Riktlinjer för informationssäkerhet

1 Inledning

En informationssäkerhetspolicy beskriver den högsta ledningens *vilja* med informationssäkerheten. Riktlinjerna beskriver de övergripande målen i policyn och *vad* som ska göras för att nå målen. Rutinbeskrivningarna ska på en funktionell nivå beskriva exempelvis *hur* skyddsåtgärder ska införas.

Detta dokument, regelverk för informationssäkerhet, innehåller policy för informationssäkerhet samt de riktlinjer som gäller för hantering av såväl information som informationsbärare i form av datorer, pappersdokument, mobiltelefoner och externa minnen etc.

Information kan finnas lagrad eller hanteras i digital form, men kan också vara i såväl skriftlig som muntlig form.

I detta dokument är informationsbäraren inte det viktiga, men i dagens organisation hanteras informationen mest i digital form och därför har dokumentet en tyngdpunkt mot datorer och dess information.

1.1 Avgränsning

Detta regelverk beskriver den informationssäkerhet som ska gälla vid arbete med information, system och program inom Värmdö kommun.

1.2 Efterlevnad

Detta regelverk gäller såväl anställda som inhyrd och kontrakterad personal inom Värmdö kommun. Regelverket gäller även anställda hos Värmdö kommuns entreprenörer som har tillgång till Värmdö kommuns information och informationssystem.

Regelverket med informationssäkerhetspolicyn och tillhörande riktlinjer är det styrande regelverket för informationssäkerhet inom Värmdö kommun. I enlighet med Värmdö kommuns informationssäkerhetspolicy ansvarar varje chef inom sitt ansvarsområde för att regelverket efterlevs.

VÄRMDÖ KOMMUN

Bakomliggande lagstiftning
Denna plan beslutas av kommunstyrelsen, och beslutas med stöd av personuppgiftslagen, sekretesslagen m.fl..

Uppföljning och uppdatering
KUA ansvarar för uppföljning och uppdatering av detta styrdokument.

2 Definitioner

All information som hanteras eller lagras i någon form måste skyddas mot oönskad förändring, påverkan eller insyn. Det ska inte heller vara möjligt för obehöriga att ta del av information och de användare som har rätt till informationen ska komma åt den efter behov och inom önskad tid. Det är också av vikt att kunna identifiera vem som har gjort vad med informationen och i datasystemen.

Därför kan området informationssäkerhet delas in i följande fyra egenskaper

Riktighet
Att information inte kan förändras vare sig obehörigen, av misstag eller på grund av funktionsstörning. Informationen ska vara tillförlitlig, korrekt och fullständig.

Sekretess
Att dokumentation, information och handlingar etc. inte görs tillgängliga eller avslöjas för obehörig.

Spårbarhet
Att i efterhand entydigt kunna härleda specifika aktiviteter eller händelser till ett identifierat objekt- användare, skrivare, dator eller system/program. Det ska gå att se vem som tagit del av informationen, vilka förändringar som har gjorts och av vem dessa har utförts.

Tillgänglighet
Att information och informationstillgångar kan utnyttjas efter behov, i förväntad utsträckning och inom önskad tid utifrån de krav som ställs på verksamheten.

3 Struktur för säkerhetsdokumentation

I *informationssäkerhetspolicyn* fastställer kommunfullmäktige sin syn på informationssäkerhet, övergripande mål och intention med informationssäkerhetsarbetet.

Riktlinjerna för informationssäkerhet beskriver vilka rutiner och säkerhetslösningar som måste etableras, för att uppfylla de mål som beskrivs i informationssäkerhetspolicyn. Riktlinjerna syftar inte till att detaljerat beskriva hur rutiner och säkerhetslösningar i praktiken ska utformas, utan ger en minsta förväntad nivå för dessa. Detta för att dels etablera en gemensam säkerhetsnivå som alltid måste uppnås, dels för att rutiner och säkerhetslösningar ska kunna

Bakomliggande lagstiftning
Denna plan beslutas av kommunstyrelsen, och beslutas med stöd av personuppgiftslagen, sekretesslagen m.fl..

Uppföljning och uppdatering
KUA ansvarar för uppföljning och uppdatering av detta styrdokument.

anpassas till verksamhetens normala rutiner och sätt att arbeta.

Utifrån detta upprättas *rutinbeskrivningar*, som detaljerat redogör för hur rutiner och säkerhetslösningar ska utformas och tillämpas, för att informationssäkerhetspolicyns krav ska efterlevas.

Övriga dokument relaterade till styrning och användning av IT inom Värmdö kommun utgörs av:

- **E - policy för Värmdö kommun**: utgår från Vision 2030 och ger förutsättningar för att IT används effektivt och ger bästa möjliga effekt inom kommunens verksamheter.
- **Riktlinjer för IT**: beskriver IT-miljön inom Värmdö kommun och krav på tekniska system. Dokumentet är främst avsett att användas som underlag i design, upphandling med mera. (Beslut om riktlinjer tas hösten 2010.)
- **Projekthandbok**: Beskriver hur projekt bör hanteras inom Värmdö kommun.
- **Telefonpolicy**: Beskriver vad som gäller kring användning av kommunens telefonitjänster och är riktad till samtliga medarbetare.
- **Regler för IT**: Beskriver vad som gäller kring användning av kommunens IT-tjänster och är riktad till samtliga medarbetare.
- **Rutin för förvaltning av IT-system**: beskriver roller och ansvar kring förvaltning av kommunens IT-system. Riktad till de som har en roll inom förvaltningen av kommunens IT-miljö.

Utöver dessa dokument kan enskilda verksamheter ha kompletterande styrande dokument inom informationssäkerhetsområdet.

Kommunens verksamheter ansvarar för att ta fram rutiner som tillser att fastställda policies, regler och riktlinjer för användning av kommunens IT-miljö efterlevs.

Värmdö kommun ska med avseende på informationshantering följa samtliga lagar och förordningar relaterade till detta (som till exempel lagen om offentlig upphandling (LOU), personuppgiftslagen (PUL) med flera).

Kommunen bör också följa riktlinjer kring IT-verksamheten samt informationshantering från SKL (Sveriges kommuner och landsting), kammarkollegiet, MSB (Myndigheten för samhällsskydd och beredskap), KSL (kommunförbundet Stockholms län) och andra kommungemensamma intresseorganisationer.

Bakomliggande lagstiftning
Denna plan beslutas av kommunstyrelsen, och beslutas med stöd av personuppgiftslagen, sekretesslagen m.fl..

Uppföljning och uppdatering
KUA ansvarar för uppföljning och uppdatering av detta styrdokument.

4 Kontinuitetshantering

Kontinuitetshantering fokuserar på att:

- säkerställa att i första hand samhällskritiska processer ska kunna fungera på en acceptabel nivå vid svåra störningar,
- avbrutna ordinarie processer ska kunna återupptas inom en acceptabel tidsrymd under vilken alternativa rutiner upprätthåller prioriterad, kritisk verksamhet,
- säkra verksamheten vid olika typer av risker,
- lägga ansvaret för åtgärder (återhämtningsrutiner mm.) på den som ”äger” den samhällskritiska resursen.

Kontinuitetshantering syftar alltså till att säkerställa rutiner för att minimera avbrott i kommunens verksamheter. Alla system och verksamheter har risker. En riskanalys ska identifiera tänkbara störningar, allvarliga händelser samt extraordinära händelser. Arbetet syftar till att skapa robusta system samt identifiera och analysera skyddsvärda verksamheter och kritiska områden inom kommunen. Kommunens förvaltning och bolag ska inventera, analysera, värdera, förebygga och åtgärda oönskade händelser inom sina ansvarsområden. Arbetet ska fokusera på förebyggande insatser och konkreta skyddsåtgärder för människor, information och egendom/verksamhet.

En analys ska omfatta:

- Vilken verksamhet som måste fungera oavsett påfrestningar och vilka system som stöder denna verksamhet.
- Vilka system som säkerställer att kärnvärdena uppfylls – både organisatoriska och tekniska system samt sårbarheten i dessa system.
- Tänkbara risker och hot som på ett avgörande sätt kan utmana förmågan att upprätthålla den kommunala servicen samt sannolikheten för att de inträffar.

De risker som identifieras ska hanteras. Detta görs genom att:

- Genomföra åtgärder som minskar riskerna till en acceptabel nivå.
- Acceptera riskerna om de inte strider mot lagstiftning eller kommunens regler.
- Undvika den aktivitet som orsakar att den identifierade risken blir verklighet.
- Överföra risken till andra parter, tex försäkringsbolag eller leverantörer.

Bakomliggande lagstiftning
Denna plan beslutas av kommunstyrelsen, och beslutas med stöd av personuppgiftslagen, sekretesslagen m.fl..

Uppföljning och uppdatering
KUA ansvarar för uppföljning och uppdatering av detta styrdokument.

5 Informationssäkerhetspolicy

Informationssäkerhetspolicyn gäller för all hantering av information som tillhör Värmdö kommun och kompletterar E-policyn för Värmdö kommun.

Värmdö kommun ska erbjuda en kommunal service som har en hög kvalitet och som är kostnadseffektiv. Värmdö kommun är beroende av att medborgare, företag och övriga intressenter har ett starkt förtroende för verksamheten. Det är därför viktigt att informationen hanteras på ett säkert sätt och inte sprids felaktigt. Bristande informationssäkerhet kan leda till allvarliga konsekvenser, så som försämrat förtroende, ökade kostnader eller rättsliga processer för kommunen.

Informationssäkerhetspolicyn finns på Värmdö kommuns intranät.

6 Säkerhetsorganisation

6.1 Allmänt

För att uppnå och bibehålla fastställda regler för informationssäkerhet krävs en tydlig ansvarsfördelning inom organisationen samt att säkerhetsarbetet koordineras.

Den utsedda informationssäkerhetsansvarige har det yttersta säkerhetsansvaret inom Värmdö kommun och det är kommunstyrelsens ansvar att se till att det finns en väl fungerande organisation för informationssäkerhetsarbetet. Kommunstyrelsen ska initiera och stödja säkerhetsarbetet med resurser så att verksamhetens behov av skydd och säkerhet bidrar till att nå verksamhetsmålen.

6.2

Informationssäkerhetschef

I korthet omfattar ansvaret för informationssäkerhetschefen att:

- Ansvara för kommunens färdriktning i långsiktiga, strategiska IT/IS-frågor.
- Utforma regelverk för informationssäkerhet och uppdatera dessa vid behov.
- Upprätta former för kontinuitetshantering, riskanalys och incidenthantering.
- Utvärdera säkerhetsnivån inom kommunen.

Bakomliggande lagstiftning
Denna plan beslutas av kommunstyrelsen, och beslutas med stöd av personuppgiftslagen, sekretesslagen m.fl..

Uppföljning och uppdatering
KUA ansvarar för uppföljning och uppdatering av detta styrdokument.

- Hantera allvarliga säkerhetsincidenter.

Systemägare
Systemägaren är övergripande ansvarig för systemet och dess användning.

I korthet omfattar systemägarens ansvar att:
- Systemet uppfyller verksamhetens behov och att bevaka verksamhetsmässiga faktorer som påverkar systemet
- Upprätta riktlinjer och tillämpningsföreskrifter för systemanvändningen
- Systemet uppfyller såväl lagkrav som kommunens policies.

Systemförvaltare
En systemförvaltare tar inom givna ekonomiska ramar det funktionella (dagliga) helhetsansvaret för ett system. Systemförvaltaren fungerar i hög grad som systemägarens utförare och tillser att systemets funktionalitet samt planerade och beslutade aktiviteter genomförs och upprätthålls. En systemförvaltare samordnar sina aktiviteter med verksamhetsrepresentanter, systemägare, driftansvarig och systemleverantör. Systemförvaltaren tillser att det finns driftsavtal (SLA – Service Level Agreement) som motsvarar verksamhetens och systemägarnas krav.

I korthet omfattar systemförvaltarens ansvar att:
- Ger stöd till användare genom att
  - Användarhandböcker upprättas och förvaltas
  - Utbildningar genomförs
  - Behörighetstilldelning och uppföljning av systemanvändning
  - Felrapporter tas emot och hanteras
  - Felsökning och felrättning genomförs

- Utövar styrning genom att
  - Ansvara för rutinbeskrivning för systemadministration
  - Ansvara för säkerhetsarbete avseende information
  - Ansvara för att nivån i systemsäkerhetsplanen upprätthålls

Informationsägare
Om förvaltningsobjektet bedöms omfatta en viktig informationstillgång ska en eller flera informationsägare utses. Systemägaren ska verka för att dessa informationsägare utses på ett korrekt sätt samt att de blir medvetna om sina respektive ansvar.

Bakomliggande lagstiftning
Denna plan beslutas av kommunstyrelsen, och beslutas med stöd av personuppgiftslagen, sekretesslagen m.fl..

Uppföljning och uppdatering
KUA ansvarar för uppföljning och uppdatering av detta styrdokument.

Informationsägaren har det övergripande och yttersta ansvaret för den information som används av ett eller flera system. Informationsägare fattar det avgörande besluten om informationen, om det behövs nyutveckling, vidareutveckling, förvaltning och avveckling av informationen.

I flertalet fall är systemägaren lika med den som är ytterst ansvarig för verksamheten och som ytterst ansvarar för informationen i systemet. I dessa fall är systemägare även informationsägare.

Systemägaren utser informationsägare.

I korthet omfattar informationsägarens ansvar att:

- Att informationen i systemet följer lagkrav.
- Att delta i och stödja IT-säkerhetsarbetet.
- Hur, av vem och vilken information ska registreras.
- Vilka uppgifter som ska tillhandahållas enligt offentlighetsprincipen och detta ska ske.
- Vilka personer inom verksamheten som ska ha tillgång till informationen i systemet.

Chef med personalansvar
I korthet omfattar personalansvariga chefers ansvar att:

- Personalen är informerad om och efterlever kommunens regler för informationssäkerhet.
- Anlitad konsult och tredje part efterlever säkerhetsreglerna i denna handbok.
- Ge personalen möjlighet att delta vid säkerhetsutbildning.
- Avsätta tid för informationssäkerhet i lämpligt forum på arbetsplatsen.

Arkivarien
Verkar för att informationen i kommunens system är åtkomlig för allmänheten enligt reglerna i offentlighets- och sekretesslagen 4 kap § 2 samt att den gallras och bevaras enligt besluten i myndigheternas dokumenthanteringsplaner.

Medarbetare
Alla medarbetare och IT-användare inom Värmdö kommun ska följa det regelverk som finns kring informationssäkerhet inklusive de regler som finns för personligt ansvar vid IT-användning. Alla ansvarar för att ta inhämta sådan information att regelverket följs.

Bakomliggande lagstiftning
Denna plan beslutas av kommunstyrelsen, och beslutas med stöd av personuppgiftslagen, sekretesslagen m.fl..

Uppföljning och uppdatering
KUA ansvarar för uppföljning och uppdatering av detta styrdokument.

IT-avdelningen
IT-avdelningen har ansvaret för tillämpningen av Värmdös informationssäkerhet i de kommungemensamma IT-plattformarna.

I korthet omfattar IT-avdelningens ansvar att:

- Rapportera till kommundirektören och informationssäkerhetschefen.
- Tillsätta resurser för IT-tekniska säkerhetslösningar inom ramen för den centrala IT-miljön

6.3 Samordning av informationssäkerhet

Informationssäkerhetschefen har ansvaret för att utarbeta, förvalta och följa upp regelverket för informationssäkerheten.

6.4 Hantering av utomstående parter

Samverkan med konsulter, externa leverantörer och entreprenörer ska regleras genom avtal och alla ska ha kännedom om Värmdö kommuns regelverk kring informationssäkerhet samt följa detta.

7 Hantering av tillgångar

Tillgångar i detta sammanhang är det som för Värmdö kommun har ett värde i form av information (till exempel handlingar, dokumentation, datafiler, utbildningsmaterial, systemdokumentation), program (till exempel datorprogram, operativsystem, utvecklingsverktyg) och fysiska tillgångar (till exempel datorutrustning, telefoner, lagringsmedia).

7.1 Ansvar för tillgångar

Kommunens informationshantering styrs främst av bestämmelser i tryckfrihetsförordningen och Offentlighet - och Sekretesslagen (OSL) 2009:400. Huvudregeln i tryckfrihetsförordningen är att information ska vara tillgänglig för allmänheten, den s.k. offentlighetsprincipen. Undantag från huvudregeln utgör information som med stöd av reglerna i OSL kan omfattas av sekretesskydd samt information inom överförmyndarverksamheten. Det är väsentligt att varje anställd känner till vilken information, inom i första hand sitt eget ansvarsområde, som är sekretessbelagd och hur den ska hanteras. Prövning av sekretess föreligger för informationen varje gång en begäran av utlämning sker. Detta oavsett om

Bakomliggande lagstiftning
Denna plan beslutas av kommunstyrelsen, och beslutas med stöd av personuppgiftslagen, sekretesslagen m.fl..

Uppföljning och uppdatering
KUA ansvarar för uppföljning och uppdatering av detta styrdokument.

handlingen är sekretessbelagd eller inte.

7.2 Klassificering av information

7.2.1 Säkerhetsnivå 3

Insynsskydd/åtkomstbegränsning /sekretess
Oönskad spridning av informationen medför **endast ringa eller ingen skada** för egen eller annan organisations verksamhet eller för enskild person.
IT-systemet eller E-tjänsten innehåller enbart allmän offentlig information.
E-tjänst med icke känsliga personuppgifter.
E-tjänsten innehåller information som den enskilde kan anses ansvara för.
E-tjänst med information som är tänkt att publiceras för en bred spridning.

Spårbarhet
Avsaknaden av möjlighet att följa upp olika händelser medför **endast ringa eller ingen skada** för egen eller annan organisations verksamhet eller för enskild person.
Finns inget behov av spårbarhet.

Tillgänglighet
Avbrott i åtkomst till IT-systemet eller E-tjänsten medför **endast ringa eller ingen skada** för egen eller annan organisations verksamhet eller enskild person. Ett IT-system där verksamhetsberoendet är lågt. En E-tjänst där avbrott upp till ett dygn är acceptabelt.

Riktighet
Oriktig information medför **endast ringa eller ingen skada** för egen eller annan organisations verksamhet eller för enskild person. Data kan accepteras mer eller mindre utan kontroll. E-tjänst där avbrott upp till ett dygn är acceptabelt.

7.2.2 Säkerhetsnivå 2

Insynsskydd/åtkomstbegränsning/sekretess
IT-systemet innehåller sådan information som om den kommer i orätta händer kan medföra **skada**.
IT-systemet eller E-tjänsten innehåller känsliga personuppgifter enligt PUL.
IT-systemet eller E-tjänsten innehåller information som kan bli föremål för sekretess

Bakomliggande lagstiftning
Denna plan beslutas av kommunstyrelsen, och beslutas med stöd av personuppgiftslagen, sekretesslagen m.fl..

Uppföljning och uppdatering
KUA ansvarar för uppföljning och uppdatering av detta styrdokument.

enligt SekrL (dock ej det som berör rikets säkerhet och säkerhet för enskild). IT-systemet innehåller information avsedd för egen personal. E-tjänst där en kundrelation föreligger, t.ex. ansökan eller abonnemang.

Spårbarhet
Avsaknaden av möjlighet att följa upp specificerade händelser kan medföra **skada**. Spårbarhetskrav finns på vissa specificerade händelser i IT-systemet eller E-tjänsten om vem som har skapat vad och tidpunkt.

Tillgänglighet
IT-systemen som ingår i eller stödjer verksamhet där avbrott kan medföra skada för egen eller annan organisations verksamhet eller för enskild person. IT-systemet ingår i eller utgör ett stöd för myndighetsutövning och/eller kärnverksamheten. E-tjänst där en kundrelation föreligger mellan kommunen (myndigheten) och intressent.

Riktighet
Oriktig information kan medföra skada.
IT-systemet omfattas av ett lagrum där riktighetskrav anges (t.ex. PUL, BFL). IT-systemet eller E-tjänsten ingår i myndighetsutövningen. Informationen har krav på spårbarhet eller oavvislighet (non repudiation).

7.2.3 Säkerhetsnivå 1

Insynsskydd/åtkomstbegränsning/sekretess
IT-systemet innehåller sådan information som om den kommer i orätta händer kan medföra **allvarlig skada** för egen eller annan organisations verksamhet eller för enskild person. IT-systemet eller E-tjänsten innehåller sådan information som kan bli föremål för sekretess enligt SekrL delar av kap 15, 18, 19, 21. sådant som berör rikets säkerhet, förebyggande av brott, enskilda personers personliga och ekonomiska förhållande o. dyl.
IT-systemet eller E-tjänsten innehåller sådan information som påverkas av lagkrav anförbara till ett visst verksamhetsområde, t.ex. patientjournallagen eller socialtjänsten.
E-tjänst som innefattar en betalningsfunktion.

Spårbarhet
Avsaknaden av möjlighet att följa upp specificerade händelser kan medföra **allvarlig skada** för egen eller annan organisations verksamhet eller för enskild person. Det är

Bakomliggande lagstiftning
Denna plan beslutas av kommunstyrelsen, och beslutas med stöd av personuppgiftslagen, sekretesslagen m.fl..

Uppföljning och uppdatering
KUA ansvarar för uppföljning och uppdatering av detta styrdokument.

stora krav på att entydigt kunna följa vem som har gjort vad, när detta har skett och liknande relaterat till revisionskraven och/eller lagar och förordningar.

Tillgänglighet
Ett avbrott kan medföra **Allvarlig skada** för egen eller annan organisations verksamhet eller för enskild person.
IT-systemet ingår i eller stödjer verksamhet där avbrott innebär att man inte kan upprätthålla nödvändig tillgänglighet och servicenivå i produktionen och det saknas alternativa (manuella) metoder och procedurer samt rutiner.
För verksamheten ett mycket kritiskt IT-system.
E-tjänst med krav på mycket hög servicenivå.

Riktighet
Oriktig information kan medföra allvarlig skada för egen eller annan organisations verksamhet eller för enskild person.
Mycket strikt kontroll av i princip all data.
IT-system med särskilt höga krav på riktighet, t.ex. affärssystem.
E-tjänst med särskilt höra krav på riktighet, t.ex. uppdatering av verksamhetssystem
IT-system eller E-tjänst där hantering av information styrs av specifika lagparagrafer t.ex. känsliga personuppgifter.
IT-system eller E-tjänst för kritiska processer i verksamheten.

7.2.4 Allmänna handlingar

En allmän handling är ett dokument eller dyl. som har ***inkommit*** till en myndighet ***eller upprättats*** inom myndighet ***och förvaras*** hos myndigheten. Med myndighet menas varje enskild nämnd eller styrelse i kommunen med tillhörande verksamhetsområden.

En handling anses ***inkommen*** så snart den har anlänt med posten, telefax, e-post eller när den har överlämnats till någon behörig representant. Hur kortfattat och bagatellartat ett meddelande än kan anses vara, är det alltså att betrakta som allmän handling om det har inkommit till myndighet och rör myndighetens verksamhet.

En handling anses ***upprättad*** när den har expedierats. Det innebär att så snart ett e-postmeddelande har sänts till en mottagare utanför myndigheten och blivit registrerad som ”skickat”, är meddelandet att betrakta som allmän handling. E-postmeddelanden ska registreras enligt samma regler som vanliga

Bakomliggande lagstiftning
Denna plan beslutas av kommunstyrelsen, och beslutas med stöd av personuppgiftslagen, sekretesslagen m.fl..

Uppföljning och uppdatering
KUA ansvarar för uppföljning och uppdatering av detta styrdokument.

pappershandlingar. Dokument som har bifogats i ett e-postmeddelande blir allmän handling enligt regler för allmänna handlingar.

7.2.5 Allt är inte allmän handling

Långt från alla handlingar är allmänna, de som inte är allmänna är tex:

- Interna handlingar som endast skickas inom myndigheten.
- Inkomna eller skickade handlingar vars innehåll inte gäller myndighetens verksamhet (privat post).
- Handlingar som utväxlas som arbetsmaterial under ett ärendes beredning. Under beredning eller samråd kan ett utkast skickas till någon utanför din egen myndighet för synpunkter utan att handlingen blir allmän.
- Meddelanden till eller från en politiker som ***enbart*** rör dennes roll som representant för ett visst politiskt parti.
- Meddelanden till eller från fackliga förtroendemän som ***enbart*** rör den fackliga verksamheten.

7.3 Märkning och hantering av information

Alla informationstillgångar, och utrustning som är svår eller kostsam att ersätta ska ha en utsedd ansvarig. Den ansvarige ska utfärda rutinbeskrivningar om hur informationen och utrustningen ska och får användas. Informationstillgångar ska vara förtecknade och i vissa fall även märkta.

7.4 Arkivering och gallring

Den information som hanteras i kommunens informationssystem utgörs till stor del av allmänna handlingar. Av detta följer att denna skall bevaras, gallra och arkiveras som all annan information enligt bestämmelserna i lagar och myndigheternas dokumenthanteringsplaner. För att tillgodose allmänhetens insynsrätt och forskningens behov kan även sådan information behöva arkiveras för all framtiden. Den grundläggande tanken är att endast rådata ur varje system skall bevaras, inte informationssystemen i sin helhet.

Rutiner för gallring av dokument, e-postlistor, skräppost, loggar, cookie- eller andra historikfiler för internetsökning ska följa kommunens övergripande gallringsföreskrifter.

Bakomliggande lagstiftning
Denna plan beslutas av kommunstyrelsen, och beslutas med stöd av personuppgiftslagen, sekretesslagen m.fl..

Uppföljning och uppdatering
KUA ansvarar för uppföljning och uppdatering av detta styrdokument.

8 Personal

Genom säkerhetsinsatser ska riskerna minskas för mänskliga misstag, stöld, bedrägeri och missbruk av informationstillgångar.

Vid rekrytering skall säkerhetsaspekterna beaktas.

Detta regelverk kompletteras av dokumentet ”IT-instruktion för IT-användare”. (2005-08-08)

8.1 Säkerhet vid rekrytering av anställd och inhyrd personal

Vid rekrytering bör kontroll och uppföljning av den arbetssökandes referenser och formella meriter, som CV, meritförteckning och yrkeslegitimationsinnehav, göras. En kontroll av den sökandes identitet bör också genomföras, för att klargöra att personen verkligen är den som den utger sig för att vara. Detsamma ska gälla vid anlitande av tillfällig personal för känsliga befattningar. För vissa tjänster kan det komma att göras en framställan om registerkontroll enligt säkerhetsskyddslagen.

Vid anställningens **början** ansvarar varje användare för att:

- Ta del av den utbildning som ges i informationssäkerhet
- Ta del av samt följa det regelverk (informationssäkerhetspolicy, riktlinjer samt rutinbeskrivningar) som finns kring informationssäkerhet.

8.2 Krav på anställd gällande informationssäkerhet

Samtliga anställda inom Värmdö kommun som använder kommunens information är skyldiga att känna till och efterleva kommunens policys, riktlinjer och rutiner med avseende på användandet.

Privat användande av kommunens IT-miljö ska normalt inte ske utanför arbetstid och på ett sätt som inte påverkar IT-miljön eller arbetsuppgifterna samt är förenliga med kommunens profil. Normalt sett kan anställda inte komma åt kommunens IT-system mellan kl 22.00 och 06.00. Arbetets art avgör åtkomsten.

Oavsett om användandet sker privat eller i tjänsten ska gällande regler och lagar följas samt god moral och etik efterlevas. Endast de IT-verktyg som tillhandahålls via, eller i samråd med, IT-avdelningen samt är godkända av kommunledningen får användas.

Bakomliggande lagstiftning
Denna plan beslutas av kommunstyrelsen, och beslutas med stöd av personuppgiftslagen, sekretesslagen m.fl..

Uppföljning och uppdatering
KUA ansvarar för uppföljning och uppdatering av detta styrdokument.

8.3 Säkerhet vid avslutande av anställning eller vid förflyttning

Vid anställningens slut ansvarar varje användare för att:

- De allmänna handlingarna gallras och bevaras enligt regelverket i myndigheternas dokumenthanteringsplan.
- Rådgöra med chefen om vilket arbetsmaterial som ska sparas. Notera att allt arbetsmaterial som har framställts anses vara Värmdö kommuns egendom och inte får tas med utan chefs godkännande.
- Meddela vilka behörigheter som har varit aktuella för åtkomst till informationssystemen så att de kan avbeställas av närmaste chef.
- Material som inte behövs för Värmdö kommuns framtida verksamhet tas bort från servrar och datorer.

9 Fysisk säkerhet

Den fysiska säkerheten syftar till att skydda mot obehörigt tillträde och åtkomst, skador och störningar. Ett bra fysiskt skydd av lokaler, utrustning och dokument ska eftersträvas. Därför ska lokaler förses med passagekontroll, inbrottsskydd och brandskydd i den omfattning som krävs. En bedömning ska göras utifrån den verksamhet som bedrivs samt de krav som ställs utifrån lagar och förordningar.

9.1 Riktlinjer för skydd av utrustning och information

Nivån på det fysiska skyddet ska baseras på genomförda riskanalyser och stå i proportion till identifierade risker. Grundregeln är att information aldrig ska lämnas oskyddad. Utrustning som är känslig i sig själv eller behandlar känslig information, ska placeras så att tillträde minimeras och utformningen av lämpliga skyddsåtgärder underlättas.

För verksamheten kritisk IT-infrastruktur, IT-system och informationstillgångar ska inrymmas i säkra utrymmen, omgärdade av skalskydd, med lämpliga tillträdesspärrar och kontroller.

9.2 Tillträdeskontroll till byggnader och lokaler

Vid behov ska tillträdeskontroll till viktiga byggnader och lokaler finnas, för att säkerställa att endast behörig personal ges tillträde.

Inom kommunen ska det finnas rutiner så att det säkerställs att endast anställda

Bakomliggande lagstiftning
Denna plan beslutas av kommunstyrelsen, och beslutas med stöd av personuppgiftslagen, sekretesslagen m.fl..

Uppföljning och uppdatering
KUA ansvarar för uppföljning och uppdatering av detta styrdokument.

och övriga behöriga personer vistas i lokalerna. Vilka som är behöriga att vistas i lokalerna avgörs av verksamhetsledningen.

9.3 Säkerhet för utrustning utanför egna lokaler

Risker i samband med hantering av utrustning utanför de egna lokalerna ska beaktas. Detta gäller för informationsbärare i vid mening och omfattar bland annat persondatorer, handdatorer, mobiltelefoner och pappersdokument.
Rutiner/instruktioner skall fastställas för hur sådan utrustning skall hanteras. Dessa ska innehålla åtaganden från den anställde som ska kvitteras. **Vid utformning av skyddsåtgärder måste det beaktas att säkerhetsrisker kan variera avsevärt mellan olika platser och vid olika tidpunkter.** Viktigt är att även beakta riskerna då utrustning lämnas ut för extern service.
Utförsel av utrustning, som innehåller känslig information, ska vara godkänd av systemförvaltaren/informationsägaren.

9.4 Avveckling av utrustning

Lagringsmedia, som innehåller känslig information eller licensierade program, ska förstöras, avmagnetiseras eller överskrivas på ett säkert sätt, i samband med avveckling eller återanvändning.

10 Styrning av kommunikation och drift

I dokumenten *Riktlinjer för IT* samt *Rutin för förvaltning av IT-system* är hantering och krav på kommunikation och drift beskrivna.

10.1 Driftrutiner och ansvar

Målet är att säkerställa korrekt och säker drift av IT-miljön så att informationens sekretess, tillgänglighet, riktighet och spårbarhet bibehålls.

Ansvar och rutiner för incidenthantering skall vara etablerad. Mer information om detta finns i dessa riktlinjer för informationssäkerhet.

Driftansvar ska fördelas på olika personer för att minska risken för oavsiktlighet eller avsiktligt missbruk.

Bakomliggande lagstiftning
Denna plan beslutas av kommunstyrelsen, och beslutas med stöd av personuppgiftslagen, sekretesslagen m.fl..

Uppföljning och uppdatering
KUA ansvarar för uppföljning och uppdatering av detta styrdokument.

10.2 Kontroll av utomstående tjänstelverantör

Utomstående leverantörer som bedriver verksamhet för Värmdö kommun kan för detta behöva tillgång till Värmdös nätverk. Informationssäkerheten och utförandet av tjänsterna ska ske enligt avtal och med bibehållen nivå av informationssäkerheten.

Det ska finnas en rutin för hur uppföljning och granskning ska göras på utomstående leverantörers tjänster.

I händelse att rutinerna ändras eller att utförandet ändras på annat sätt ska en förnyad riskanalys göras.

10.3 Systemplanering och systemgodkännande

Alla informationssystem ska godkännas av systemägaren innan driftsättning och vid förändringar i systemet ska en bedömning göras ifall driftgodkännandet ska förnyas. En viktig parameter i ett driftgodkännande är systemets klassning och dess skydd av informationen avseende sekretess, tillgänglighet, riktighet och spårbarhet.

10.4 Skadlig kod

Skadlig kod innehåller funktioner som har till syfte att påverka datorer, kommunikation och information på ett negativt sätt. Programvaror för skydd mot skadlig kod skall installeras och kontinuerlig uppdateras på kommunens datorer.

10.5 Säkerhetskopiering

Den information som lagras på Värmdö kommuns gemensamma diskutrymmen säkerhetskopieras automatiskt. Information ska därför lagras på enheterna G: eller H:.

H: (personlig hemkatalog) är den personliga enheten som används för lagring av personligt arbetsmaterial och inte för allmänna handlingar. Om information lagras på denna enhet kommer andra medarbetare inte åt informationen och informationen säkerhetskopieras.

I förekommande fall kan ytterligare enhetsbeteckningar finnas.
Informationen ska inte lagras på datorns hårddisk. Undvik av både sekretesskäl samt avsaknad av säkerhetskopiering att lagra på hårddisken. Detta gäller både för

Bakomliggande lagstiftning
Denna plan beslutas av kommunstyrelsen, och beslutas med stöd av personuppgiftslagen, sekretesslagen m.fl..

Uppföljning och uppdatering
KUA ansvarar för uppföljning och uppdatering av detta styrdokument.

stationära som för bärbara datorer.

När informationen ändå lagras på den lokala hårddisken (C:) är användaren personligen ansvarig för säkerhetskopiering. Den informationen som finns på den lokala hårddisken (C:) riskerar att förloras vid t.ex. en diskkrasch om den inte kan återskapas till rimliga kostnader. Information som är lagrad på en dators lokala hårddisk kan vid förlust av datorn bli tillgänglig för obehöriga. Om en bärbar dator som tillhör Värmdö kommun används måste användaren vara medveten om att datorn kan utgöra en säkerhetsrisk och att det därför inte får lagras sekretessbelagd eller för verksamheten hemlig information på den, om inte hårddisken har godkänd kryptering.

10.6 Styrning av nätverk

Skyddet av kommunens egna nätverk för informationsöverföring ska styras utifrån verksamhetens krav och kopplingar mot externa datanät. Hantering av säkerheten för nätverk, som kan sträcka sig över organisationsgränserna, kräver särskilda åtgärder.

10.7 Mediahantering och mediasäkerhet

Som flyttbara media räknas CD-/DVD- skivor, usb-enheter, externa hårddiskar, minneskort men också telefoner med inbyggd minnesenhet m.m. Dessa flyttbara media kan medföra stor skada om de innehåller sekretessbelagd information och kommer i orätta händer. Flyttbara media skall aldrig innehålla känslig information eller mer information än vad som är absolut nödvändigt. Vid undantag för detta ska kryptering av data användas.

10.8 Utbyte av information och program

Vid informationsutbyte mellan kommunen och andra organisationer eller externa parter ska gemensamma bedömningar göras av behovet av skydd mot åtkomst, skydd av riktighet samt kraven på tillgänglighet. Ansvarsförhållanden ska vara klarlagda.

Utbyte av information är t.ex. information som skickas med brev, e-post, skrivs på blädderblock eller whiteboard eller samtalas mellan människor både personligen och över telefon.

Bakomliggande lagstiftning
Denna plan beslutas av kommunstyrelsen, och beslutas med stöd av personuppgiftslagen, sekretesslagen m.fl..

Uppföljning och uppdatering
KUA ansvarar för uppföljning och uppdatering av detta styrdokument.

10.9 Elektroniskt offentliggjord information

Innan information görs allmänt tillgänglig på t.ex. webb-sida, ska åtgärder vidtagas för att skydda riktigheten av informationen. Förvaltningen ansvarar för att information som publiceras av den egna verksamheten är korrekt och inte är sekretessbelagd.

10.10 Övervakning

Kritiska och säkerhetsrelevanta händelser i drift och datakommunikation ska vara spårbara.

Varje transaktion ska kunna knytas till den som utfört den. Detta ska i första hans åstadkommas med automatiska loggningsfunktioner. Behovet av loggning och uppföljning av loggar (analys) fastställs av systemägaren efter verksamhetens behov samt genomförd informationsklassificering.

11 Åtkomst till system och nätverk

I dokumentet Riktlinjer för IT samt *Rutiner för förvaltning av IT-system* är hantering och krav på åtkomst beskrivna.

11.1 Verksamhetskrav på styrning av åtkomst

Åtkomst till system och information ska styras utifrån verksamhetens behov och säkerhetskrav. Den som har behov av tillgång till viss information för att kunna utföra sina arbetsuppgifter ska tilldelas åtkomsträttigheter. All åtkomst ska vara baserad på behovsprincipen (need-to-know-basis).

11.2 Styrning av användares åtkomst

Det skall finnas rutiner för att säkerställa de behörigas åtkomst och för att förhindra obehörigas åtkomst till kommunens information.

11.2.1 Styrning av åtkomst för administratörer

Alla administratörer ska ha individuella användaridentiteter. Användningen av verktyg eller hjälpmedel som gör det möjligt att kringgå eller åsidosätta

Bakomliggande lagstiftning
Denna plan beslutas av kommunstyrelsen, och beslutas med stöd av personuppgiftslagen, sekretesslagen m.fl..

Uppföljning och uppdatering
KUA ansvarar för uppföljning och uppdatering av detta styrdokument.

säkerhetssystem och behörighetsskydd ska föregås av ett godkännande av IT-chefen. Inloggningsuppgifter som används för en specifik produkt vid leverans och andra standardlösenord med höga behörigheter ska förvaras inlåsta.

11.3 Användares ansvar

Användare ska hantera sina inloggningsuppgifter på ett sätt så att obehörig åtkomst undviks, samt tillse att utrustningen inte utsätts för obehörigt användande av t.ex. familjemedlemmar. Pappersdokument, övriga lagringsmedia samt anteckningar på t.ex. whiteboard i användarens arbetsrum måste hanteras i enlighet med hur informationen har klassats.

11.4 Styrning av åtkomst till nätverk

Interna och externa nätverk är informationstillgångar och ska betraktas som sådana. Kommunens nätverk ska vara tydligt avgränsat mot omvärlden genom lämplig teknik.

11.5 Styrning av åtkomst till operativsystem

Operativsystem och dess behörighetskontroll ska utformas så att möjligheterna till obehörig åtkomst minimeras.

11.6 Styrning av åtkomst till information och tillämpningar

Systemägaren för respektive system beslutar om systemet och dess information ska vara tillgängligt från externa platser.

11.7 Mobil datoranvändning och distansarbete

Systemägaren för respektive system beslutar om systemet och dess information kan få bearbetas på distans med stationär eller mobil utrustning. Information som är skyddad av sekretess bör inte hanteras under distansarbete, men om chef godkänner detta ska handlingarna hanteras med bibehållen sekretess.

Bakomliggande lagstiftning
Denna plan beslutas av kommunstyrelsen, och beslutas med stöd av personuppgiftslagen, sekretesslagen m.fl..

Uppföljning och uppdatering
KUA ansvarar för uppföljning och uppdatering av detta styrdokument.

12 Anskaffning, utveckling och underhåll av programvaror

I dokumentet *Riktlinjer för IT* samt *Rutin för förvaltning av IT-system* är hantering och krav på anskaffning, utveckling och underhåll av programvaror beskrivna.

12.1 Säkerhetskrav på informationssystem

Alla system och all information som nyttjas av Värmdö kommun skall ha erforderligt skydd avseende sekretess, tillgänglighet, riktighet och spårbarhet. Nivån av nödvändigt skydd framkommer vid informationsklassificeringen.

Säkerheten byggs i flera lager med behörighetskontroller, loggning, intrångsskydd, intrångsdetektering, skydd mot skadlig kod och kryptering.

12.2 Säkerhet i tillämpningar

Kontrollmekanismer bör finnas så att förväntad informationskvalitet garanteras, i synnerhet för känslig information. Sådan kontrollmekanism kan vara elektronisk underskrift och sigill.

För varje program bör en systemsäkerhetsanalys upprättas som innehåller systemets samlade krav på informationssäkerhet.

12.3 Kryptering

Kryptering bör användas både inom Värmdö kommun samt vid extern uppkoppling för information som ställer höga krav på.

- Skydd mot obehörig avlyssning.
- Skydd mot obehörig insyn.
- Skydd mot obehörig förändring.
- Skapande av elektronisk underskrift.
- Säker autenticering (stark autenticering).
- Säkerhet i databaser och program.

12.4 Säkerhet i databaser och program

För samtliga IT-system som används inom Värmdö kommun skall kommunens förvaltningsmodell tillämpas. Se dokumentet *Rutin för IT-system i Värmdö*

Bakomliggande lagstiftning
Denna plan beslutas av kommunstyrelsen, och beslutas med stöd av personuppgiftslagen, sekretesslagen m.fl..

Uppföljning och uppdatering
KUA ansvarar för uppföljning och uppdatering av detta styrdokument.

kommun.

Information lagrade i olika verksamhetssystem ska i förekommande fall ha identifierade informationsägare. Information som används inom flera delar av verksamheten ska eftersträvas att lagras i endast en originaldatabas.

13 Hantering av incidenter

13.1 Rapportering av säkerhetshändelser och svagheter

Incidenter och säkerhetsmässiga svagheter ska rapporteras snarast så att åtgärder kan påbörjas för att minimera skada, åtgärda brister och utreda eventuell brottslighet.

13.2 Hantering av säkerhetsincidenter och förbättringar

Om det finns misstanke eller det upptäcks att en användare i Värmdö kommuns nät har använt en dator till något olagligt eller till något som bryter mot kommunens styrande dokument ska detta anmälas till användarens chef.

Om det upptäcks fel och brister i de system som används ska detta rapporteras till närmaste chef eller till IT-avdelningen.
IT-avdelningen bedriver genom logganalys och stickprover ett förebyggande arbete för att förhindra uppkomsten av incidenter.

14 Efterlevnad

En väl fungerande informationshantering bidrar till att kommunen kan fullgöra sina uppgifter. Det är därför viktigt att lagar och förordningar följs.

14.1 Efterlevnad av rättsliga krav

Områden som är av särskild vikt att beakta efterlevanden av är t.ex.:

- Arkivlagen
- Arkivförordningen och gallringsförordningen

Bakomliggande lagstiftning
Denna plan beslutas av kommunstyrelsen, och beslutas med stöd av personuppgiftslagen, sekretesslagen m.fl..

Uppföljning och uppdatering
KUA ansvarar för uppföljning och uppdatering av detta styrdokument.

- Personuppgiftslagen
- Offentlighet och sekretesslagstiftning
- Upphovsrättslagen
- Bokföringslagen och –förordningen
- Lagen om kommunal redovisning
- Särskild myndighetslagstiftning

14.2 Efterlevnad av säkerhetspolicy, -standard och teknisk efterlevnad

Vid oklarheter beträffande tillämpningen av detta regelverk ska varje anställd kontakta sin chef eller motsvarande. Missbruk ska beivras. Disciplinära åtgärder ska i tillämpliga fall vidtas. Vid överträdelse av Riktlinjer för informationssäkerhet kommer detta anmälas till kommundirektören och ärendet kommer att behandlas i enlighet med kommunens personalpolicy.

Du är som användare personligen ansvarig för dina handlingar. Alla olagliga aktiviteter med kommunens informationshantering kommer att polisanmälas och utredas.

14.3 Hänsysntagande av revision av informationssystem

Revisioner av användandet av informationssystem kan genomföras löpande inom Värmdö kommuns alla informationssystem och IT-miljö. Detta omfattar hela kommunens verksamhet.

All information, informationsbehandlingsr esurser samt kringutrustning och konton ägs av Värmdö kommun. Detta innebär att allt som finns på datorerna, i nätverk och i molnet samt i arkiv är Värmdö kommuns egendom. Arbetsgivaren har rätt att kontrollera vad som finns i datorn som medarbetarna använder, samt att återställa infrastruktur och data i enlighet med detta regelverk.

I varje enskilt fall där någon verksamhet begär att göra avsteg från detta regelverk eller de övriga dokument som beskriver riktlinjer och rutiner för kommunens IT-miljö ska detta godkännas av kommundirektör eller informationssäkerhetschef. Grund för begäran kan vara:

- Stöd för att utveckla verksamheten genom tjänster som inte redan erbjudits inom kommunens befintliga eller planerade IT-tjänster.

Bakomliggande lagstiftning
Denna plan beslutas av kommunstyrelsen, och beslutas med stöd av personuppgiftslagen, sekretesslagen m.fl..

Uppföljning och uppdatering
KUA ansvarar för uppföljning och uppdatering av detta styrdokument.

- Identifierade rationaliseringsmöjligheter inom verksamheten
- Ändrade lagkrav

Undantag ska dokumenteras och bör normalt vara tidsbegränsande.

15 Ordlista

Bits
Basnivå för Informationssäkerhet – ett koncept för informationssäkerhet utgiven av Myndigheten för samhällsskydd och beredskap. Konceptet består bl.a. av en bok där det anges ett antal rekommenderade säkerhetsåtgärder som minst bör vidtas för att uppnå en acceptabel säkerhetsnivå för informationssäkerheten.
Enligt Värmdö kommuns regelverk för informationssäkerhet ska informationssäkerhetsarbetet bedrivas utifrån BITS.

Informationssäkerhet
Säkerhet för informationstillgångar avseende förmågan att upprätthålla önskad sekretess, riktighet, tillgänglighet och spårbarhet. Begreppet innefattar både fysisk säkerhet, IT-säkerhet samt administrativ säkerhet.

Informationsteknik
Den teknik som används för att på elektronisk väg samla in, lagra, bearbeta, kommunicera samt presentera data, bild, text och ljud. Den omfattar all användning av elektronisk informationsteknik och omfattar därmed samtliga skolsystem, vård och omsorgssystem, geografiska informationssystem, administrativa stödsystem, allmänna informationssystem samt system som är eller kan kopplas upp på nätverk. Datorer med kringutrustning, nätverk, tekniska stödsystem (operativsystem, databas, säkerhet, virusskydd, med mera), telefonkommunikationslösningar omfattas också.

Informationstillgångar
En organisations skyddsvärda informationsrelaterade tillgångar. Exempel på informationstillgångar är:

- Information (databaser, filer, metodik, dokument, etc.)
- Program (tillämpningar, operativsystem, etc.)
- Tjänster (nätförbindelser, abonnemang, etc.)
- Fysiska tillgångar (datorer, datamedia, lokala nätverk, etc.)

Bakomliggande lagstiftning
Denna plan beslutas av kommunstyrelsen, och beslutas med stöd av personuppgiftslagen, sekretesslagen m.fl..

Uppföljning och uppdatering
KUA ansvarar för uppföljning och uppdatering av detta styrdokument.

Incident
En händelse som avviker från det normala och som innebär en störning eller överhängande risk för störning i det dagliga arbetet, potentiellt kunde händelsen ha orsakat allvarliga konsekvenser för verksamheten.

Kontinuitetsplan
Dokument som beskriver hur verksamheten ska bedrivas och återställas när identifierade, kritiska verksamhetsprocesser allvarligt påverkas under en längre, specificerad tidsperiod.

Rutinbeskrivning
Dokument som beskriver som detaljerat redogör för hur rutiner och säkerhetslösningar ska utformas och tillämpas, för att Informationssäkerhetspolicyns krav ska efterlevas.

Andra namn på en rutinbeskrivning kan vara instruktion, anvisning eller rutin.

Tillgång
Allt som är av värde för Värmdö kommun. Innefattas förutom informationstillgångar även immateriella värden, som t.ex. goodwill.

Bakomliggande lagstiftning
Denna plan beslutas av kommunstyrelsen, och beslutas med stöd av personuppgiftslagen, sekretesslagen m.fl..

Uppföljning och uppdatering
KUA ansvarar för uppföljning och uppdatering av detta styrdokument.