säkerhetsprövning av kandidaten.
b) Anställningsvillkoren ska tydligt definiera det ansvar samt de rättigheter och skyldigheter en anställning medför utifrån ett informationssäkerhetsperspektiv.
c) Botkyrka kommun ska ha standardiserade avtalstexter gällande sekretess och hantering av digitala verktyg att använda vid upprättande av anställningsavtal.
d) Aktiviteter som rör informationssäkerhetsfrågor och som sker i samband med att en ny medarbetare anställs ska följa en fastställd process.

7.2 Under anställningstiden

Medarbetare ska vara medvetna om och uppfylla sitt ansvar för Botkyrka kommuns informationssäkerhet.

Säkerhetsåtgärder

a) Samtliga medarbetare ska utbildas i och påminnas regelbundet om:

- Sitt ansvar i sin nuvarande roll gällande skydd av Botkyrka kommuns information och informationssystem.
- Risker som kan uppstå vid hantering av Botkyrka kommuns information och informationssystem.
- Hur rapportering sker av eventuella brister i skyddet av, samt incidenter gällande, Botkyrka kommuns information och informationssystem.

b) Genomförandet av utbildning ska dokumenteras för att säkerställa att medarbetare ska ha genomfört relevanta utbildningar.

7.3 Vid förändring eller upphörande av anställning och uppdrag

När anställda, uppdragstagare och utomstående användare lämnar Botkyrka kommun eller ändrar anställningsförhållande ska det ske på ett ordnat sätt.

Säkerhetsåtgärder

Botkyrka kommun ska följa en dokumenterad process vid förändring och upphörande av anställning eller uppdrag. Processen ska innehålla minst kontrollpunkter för:

- Återlämnande av digitala verktyg som tillhör Botkyrka kommun.
- Indragning eller förändring av behörigheter.
- Att all information som medarbetaren ansvarar för överlämnas till en ny utsedd informationsägare.

7.4 Disciplinär process

Botkyrka kommun ska ha en fastställd och kommunicerad process för att vidta åtgärder mot medarbetare som bryter mot Botkyrka kommuns styrande dokument.

8. Behandling av tillgångar

Botkyrka kommuns informationstillgångar ska vara skyddade på ett säkert sätt avseende konfidentialitet, riktighet och tillgänglighet. Arbetet med informationssäkerhet ska sträva efter att balansera risker mot skyddsåtgärder. Arbetet ska inom varje område planeras, styras och utföras konsekvent.

Inledning

Samtliga informationstillgångar ska vara identifierade, informationssäkerhetsklassificerade och förtecknade. Av förteckningen ska framgå vem som är informationsägare.
Risk- och sårbarhetsanalys ska identifiera tänkbara störningar, allvarliga händelser samt extraordinära händelser. Arbetet syftar till att skapa robusta informationssystem samt identifiera och analysera skyddsvärda informationstillgångar. Arbetet ska fokusera på förebyggande insatser och konkreta skyddsåtgärder för människor, egendom och miljö.

8.1 Ansvar för tillgångar

Botkyrka kommun ska ha en dokumentation över informationstillgångar och informationssystem. Ansvaret för att skydda dessa tillgångar ska dokumenteras.

8.2 Förteckning över tillgångar

Säkerhetsåtgärder

a) Information och informationssystem ska vara förtecknade och ha ett utsett ägarskap.
b) Verktyg, för att behandla och lagra information, ska vara förtecknade och ha ett utsett ägarskap.

c) Interna och externa tjänster som exempelvis kommunikationstjänster, molntjänster, etc. ska vara förtecknade och ha ett utsett ägarskap samt hanteras i enlighet med Botkyrka kommuns gällande styrdokument för informationssäkerhetskrav på leverantörer.

8.3 Användning av tillgångar

Säkerhetsåtgärder

Regler för användning av Botkyrka kommuns informationssystem, information samt tjänster och funktioner som är tillgängliga för medarbetare via Botkyrka kommuns infrastruktur ska vara dokumenterad och kommunicerad till respektive medarbetare.

8.6 Informationssäkerhetsklassificiering

Botkyrka kommuns information ska informationssäkerhetsklassificeras för att kunna säkerställa att informationen skyddas och hanteras i enlighet med dess betydelse. Detta innefattar skydd mot otillåten behandling samt bevarande av informationens konfidentialitet, riktighet och tillgänglighet.
Säkerhetsåtgärder som vidtas för att skydda informationen ska, förutom identifierade risker även beakta den senaste utvecklingen, genomförandekostnader och informationsbehandlingens art, omfattning, sammanhang och ändamål.

Vid informationssäkerhetsklassificiering ska det bedömas i vilken grad förlust av konfidentialitet, riktighet och tillgänglighet hos information innebär en negativ påverkan på egen eller annan verksamhet och dess tillgångar, eller på enskild individ.

Säkerhetsåtgärder

Informationssäkerhetsklassificiering ska ske regelbundet med hänsyn till krav på konfidentialitet, riktighet och tillgänglighet enligt en fastställd process.

8.7 Märkning av information

Utöver att information ska informationssäkerhetsklassas ska dokument märkas enligt rådande metadatastruktur med hänsyn till dokumentens informationssäkerhetsklassificiering. Syftet med att märka dokument är att synliggöra vilka dokument som kräver särskild behandling på grund av innehållet i dokumentets säkerhetsvärde, vilket metadatastrukturen ska tillgodose.

8.8 Hantering av information

Säkerhetsåtgärder

a) Respektive informationsklass ska ha dokumenterade regler för hur information ska hanteras och skyddas i olika behandlingssituationer.
b) Information som behandlas av Botkyrka kommun på uppdrag av extern part ska hanteras och skyddas enligt dokumenterade instruktioner från den externa parten godkända av Botkyrka kommun.

8.9 Informationssäkerhetsklassificiering av informationssystem och verktyg

Informationssystem och verktyg ska informationssäkerhetsklassificeras för att kunna säkerställa verksamhetens krav på konfidentialitet, riktighet och tillgänglighet.

Säkerhetsåtgärder

Informationssystem ska minst uppfylla de informationssäkerhetskrav som ställs på dessa.

9. Hantering av digitala verktyg

9.1 Mobil datoranvändning och distansarbete

Användning av bärbara digitala verktyg, exempelvis datorer, mobiltelefoner, som lagrar eller har tillgång till information som tillhör Botkyrka kommun ska ske på ett sådant sätt att risken för obehörig tillgång till information minimeras.

Säkerhetsåtgärder

a) Bärbara digitala verktyg ska vara försedda med skydd mot obehörig användning samt skydd mot obehörig tillgång till information som är lagrad på utrustningen.
b) Medarbetares hantering, ansvar, rättigheter och skyldigheter gällande digitala verktyg ska i regleras i styrande dokument, inkluderas i anställningsförfarandet samt utbildas i regelbundet.

9.2 Distansarbete

Säkerhetsåtgärder

a) Distansarbete och uppkoppling från externt nätverk till Botkyrka kommuns interna nätverk ska endast ske via Botkyrka kommuns godkända metoder och från hanterade digitala verktyg.
b) Distansarbete och uppkoppling från externa nätverk till Botkyrka kommuns verksamhetssystem ska endast ske via Botkyrka kommuns godkända metoder och från hanterade digitala verktyg.
c) Metoden för uppkoppling mot Botkyrka kommuns interna nätverk vid distansarbete ska kräva multifaktorsautentisering.

10. Styrning av behörigheter

Åtkomst till information och IT-system ska styras enligt dokumenterade processer.

10.1 Regler för styrning av åtkomst

Säkerhetsåtgärder

a) Tilldelning av behörigheter till information, informationssystem och IT-tjänster ska utgå från medarbetarens ”behov-att-känna-till” och ”behov-att-kunna-utföra” för att kunna fullgöra sina arbetsuppgifter.
b) Beställning och godkännande av användarkonton och behörigheter ska vara uppdelat på två olika roller.

- Närmaste chef ansvarar för behörighetsbeställningar.
- Informationsägaren ansvarar för godkännanden.

10.2 Registrering av användare

Säkerhetsåtgärder

a) Registrering av användarkonton ska ske enligt en fastställd process. Processen ska innehålla minst kontrollpunkter innan aktivering för att:
- Det finns en formell och spårbar beställning.
- Användarkonton är personliga så att användarna kan vara kopplade till och hållas ansvariga för sina handlingar.
- Användare ska ha genomgått utbildning inom informationssäkerhet, genomförd utbildning loggas.

b) Registrering av användarkonton loggas.

10.3 Tilldelning av behörigheter

Säkerhetsåtgärder

a) Tilldelning av behörigheter ska ske enligt en fastställd process. Processen innehåller minst kontrollpunkter för att:
- Det ska finnas en formell och spårbar beställning.
- Tilldelning av förhöjda åtkomsträttigheter, som exempelvis *administrator* är restriktiv och ska tilldelas till ett användarkonto som skiljer sig från det användarkonto som används för ordinarie verksamhet.

b) Tilldelning av åtkomsträttigheter ska loggas.
c) Tilldelning av åtkomsträttigheter ska om tekniskt möjligt alltid styras av fastställda roller.

10.4 Hantering av förhöjda åtkomsträttigheter

Säkerhetsåtgärder

Inloggning med användarkonton med förhöjda behörigheter ska använda multifaktorsautentisering.

105 Granskning av användarkonton och åtkomsträttigheter

Säkerhetsåtgärd

Granskning av användarkonton, behörigheter samt förhöjda behörigheter ska ske enligt informationsäkerhetsklassificeringskraven.

106 Borttagning och förändring av användarkonton och behörigheter

Säkerhetsåtgärder

a) Förändring och upphörande av anställning eller uppdrag ska hanteras enligt avsnitt 7.3.
b) Inaktivering eller annan förändring av användarkonton och åtkomsträttigheter ska loggas.

10.7 Begränsning av åtkomst till information och funktioner i informationssystem

Säkerhetsåtgärder

Typ av behörighet (skapa, läsa, ändra, radera) till information och funktioner i informationssystem ska styras av användarens roll.

10.8 Säkra inloggningsrutiner

Säkerhetsåtgärder

Inloggning ska använda multifaktorsautentisering oavsett enhet eller plats.

10.9 Hantering av lösenord

Organisationen ska sträva efter att minimera användandet av lösenord och i stället använda multifaktorautentisering. Vid tillfällen där MFA inte är applicerbart och lösenord krävs, ska nedanstående följas.

Säkerhetsåtgärder

a) Informationssystem ska ha följande funktioner aktiverade som ska säkerställa att:

- Lösenord med hög kvalitet väljs.
- Lösenord regelbundet förnyas.
- Lösenord inte visas.
- Lösenord aldrig lagras och överförs i klartext.

b) För Informationssystem som inte har stöd för funktionerna enlig ovan ska användarna bli påminda om att regelbundet byta lösenord samt att välja lösenord av hög kvalitet.
c) Vid installation av Informationssystem ska eventuella standardlösenord och roller bytas.

11. Kryptering

Ej krypterad information är läsbar för alla. Kryptering innebär att informationen kodas så att den inte går att läsa utan en nyckel för dekryptering. Skyddsvärd information i informationssystem och IT-tjänster ska skyddas genom kryptering, antingen av informationen i sig, lagringsmedia eller kommunikationsvägarna.

11.1 Användning av kryptering

Botkyrka kommuns information ska, i enlighet med informationssäkerhetskraven, skyddas mot obehörig åtkomst genom kryptering av informationen.

Säkerhetsåtgärder

a) Användning av kryptering för att skydda information mot obehörig åtkomst ska styras av:

- Hanteringsregler som är en följd av informationens informationssäkerhetsklassificiering.
- Risker som identifierats mot Botkyrka kommuns information.
- Externa krav.

b) Endast väl etablerade och ej brutna krypteringsalgoritmer och längder på kryptografiska nycklar ska användas vid kryptering av information.

11.2 Nyckelhantering

Kryptografiska nycklar ska skyddas mot förändring och förlust.

Säkerhetsåtgärder

Hantering av kryptografiska nycklar ska följa en fastställd process som omfattar moment för att generera, lagra, arkivera, distribuera, återkalla samt förstöra nycklar.

12. Fysisk säkerhet

12.1 Skydd av utrymmen

Botkyrka kommuns information ska skyddas i enlighet med dess skyddsvärde och utrymmen ska skyddas mot obehörigt tillträde, skador och störningar.

12.2 Fysisk säkerhetsavgränsning och tillträdesbegränsningar

Säkerhetsåtgärder

Utrymmen där informationssystem och information förvaras ska skyddas i förhållande till informationens informationssäkerhetsklass.

12.3 Skydd av utrustning

Säkerhetsåtgärder

Botkyrka kommuns utrustning som direkt eller indirekt medverkar vid behandling och lagring av information ska skyddas mot obehörigt tillträde, skador och störningar.

12.4 Placering och skydd av utrustning

Säkerhetsåtgärder

Nätverksutrustning, servrar och annan IT-utrustning som hanterar information ska placeras i utrymmen med fysisk säkerhetsavgränsning samt tillträdesbegränsning enligt rådande riktlinje för datorhallar MSB.

12.5 Tekniska försörjningssystem

Säkerhetsåtgärder

Tekniska försörjningssystem som exempelvis internet, elkraft och kyla, ska vara dimensionerade för att möta verksamhetskrav på tillgänglighet av informationssystem.

13. Driftsäkerhet

Botkyrka kommun ska ha en säker drift av sina informationssystem.

13.1 Dokumenterade driftsrutiner

Säkerhetsåtgärder

a) Driftdokument ska vara upprättade för samtliga informationssystem som betraktas ingå i Botkyrka kommuns verksamhet och ska revideras vid behov eller enligt fastställt schema.
b) Driftdokument ska vara tillgängliga för de medarbetare som behöver den.

13.2 Ändringshantering

Förändringar av informationssystem och IT-infrastruktur ska ske kontrollerat.

Säkerhetsåtgärder

Förändringar av informationssystem och IT-infrastruktur ska följa en fastställd process. Processen ska innehålla minst kontrollpunkter för att:

- Identifiera och hantera eventuella informationssäkerhetsrelaterade risker (konfidentialitet, riktighet, tillgänglighet), som kan uppstå som en konsekvens av förändringen.
- Funktionella samt säkerhetstester är genomförda.
- Eventuell påverkan på kontinuitets- och återställningsplaner identifieras och behandlas.
- Säkerställa integriteten i installationsförfarandet mellan acceptanstest och produktion.

13.3 Uppdelning av test och produktionsmiljöer

Säkerhetsåtgärder

a) Produktions-, test- och utvecklingsmiljöer ska vara åtskilda i syfte att minska risken för obehörig åtkomst samt risken för att någon av miljöerna påverkas på ett okontrollerat sätt.
b) Föreligger behov av testaktiviteter i produktionsmiljön ska ett riskbaserat angreppssätt i enlighet med avsnitt 5 i dessa riktlinjer styra eventuellt godkännande av undantag.

13.4 Skydd mot skadlig kod

Godkända informationssystem som kan påverkas av skadlig kod ska kontrolleras och skyddas mot detta.

Säkerhetsåtgärder

a) informationssystem ska ha ett skydd mot skadlig kod installerat.
b) Uppdatering av signaturer för skadlig kod ska ske regelbundet och med automatik.
c) För kritiska informationssystem ska, utöver signaturer, även kompletterande skydd användas såsom analys av beteende och trafikmönster för att upptäcka eventuell skadlig kod.

13.5 Säkerhetskopiering

Säkerhetskopiering av information och programvara ska utföras regelbundet och med en omfattning i enlighet med verksamhetens samt gällande skyddskrav för att uppnå tillräcklig redundans.

Säkerhetsåtgärder

a) Säkerhetskopiering ska ske efter verksamhetens fastställda krav.
b) Tester för att återskapa information från säkerhetskopior ska ske regelbundet.
c) Säkerhetskopior ska skyddas i enlighet med de behandlingskrav som följer av informationssäkerhetsklassen på den kopierade informationen.

d) Säkerhetskopior ska förvaras på en annan plats och på ett tillräckligt avstånd för att inte utsättas för eventuella skador vid en informationssäkerhetshändelse på det ordinarie driftstället.

13.6 Loggning

Säkerhetsåtgärder

Händelser i informationssystem ska loggas i enlighet med informationens informationssäkerhetsklass för att kunna vara underlag för övervakning och utredningar.

13.7 Loggning av händelser

För att möjliggöra identifiering och uppföljning av avvikande beteenden ska loggning vara aktiverat på godkända informationssystem.

Säkerhetsåtgärder

a) Händelseloggar som registrerar användaraktiviteter, administratörsaktiviteter, avvikelser, fel och informationssäkerhetshändelser skapas, granskas och bevaras.
b) Avvikelser från normala beteenden kunna detekteras och ska resultera i ett larm.

13.8 Synkronisering av tid

Säkerhetsåtgärder

Informationssystem ska synkronisera sin tid med en av kommunen definierad källa för korrekt tid.

13.5 Styrning av informationssystem

Informationssystem ska vara installerade och konfigurerade så att beslutad nivå på skydd av Botkyrka kommuns information upprätthålls.

Säkerhetsåtgärder

Botkyrka kommun ska dokumentera en lägsta accepterad nivå gällande informationssäkerhet för informationssystem.

13.6 Hantering av tekniska sårbarheter

Informationssystem ska skyddas i nivå med informationssäkerhetsklassningen avseende utnyttjande av tekniska sårbarheter.

Säkerhetsåtgärder

a) Det ska finnas fastställda rutiner för säkerhetsuppdatering.
b) Härdning ska ske utifrån informationens behov av skyddsåtgärder.

14. Kommunikationssäkerhet

Nätverk ska vara skyddade mot obehörig åtkomst och obehörig påverkan.

14.1 Säkerhetsåtgärder för nätverk

Säkerhetsåtgärder

a) Botkyrka kommun ska ha en dokumenterad nätverksarkitektur som definierar arkitekturprinciper, inklusive zonmodell och övergripande nätverkstopologi, för att uppfylla informationssystemens krav på konfidentialitet, riktighet, tillgänglighet.
b) Botkyrka kommun ska ha fastställda processer samt personella och tekniska resurser för att upptäcka och larma för avvikande trafikmönster och beteenden.
c) Förändringar i nätverkstopologi samt regler som styr nätverkstrafik ska följa den fastställda processen för ändringshantering, avsnitt 13.2 Ändringshantering.

15. Anskaffning, utveckling, underhåll och avveckling av informationssystem

Vid upphandling/anskaffning av informationssystem ska dataskydd, gallring och arkivering vägas in och beaktas särskilt för att stötta informationens hela livscykel. Plan för avveckling ska finnas redan vid anskaffning av ett informationssystem (informationens livscykel). Information som gallras ska förstöras på ett sådant sätt att uppgifterna inte kan återskapas eller komma i orätta händer.

15.1 Säkerhetskrav på informationssystem

Anskaffning, utveckling, underhåll och avveckling av informationssystem ska föregås av analys och specifikation av informationsmängd och informationssäkerhetskrav.

Säkerhetsåtgärder

Processer ska finnas för att analysera och specificera informationssäkerhetskrav i samband med anskaffning, utveckling, underhåll och avveckling av informationssystem.

15.2 Säkerhet i utvecklings- och supportprocesser

Säkerhetsåtgärder

Informationssystem ska utformas för att stödja beslutad nivå av informationssäkerhet.

15.3 Säker utveckling

Säkerhetsåtgärder

a) Kontrollpunkter för informationssäkerhetskrav ska ingå i alla steg i Botkyrka kommuns utvecklingsprocess.
b) Anställda och anlitade systemutvecklare ska vara utbildade i att utveckla säker programkod.
c) Generella informationssäkerhetskrav samt praxis för att skriva säker programkod i samband med utveckling av informationssystem ska vara dokumenterade.

15.4 Utlagd systemutveckling

Säkerhetsåtgärder

Botkyrka kommun ska övervaka systemutveckling som är utlagd till extern part. Övervakningen ska säkerställa att minst:

- Äganderätten är reglerad.
- Systemutvecklingen följer Botkyrka kommuns krav på säker utveckling eller motsvarande.

15.5 Säkerhetstestning

Säkerhetsåtgärder

Nya och förändrade informationssystem som behandlar eller lagrar information ska testas med avseende på beslutad informationssäkerhetsnivå under utvecklingsfasen samt innan informationssystem tas i drift.

15.6 Skydd av testdata

Data som används i utvecklings och testmiljöer ska inte överstiga informationssäkerhetsklass 2.

Säkerhetsåtgärder

a) Information ska anonymiseras i de fall informationen används i samband med utveckling och test av informationssystem.
b) Testsystem och utvecklingssystem ska följa de krav på säkerhetsåtgärder som är en följd av informationens informationssäkerhetsklassificiering.

15.7 Avveckling av informationssystem

Vi varje avveckling av informationssystem ska riskbedömning genomföras och dokumenteras.

Säkerhetsåtgärder

a) Vid avveckling av informationssystem ska informationen förstöras på ett sådant sätt att uppgifterna inte kan återskapas eller komma i orätta händer.
b) Den utvalda metoden för radering av information vid avveckling av informationssystem ska dokumenteras.
c) Den utvalda metoden för radering av information vid avveckling av molntjänst ska regleras i avtal.

16. Relationer med externa och interna leverantörer samt samarbeten med andra externa parter

Samverkan med konsulter, externa leverantörer och entreprenörer ska regleras genom avtal. Vid behov av åtkomst till informationsresurser ska en riskbedömning göras för att säkerställa att informationens skyddsbehov upprätthålls. Informationssäkerhetskrav enligt kommunens riktlinjer ska vara reglerade och dokumenterade med externa och interna leverantörer samt andra externa parter.

Säkerhetsåtgärder

Nivån på säkerhet gällande Botkyrka kommuns information ska bibehållas då dessa behandlas (är åtkomliga, eller lagras m.m.) av en leverantör eller annan extern part och då detta sker utan övervakning från Botkyrka kommun.

16.2 Hantering av informationssäkerhet i avtal med externa leverantörer och andra externa parter

Säkerhetsåtgärder

Informationssäkerhetskrav ska ingå i avtal med externa leverantörer och andra externa parter då dessa behandlar information som Botkyrka kommun äger. Avtalen ska innehålla minst:

- Regler för användning, hantering samt skydd av informationen.
    - endast personal hos den externa leverantören som behöver ta del av informationen/utrustningen för att kunna utföra sitt uppdrag gentemot Botkyrka kommun ska ha rätt att ta del av den samt att den externa leverantören håller en förteckning över vilka individer/grupper/roller som har rätt att ta del av/behandla informationen/utrustningen.
- Skyldighet att underteckna sekretessförbindelser.
- Ägarskap och hantering av såväl materiella som immateriella tillgångar vid avtalets upphörande.
- Botkyrka kommuns rätt till uppföljning och granskning av avtalspartens efterlevnad av avtalet.

16.3 Hantering av informationssäkerhet i dokumenterade överenskommelser med interna leverantörer

Säkerhetsåtgärd

Informationssäkerhetskrav ska ingå i dokumenterade överenskommelser mellan informationsägare och interna leverantörer då dessa behandlar information som informationsägare äger. Den dokumenterade överenskommelsen ska innehålla minst:

- Regler för användning, hantering samt skydd av informationen.
- Föreskrivning om att endast personal hos den interna leverantören som behöver ta del av informationen/utrustningen för att kunna utföra sitt uppdrag gentemot informationsägare. Informationsägaren ska ha rätt att ta del av den samt att den interna leverantören håller en förteckning över vilka individer/grupper/roller som har rätt att ta del av/behandla informationen/utrustningen.
- Skyldighet att dokumentera sekretessförbindelser.
- Ägarskap och hantering av såväl materiella som immateriella tillgångar vid den dokumenterade överenskommelsens upphörande.
- Informationsägarens rätt till uppföljning och granskning av den interna leverantörens efterlevnad av den dokumenterade överenskommelsen.

16.4 Hantering av informationssäkerhet i avtal vid överföring av informationsägarskap

Säkerhetsåtgärd

Vid överföring av information där ägarskapet av informationen övergår till annan part ska överlämning av ägarskap samt bedömd säkerhetsnivå regleras i avtal.

17. Hantering av incidenter och brister i informationssäkerheten

Informationssäkerhetsincidenter och brister i informationssäkerheten ska hanteras systematiskt och dokumenteras.
Brister ska följas upp med intentionen att en grundorsak identifieras.
Som brister räknas avsaknad eller fel i informationssystem och skyddsåtgärder som kan medföra obehörig åtkomst till information, påverka riktigheten i information eller påverka tillgängligheten för någon av Botkyrka kommuns informationstillgångar.

17.1 Ansvar och rutiner

Säkerhetsåtgärder

a) Ansvar för hantering av informationssäkerhetsincidenter ska fastställas och kommuniceras.

b) Rutiner för att rapportera, dokumentera samt hantera informationssäkerhetsincidenter och rapportera de brister i informationssäkerheten ska vara fastställda. Rutinerna inkluderar minst sätt att:

- Rapportera brister i informationssäkerheten.
- Dokumentera samtliga informationssäkerhetsincidenter.
- Aktivt hantera informationssäkerhetsincidenter.
- Eskalera en informationssäkerhetsincident.
- Kommunicera informationssäkerhetsincidenter internt samt till myndigheter och andra relevanta externa parter.

c) Om ej kompetensen finns internt ska avtal finnas med extern leverantör som kan kallas in i det akuta skedet och agera vid allvarlig pågående informationssäkerhetsincident, så som exempelvis ransomware attack.

17.2 Rapportering av informationssäkerhetsincidenter

Säkerhetsåtgärder

Medarbetare ska informeras om sin skyldighet att rapportera informationssäkerhetsincidenter samt hur denna rapportering sker.

17.3 Rapportering av brister

Säkerhetsåtgärder

Medarbetare ska informeras om sin skyldighet att rapportera upplevda brister i skyddet av information och informationssystem samt hur denna rapportering sker.

17.4 Bedömning av informationssäkerhetsincidenter

Säkerhetsåtgärder

Botkyrka kommun ska ha en modell för att bedöma och gradera allvarligheten i en informationssäkerhetsincident.

17.5 Uppföljning av informationssäkerhetsincidenter

Säkerhetsåtgärder

Inträffade informationssäkerhetsincidenter ska sammanställas, utvärderas och dokumenteras samt ligga till grund för Botkyrka kommuns arbete med informationssäkerhetsrisker.

17.6 Insamling av bevis

Säkerhetsåtgärder

Botkyrka kommun ska ha kapacitet och rutiner för insamling och bevarande av bevis i samband med informationssäkerhetsincidenter med hänsyn till att incidenter kan få rättsliga följder.

18. Kontinuitetsplanering

Beredskaps-och kontinuitetsplaner för Botkyrka kommuns kritiska verksamhetsprocesser och kritiska informationssystem ska finnas. Planerna ska beskriva de åtgärder som ska vidtas för att hantera och upprätthålla verksamheten vid allvarliga och omfattande avbrott, störningar eller kriser.

18.2 Utveckling av beredskapsplaner

Säkerhetsåtgärder

a) Möjliga scenarier som påverkar verksamhetsprocesser ska identifieras tillsammans med sannolikheten och effekten av dessa.
b) Identifiering av verksamhetskrav och bedömning av risker ska ske minst vartannat år eller vid större förändringar i verksamheten eller kravställningar.
c) Botkyrka kommuns olika verksamheter ska ha utvecklade beredskapsplaner som beskriver de åtgärder som ska vidtas för att hantera allvarliga och omfattande avbrott, störningar och kriser. Planerna ska underhållas beroende på förändrade krav och förutsättningar.

18.3 Test av beredskapsplaner

Säkerhetsåtgärder

a) Beredskapsplaner ska testas årligen eller i samband med större förändringar.
b) Resultat från tester ska dokumenteras och ligga till grund för förbättringar av planerna.

18.4 Utveckling av kontinuitetsplaner

Säkerhetsåtgärder

a) Botkyrka kommuns olika verksamheter ska ha utvecklade kontinuitetsplaner. Planerna ska underhållas beroende på förändrade krav och förutsättningar.
b) Kontinuitetsplaner ska följa definierade krav på konfidentialitet, riktighet och tillgänglighet för informationen.
c) Krav och mandat för att aktivera kontinuitetsplaner ska fastställas och dokumenteras.

18.5 Test av kontinuitetsplaner

Säkerhetsåtgärder

a) Kontinuitetsplaner ska testas årligen eller i samband med större förändringar.
b) Resultat från tester ska dokumenteras och ligga till grund för förbättringar av planerna.

18.6 Återställningsplaner

Säkerhetsåtgärder

Baserat på verksamhetens krav på tillgång till information ska återställningsplaner utformas. Planerna ska beskriva enligt vilka prioriteringar och rutiner Botkyrka kommun ska återgå till normal verksamhet efter ett avbrott eller en större verksamhetsstörning.

18.7 Utveckling av återställningsplaner

Säkerhetsåtgärder

a) Botkyrka kommun ska ha utvecklade återställningsplaner för kritiska verksamhetsprocesser samt kritiska informationssystem.
b) Planerna ska underhållas beroende på förändrade krav och förutsättningar.

18.8 Test av återställningsplaner

Säkerhetsåtgärder

a) Återställningsplaner ska testas årligen eller i samband med större förändringar.
b) Resultat från tester ska dokumenteras och ligga till grund för förbättringar av planerna.

19. Efterlevnad

19.1 Identifiering av tillämpliga interna och externa krav

Tillämpliga styrande dokument, lagstiftning, eventuella krav i avtal och dokumenterade överenskommelser som har påverkan på utformning, drift, användning av informationssystem ska identifieras.

Säkerhetsåtgärder

a) Ansvar för identifiering av tillämplig lagstiftning, eventuella krav i avtal och dokumenterade överenskommelser ska dokumenteras och kommuniceras.
b) Tillämpliga lagstiftning, eventuella krav i avtal och dokumenterade överenskommelser som har påverkan på utformning, drift, användning av informationssystem ska återspeglas, där så är lämpligt, i form av säkerhetsåtgärder i Botkyrka kommuns styrande dokument för informationssäkerhet.

19.2 Granskning av informationssäkerhet

Säkerhetsåtgärder

a) Efterlevnad av säkerhetsåtgärder som är definierade i riktlinje för informationssäkerhet samt i Botkyrka kommuns övriga styrande dokument för informationssäkerhet ska granskas regelbundet.
b) Botkyrka kommuns tillvägagångssätt för att hantera informationssäkerhet och införande av säkerhetsåtgärder bör även granskas regelbundet av en oberoende part.
c) Botkyrka kommuns styrande dokument för informationssäkerhet ska minst granskas i enlighet med Riktlinje för styrande dokument i Botkyrka kommun.

19.3 Efterlevnad av policy, regler och anvisningar

Säkerhetsåtgärder

Botkyrka kommuns ska ha metoder och verktyg för att regelbundet mäta och rapportera efterlevnad av Botkyrka kommuns styrande dokument för informationssäkerhet.

19.4 Säkerhetstester

Säkerhetsåtgärder

a) En testplan gällande säkerhetstester av informationssystem ska upprättas årligen. Planerna ska innehålla minst att sårbarhetsavsökning och intrångstester ska genomföras vid ett flertal tillfällen per år.
b) Resultat från genomförda säkerhetstester ska dokumenteras och ligga till grund för förbättringsarbete.