Borgholms kommun
KOMMUNLEDNING

Niklas Palmquist, 0485-88221
niklas.palmquist@borgholm.se

POLICY

Datum
2019-01-02

Godkänd/ansvarig

Utgåva

Informationssäkerhetspolicy

Denna informationssäkerhetspolicy gäller för all verksamhet inom Borgholms kommun, inklusive kommunala bolag.

Samtliga anställda, politiker och extern personal omfattas av policyn och dess tillhörande instruktioner.

Instruktioner Användare (InfoSäk A), vänder sig till användarna. Tar bland annat upp områdena behörighet, inloggning och lösenord, utrustning, upplåtelse av arbetsplats, programvaror, hantering av information, utskrifter, e-post, virus, distansarbete, IT-incidenthantering och användning av Internet.

Instruktioner Förvaltning (InfoSäk F), roller och ansvar. Tar bland annat upp områdena behörighetsadministration, behörighetskontroll, loggning och spårbarhet, risk- och sårbarhetsanalys, införande, driftgodkännande, avveckling av informationssystem.

Instruktioner Kontinuitet och Drift (InfoSäk KD), gäller för kommunens IT-organisation (IT-avdelningen). Tar bland annat upp områdena helpdesk, säkerhet, krav på nätverk, system- och driftdokumentationer, förvaring.

Instruktioner Klassa (infoSäk K), tar upp informationsklassificering och sekretess.

Policyn ska kommuniceras till samtliga anställda vid nyanställning samt när policyn är ny eller reviderad. Policyn ska vara känd och tillgänglig i aktuell version på kommunens Intranät och på kommunens hemsida.
Avtal och överenskommelser får inte skrivas som åsidosätter kraven i denna policy.
Informationssäkerhetspolicys ska fastställas i kommunfullmäktige.

Definitioner

Med informationssäkerhet avses skydd av informationstillgångar i syfte att upprätthålla nödvändig nivå på sekretess, riktighet, tillgänglighet och spårbarhet.

- Sekretess – att information skyddas för obehörig insyn
- Riktighet – att information är tillförlitlig, korrekt och fullständig
- Tillgänglighet – att information är nåbar vid rätt tillfälle
- Spårbarhet – att specifika aktiviteter som rör information kan spåras

Informationssäkerhet delas upp i två delar.
Den administrativa säkerheten består av styrning, organisation, roller och ansvar, liksom regelverk, processer och systematik.
Den tekniska säkerheten är den delen som generellt beskrivs som IT-säkerhet. Här återfinns nätverk, servrar, arbetsstationer, hård- och mjukvara samt serverrum och utrymme för reservkraft, säkerhetskopior etc IT-säkerhet är en mindre del av informationssäkerhetsbegreppet.

Informationstillgång

Med informationstillgång avses all information oavsett om den behandlas i ett IT-system, förekommer på ett utskrivet papper, i ett anteckningsblock, som ett samtal i korridoren eller i telefonen. Även film, ljud och bild omfattas av informationssäkerhetsbegreppet.
Informationssäkerhet omfattar alla kommunens informationstillgångar.

Samhällsviktiga system

Kommunstyrelsen fastställer vilka system som är samhällsviktiga. Definitionen av samhällsviktiga system är den information som vid ett bortfall eller en svår störning kan leda till stor risk eller fara för befolkningens liv och hälsa, samhällets funktionalitet eller samhällets grundläggande värden.

Grundläggande mål för informationssäkerhetsarbetet

Borgholms kommuns informationssäkerhetsarbete syftar till att uppfylla följande mål.

Medborgares och intressenters förtroende	• Informationssäkerhet ska bidra till att medborgare och andra intressenter ska känna sig trygga vid informationsutbyte med kommunen och vår förmåga att hantera känsliga personuppgifter.
Verksamhetens informationssäkerhet	• Samtliga anställda inom kommunens verksamheter ska ha kännedom och kunskap om aktuellt regelverk beträffande informationssäkerhet. • Det systematiska informationssäkerhetsarbetet ska minst omfatta informationsklassning, hot- och riskanalys, incidenthantering, kontinuitetsplaner samt uppföljning, åtgärder och återkoppling. • Det ska finnas en kommunikationsplan som aktiveras vid händelser som har påverkan på informationssäkerheten. • Information ska skyddas i paritet med de konsekvenser som otillräcklig säkerhet kan medföra.

Krishantering	• Informationssäkerheten ses som en del av kommunens krishanteringsplan, i syfte att stärka förmågan att driva verksamheten vidare i händelse av en kris.

Organisation, Roller och Ansvar

Organisation, roller och fördelning av ansvar ska säkerställa att IT-system och tjänster kan administreras och hanteras på ett sådant sätt att det under hela sin livstid bidrar till att stödja avsedd verksamhet och uppfylla informationssäkerhetspolicyns mål.

All information ska klassificeras utifrån dess krav på konfidentialitet (sekretess), riktighet, tillgänglighet och spårbarhet.

Organisation av informationssäkerhetsarbetet

- **Kommunfullmäktige** uttrycker sin viljeinriktning i denna policy.
- **Kommunstyrelsen** har det yttersta ansvaret för kommunens informationssäkerhetsarbete.
- **Kommunchefen** utser, i samråd med förvaltningschef, system-ägare och informationsägare för respektive system. Kommunchefen utser även informationssäkerhetssamordnare.
- **VD** utser systemägare och informationsägare för bolagen.

Övriga roller och organisationen i detalj beskrivs i Instruktioner Förvaltning.

Uppföljning

Kommunstyrelsen, facknämnder och bolagstyrelser ska minst en gång per år informera sig om hur arbetet med informationssäkerhet går.

Uppföljningen ska baseras på underlag med rekommendationer som tas fram av Informationssäkerhetssamordnaren.
Underlaget ska innefatta information om:

- Förändringar utanför kommunen som kan påverka informationssäkerheten.
- Utbildning (status och behov).
- Inträffade incidenter av större påverkan på verksamheten.
- Resultat från genomförda granskningar.
- Aktuella och planerade säkerhetsåtgärder.

– – – – – – – – – –

Borgholms kommun

Kommunledningskontoret
Niklas Palmquist, 0485-88221
niklas.palmquist@borgholm.se

INSTRUKTION

Datum
2018-12-27

Informationssäkerhetsinstruktioner Användare

InfoSäk A

Innehållsförteckning

1 Chefens ansvar

Närmast berörd chef ansvarar för att gå igenom Informationssäkerhetspolicyn med dess bilagor med sina medarbetare enskilt eller vid exempelvis en arbetsplatsträff.

Information är en viktig tillgång för kommunen. För att skydda informationen krävs ett säkerhetsmedvetande hos alla medarbetare. Som användare har **Du** därmed en del i ansvaret för säkerheten i informationshanteringen.

Varje användare ska följa gällande regler för informationssäkerhet. I detta ansvar ingår att:

- delta i och stödja informationssäkerhetsarbetet,
- noga ta del av och följa Informationssäkerhetsinstruktion InfoSäk A,
- föreslå förändringar till systemförvaltare.

För stöd och hjälp när det gäller användningen av verksamhetens informationssystem kontaktar du aktuell systemförvaltare.

Har du problem med din datorutrustning, kommunikation, utskrifter etcetera ska du kontakta IT-avdelningens helpdesk.

2 Behörighet

Kommunens informationssystem är i olika utsträckning utrustade med behörighetskontrollsystem för att säkerställa att endast behöriga användare kommer åt information.

De behörigheter du blir tilldelad beror på dina arbetsuppgifter och avgörs av informationsägaren, som är din närmast ansvarige chef.

Du lämnar spår efter dig när du är inloggad och arbetar i systemen. De loggningsfunktioner som finns används för att spåra obehörig åtkomst. Detta för att skydda informationen och för att undvika att oskyldiga misstänks om oegentligheter inträffar.

Loggarna sparas i upp till två månader, undantag för informationssystem som regleras av särskild lagstiftning. Loggarna används även för att kontrollera ändringar.

Personalchefen (eller dennes ersättare) får fatta beslut om granskning av loggar om en anställd misstänks för brott, rektor eller motsvarande fattar beslut i fråga om misstanke mot elev som misstänks för brott. Resultatet av granskningen lämnas till den som begärt granskningen. Loggfilen är en allmän handling.

Kriminell verksamhet (exempelvis en hackerattack/sabotage) polisanmäls alltid.

Förutom vid misstanke om brott kan loggarna analyseras för att kartlägga belastningen av vår internetförbindelse, eller för att sammanställa icke individualiserad statistik över användningen.

3 Inloggning och lösenord

Lösenord är strängt personliga och ska skyddas från obehörig åtkomst! Kom-ihåg-lappar på eller under tangentbord, skärmar eller på annan synlig plats är inte tillåtna.

Det lösenord du får av IT-avdelningen eller av systemförvaltaren ska du byta till ett personligt lösenord vid första inloggningen.

För lösenord gäller att det ska:

- Vara minst åtta tecken långt.
- Inte innehålla personlig information.

Dessutom bestå av en blandning av tecken ur minst tre av följande fyra kategorier:

- Stora bokstäver (A-Z)
- Små bokstöver (a-z)
- Siffror (0-9)
- Specialtecken (! ” # $ ’ ( ) * , - . / [\ ] ^ _ `{ | } ~ : ; < = > @)

Lösenord för heller inte återanvändas.

Byte av lösenord är aktuellt:

- Var 360:e dag när det gäller interna nätverket. En dialogruta visas automatiskt på bildskärmen när det är dags.
- För enskilda system efter en viss tidsintervall som bestäms av respektive systemägare.
- Omedelbart om du misstänker att någon annan känner till det eller om din dator har utsatts för virus.

Lösenorden spärras vid 5 felaktiga inloggningsförsök.

Exempel på lösenord:

Ett bra exempel är att använda ett ord som du lätt kan komma ihåg och byta ut bokstäver mot specialtecken samt att lägga till en siffra. Ordet diplomet kan t.ex. bli d4ipl@meT

4 Utrustning

Följande gäller för den utrustning du förfogar över, det vill säga stationär och/eller bärbar PC med tillhörande utrustning:

- Fysiska ingrepp får endast utföras av IT-avdelningen.
- Fel ska omgående anmälas till IT-avdelningens helpdesk.
- All installation och konfiguration ska utföras av eller i samråd med IT-avdelningen.

Din arbetsplatsutrustning är kommunens egendom och får inte bytas, flyttas permanent eller förändras utan IT-avdelningens medverkan.

När du lämnar arbetsplatsen för dagen ska du alltid stänga av din dator av miljö- och säkerhetsskäl. En bordsdator, som står påslagen dygnet runt, kan under ett år förbruka upp till 500 kWh el. Vissa säkerhetsuppdateringar aktiveras endast vid omstart eller inloggning.

Utöver de regler som gäller för stationära datorer gäller särskilda säkerhetsregler för dig som använder en personlig, bärbar tjänstedator:

Du ska inte lämna datorn utan uppsikt, t.ex. i bilen eller på allmänna platser.

Endast mobil utrustning som tillhör kommunen får anslutas i kommunens lokala nät. Inkoppling får endast ske i samråd med IT-avdelningen.

4.1 Kassering av utrustning

Kasserad utrustning ska alltid lämnas till IT-avdelningen. Kontakta IT-avdelningens helpdesk för instruktioner.

4.2 Lås dator när du lämnar din arbetsplats

Vid tillfällen när du inte har uppsikt över arbetsstationen ska du alltid låsa arbetsstationen (windowsflaggan+L eller Ctrl+Alt+Del och Enter).

4.3 Upplåtelse av din arbetsplats

Du får aldrig låta någon annan använda din arbetsplats (dator) utan att först logga ut. Undantag kan göras för IT-avdelningens personal eller av IT-avdelningens anvisad/godkänd person.

4.4 Programvaror

Egna program får inte installeras i Borgholms kommuns datorer.

Programvaror ska godkännas och installeras av IT-avdelningen.

Appar i mobiltelefoner/läsplattor får installeras av användaren men enbart om de behövs för arbetsuppgiften.

***Obs!** Appar bör hanteras med försiktighet då dessa i vissa fall samlar in mer information från mobilen än vad den behöver för uppgiften. De insamlade uppgifterna kan sedan företaget bakom appen förädla och sälja vidare till andra aktörer.*

5 Hantering av information

I ditt dagliga arbete kommer du i kontakt med information i många olika former. Informationen kan vara muntlig, skriftlig, lagrad i datorer via e-post med mera. För att du ska få den information som du behöver, vid rätt tidpunkt och med korrekt innehåll, har kommunen som övergripande mål för informationssäkerhetsarbetet att vi ska:

- Behandla information på ett tydligt, korrekt, säkert och relevant sätt.
- Kunna leverera och hämta information vid rätt tidpunkt.

En stor mängd handlingar och uppgifter kan vara sekretesskyddade. Det är därför viktigt att du känner till de sekretessregler handlingarna och uppgifterna omfattar.

5.1 Klassning av information

All information i en organisation har inte samma behov av skydd och därför är en central aktivitet i säkerhetsarbetet informationsklassning vars funktion är att bedöma informationens värde och känslighet. Bedömningen sker både utifrån den egna verksamhetens behov och utifrån externa krav. Avsikten är att varje informationstillgång ska omges med rätt skydd.

Informationssystemen klassas utifrån den information som hanteras. Klassning görs från aspekterna konfidentialitet (sekretess), riktighet, tillgänglighet och spårbarhet:

- Sekretess: Att informationen skyddas från obehörig insyn.
- Riktighet: Att informationen inte ändras på ett obehörigt sätt.
- Tillgänglighet: Att informationen finns tillgänglig för rätt person vid rätt tillfälle.
- Spårbarhet: Att specifika aktiviteter som rör informationen kan spåras.

Tas information ut ur systemet och lagras på andra media, eller används i ett annat sammanhang, måste den klassas där den används och hanteras därefter. Även information i arbetsmaterial måste klassas. Kontakta informationsägaren (din närmaste chef) för frågor.

Innan du lagrar eller hanterar dokument bör du alltid fråga dig:

- Vem ska kunna se informationen?
- Vem ska kunna ändra informationen?
- Var bör informationen lagras?

5.2 Lagring av information

Som stöd i det dagliga arbetet har vi flera olika IT-baserade verksamhetssystem, t.ex. ekonomi- och lönesystem, system för elevadministration och journalhantering. I dessa system finns inbyggda regelverk som ger rättigheter eller sätter begränsningar för dig att hantera informationen.

Utöver att arbeta i våra verksamhetssystem kommer du att upprätta egna handlingar och dokument, exempelvis med Word eller Excel. Du är vid sådana lägen ansvarig för informationen.

5.3 Lagring på administrativt nätverk

Den information du lagrar på vårt nätverk säkerhetskopieras automatiskt.

Utrymmen på nätet som kan läsas och användas av fler personer ska inte användas för att lagra sekretesskyddad information.

Information ska heller inte lagras på dators hårddisk (C:) då vi inte kan säkerställa att informationen bevaras.

5.4 Lagring på mobila enheter

Mobila enheter är som regel stöldbegärlig egendom. Alla mobila lagringsenheter kräver därför särskild uppmärksamhet ur ett informationssäkerhetsperspektiv.

Mobila lagringsenheter kan vara fristående eller integrerade.

Exempel på mobila lagringsenheter är CD- och DVD-skivor, USB-minnen, fristående hårddiskar eller hårddisken i en bärbar dator, internminnet i en mobiltelefon, en MP3-spelare eller en digitalkamera och de löstagbara minneskorten till dessa. Lagring av arbetsrelaterad information på privata enheter är inte tillåtet. Däremot kan man via Internet till exempel logga in på email.morbylanga.se för att läsa sin e-post utan att lagra någon information på sin enhet.

Kontakta IT-avdelningens helpdesk om du har frågor kring säkerheten för mobila enheter.

En bärbar tjänstedator som används utanför kommunens nätverk utsätts för större risker än en stationär dator. Därför ska du vara extra försiktig med vad du lagrar på din bärbara dator i fall den blir stulen.

Följande gäller för lagring av information på bärbar dator:

Kontrollera med informationsägaren (din närmast ansvarige chef) om det är tillåtet att kopiera informationen till flyttbart media som du sedan till exempel tar med hem.

När det gäller bärbara datorer där offlinehanteringen är aktiverad bör du kontinuerligt kontrollera att ingen information går förlorad vid synkroniseringen, och att all viktig information säkerhetskopieras. Kontakta IT-avdelningens helpdesk för frågor.

Din mobil eller läsplatta

Din mobiltelefon/läsplatta har inte samma skyddsmekanismer som en bärbar dator. Den saknar oftast brandvägg, virusskydd och krypteringsmöjlighet. Även om du har låskoder på telefonen/läsplattan så kan en obehörig ändå plocka ut minneskortet och läsa det på olika sätt. Därför ska du inte lagra verksamhetsinformation på din mobil/läsplatta.

Låskoden ska dock alltid vara aktiverad på telefonen/läsplattan.

Lämna aldrig mobiltelefonen/läsplattan obevakad – den är stöldbegärlig.

Funktionerna i telefonen/läsplattan medger att andra kan ansluta till den genom att du ändrar i olika inställningar i programvaran. Det bör undvikas då risken därmed ökar för obehöriga att manipulera din enhet.

6 Utskrifter

Utskrifter av känslig eller sekretessbelagd information på gemensamma nätverksskrivare kräver särskild försiktighet.

Tänk på att du är ansvarig för att informationen du skriver ut skyddas mot obehöriga.

Låt inte dina utskrifter ligga kvar i skrivaren, hämta dem omgående. Detta gäller för gemensamma skrivare där dina utskrifter inte säkras från obehöriga genom personlig kod, tagg eller SITHS-kort.

Makulerad, känslig information ska omgående förstöras i papperstuggen. En papperstugg bör därför finnas tillgänglig för alla.

7 Internet

När du använder Internet kan säkerheten i Borgholms kommuns lokala nätverk påverkas i mycket hög grad beroende på ditt beteende.

Den som från sin arbetsplats surfar eller laddar ner filer från Internet ska göra det med gott omdöme och endast hämta in sådant som är relevant för arbetet, och kommer från välkända och seriösa webbplatser.

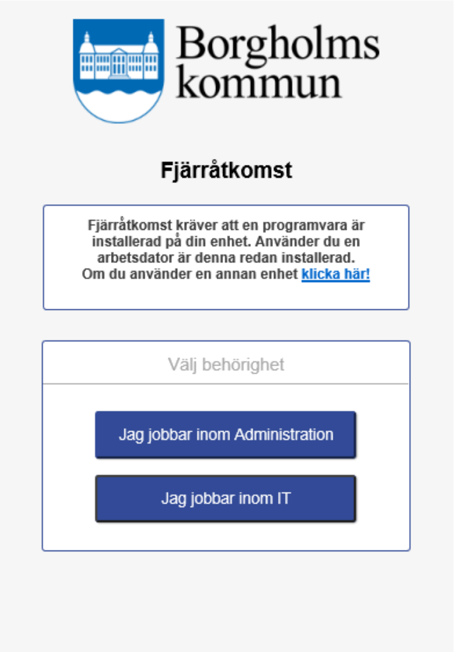
Det är inte tillåtet att via Internet titta eller lyssna på material av pornografisk eller rasistisk karaktär. Förbudet gäller också material som är diskriminerande eller har anknytning till kriminell verksamhet.

I specifika fall kan det dock vara motiverat för arbetet, till exempel vid utredningar, omvärldsanalyser med mera, att besöka sidor som normalt är förbjudna. Beslut om detta ska fattas av närmaste chef.

Tänk på att när du surfar på Internet representerar du Borgholms kommun.

8 Andra externa nät

Arbete utanför kommunens lokaler som kräver uppkoppling mot våra interna nätverk får enbart ske via lösning som tillhandahålls av IT-avdelningen. Kontakta IT-avdelningens helpdesk om du har frågor.



Fjärråtkomst

Fjärråtkomst kräver att en programvara är installerad på din enhet. Använder du en arbetsdator är denna redan installerad. Om du använder en annan enhet klicka här!

Exempel på lösning för uppkoppling mot vårt nät.

9 E-post

Din e-postadress representerar Borgholms kommun och får endast användas i arbetet.

E-postsystemet ska bara användas för information som inte kan hanteras via verksamhetssystem. E-postsystemet får inte användas för att skicka sekretessbelagd information eller känsliga personuppgifter eller personnummer om inte meddelandet är krypterat.

För e-post gäller samma offentlighets-, sekretess- och arkivbestämmelser som för handlingar som skickas med vanlig post eller fax.

E-post är ofta bärare av skadlig kod och andra bedrägeriförsök. All e-post skannas men kan ändå innehålla skadlig kod eller vara ett bedrägeriförsök.

Bilagor, länkar och bilder kan vara skadliga även om e-posten ser ut att komma från en känd avsändare. Kontakta alltid IT-avdelningens helpdesk om du är osäker.

Kontrollera vilka som är medlemmar på sändlistor (lokala och centrala sändlistor) innan du använder dem så att inte information når fel mottagare. Är du osäker kontakta IT-avdelningens helpdesk.

E-postsystemet ska inte användas som ett arkivsystem!

10 Incidenter, virus med mera

En IT-incident är en oönskad och oplanerad IT-relaterad händelse som påverkar säkerheten i organisationens eller samhällets informationshantering och som kan innebära en störning av organisationens förmåga att bedriva sin verksamhet.

En incident kan vara i stort sett vad som helst, från borttappade lappar med lösenord till misslyckad säkerhetskopiering, driftavbrott, försök till dataintrång och virusangrepp. En incident kan vara en medveten handling eller ske helt oavsiktligt.

Säkerhetsincidenter och brister som kan utgöra ett hot mot säkerheten måste snarast rapporteras till IT-avdelningen.

Om du misstänker att någon använt din användaridentitet eller att du varit utsatt för någon annan typ av incident ska du:

- Notera när du senast var inne i IT-systemet.
- Notera när du upptäckte incidenten.
- Omedelbart anmäla förhållandet till IT-avdelningen och din chef.
- Dokumentera alla iakttagelser i samband med upptäckten och försöka fastställa om kvaliteten på din information har påverkats. Blankett för incidentrapportering finns på kommunens intranät.

Om du upptäcker fel och brister i de system du använder ska du rapportera dessa till systemförvaltaren.

Borgholms kommun har programvaror för viruskontroll både i klienterna och i nätverket, men kan ändå drabbas av effekter av så kallad skadlig kod.

Om du misstänker att din dator innehåller virus ska du:

- Dra ut nätverkskabeln ur antingen datorn eller vägguttaget, men låta datorn vara på.
- Omedelbart anmäla förhållandet till IT-avdelningen. OBS! Anmälan ska ske per telefon eller besök, inte per e-post.

Om du får brev med virusvarning (från annan avsändare än IT-avdelningen) där man talar om att ett virus är på gång, ska du inte skicka meddelandet vidare. Kontakta IT-avdelningen, de kan avgöra om det är en seriös varning eller ett falsklarm.

Bärbara datorer, läsplattor, digitala kameror, mobiltelefoner med mera kan lätt bli virusbärare eftersom du kan mellanlagra information från olika datorer i dessa. Var noga med att den dator du ansluter sådan kringutrustning till har ett uppdaterat antivirusprogram. Kontakta IT-avdelningens helpdesk vid frågor om antivirusprogram till mobiltelefoner och läsplattor.

10.1 Vad är personuppgiftsincidenter?

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks. Exempel:

- diskriminering, identitetsstöld, bedrägeri, skadlig ryktesspridning
- finansiell förlust
- brott mot sekretess eller tystnadsplikt.

En personuppgiftsincident har till exempel inträffat om uppgifter om en eller flera registrerade personer har

- blivit förstörda
- gått förlorade på annat sätt
- kommit i orätta händer.

Det spelar ingen roll om det har skett oavsiktligt eller med avsikt. I båda fallen är det personuppgiftsincidenter.

11 Avslutning av anställning eller förändrad anställning

Om din anställning i kommunen ändras eller din anställning upphör ansvarar du för att:

- Rådgöra med din chef om vilka delar av ditt arbetsmaterial som ska sparas. Notera att arbetsmaterial anses vara Borgholms kommuns egendom och får inte tas med utan chefs godkännande.

- Om din anställning i kommunen ändras är närmaste chef ansvarig för att se till att du har rätt behörighet till de IT-system du behöver i arbetet.

12 Stöd och hjälp

Om du behöver hjälp med din IT-utrustning eller om du undrar över något som gäller informationssäkerhet ska du kontakta IT-avdelningens helpdesk:

- Telefon: Anknytning 854 00
- E-post: helpdesk@borgholm.se

13 Information på datamedia

Med datamedia menas DVD-skivor, CD-skivor, disketter, USB-minnen, minnen till mobiltelefoner eller läsplattor etcetera. Dessa medier ska inte ses som slutliga förvaringsformer, såvida de inte avser backup-tagning. Information på datamedia är alltid kopierad och måste hanteras med samma säkerhet som det system som den kommer ifrån vad gäller riktighet och konfidentialitet.

De krav på sekretess, tillgänglighet, riktighet och spårbarhet som ställs för ett specifikt IT-system (informationssystem) framgår av den informationsklassning som löpande genomförs och är kända av systemägaren, systemförvaltaren, informationsägaren, dataskyddssamordnaren, dataskyddsombudet, informationssäkerhetssamordnaren samt IT-avdelningen.

För information på datamedia gäller följande krav:

Krav på sekretess	**Åtgärder**

Nivå 4	**Förvaring** Bärbar dator, USB-minnen och dylikt som används ska förvaras i låst säkerhetsskåp när de inte används. Bärbar dator får ej anslutas till mobilt eller fast nätverk. Endast lokal skrivare (ska förvaras i låst säkerhetsskåp när den inte används) får anslutas till datorn. **Kopiering** Kopiering får endast ske efter godkännande av informationsägaren. **Spridning** Får flyttas fysiskt efter samråd med informationsägaren om lämpligt tillvägagångsätt. Får endast distribueras till behöriga (skriftlig kvittens ska alltid begäras vid överlämning av mediet. Kvittens förvaras hos informationsägaren). **Återanvändning** Mediet får inte användas för annan information. **Makulering** Lämnas till IT-avdelningen för förstöring.
Nivå 3	**Förvaring** Vid lagring på bärbar dator och dylikt ska godkänd kryptering användas. CD-skivor, USB-minnen och dylikt som används ska förvaras säkert så att de ej är tillgängliga för obehöriga. **Kopiering** Kopiering får endast ske efter godkännande av informationsägaren. **Spridning** Får flyttas fysiskt efter samråd med informationsägaren om lämpligt tillvägagångsätt. Får endast distribueras till behöriga. **Återanvändning** Får inte användas för annan information utan att först ha överskrivits med programvara för säker filradering. **Makulering** Lämnas till IT-avdelningen för förstöring.

Nivå 2	**Förvaring** Vid lagring på bärbar dator och dylikt ska godkänd kryptering användas. De CD-skivor, USB-minnen och dylikt som används ska förvaras säkert så att de inte är tillgängliga för obehöriga. **Kopiering** Får endast kopieras i samråd med informationsägare. **Spridning** Får endast distribueras till behöriga läsare. **Återanvändning** Får inte användas för annan information utan att först ha överskrivits med programvara för säker filradering. **Makulering** Lämnas till IT-avdelningen för förstöring.
Nivå 1	**Förvaring** Inga krav på kryptering. **Kopiering** Tillåten. **Spridning** Får ske då det rör sig om allmänna offentliga handlingar utan personuppgifter som kan upplevas som känsliga i något avseende. **Återanvändning** Får användas för annan information. **Makulering** Krävs ej.

14 Information på andra media som inte är elektroniska

Med andra media menas papper, film, OH-bilder etcetera. Information på dessa media är alltid kopierad och måste hanteras med samma säkerhet som det system som den kommer ifrån vad gäller riktighet och konfidentialitet.

De krav på sekretess, tillgänglighet, riktighet och spårbarhet som ställs för ett specifikt IT-system (informationssystem) framgår av den informationsklassning som löpande genomförs och är kända av systemägaren, systemförvaltaren, informationsägaren, dataskyddssamordnaren, dataskyddsombudet, informationssäkerhetssamordnaren samt IT-avdelningen.

För information på ovanstående media gäller följande krav:

Krav på sekretess	**Åtgärder**
Nivå 4	**Förvaring** Förvaras inlåsta i säkerhetsskåp. **Kopiering** Får kopieras endast med godkännande från informationsägaren. **Överföring** Rekommenderat brev. Eller per bud med kvittens. **Destruktion** Destrueras (strimlas).
Nivå 3	**Förvaring** Förvaras inlåsta. **Kopiering** Får kopieras endast med godkännande från informationsägaren. **Överföring** Rekommenderat brev. Eller per bud. **Destruktion** Destrueras (strimlas).
Nivå 2	**Förvaring** Ej förvaras synligt. **Kopiering** Får kopieras endast i samråd med informationsägaren. **Överföring** Fax eller per brev. **Destruktion** Destrueras (strimlas).

Nivå 1	**Förvaring** Inga krav. **Kopiering** Tillåten. **Överföring** Inga restriktioner. **Destruktion** Krävs ej.

Borgholms kommun

Kommunledningskontoret
Niklas Palmquist, 0485-88221
niklas.palmquist@borgholm.se

INSTRUKTION

Datum
2018-12-28

Informationssäkerhetsinstruktioner Förvaltning

InfoSäk F - Roller och ansvar

Innehållsförteckning

1 Personuppgiftsansvarig

Ansvaret för personuppgiftsbehandlingarna kan skifta beroende på var de hanteras. I en kommun är kommunfullmäktige, kommunstyrelsen och övriga kommunala nämnder personuppgiftsansvariga, var och en i sin verksamhet.

Personuppgiftsansvarig är den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Den personuppgiftsansvarige har ansvar för att behandlingen av personuppgifter sker på ett lagligt och korrekt sätt i enlighet med dataskyddsförordningens krav. Det innebär bland annat att man ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att personuppgiftsbehandlingen sker på ett integritetsrättsligt säkert sätt.

Ytterligare krav är att den personuppgiftsansvarige ska se till att den enskilde får rätt information om personuppgiftsinsamlingen och att informationen lämnas på ett enkelt och för den enskilde anpassat språk.

2 Personuppgiftsbiträde

Personuppgiftsbiträde är den som behandlar personuppgifter för den personuppgiftsansvariges räkning. Ett personuppgiftsbiträde finns alltid utanför den egna organisationen. En anställd eller någon annan som behandlar personuppgifter inom den personuppgiftsansvariges direkta ansvar är inte personuppgiftsbiträde.

Ett personuppgiftsbiträde kan vara antingen en fysisk eller en juridisk person. Om en personuppgiftsansvarig till exempel anlitar en tjänsteleverantör blir denna ett personuppgiftsbiträde som får behandla personuppgifter enligt den personuppgiftsansvariges instruktioner. Ett skriftligt avtal (personuppgiftsbiträdesavtal) måste upprättas.

Det är den personuppgiftsansvarige som ansvarar för att avtalet finns. I avtalet ska det särskilt föreskrivas att personuppgiftsbiträdet får behandla personuppgifterna bara i enlighet med instruktionerna och att biträdet måste vidta de säkerhetsåtgärder som den personuppgiftsansvarige ska vidta.

Alla frågor som rör personuppgiftsbiträdesavtal ska hanteras tillsammans med dataskyddssamordnaren.

3 Dataskyddsombud

Dataskyddsombudet är den person som har särskilt ansvar för att se till att dataskyddslagstiftningen efterföljs och som bistår den som behandlar personuppgifter att bevaka dataskyddsfrågor. Dataskyddsombudet kan jämföras med en internrevisor som påpekar fel och brister i behandlingen av personuppgifter till den som är personuppgiftsansvarig. Dataskyddsombudet är en fysisk person, till skillnad från personuppgiftsansvarig och biträdet. Dataskyddsombudet kan vara en anställd eller externt anlitad person som har särskild kunskap och insikt i personuppgiftsbehandling och dataskyddsförordningen (GDPR).

Som ett led i skyldigheten att övervaka efterlevnaden ska dataskyddsombuden

- samla in information för att identifiera hur behandling av personuppgifter sker,
- analysera och kontrollera huruvida bestämmelser om behandlingen efterlevs, och
- informera samt ge råd och utfärda rekommendationer till den personuppgiftsansvarige eller personuppgiftsbiträdet.

Det är den personuppgiftsansvarige som har ansvaret för att reglerna i dataskyddsförordningen efterlevs, inte dataskyddsombudet.

3.1 Dataskyddsombudets ställning[1]

Enligt artikel 38 i den allmänna dataskyddsförordningen ska den personuppgiftsansvarige och personuppgiftsbiträdet säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter.

Dataskyddsombudet ska informeras och rådfrågas på ett tidigt stadium i alla frågor som rör personuppgifter. Dataskyddsombudet ska ses som en viktig diskussionspartner och bör ingå i de arbetsgrupper som har ansvar för behandling av personuppgifter inom organisationen.

Kommunen ska bland annat säkerställa följande:

- Dataskyddsombudet ska regelbundet inbjudas att delta i möten på högsta och mellanliggande förvaltningsnivå,
- Dataskyddsombudet inbjuds att delta när beslut med följder för dataskyddet fattas. All relevant information ska i god tid förmedlas till dataskyddsombudet så att han eller hon kan ge lämpliga råd.
- Dataskyddsombudets åsikt måste alltid ges tillbörlig vikt. I händelse av oenighet ska skälen till att dataskyddsombudets råd inte har följts dokumenteras.
- Dataskyddsombudet ska omedelbart kontaktas när en personuppgiftsincident eller annan incident har inträffat.

I dataskyddsförordningens artikel 38.3 fastställs vissa grundläggande garantier för att bidra till att säkerställa att dataskyddsombuden kan fullgöra sitt uppdrag och utföra sina uppgifter på ett tillräckligt självständigt sätt inom organisationen.

Personuppgiftsansvariga/personuppgiftsbiträden ska säkerställa att dataskyddsombudet inte tar emot instruktioner som gäller utförandet av sina uppgifter. Dataskyddsombudet ska, oavsett om de är anställda av den personuppgiftsansvarige eller ej, kunna fullgöra sitt uppdrag och utföra sina uppgifter på ett oberoende sätt.

Detta innebär att dataskyddsombud, när de utför sina uppgifter inte får instrueras om hur de ska hantera en fråga, till exempel vilka resultat som

---

[1] *Riktlinjer om dataskyddsombud. Artikel 29-arbetsgruppen för skydd av personuppgifter.*

bör uppnås, hur ett klagomål ska utredas eller huruvida tillsynsmyndigheten ska rådfrågas eller ej. Dataskyddsombuden får inte heller instrueras att inta en viss ståndpunkt i frågor som rör dataskyddslagstiftningen, till exempel en viss tolkning av lagen.

4 Dataskyddssamordnare

Dataskyddssamordnaren är den person i kommunen som har det samordnande ansvaret kring arbetet med gällande dataskyddslagstiftning och den som bistår dataskyddsombudet i frågor som rör personuppgiftshantering.

Dataskyddssamordnaren fungerar som organisationens tjänsteman kring personuppgiftshantering, och är personuppgiftsansvariges koppling till dataskyddsombudet.

Dataskyddssamordnaren är en fysisk person och har rapporteringsskyldighet till ledningsgruppen.

Dataskyddssamordnaren är en anställd som har särskild kunskap och insikt i personuppgiftsbehandling och dataskyddsförordningen (GDPR). I uppdraget ingår bland annat att

- samla in information för att identifiera hur behandling av personuppgifter sker,
- analysera och kontrollera huruvida bestämmelser om behandlingen efterlevs,
- informera samt ge råd och utfärda rekommendationer till den personuppgiftsansvarige eller personuppgiftsbiträdet,
- informera, ge råd och utfärda rekommendationer på individ- och verksamhetsnivå,
- praktiskt i kommunen arbeta med frågor rörande personuppgifter.

4.1 Dataskyddssamordnarens ställning

Organisationen ska säkerställa att dataskyddssamordnaren alltid informeras och rådfrågas i frågor som rör hantering av personuppgifter och vara sammankallande i den centrala GDPR-gruppen.

- Dataskyddssamordnaren ska regelbundet inbjudas att delta i möten på högsta och mellanliggande förvaltningsnivå,
- Dataskyddssamordnaren ska delta när beslut med följder för dataskyddet fattas. All relevant information ska i god tid förmedlas till dataskyddssamordnaren så att han eller hon kan ge lämpliga råd.
- Dataskyddssamordnaren ska rådfrågas omedelbart när en personuppgiftsincident eller annan incident har inträffat.

5 Informationssäkerhetssamordnaren

Leder och samordnas Informationssäkerhetsarbetet och ska tillsammans med verksamheterna;

- hålla styrande dokument inom området aktuella, som informationssäkerhetspolicy och riktlinjer för informationssäkerhet,
- utveckla och förvalta metoder, vägledningar och annat stödmaterial inom informationssäkerhetsområdet,
- ta fram kompetensförsörjningsplaner för att öka informationssäkerhetsmedvetandet inom kommunen, tex genom rådgivning och utbildning,
- stödja verksamheterna i frågor som rör informationssäkerhet,
- kontrollera och följa upp informationssäkerheten,
- omvärldsbevaka inom informationssäkerhetsområdet
- Informationsäkerhetssamordnaren ska även stödja dataskyddsombudet i sitt arbete.

6 Förvaltningschef

Respektive förvaltningschef ansvarar för att informationssäkerhetsarbetet bedrivs i linje med informationssäkerhetspolicyn.

Förvaltningschefen ansvarar för att systemägare och informationsägare utses för respektive informationssystem.

Förvaltningschefen är per automatik systemägare och informationsägare för ett informationssystem så länge annan systemägare och informationsägare inte är utsedda och anmälda till IT-avdelningen och dataskyddsombudet.

Ansvarsfördelning och roller ska säkerställa att ett informationssystem kan administreras och hanteras på ett sådant sätt att det under hela sin livstid bidrar till att stödja avsedd verksamhet och uppfylla informationssäkerhetspolicyns mål.

För varje informationssystem utses nedanstående roller för att ge en tydlig ansvarsfördelning. I vissa fall kan samma person inneha flera av dessa roller.

Kommunens ledningsgrupp beslutar om vilka informationssystem som är verksamhetskritiska. Systemägare för dessa verksamhetskritiska system ansvarar för att en informationsklassning av systemets information utförs. Det verktyg som används i Borgholms kommun är Klassa.

7 Systemägare

Förvaltningschefen utser de personer, med resurser och befogenheter att klara nedanstående ansvar, som ska vara systemägare.

Systemägaren ansvarar för att egna informationssystem förvaltas på för verksamheten bästa sätt. Vid nyanskaffning eller större förändringar av informationssystem ska systemägaren alltid samråda med IT-chefen, dataskyddsombudet och arkivansvariga på ett tidigt stadium.

Systemägaren fattar de avgörande besluten om informationssystemets införande, förvaltning, drift och avveckling. Systemägarens ansvar kan inte, med undantag för funktionen IT-chef, delegeras till funktion/person utanför den kommunala organisationen.

Systemägaren har ansvar för bland annat följande inom ramen för tilldelade resurser (både personella och ekonomiska):

- att genomföra systemsäkerhetsanalys av systemet, se rubrik Systemsäkerhetsanalys,
- att utse systemförvaltare,
- att informationen i systemet hanteras i enlighet med informationssäkerhetspolicyn,
- att det finns en överenskommelse med IT-avdelningen för reglering av driftansvaret,
- att regler och riktlinjer för systemet finns,
- att information och utbildning ges till berörd personal,
- att systemet utvecklas i linje med kommunens IT-strategi och informationssäkerhetspolicy,
- att godkänna nya versioner av systemet,
- att licenser finns i erforderlig mängd och att en överlämning sker av licenserna och programvara till IT-avdelningen vid installation,
- att fastställa felhanteringsrutiner, gallringsrutiner och rutiner för arkivleveranser för systemet,
- att besluta om avveckling av systemet,
- att systemet är väldokumenterat,
- att besluta om vilka i kommunen som har behörighet (inklusive rätt behörighetsnivå) till systemet,
- att en kontinuitetsplanering utförs, se rubrik kontinuitetsplanering
- att driftgodkänna informationssystemet.

7.1 Systemägaren - dataskyddsförordningen och dataskyddslagen

Ansvarar för att behandlingen är laglig. Det innebär att innan en behandling påbörjas ska systemägaren säkerställa att behandlingen uppfyller alla de lagkrav som finns.

Dessutom ansvarar systemägaren för att rutiner finns för hur fritextfält får användas och att en anmälan har gjorts till dataskyddsombudet innan behandlingen påbörjas.

Systemägaren ska tidigt i processen med att skaffa det nya systemet eller planera för den nya behandlingen se till att dataskyddsombudet, dataskyddssamordnaren, Informationssäkerhetssamordnaren informeras via e-post: gdpr@borgholm.se

Utöver detta ska systemägaren se till att vid behov personuppgiftsbiträdesavtal har upprättats.

8 Systemförvaltare

Systemförvaltare är de som aktivt förvaltar IT-systemet på systemägarens uppdrag. Systemförvaltare utses av systemägaren.

Systemförvaltarens roll är bland annat att:

- Ansvara för att all information och användarstöd finns tillgänglig,
- ansvara för utbildningsfrågor samt kontakter med leverantören gällande systemets funktioner,
- stödja genom att analysera, kartlägga och dokumentera systemet,
- uppmärksamma förbättringar, initiera och implementera förändringar,
- säkerställa interaktion med andra system,
- följa upp genom att ansvara för att krav och behov samlas in från verksamheten samt att dessa rapporteras till systemägaren,
- verkställa beslut som systemägaren fattar,
- informera sig om och bli väl förtrogen med programmets innehåll struktur och termer,
- upprätta, dokumentera, införa och utvärdera systemförvaltarrutiner,
- regelbundet göra stickprov i systemets loggar utifrån kraven på informationssäkerhet och i enlighet med systemägarens beslut,
- se till att uppgifterna i systemet är aktuella och korrekta,
- se till att användarna/grupperna har rätt behörighet i systemet,
- tillhandahålla aktuell användarhandledning,
- ansvara för användarsupporten rörande verksamhetsrelaterade frågor i systemet,
- rapportera och förbereda ärenden och beslut som ska hanteras av systemägaren,
- rapportera fel, brister, regelbrott och oegentligheter till systemägaren, dataskyddsombudet, IT-chef.
- hantera felanmälningar från IT-avdelningens helpdesk och åtgärda eller vidarebefordrar problemet till leverantören,
- ge förslag till ändringar/utveckling av systemet,
- ansvara för arbetet med säkerhetsfrågor som rör systemet,

- ansvara för planering av datum för produktionssättning inför nya releaser/versioner i samråd med IT-avdelningen,
- ansvara för att samtliga användare i systemet är informerade om planerade driftavbrott,
- ansvara för tester vid uppdateringar, felrättningar och återläsning från backup,
- ansvara för kontroll och uppföljning av överenskommelse med IT-avdelningen om reglering av driftansvaret,
- se till att reservrutiner, serviceavtal med mera finns så att systemägarens krav på lägsta tillåtna avbrottstid kan tillgodoses,
- se till att det finns lättillgänglig användardokumentation och handböcker till systemen, samt att dessa hålls aktuella och väl spridda hos användarna,
- ansvara för att skicka information till IT-avdelningen,
- ansvara för arkivleveranser,
- besluta i samråd med driftsansvarig tekniker hur informationen ska säkerhetskopieras.
- Upprätthålla dokumentationen kring systemet

Dokumentation kring systemet skall minst innehålla (se rubrik Dokumentation):

- Lista på informationsägare
- Kontaktuppgifter till leverantör
- Avtalsinformation (slutdatum och förvaring av original)
- Utsedd driftansvarig tekniker
- Rutiner och riktlinjer kring systemet
- Kontinuitetsplanering, se rubrik Kontinuitetsplanering,
- Systemsäkerhetsanalyser

8.1 Systemförvaltare - dataskyddsförordningen och dataskyddslagen

Systemförvaltaren biträder systemägaren i frågor som rör behandlingens laglighet. Dessutom ser systemförvaltaren till att det finns regler för behörighetstilldelning och att de följs.

Systemförvaltaren ser också till att alla de regler och rutiner som bestämts för behandlingen efterlevs i vardagen. Systemförvaltaren ser till att föreskriven gallring genomförs, att information enligt artikel 15 lämnas, att rättelse enligt artikel 16 görs, att personuppgifter inte olagligt överförs till tredje land samt att anmälan till personuppgiftsombudet görs varje gång någon förändring sker av de uppgifter som tidigare anmälts till ombudet.

Systemförvaltaren ska också hålla sig uppdaterad på förändringar i lagstiftningen som kan komma att påverka behandlingen. Systemförvaltaren ska hålla systemägaren informerad om sådant som kan påverka systemägarens uppdrag och ansvar.

Systemförvaltaren är också den som oftast har den direkta kontakten med ev. personuppgiftsbiträden och kontrollera att de lever upp till reglerna i dataskyddsförordningen, dataskyddslagen och i biträdesavtalet.

9 Informationsägare

Informationsägare är den som äger och ansvarar för att informationen är riktig och tillförlitlig samt för det sätt informationen sprids. Informationsägaren är därmed riskägare för den information som ska hanteras inom sitt ansvarsområde. För att hantera risken bör även informationsägaren genomföra en riskanalys. Om det finns flera informationsägare bör samtliga delta i riskanalysen.

Eftersom skadeverkningarna av bristande informationssäkerhet uppstår hos informationsägaren är det informationsägaren som måste bedöma risker och ställa krav om bland annat informationsklassning.

De interna relationerna mellan informationsägare och systemägare bör, när det gäller informationssäkerhet, utgå från informationsägaren.

9.1 Informationsägare - dataskyddsförordningen och dataskyddslagen

Informationsägaren ansvarar för att informationen uppfyller kraven enligt lag så att alla uppgifter är korrekta, aktuella och adekvata i förhållande till behandlingens ändamål och att uppgifter som ska gallras verkligen också blir gallrade ur systemet.

Informationsägaren måste arbeta nära tillsammans med systemförvaltaren i de fall informationen finns i ett verksamhetssystem och i viss utsträckning se till att systemförvaltaren utför det som måste göras för att reglerna i dataskyddsförordningen och dataskyddslagen följs. Informationsägaren ser också till att alla uppgifter som behandlas är tillåtna enligt lagen.

Informationsägaren måste också se till att känsliga personuppgifter, personnummer och uppgifter om brott behandlas endast i överensstämmelse med reglerna i lagen. Till exempel att samtycken inhämtas när så behövs och att dessa hanteras på ett korrekt sätt.

Informationsägaren måste också bevaka att informationen är skyddad på en tillräcklig nivå utifrån resultatet av riskanalysen och informationsklassningen.

10 IT-chef

IT-chefen är ansvarig för IT-säkerheten (teknik och rutiner). IT-chefen är systemägare inom området teknisk infrastruktur och har det övergripande ansvaret för att ett systems tekniska delar fungerar.

IT-chefen samverkar med systemägare vad avser drift och resurstilldelning för ett informationssystem och ansvarar också för att informationssäkerhetsinstruktion Kontinuitet och drift samt en kontinuitetsplan för driften av IT-verksamheten upprättas och att den senare integreras med Borgholms kommuns gemensamma kontinuitetsplan.

IT-chefen har bland annat ansvar för:

- att systemsäkerhetsanalys för teknisk IT-infrastruktur upprättas och hålls aktuell,
- att delta i och stödja informationssäkerhetsarbetet,
- att efter beställning tilldela och administrera behörigheter till den gemensamma infrastrukturen,
- utformning av förslag på den strategiskt långsiktiga och övergripande IT-utvecklingen för Borgholms kommun,
- att omvärldsbevakning för Borgholms kommun sker,
- att i samråd med systemägare se till att systemet fungerar ihop med samverkande informationssystem,
- att testmiljö finns tillgänglig vid behov,
- att teknisk IT-infrastruktur hålls uppdaterad med buggfixar och säkerhetsuppdateringar,
- att rutiner för säkerhetskopiering uppfyller systemägarnas krav,
- att säkerhetskopierat material förvaras på ett betryggande sätt och att det regelbundet kontrolleras att återläsningsrutiner fungerar,
- att IT-avdelningens reservrutiner, serviceavtal med mera finns så att systemägarnas krav på längsta tillåtna avbrottstid kan tillgodoses,
- att tillhandahålla teknisk support för användare (Helpdesk),
- att biträda systemägarna i avbrottsplaneringen,
- att vara teknisk rådgivare till systemägarna då förändringar i systemen är aktuella,
- att den tekniska IT-infrastrukturens säkerhet motsvarar systemägarnas krav och uppfyller krav enligt systemsäkerhetsanalyserna,
- att ett informationssystem håller den tekniska och funktionella kvalitet som överenskommits med systemägaren,
- administration av organisationens brandväggar och skydd mot skadlig kod,
- att dokumentet InfoSäk KD upprättas och är aktuell,
- att sammanställa och rapportera IT-säkerhetsincidenter till dataskyddsombudet,
- att stödja systemägarna i informationssäkerhetsarbetet,
- äger ansvaret för det interna nätverket och annan kommunikation som sker med Borgholms kommuns nätverksutrustning.

11 IT-avdelningens driftansvarige tekniker

Driftsansvarig tekniker tillhör IT-avdelningen, innehar den tekniska kompetensen, och ansvarar tillsammans med systemägare och systemförvaltare för att den dagliga driften upprätthålls enligt överenskommelse mellan systemägaren och IT-chefen.

Driftsansvarig tekniker utför på uppdrag av systemägaren eller systemförvaltare överenskomna tekniska drift- och servicerutiner. Driftsansvarig tekniker ska ha tillgång till installationsanvisningar från respektive systemförvaltare.

Driftsansvarig tekniker har bland annat följande uppgifter:

- Tillhandahålla teknisk support,
- delta i och stödja informationssäkerhetsarbetet,
- initiera felsökning vid driftstörningar, vidta nödvändiga åtgärder och dokumentera dessa,
- ansvara för att rutiner för säkerhetskopiering och förvaring av säkerhetskopierat material följs.

12 Leverantör

Leverantör är den som levererar IT-system till Borgholms kommun och i förekommande fall sköter drift av dessa. I de fall där leverantören sköter driften sker detta under överinseende av IT-avdelningen.

I leverantörsupphandlingar ställs säkerhetskrav på det aktuella systemet och i avtal mellan Borgholms kommun och leverantören säkerställs ansvar för systemet. Det är Borgholms kommuns säkerhetsramverk som reglerar inloggning och behörighet i system där drift sker på annan plats.

Leverantör är ofta personuppgiftsbiträde.

13 Användare

Användare är varje person som använder ett informationssystem och/eller IT-stöd tillhandahållet av Borgholms kommun eller avtalad leverantör. Medarbetare, förtroendevalda, elever, kunder och extern personal kan vara användare.

14 Åtkomst till IT-resurser och behörighetskontroll

För att säkerställa att endast behöriga användare har tillgång till informationssystemen ska följande rutiner gälla:

Beställning av åtkomst till IT-infrastrukturen (filserver, e-post, med mera) ska ske via IT-avdelningens helpdesk.

Närmaste chef är behörig beställare.

Om medarbetare ska ha behörighet till ett verksamhetssystem ska närmaste chef beställa behörighet hos respektive systemförvaltare.

Närmaste chef ska snarast se till att behörigheter återkallas eller ändras om medarbetaren slutar eller byter arbetsuppgifter. Detta omfattar inte bara behörighet till verksamhetssystemet.

En anmälan om förändrad eller återkallelse av behörighet för medarbetaren ska skickas till personalavdelningen, IT-avdelningens helpdesk samt till berörda systemförvaltare via e-post.

15 Behörighetskontroll externa användare

Leverantörslösenord och behörigheter ska förvaras inlåsta hos både IT-avdelningen och hos systemförvaltaren.

Konsulter/leverantörer som vill koppla upp sig på distans måste kontakta IT-avdelningens helpdesk för instruktioner. Leverantörslösenord ska inte vara standardiserade och ska ändras i anslutning till installationsfasen.

16 Systemsäkerhetsanalys

Systemägarna ansvarar för att systemsäkerhetsanalys genomförs regelbundet på sina system. En systemsäkerhetsanalys inkluderar klassning av informationen, sårbarhetsanalys av systemet och åtgärdsplaner för sårbarheter.

Analysen ska även besvara frågorna:

- Hur ofta ska säkerhetskopiering utföras?
- Hur länge ska säkerhetkopior sparas?

17 Loggning och spårbarhet

Systemägarnas krav på säkerhets- och transaktionsloggar ska framgå av de systemsäkerhetsanalyser som respektive systemägare upprättar. Se även dokumentet InfoSäk KD.

18 Loggning i brandväggar

IT-chefen beslutar i samråd med dataskyddsombud och informationssäkerhetssamordnaren:

- Vad som ska loggas i brandväggen.
- Vem som ansvarar för uppföljning av loggar.
- Hur ofta uppföljning ska ske.

19 Dokumentation

Dokumentation kring systemet kan utnyttjas i uppsåt att skada kommunen och ska därför förvaras på ett säkert sätt.

20 Distansarbete, extern anslutning, bärbar dator

Distansarbete ska följa kommunens riktlinjer för distansarbete (se även medarbetarhandboken) .

21 Införande och drift av IT-system

Följande är viktigt för förvaltningsorganisationen att ha kunskap kring;

21.1 Anskaffning/-införandeplan

Denna plan ska minst omfatta:

- integrationskrav med andra system
- personella och ekonomiska resurser
- klarlägga behov av användarutbildning

21.2 Förberedande och införande av IT-system

Innan ett IT-system införs ska en risk- och sårbarhetsanalys göras. Den utgör ett viktigt underlag för den kravspecifikation som ska upprättas och syftar bland annat till att klarlägga de säkerhetskrav som verksamheten ställer i form av:

- Krav på säkerhet avseende sekretess, riktighet och tillgänglighet,
- rättsliga, verksamhets- och hotrelaterade krav,
- kommunikationsberoende (internt och externt),
- reservrutiner m.m,
- möjligheten att lämna över information till E-arkiv,
- systemet klarar att hantera personuppgifter enligt dataskyddsförordningen och dataskyddslagen.

När kravspecifikationen fastställs måste även punkterna i avsnittet *Avveckling av IT-system* beaktas.

21.3 Risk- och sårbarhetsanalys

Kraven från risk- och sårbarhetsbedömningen utökas med bland annat följande:

- integrationskrav med andra system,
- krav vid införande,
- krav på test och acceptans,
- tidplan,
- resurser (personella och ekonomiska),
- när och hur uppföljning, utvärdering och avrapportering ska ske,
- när och hur medarbetarna ska informeras och utbildas.

21.4 Driftgodkännande

Driftgodkännande avser den process som syftar till att fastställa om ett IT-system uppfyller ställda säkerhetskrav.

I samband med att en systemsäkerhetsanalys upprättas granskas om IT-systemet uppfyller:

- Basnivå,
- de tilläggskrav som ställs utifrån rättsliga, verksamhetsspecifika och hotrelaterade krav.

Systemägaren beslutar om driftgodkännande tillsammans med IT-avdelningen och dataskyddsombudet samt eventuella externa konsulter. Beslutet baseras på en granskning och säkerhetsutvärdering som bygger på jämförelser mellan verksamheternas krav och vidtagna säkerhetsåtgärder.

Beslut om driftgodkännande relateras till aktuell systemsäkerhetsanalys och ska omfatta:

- granskning av säkerhetsåtgärder i IT-systemet,
- utvärdering av granskningen i förhållande till systemsäkerhetsanalysens krav,
- redovisning av beslutsunderlag samt beslut.

Beslutsunderlaget ska innehålla en sammanfattning av förslag till beslut som kan vara att;

- driftgodkänna IT-systemet,
- driftgodkänna IT-systemet med beslut om när kompletterande säkerhetsåtgärder ska vara genomförda,
- inte driftgodkänna IT-systemet.

22 Drift

Kommunens regler för systemdrift ska vara samlade i InfoSäk KD som ska innehålla regler för:

- Systemdokumentationer,
- driftdokumentationer,
- bemanningsplan (nyckelpersonberoende),
- tillträdes- och brandskydd,
- elförsörjning,
- säkerhetskopiering,
- förvaring av datamedia,
- avveckling av datamedia.

Den tekniska IT-infrastrukturen ska vara dokumenterad i särskild systemsäkerhetsanalys.

23 IT-incidenthantering

En IT-incident är en oönskad och oplanerad IT-relaterad händelse som påverkar säkerheten i organisationens eller samhällets informationshantering och som kan innebära en störning av organisationens förmåga att bedriva sin verksamhet.

Att återkoppla erfarenheter från incidenter av olika slag är ett viktigt moment när det gäller att spåra brister och svagheter i IT-verksamheten.

Riktlinjer för hur incidenter följs upp är därför angelägna. Vid misstanke om intrång eller andra incidenter ska användare agera enligt dokumentet InfoSäk A. Blankett med instruktioner för anmälan av incident ska finnas på kommunens intranät.

Dataskyddssamordnaren och IT-chefen ska i samverkan med Informationssäkerhetssamordnaren sammanställa och rapportera till kommunens ledningsgrupp:

- Intrång och försök till intrång,
- brott mot lagstiftning och internt regelverk,
- incidenter som orsakar eller skulle kunna orsaka betydande avbrott och störningar.

24 Säkerhetskopiering och lagring

Systemägarnas krav på säkerhetskopiering och lagring för de egna systemen ska framgå av de systemsäkerhetsanalyser som respektive systemägare upprättar. Det ska vara tydligt hur ofta säkerhetkopia ska tas och hur länge dessa ska sparas. Kraven i dessa planer ska vara koordinerade i systemsäkerhetsanalys för IT-infrastrukturen. Informationsklassning av ett informationssystem, där krav på säkerhetskopiering och lagring ställs, utförs i verktyget Klassa.

25 Avveckling av IT-system

IT-system som inte längre behövs för verksamheten ska avvecklas snarast.

Systemägare beslutar om och när ett IT-system ska avvecklas. Vid avveckling ska särskilt uppmärksammas:

- Rättsliga regler såsom arkivlagen och personuppgiftslagen (dessa ska även beaktas vid inköp/införande av IT-system).
- Vad ska tas ut ur systemet före avveckling (på papper eller media)?
- Innehåller systemet ärenden som behöver avslutas i diariet?
- Behöver återläsning av innehåll kunna ske längre fram?
- Behöver uppgifter flyttas över till annat IT-system?
- Destruktion av media som innehållit information.

- Regler för destruktion av media som innehållit sekretessbelagd information.

26 Avveckling av datamedia

Datamedia med sekretessbelagd information ska avvecklas i enlighet med systemägarens instruktioner.

27 Intern datakommunikation

Kommunens nät ska vara väl dokumenterat och vara tillgängligt för alla medarbetare i organisationen.

28 Externa anslutningar

Kommunen är för sin verksamhet beroende av datakommunikation med medborgarna, andra organisationer och centrala myndigheter främst via Internet.

Följande riktlinjer gäller:

- För att försvåra för obehöriga att göra intrång i organisationens datasystem via externa anslutningar ska det finnas en s.k. brandvägg installerad.
- Kontroller ska ske av vem som får släppas in och ut samt vad de får göra.

29 Användningen av e-post och Internet.

Riktlinjer för användningen av Internet och e-post ska framgå av InfoSäk A.

30 Kontinuitetsplanering

Av systemsäkerhetsanalyserna ska framgå de enskilda IT-systemens krav på avbrotts- och katastrofplanering. Frågan om avbrottstid ställs i samband med informationssäkerhetsklassningen i verktyget Klassa.

Systemägaren ansvarar för att ta fram kontinuitetsplan för både kortare och längre systemavbrott samt driftsavbrott vid särskilt kritiska tidpunkter.

Borgholms kommun
KOMMUNLEDNING

Kommunledningskontoret
Niklas Palmquist, 0485-88221
niklas.palmquist@borgholm.se

INSTRUKTION

Datum
2018-12-28

Informationssäkerhetsinstruktioner Kontinuitet och drift

InfoSäk KD

Innehållsförteckning

Informationssäkerhetsinstruktion Kontinuitet och drift gäller för kommunens IT-organisation (IT-avdelningen) på ett likvärdigt sätt som Informationssäkerhetsinstruktion Förvaltning gäller för systemägare och systemförvaltare.

Det finns separata informationssäkerhetsinstruktioner för förvaltning samt användare.

Informationssäkerhetsinstruktion Kontinuitet och drift, utgår från och är underställd policyn och syftar till att redovisa:

- Dokumentering av rutiner för drift av Borgholms kommuns informationssystem och IT-stöd.
- Omfattningen av det ansvar som vilar på IT-avdelningen för informationssäkerhetsarbetet.
- Hur förebyggande åtgärder ska utföras för att upprätthålla informationssäkerheten.
- Kontinuitetsplan för verksamheten på IT-avdelningen.

1 Samverkan

IT-verksamheten sker i samverkan med Mörbylånga kommun. Samverkan regleras av ett samverkansavtal.

2 Hantering av händelser

Nedanstående tabell beskriver hur avbrott hanteras under olika faser av störning/avbrott.

	Hanteras av	**Beskrivning**
Planerat avbrott	Berörd funktion på IT-avdelningen	Ett planerat avbrott som initierats av IT-avdelningen eller systemförvaltare. Uppgraderingar och driftunderhåll
Incident/störning	HelpDesk	En oönskad händelse som hanteras inom accepterad avbrottstid med interna eller externa resurser.
Avbrott	IT-avdelningen	En oönskad händelse som inte kan hanteras inom accepterad avbrottstid med interna resurser.
Kris	IT-avdelningen och krishanteringsorganisationen	En mycket allvarlig händelse bortom all

		kontroll som kraftigt påverkar verksamheten.

3 Roller och ansvar

Rollerna nedan ska vara definierade för att det organisatoriskt inte ska finnas några tveksamheter kring vem som ansvarar för vad. Det fulla ansvaret som ingår i varje roll ska finnas dokumenterat i en arbetsbeskrivning utfärdad av IT-chefen. För att undvika att all kompetens inom ett område läggs på en och samma fysiska person ska kompetenssäkring ske i form av kunskapsdelning[1].

Beskrivning av roller och ansvar finns i informationssäkerhetspolicyn samt informationssäkerhetsinstruktion InfoSäk F.

4 Dokumentation och ärendehantering

IT-avdelningen använder ett system för dokumentation och ärendehantering, InDoc. I systemet finns:

- Alla ärenden,
- dokumentation kring nätverksresurser såsom system, applikationer, tjänster och servrar,
- rutiner.

IT-incidenter dokumenteras i kommunens ärendehanteringssystem, Evolution.

5 Helpdesk

Helpdesk är alltid bemannad under ordinarie öppettider och är en viktig funktion i IT-avdelningens verksamhet. Helpdesk ska:

- Ta emot anmälan om problem gällande nätverksåtkomst, hård- eller mjukvarurelaterade problem, kommunikationsproblem m.m.
- Logga ett ärende enligt gällande rutin.
- Lösa problemet/en alternativt tilldela ärendet till lämplig person med expertkompetens eller ansvar.

Hos helpdesk ska minst finnas:

- En förteckning över rollinnehavarna.
- Förteckning över aktuella avtal med leverantörer som kan bli berörda.
- Förteckning över aktuella överenskommelser med systemägarna.

Hos helpdesk ska också checklistor för de allvarligaste hoten som:

---

[1] Kunskapsdelning kan bland annat innefatta utbildningar, arbetsrotation, handledarhjälp som dokumentering av rutiner.

- Checklista angrepp skadlig kod.
- Checklista för återläsning och återställande.
- Checklista kommunikations- eller serverproblem.

6 Organisationens nätverk

För att övervaka det interna nätverket ska det finnas ett nätverksövervakningssystem. Informationen i detta system ska vara tillgänglig även om systemet är nere.

7 Kraven på nätverkets resurser

Samtliga resurser i det interna nätverket och kraven på tillgänglighet ska dokumenteras. De krav som finns på respektive enhet baseras på den

- samlade risk- och sårbarhetsanalysen för de applikationer i organisationen som ingår i det interna nätverket,
- information som lagras eller transporteras.

8 Åtgärder för hög säkerhet

IT-avdelningen ska ständigt jobba för att hålla så hög tillgänglighet som möjligt för informationshantering, servrar och kommunikation. Genom följande åtgärder säkerställs att klienter och servrar är uppdaterade samt att övrig hårdvara kontrolleras regelbundet.

Resurs	**Åtgärd**
Klienter	Senaste säkerhetsrelaterade uppdateringarna ska installeras både vad det gäller operativsystemet och applikationerna. Antivirusprogram är installerat och ska uppdateras kontinuerligt på samtliga klienter.
Servrar	Senaste säkerhetsrelaterade uppdateringarna ska installeras både vad det gäller operativsystemet och applikationerna.
Brandväggar	Brandvägg ska vara redundant eller finnas i reserv för omedelbar inkoppling om nätverket skall vara i funktion.
Routrar	Router ska vara redundant eller finnas i reserv för installation vid behov.
Datorhall	Utrustning för fukt- och temperaturlarm ska finnas. Skydd mot översvämning ska finnas. Redundant kylanläggning ska finnas. UPS ska finnas. Reservkraft ska finnas i form av dieselaggregat Automatisk brandsläckningsutrustning ska finnas.

	Ovanstående funktioner ska genomgå funktionskontroll minst en gång per år.

9 Daglig drift

Nedan redovisas punktvis de områden som bör dokumenteras. Dokumentationen ska förvaras eller lagras så att den är lätt åtkomlig för dem som behöver den. Samma princip som för övrig information gäller även dokumentation av rutiner.

Rutiner ska dokumenteras för att säkerställa att kunskapen finns lätt tillgänglig även i kris samt att kunskapen finnas kvar inom verksamheten om en nyckelperson slutar sin anställning.

10 Resurser

10.1 Utrustning

Utrustning som innehåller information märks ”Borgholms kommun”.

Nätverksutrustning, servrar, datorer, surfplattor och mobiltelefoner ska förtecknas. Av förteckningen ska framgå var utrustningen är placerad samt vem som ansvarar för den. Omflyttning ska rapporteras.

10.2 Programvaror/register – kommunikation

IT-avdelningen ska arbeta för att hålla säkerheten i det interna nätverket med tillhörande programvara på tillräckligt hög nivå. Rutiner för hanteringen av det interna nätverket ska finnas dokumenterade.

10.3 Programvaror/register – applikationer

För programvara gäller att användare inte får köpa in eller installera egna programvaror utan kontakt med IT-avdelningen. Vid tillfällen där särskild programvara efterfrågas av personer i Borgholms kommuns verksamhet ska IT-avdelningen undersöka vilka alternativ som finns. Det standardpaket med programvara som installeras på en dator ska finnas dokumenterat. Programvarulicenser ska finnas dokumenterade i ett centralt register.

Anledningen till att alla förfrågningar gällande programvara ska gå genom IT-avdelningen är av skäl som rör säkerhet, standarder, avtal och garantier samt av ekonomiska skäl.

- Omflyttning och överlåtelse av IT-utrustning

Rutin för införande av uppgifter i licensregistret vid t.ex. omflyttning av IT-utrustning till annan fysisk plats ska finnas dokumenterad.

10.4 Fysiskt skydd

IT-chefen ansvarar för att nätverk och servrar skyddas mot yttre hot i samspel med fastighetsavdelningarna i kommunen och Borgholm Energi.

10.5 Larm

Lokaler där det finns IT-utrustning bör vara larmade. Kontaktuppgifter till leverantör av larmutrustning ska finnas dokumenterat.

10.6 Klimatutrustning

Kontaktuppgifter till vaktbolag, leverantörer, installationsfirmor, service och liknande och eventuella avtal om inställelsetider för service ska finnas dokumenterat.

10.7 Brandskydd

Kontaktuppgifter till brandmyndigheter, vaktbolag, leverantörer, installationsfirmor, service och liknande och eventuella avtal om inställelsetider för service ska finnas dokumenterat.

10.8 Tillträdeskontroll

En rutin för vem som ska ha tillgång till samt hur aktuell person får tillgång till olika utrymmen som t.ex. skolor och andra utrymmen där det finns server- eller kommunikationsutrustning ska finnas dokumenterad. Nycklar, passerkort och andra eventuella koder m.m. ska förvaras säkert.

Samtliga Borgholms kommuns servrar som innehåller känslig information ska finnas i serverhallar som ska vara försedda med kontrollsystem för in- och utpassering. Utrymmen med kopplingspunkter ska vara låsta. Service-personal skall ej lämnas obevakade i säkrade utrymmen.

11 Kommunikation

11.1 WAN

De WAN-anslutningar som finns kopplade till Borgholms kommuns nätverk ska finnas dokumenterade.

11.2 LAN

Borgholms kommuns LAN och dess nätverksenheter ska finnas dokumenterade.

11.3 Fjärraccess/VPN

Se dokument Riktlinjer för distansarbete.

11.4 Brandvägg

Rutin för kontroll av eventuell onormal aktivitet i brandväggsloggarna samt med vilken intervall och på vilka villkor detta ska kontrolleras ska finnas dokumenterad.

12 Spamhantering

E-post ska filtreras för att hindra att SPAM och skadlig kod når mottagarna. En sammanställning av stoppade SPAM skickas till mottagarna varje dag.

13 Åtkomsträttigheter - användare

13.1 Användarkonton

Användarkonton skapas automatiskt från den information som finns i kommunens PA-system. IT-avdelningen tar emot beställningar av konton till konsulter som inte finns med i PA-systemet. Beställningen ska komma från närmast berörd chef. Behörighet till de verktyg och system en användare ska ha tillgång till sätts automatiskt eller enligt gällande rutin av systemförvaltaren. Denna rutin ska finnas dokumenterad. Användarkonton för externa konsulter, vikarier och projektanställda ska tidsbegränsas.

13.2 Val av lösenord

För lösenord gäller att det ska:

- Vara minst åtta tecken långt.
- Inte innehålla personlig information.
- Bestå av en blandning av tecken ur minst tre av dessa fyra kategorier:
    - stora bokstäver (A – Z)
    - små bokstäver (a - z)
    - siffror (0 - 9)
    - specialtecken (! " # $ ' ( ) * , - . / [\ ] ^ _ ` { | } ~ : ; < = > @)
- Inte återanvändas.

Lösenordet i det interna nätverket ska bytas var 360 dag. I helpdeskärenden där användaren behöver få ett nytt lösenord gäller följande:

- Användaren måste byta lösenord vid första inloggning med ett tillfälligt lösenord.
- Helpdesk ger ut ett tillfälligt lösenord om personen kan identifiera sig.

14 Loggning och spårbarhet

14.1 Övervakning

Loggning av aktivitet i informationssystem kan göras för att kunna spåra vem som har gjort vad. Vilka system som övervakas ska finnas dokumenterat.

14.2 Logghantering

Loggar ska gallras enligt beslutade gallringsregler. För informationssystems loggar ska systemägare besluta:

- Vad som ska loggas.
- Hur ofta de ska analyseras.
- Vem som ansvarar för analyser av dem.

- Hur de ska förvaras.

Detta beslut ska sedan dokumenteras.

En grundläggande säkerhetsloggning ska omfatta:

- Användaridentitet.
- Godkänd inloggning.
- Utloggning.
- Datum och klockslag.
- IP-adress.

Av andra skäl kan ytterligare uppgifter behöva loggas såsom:

- Händelse samt om händelsen utförts eller inte.
- Misslyckade inloggningsförsök
- Behörighetstilldelningar och förändringar av behörighet.

14.3 Logganalys

Det ska finnas dokumenterade rutiner för analys av loggar.

15 Säkerhetskopiering – Intervall och omfattning

Systemförvaltare beslutar i samråd med driftsansvarig tekniker hur informationen ska säkerhetskopieras. Dokumentation ska finnas över varje systemförvaltares beslut avseende:

- Vilken information som ska omfattas av säkerhetskopiering,
- intervall för säkerhetskopiering,
- hur många generationer säkerhetskopior som ska finnas,
- hur säkerhetskopior ska förvaras,
- om vissa säkerhetskopior ska förvaras på plats geografiskt skild från driftstället,
- när kontroll av säkerhetskopiornas läsbarhet ska genomföras (dock minst en gång per år) ska finnas.

16 Hantering av datamedia

16.1 Val av media

Regler som ska gälla vid val av datamedia och vad dessa ska användas till, till exempel band för säkerhetskopiering eller krypteringsbara USB-minnen, ska finnas.

16.2 Klassning

Datamedia som lagrar information ska klassas enligt Borgholms kommuns klassningsmodell. Se InfoSäk K.

16.3 Förvaring

Regler för hur datamedia ska förvaras beroende på informationsklassning samt regler för vilka förvaringstider som gäller för olika media ska finnas.

16.4 Avveckling

Datamedia ska raderas enligt certifierad metod. Går inte det ska det förstöras.

17 Drift- och övervakningssystem

Ett drift-/övervakningssystem ska finnas för att på ett effektivt sätt övervaka servrar samt installera programvara och uppdateringar på distans samt övervaka att operativsystemet, antivirusklienten och övriga applikationer är uppdaterade. För helpdesk ska även ett system för fjärraccess för att kunna ta över en användares dator finnas.

18 Kontinuitetsplan

Varje verksamhet ansvarar för sin kontinuitetsplanering.

En kontinuitetsplan för IT-avdelningen ska innehålla återstartsplaner och annan information som behövs om en allvarlig störning skulle inträffa.

Grunden till kontinuitetsplanen utgörs av en risk- och sårbarhetsanalys.

I kontinuitetsplanen ska det finnas identifierat vilka system som för verksamheten är mest kritiska och i vilken ordning dessa ska återstartas. En kontinuitetsplan ska minst innehålla:

- Organisation och ledning.
- Återstartsrutiner och plan för återstart av system.
- Rutiner för reservdrift och inkoppling av reservkraft.
- Alternativt driftställe.
- Inventarielista och licenser.
- Kontaktuppgifter.
- Manuella reservrutiner.
- Hur man ska gå tillväga för att aktivera planen.
- Testplan.
- Krisarbetsplats för åtkomst till datorhall.

19 Incidenthantering

19.1 Uppdatering av antivirusprogram

Antivirusprogrammet uppdateras automatiskt så snart programmet känner av att datorn är ansluten till Borgholms kommuns interna nätverk eller Internet.

19.2 Åtgärder för spårning av incidenter

En skriftlig rutin för genomgång av loggar och trender samt oväntade händelser i systemen i händelse av en incident ska finnas.

19.3 Förebyggande åtgärder

Rutin för säkring av data, spårning av källa och säkring av eventuellt bevismaterial ska finnas. IT-avdelningen ska jobba för att förebygga och motverka att incidenter inträffar samt att eventuella incidenter inte upprepas.

19.4 Dokumentation av inträffade incidenter

Incidenter ska i samtliga fall dokumenteras i syfte att snabbt kunna åtgärda liknande incidenter om de skulle inträffa igen. Om incidenten har orsakats av en hackerattack utifrån eller att någon användare internt har orsakat incidenten i illasinnat syfte se punkt 19.5 nedan. Om incidenten har inträffat av driftmässiga orsaker ska anledningen till detta dokumenteras i syfte att undvika liknande problem i framtiden. Se punkt 19.6 nedan för rutiner kring hanteringen av driftavbrott.

19.5 Rutiner för hantering av säkerhetsincidenter

När en anmälan kommit in om att en eventuell säkerhetsincident har inträffat eller om en incident på annat sätt har upptäckts ska loggar analyseras enligt punkt 14.3 ovan i syfte att säkerställa vilket/vilka användarkonton som varit aktuella alternativt om det är ett externt angrepp. Därefter ska en utredning göras i syfte att säkerställa om t.ex. information/data har ändrats och som minst innehåller svar på följande frågor:

- Om det varit ett intrång eller försök till intrång
- Om brott mot lagstiftning och/eller internt regelverk har begåtts
- Om incidenten orsakat eller hade kunnat orsaka betydande avbrott och störningar
- Konsekvenser och förslag till åtgärder.

19.6 Rutiner för hantering av driftavbrott

Om ett driftavbrott har uppstått där orsaken inte är kopplad till ett angrepp mot det aktuella systemet/nätverksresursen ska orsaken till avbrottet undersökas så snabbt som möjligt med de resurser som finns tillgängliga och med hjälp av dokumentation av eventuella tidigare inträffade och liknande avbrott.

20 Systemhantering

20.1 Underhåll/-utveckling

En sammanställning av tidpunkter för systemunderhåll ska finnas. Syftet med detta är att undvika att systemunderhåll görs vid tidpunkter då verksamheten är extra beroende av sina system. Systemförvaltare ska tillsammans med driftsansvarig tekniker jobba för att hålla systemen uppdaterade samt rapportera förbättringar till systemleverantören för att bidra till utvecklingen av systemen.

20.2 Avveckling

När det är beslutat att ett system ska avvecklas ska systemägare i samråd med driftsansvarig tekniker se till att avvecklingen sker på ett säkert sätt och att information raderas från datamedia som har använts för systemet.

20.3 Utveckling

Vid upphandling av informationssystem ska informationssäkerheten integreras redan i designstadiet av hur implementeringen av det nya systemet ska utföras. Den generella driften av Borgholms kommuns nätverk och de olika verksamheternas informationssystem ska genomsyras av en balans mellan säkerhet, funktionalitet och ekonomi.

21 Dokumentation

Ansvaret för innehållet i denna instruktion samt dokumentation av rutiner enligt denna instruktion ägs av IT-chefen.

Borgholms kommun
KOMMUNLEDNING

Kommunledningskontoret
Niklas Palmquist, 0485-88221
niklas.palmquist@borgholm.se

Informationssäkerhetsinstruktioner Klassning

InfoSäk K

Innehållsförteckning

1 Klassning av information

För information som lagras i IT-system måste inte bara sekretessaspekten beaktas, utan även kraven på riktigheten i informationen och tillgängligheten till den.

All information i en organisation har inte samma behov av skydd och därför är en central aktivitet i säkerhetsarbetet informationsklassning vars funktion är att bedöma informationens värde och känslighet. Bedömningen sker både utifrån den egna verksamhetens behov och utifrån externa krav. Avsikten är att varje informationstillgång ska omges med rätt skydd.

Informationsklassningen är i sig en process som innebär en kravställning på säkerhetsåtgärder från verksamheten till interna och externa leverantörer av system samt it (drift och förvaltning) och av resurser som lokaler och annan utrustning som påverkar informationshanteringen. Klassningen innebär även krav på användare av informationstillgångar.

Kommunens målsättning är att regelbundet genomföra en klassning av informationen i samtliga verksamhetskritiska IT-system. För det ändamålet använder kommunen det webbaserade verktyget Klassa som utvecklas och förvaltas av Sveriges Kommuner och Landsting (SKL). *(information nedan är hämtad från Klassa*):

1.1 Konfidentialitet - att informationen kan åtkomstbegränsas:

Nivå 0 (ingen eller försumbar skada)

- Inga svårigheter för verksamheten att nå målen.
- Ingen eller endast försumbar påverkan på samhällsviktiga funktioner vid egen eller annan organisation.

Nivå 1 (måttlig skada)

- Inga märkbara större svårigheter för verksamheten att nå målen.
- Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation.
- Enskilda individer eller andra myndigheter och organisationer kan notera störningen eller uppleva lindriga besvär men utan påvisbar ekonomisk påverkan.

Nivå 2 (betydande skada)

- Verksamheten kan fullfölja sina uppdrag, men med trolig risk för kännbar påverkan (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder).
- Andra myndigheter och organisationer kan påverkas (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Samhällsviktiga funktioner i egen eller annan organisation påverkas troligen inte.
- Enskilda individer kan uppleva konsekvenser, såsom stora besvär eller stor ekonomisk påverkan, av störningen.

Nivå 3 (allvarlig skada)

- Skapar stora svårigheter för organisationens verksamhet. Omöjligt eller nästan omöjligt att fullfölja uppdragen.
- Samhällsviktiga funktioner i egen eller annan organisation påverkas sannolikt.
- Individers liv och hälsa äventyras.

Nivå 4 (Synnerligen allvarlig skada)

- Röjande av uppgifterna medför skada för rikets säkerhet som inte endast är ringa.
- Systemet behandlar uppgifter som omfattas av sekretess och rör rikets säkerhet (hemliga uppgifter) där röjande av information kan ge överskådliga konskevenser där t ex omfattande fara för liv och hälsa föreligger.
- Informationen omfattas av t ex säkerhetsskyddslagstiftningen.

1.2 Riktighet - att informationen ska vara tillförlitlig, korrekt och fullständig.

Nivå 0 (ingen eller försumbar skada)

- Inga märkbara större svårigheter för verksamheten att nå målen.
- Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation.

Nivå 1 (måttlig skada)

- Inga märkbara större svårigheter för verksamheten att nå målen.
- Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation.
- Enskilda individer eller andra myndigheter och organisationer kan notera störningen eller uppleva lindriga besvär men utan påvisbar ekonomisk påverkan.

Nivå 2 (betydande skada)

- Verksamheten kan fullfölja sina uppdrag, men med trolig risk för kännbar påverkan (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder).
- Andra myndigheter och organisationer kan påverkas (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Samhällsviktiga funktioner i egen eller annan organisation påverkas troligen inte.
- Enskilda individer kan uppleva konsekvenser, såsom stora besvär eller stor ekonomisk påverkan, av störningen.

Nivå 3 (allvarlig skada)

- Skapar stora svårigheter för verksamheten. Omöjligt eller nästan omöjligt att fullfölja uppdragen.
- Samhällsviktiga funktioner vid egen eller annan myndighet påverkas sannolikt.

- Individers liv och hälsa äventyras.

Nivå 4 (Synnerligen allvarlig skada)

- Uppgifter som obehörigen, av misstag eller på grund av funktionsstörning ändrats kan antas medföra allvarlig skada eller skada för rikets säkerhet som inte endast är ringa.
- Systemet behandlar information som omfattas av sekretess och rör rikets säkerhet (hemliga uppgifter) där felaktig information kan ge oöverskådliga konsekvenser där t ex omfattande fara för liv och hälsa föreligger.
- Informationen omfattas av t ex säkerhetsskyddslagstiftningen.

1.3 Tillgänglighet - att informationen ska kunna nyttjas efter behov, i förväntad utsträckning samt av rätt person med rätt behörighet.

Nivå 0 (ingen eller försumbar skada)

- Inga eller försumbara svårigheter för verksamheten att nå målen.
- Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation.
- Verksamhetens förmåga att utföra sina arbetsuppgifter påverkas inte eller i försumbar omfattning av otillgänglighet till systemet.

Nivå 1 (måttlig skada)

- Inga märkbara större svårigheter för verksamheten att nå målen.
- Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation.
- Externa individer eller andra myndigheter och organisationer kan notera störningen eller uppleva lindriga besvär men utan påvisbar ekonomisk påverkan.
- Verksamhetens förmåga att utföra sina arbetsuppgifter påverkas endast i begränsad omfattning av otillgänglighet i systemet.

Nivå 2 (betydande skada)

- Verksamheten kan fullfölja sina uppdrag, men med trolig risk för kännbar påverkan (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder).
- Andra myndigheter och organisationer kan påverkas (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Samhällsviktiga funktioner vid egen eller annan organisation påverkas troligen inte.
- Enskilda individer kan uppleva konsekvenser, såsom stora besvär eller stor ekonomisk påverkan, av störningen.
- Verksamhetens förmåga att utföra sina arbetsuppgifter påverkas i en betydande omfattning av otillgänglighet i systemet.

Nivå 3 (allvarlig skada)

- Skapar stora svårigheter för organisationens verksamhet. Omöjligt eller nästan omöjligt att fullfölja uppdragen.
- Samhällsviktiga funktioner i egen eller annan organisation påverkas sannolikt.
- Individers liv och hälsa äventyras.
- Verksamhetens förmåga att utföra sina arbetsuppgifter påverkas i en allvarlig/katastrofal omfattning av otillgänglighet i systemet.

Nivå 4 (Synnerligen allvarlig skada)

- Ett avbrott som medför skada för rikets säkerhet som inte endast är ringa.
- Systemet behandlar information som omfattas av sekretess och rör rikets säkerhet (hemliga uppgifter) där otillgänglighet kan ge oöverskådliga konsekvenser där t ex omfattande fara för liv och hälsa föreligger.
- Informationen omfattas av t ex säkerhetsskyddslagstiftningen.

1.4 Spårbarhet - att specifika aktiviteter som rör informationen kan spåras.

Spårbarhet uttrycker förmågan och kravet att i efterhand kunna kontrollera tillståndet hos de tre centrala begreppen ”konfidentialitet”, ”riktighet” och ”tillgänglighet”, snarare än att vara ett eget centralt begrepp i webbverktyget Klassa.

Exempelvis kan höga krav (val av nivå) på ”riktighet” medföra krav på spårbarhet genom säkerhetsåtgärderna loggning och logguppföljning för att kunna spåra historiska förändringar hos informationstillgångar. Kraven (val av nivå) på de tre övriga centrala begreppen påverkar därmed automatiskt begreppet ”spårbarhet” i webbverktyget Klassa.

Arbetet med informationsklassningen med hjälp av webbverktyget Klassa är tänkt att vara en kontinuerlig process med regelbundna revisioner av verksamhetskritiska IT-system.

Till det kommer riskanalyserna som är en separat process och som genomförs efter informationsklassningen.

I styrgruppen för utvecklingen av Klassa ingår (förutom SKL) för närvarande representanter från Skellefteå, Stockholm, Lund, Region Jönköping, Norrköping, Lidingö och Sollentuna. MSB är med som remiss och stödinstans i syfte att integrera användning av verktyget till deras stödmaterial.