Policy och riktlinjer för

Informationssäkerhet

Stockholms stad

Beslutad av kommunfullmäktige 2005-

INNEHÅLLSFÖRTECKNING

1 Inledning och omfattning

1.1 Inledning

En väl fungerande informationshantering är en väsentlig förutsättning för Stockholms stads effektivitet.
Informationssäkerhetsarbetet bidrar till en tryggad informationshantering. Det måste ske förebyggande, på lång sikt och för att vara effektivt och heltäckande, genomföras väl strukturerat och med tydligt stöd från verksamhetsledningen.
Förankringen och medvetandet hos medarbetarna utgör själva grunden för informationssäkerhetsarbetet.

Informationssäkerhet handlar om

- **sekretess**, skydd mot obehörig åtkomst av information
- **riktighet**, åtgärder för att åstadkomma rätt kvalitet på information
- **tillgänglighet**, åtgärder för att säkra drift och funktionalitet
- **spårbarhet**, möjligheten att fastställa vem som gjort vad eller att kunna verifiera orsaken till en händelse

Säkerhet åstadkoms genom många samverkande faktorer, inte en avancerad teknikkomponent eller en enstaka säkerhetsåtgärd.

Rätt säkerhetsnivå uppnås när:
- system/information har klassificerats och aktuella krav är uppfyllda
- riskanalyser och säkerhetsuppföljningar har genomförts och identifierade brister åtgärdats.
Detta innebär även att Revisionskontorets krav på säkerheten i stadens IT-system, ur internkontrollsynpunkt, är uppfyllda.

Informationssäkerhetsinsatser skall bidra till att **rätt person**
har tillgång till **rätt information**
i **rätt tid.**

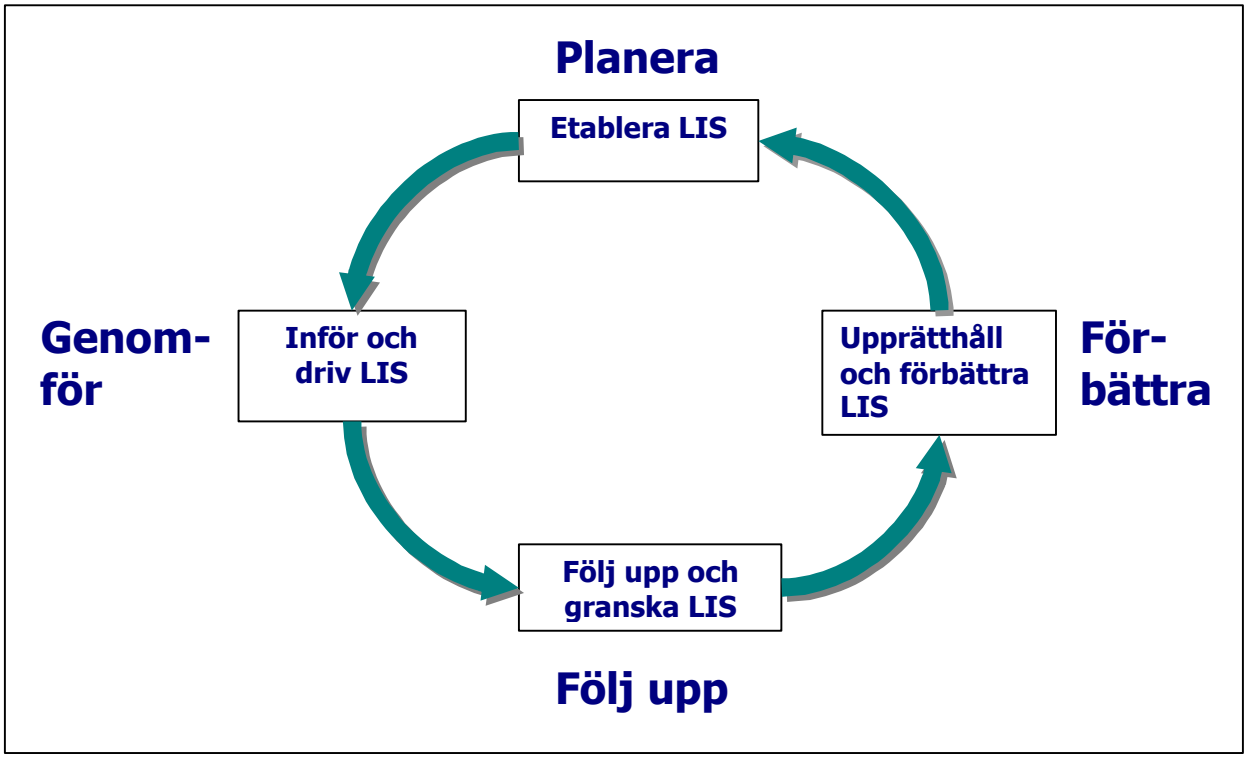
1.2 Omfattning

Säkerhetsarbetet omfattar alla åtgärder vars samlade effekt är att förebygga och begränsa konsekvenserna av störningar för informationshantering inom verksamheter i koncernen Stockholms stad.
Personer som omfattas är förtroendevalda och anställda och i viss omfattning skolelever samt konsulter/entreprenörer om uppdragens karaktär är relevanta för informationssäkerheten.

1.2.1 Processinriktning

PDCA (PlanDoCheckAct)är en modell (hämtad från standarden Ledningssystem för InformationsSäkerhet [LIS], SS-ISO/IEC 17799) som utgör grunden för informationssäkerhetsarbetet i Stockholms stad.
Standarden förordar tillämpning av processinriktning för att etablera, införa, driva, följa upp, granska, upprätthålla och förbättra effektiviteten i detta informationssäkerhetsarbete.
Målet är att uppnå ständiga förbättringar.

Nedanstående figur är en grafisk beskrivning av processen.



[P] Planera:	Fastställande av policy och riktlinjer. Riskhantering.
[D] Genomför:	Införande av anvisningar och instruktioner.
	Genomförande av analyser, informationsklassificeringar, etc.
	Skapande av skyddsåtgärder enligt gällande regelverk.
[C] Följ upp:	Kontinuerlig uppföljning mot modellen.
[A] Förbättra:	Genomföra korrigerande åtgärder.
	Komplettera och förbättra modellen.

1.3 Dokumentstruktur och roller

Dokumentet bygger på en hierarki utgående från begreppen **Policy, Riktlinjer, Anvisningar** och **Instruktioner** och med en kapitelindelning enligt SS-ISO/IEC 17799.

- **Policyn** formuleras på en övergripande nivå och uttrycker ledningens viljeinriktning
- **Riktlinjer** anger VAD som skall göras och pekar ut ansvar, säkerhetsprocesser och mål
- **Anvisningar** anger HUR skydd skall införas och vilka säkerhetsåtgärder som skall vidtas
- **Instruktioner** är detaljerad information till Anvisningarna.

Policy och Riktlinjer (rubriknivå X.X.X) återfinns i detta dokument medan Anvisningar (rubriknivå X.X.X.X) och Instruktioner är separat samlade i Appendix A. Vid behov kan lokal anpassning av Appendix A göras och detta beslutas av respektive nämnd eller styrelse.

Dokumentet utgör en samlad bild av informationssäkerheten inom staden.
Den roll man representerar avgör vilka delar av dokumentet som är tillämpliga.

I nedanstående tabell visar + markeringar vilka kapitel som är aktuella för respektive roll. Rollerna beskrivs i kapitel 4.

Roll / Kapitel	System-ägare	Förv.-Bolags-V-ansv chef	System-ägar-repre-sentant	An-vänd-are	IT-chef	Tekniskt system-ansvarig	Extern tjänste-leveran-tör	Info.säker-hetschef/-samordn.
1 Inledning/ Omfattning	+	+	+	+	+	+	+	+
2 Termer/ Definitioner	+	+	+	+	+	+	+	+
3 Policy	+	+	+	+	+	+	+	+
4 Organisatorisk säkerhet	+	+	+	+	+	+	+	+
5 Klassificering och styrning av tillgångar								
Riktlinjer	+	+	+	+	+	+	+	+
Anvisningar	-	-	+	-	+	-	-	+
6 Personal och säkerhet								
Riktlinjer	+	+	+	+	+	-	+	+
Anvisningar	-	+	+	-	+	-	-	+
7 Fysisk och miljö-relaterad säkerhet								
Riktlinjer	-	+	+	-	+	+	+	+
Anvisningar	-	-	+	+	+	+	+	+
8 Styrning av kommunikation och drift								
Riktlinjer	-	-	+	-	+	+	+	+
Anvisningar	-	-	-	+[1]	+	+	+	+
9 Styrning av åtkomst								
Riktlinjer	-	+	+	-	+	+	+	+
Anvisningar	-	-	-	+	+	+	+[1]	+
10 Systemutveckling /-anskaffning och /-underhåll								
Riktlinjer	-	-	+	-	+	+	+	+
Anvisningar	-	-	-	-	+	+	+	+

[1] Valda delar av innehållet

Roll Kapitel	System-ägare	Förv.-Bolags-V-ansv chef	System-ägar-repre-sentant	An-vänd-are	IT-chef	Tekniskt system-ansvarig	Extern tjänste-leveran-tör	Info.säker-hetschef/-samordn.
11 Kontinuitets- och avbrottsplanering								
Riktlinjer	+	+	+	-	+	+	+	+
Anvisningar	-	+	+	-	+	+	+	+
12 Efterlevnad								
Riktlinjer	+	+	+	+	+	+	+	+
Anvisningar	+	+	+	+	+	+	-	+

1.4 Avgränsningar

Inga avgränsningar finns utan dokumentet är tillämpligt för all informationshantering, oberoende av media.

1.5 Styrande dokument

Säkerhetspolicy, Brandförsvaret, 1993-09-06
e-strategi, 2001-02-19
Informationsteknisk plattform [ITP], Förslag 2003-08-20

2 Termer och definitioner

2.1 Termer

Beskrivning av termer som påverkat utformningen av och innehållet i detta dokument.

SS-ISO/IEC 17799 – Ledningssystem för **I**nformations**S**äkerhet **(LIS)** är en internationell standard som omfattar riktlinjer eller ”code of practice” för ledning av informationssäkerhet.
Standarden ger råd om hur man på ett strukturerat och systematiskt sätt styr informationssäkerhetsarbetet i en verksamhet.

PDCA – PlanDoCheckAct (PDCA) är en modell som bygger på ett ramverk av riktlinjer för hur ett LIS fungerar.

2.2 Definitioner

Begrepp	Beskrivning
Policy	Anger ledningens viljeinriktning och stöd för informationssäkerhet. Policyn beskriver ”att något ska finnas”.
Riktlinjer	Anger VAD som skall göras för att uppfylla de övergripande målen i policyn.
Anvisningar	Anger på en funktionell nivå HUR (på vilket sätt) skyddsåtgärder och administrativa processer skall utformas.
Instruktioner	Ges för specifika system och/eller anvisningar. Instruktioner beskriver "hur och av vem" anvisningarna ska införas/följas.
Användare	Individ som utnyttjar informationstillgångar.
Autenticering	Verifiering av uppgiven identitet.
Avbrottsplan [IT]	Plan för att kunna återuppta driften efter driftstörning eller då IT-system inte fungerar som avsett. Avbrottsplanen baseras på vad som beskrivs i kontinuitetsplanen.
Hot	Möjlig, oönskad händelse med negativa konsekvenser för verksamheten.
Identitet	Unik beteckning för en viss individ.
Incident	Säkerhetshändelse som kan/kunnat få/har fått allvarliga konsekvenser för verksamheten.
Informations-klassificering	Ett formellt sätt att fastställa rätt skyddsnivå för ett IT-system. Uttrycks i en s.k. säkerhetsprofil**.**
Informations-säkerhet	Säkerhet beträffande informationstillgångar avseende förmågan att upprätt-hålla önskad åtkomstbegränsning, riktighet, tillgänglighet och spårbarhet.
Informations-tillgångar	En organisations informationsrelaterade tillgångar, vilka har ett värde för organisationen och därmed är skyddsvärda. *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.)*

IT-system	Är en konstellation av datorer, in- och utmatningsutrustning, minnesenheter, program, kommunikationsutrustningar, metoder och procedurer organiserade med uppgift att genomföra elektronisk behandling av information i syfte att tillgodose ett uttalat behov.
Kontinuitetsplan [för verksamheten]	Dokument som beskriver hur verksamheten skall bedrivas när identifierade, kritiska verksamhetsprocesser allvarligt påverkas under en längre, specificerad tidsperiod.
Logg	Insamlad information om de operationer som utförs i ett IT-system. Tre typer av loggar är aktuella: Säkerhetslogg, driftlogg och transaktionslogg.
Riktighet	Egenskap att information inte obehörigen, av misstag eller på grund av funktionsstörning har förändrats.
Risk	Produkten av sannolikheten för att ett givet hot realiseras och därmed uppkommande skadekostnad.
Riskanalys	Process som identifierar säkerhetsrisker, bestämmer deras betydelse och identifierar skyddsåtgärder.
Sekretess	Avsikten att innehållet i ett informationsobjekt (eller ibland även dess existens) inte får göras tillgängligt eller avslöjas för obehöriga. Begreppet ersätts med **Åtkomstbegränsning** i detta dokument.
SLA [Service Level Agreement]	Dokument som reglerar vad som överenskommits mellan systemägare/-representant och IT-chef gällande drift och förvaltning av visst IT-system.
Spårbarhet	Möjlighet att entydigt kunna härleda utförda aktiviteter i IT-systemet till en identifierad användare. För att åstadkomma spårbarhet krävs åtminstone identifiering och autenticering av användare samt loggning av relevanta händelser i IT-systemet.
Sårbarhet	Brist i skyddet av en tillgång exponerad för hot.
Säkerhet	Egenskap eller tillstånd som innebär skydd mot risk i samband med insyn, förlust eller påverkan; oftast i samband med medvetna försök att utnyttja eventuella svagheter.
Säkerhetsprofil	Alla IT-system har ett skyddsbehov. Skyddsbehovet varierar beroende på typ av informationstillgång. Genom att klassificera informationen med avseende på åtkomstbegränsning, riktighet, tillgänglighet och spårbarhet erhålls en säkerhetsprofil. Denna avgör vilka säkerhetskrav som ställs på informationstillgången.
Tillgänglighet	Möjligheten att utnyttja informationstillgångar efter behov i förväntad utsträckning och inom önskad tid.
Åtkomst-/behörighets-kontroll	Syftar till att reglera och kontrollera en användares åtkomst till olika informationstillgångar samt att skydda information och program, så att de endast är tillgängliga utifrån tilldelad (roll-)behörighet.

3 Informationssäkerhetspolicy

För att uppnå en trygg och effektiv informationshantering vid Stockholms stad krävs en enhetlig syn på säkerhetsbedömningar och åtgärder.
Gemensamma styrande dokument är ett medel för att uppnå en homogen, grundläggande utgångspunkt och ge likvärdiga förutsättningar för säkerhetsarbetet.

Avsikten med denna policy är att skydda stadens informationstillgångar mot alla hot – interna eller externa, avsiktliga eller oavsiktliga.

Via riskanalyser fastställs rätt avvägd riskkostnad, dvs säkerhetsåtgärderna skall vara ekonomiskt försvarbara.

Informationssäkerhetspolicy Stockholms stad

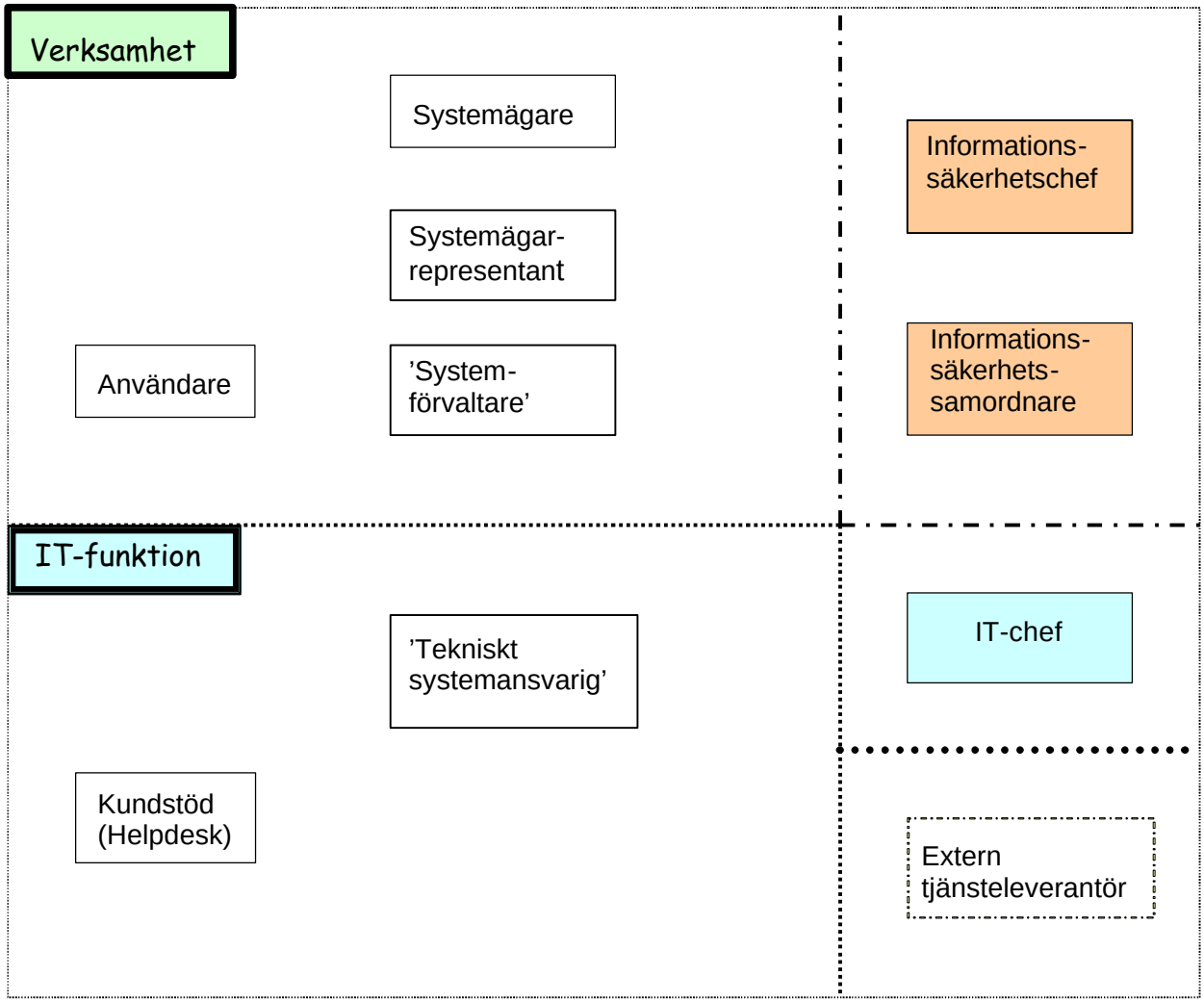
- Stadens styrande dokument skall vara kända
- Stadens säkerhetsorganisation skall vara känd
- Grundnivån för säkerheten skall fastställas genom informationsklassificering
- Berörd personal skall ha nödvändiga kunskaper om aktuella IT-system och gällande säkerhetsregler
- Fysiskt skalskydd skall anpassas efter genomförd riskanalys
- Skriftligt godkänt SLA/motsvarande skall finnas före driftsättning
- Åtkomst/behörighet skall tilldelas formellt och endast efter behov samt följas upp regelbundet
- Säkerhetsaspekter skall beaktas vid utveckling och anskaffning av IT-system
- Uppfyllnad av rättsliga krav skall tillgodoses i alla IT-system
- Kontinuitetsplan skall finnas för verksamheter med starkt beroende av IT-system
- Alla incidenter skall rapporteras och kontinuerlig uppföljning skall ske mot fastställda regler

4 Organisatorisk säkerhet

4.1 Infrastruktur för informationssäkerhet

Nedan beskrivs schematiskt de viktigaste rollerna vid drift och förvaltning av IT-system.
I nedanstående figur skall informationssäkerhetschef och informationssäkerhetssamordnare enbart ses som oberoende intressenter.
Roll- och ansvarsfördelning mellan central och lokal instans framgår inte.

Drift och förvaltning av IT-system



4.2 Roller

Nämnd/styrelse är juridisk ägare av IT-system.

Nedanstående roller är aktuella i samband med informationssäkerhetsarbetet:

Systemägare	-rollen innebär ett funktionellt, ekonomiskt och säkerhetsmässigt ansvar för aktuellt IT-system -utser systemägarrepresentant
Förvaltnings-/ Bolags-/ Verksamhets-ansvarig chef	-har det övergripande linjeansvaret för informationssäkerheten inom sitt ansvarsområde -tillser att säkerhetsutbildning ges till personalen -tillser att resurser och medel avsätts för säkerhetsarbetet vari ingår att utse informationssäkerhetssamordnare -ansvarar för tilldelning av behörigheter
Systemägar-representant	-systemägarrepresentant utses via nämnd/styrelsebeslut -rollen tilldelas normalt chef med ansvar för hel eller del av verksamhet -verkställer systemägarens beslut -ansvarar för att informationsklassificering av IT-system genomförs och att aktuella säkerhetskrav uppfylls
System-förvaltare	-utses av systemägare/-representant och ansvarar för den löpande uppföljningen av aktuellt IT-system -ger användarstöd gällande verksamhetsrelaterade frågor
Användare	-skall följa stadens regelverk för informationssäkerhet -skall rapportera funktionsstörningar/-fel till systemförvaltare för aktuellt IT-system -skall rapportera alla incidenter till informationssäkerhetssamordnare
IT-chef	-ansvarar bl a för IT-infrastruktur och drift samt teknisk förvaltning av aktuella IT-system
Tekniskt system-ansvarig	-ansvarar för att den dagliga driften upprätthålls enligt upprättat SLA mellan systemägarrepresentant och IT-chef -har det övergripande ansvaret för att de IT-tekniska delarna fungerar och uppfyller ställda krav på åtkomstbegränsning, riktighet, tillgänglighet och spårbarhet
Extern tjänste-leverantör	-ansvarar för att produktionsmiljö, dator- och kringutrustning uppfyller aktuella säkerhetskrav -samråder med stadens informationssäkerhetschef/-samordnare i säkerhetsfrågor -har en utsedd informationssäkerhetssamordnare/säkerhetschef
Informations-säkerhetschef	-har huvudansvaret för samordning av informationssäkerhetsarbetet och verkar som internkonsult inom staden -har en rådgivande icke beslutande roll -ansvarar för att övergripande policies och riktlinjer för informationssäkerhetsarbetet utarbetas och beslutas

	-övervakar att policies och riktlinjer för informationssäkerhetsarbetet följs och vid behov föreslår förbättringar -skall tillse att staden har tillgång till effektiva metoder och tekniker för säkerhetsarbetet -skall verka för att erforderliga resurser avsätts för säkerhetsarbetet -skall ta initiativ till och medverka i informations- och utbildningsaktiviteter gällande informationssäkerhet -kontrollerar att befintliga säkerhetsregler följs och vid behov föreslår förbättringar
Informations-säkerhets-samordnare	-sprider kunskap om policies, riktlinjer och anvisningar -är kontaktperson mot stadens informationssäkerhetschef -tillser att erforderliga riktlinjer utformas och beslutas inom respektive förvaltning/bolag -samordnar och följer upp informationssäkerhetsarbetet inom respektive förvaltning/bolag -rapporterar incidenter till stadens informationssäkerhetschef
Projektledare	-skall tillse att verksamhetskraven på säkerhet beaktas -skall svara för att projektet följer stadens regelverk för informationssäkerhet

4.2.1 Samordning av informationssäkerhet

Kommunstyrelsen har delegerat uppgifterna att utarbeta, förvalta, sprida och följa upp de riktlinjer, anvisningar och instruktioner avseende informationssäkerheten som är gemensamma för staden till en Informationssäkerhetschef.

För varje förvaltning/bolag utses informationssäkerhetssamordnare.

4.2.2 Samarbete mellan organisationer

Informationssäkerhetschefen skall bidra till att övervaka att kontakter etableras med viktiga tjänsteleverantörer med betydelse för kritiska informationstillgångar, elförsörjning, telekommunikation, lokalresurser etc.

4.3 Säkerhet vid tredjepartsåtkomst

Avtal mellan parterna skall reglera gemensamma synsätt för informationssäkerhet samt villkor för beviljad åtkomst, tillträde, brandskydd etc.

4.4 Utkontraktering (outsourcing)

Avtal mellan parterna som reglerar överenskommelse både affärsmässigt och säkerhetsmässigt skall tecknas.
Stadens krav på informationssäkerhet skall säkerställas när driftansvaret lagts ut på entreprenad.

5 Klassificering och styrning av tillgångar

Ansvarig för informationstillgångar skall också ansvara för att informationsklassificering görs och att aktuella säkerhetskrav tillgodoses.

5.1 Ansvar för tillgångar

5.1.1 Förteckning över tillgångar

Informationstillgångar skall vara förtecknade och i vissa fall även vara märkta.

Anvisningar

5.1.1.1 *Anvisningar för förteckning och märkning av tillgångar [Appendix A]*

5.2 Klassificering av information

5.2.1 Riktlinjer för informationsklassificering

Informationstillgångar skall klassificeras (värderas) så att rätt skyddsnivå kan fastställas.
Klassificering skall ske tidigt i samband med systemutveckling/-anskaffning och återkommer i förvaltningsskedet.
Klassificeringen utgår från faktorerna Åtkomstbegränsning, Riktighet, Tillgänglighet och Spårbarhet.
Av staden fastställd metod för informationsklassificering skall användas.

Anvisningar

5.2.1.1 *Anvisningar för Informationsklassificering [Appendix A]*

5.2.2 Märkning och hantering av information vid sekretess

Information som är belagd med sekretess skall märkas så att detta framgår.
Det skall även framgå om informationen utgör original eller kopia.
Sekretessprövning skall föregå beslut om utlämnande av information som kan bli föremål för sekretessmärkning.
Hemlig information enligt sekretesslagen 2 kap 2§ hanteras ej i detta dokument.

Anvisningar

5.2.2.1 *Anvisningar för märkning och hantering av information vid sekretess [Appendix A]*
5.2.2.2 *Anvisningar för hantering av arbetsmaterial [Appendix A]*

6 Personal och säkerhet

Genom säkerhetsinsatser skall riskerna minskas för mänskliga misstag, stöld, bedrägeri och missbruk av informationstillgångar.
Målgruppen i kapitlet är förutom anställda i vissa fall även förtroendevalda och konsulter/entreprenörer.

6.1 Säkerhet vid rekrytering och för anställd personal

Gällande säkerhetsbestämmelser skall beaktas vid rekryteringstillfället.
Platssökande skall kontrolleras på lämpligt sätt särskilt om anställningen medför åtkomst till sekretessbelagda uppgifter eller på annat sätt omfattar säkerhetskritiska aktiviteter.
Information hur informationssäkerheten hanteras inom Stockholms stad skall lämnas till nyanställd personal.

6.1.1 Krav på anställda gällande informationssäkerhet

Förhållanden och villkor för anställning skall klart uttala den anställdes ansvar för informationssäkerhet.

Anvisningar

6.1.1.1 *Anvisningar gällande personal och säkerhet [Appendix A]*
6.1.1.2 *Anvisningar för hantering av e-post [Appendix A]*
6.1.1.3 *Anvisningar för åtkomst till och användning av Internet [Appendix A]*

6.2 Användarutbildning

Utbildning och information till all egen och inhyrd personal skall ingå i en kontinuerlig process för att skapa medvetande om informationssäkerhet och gällande säkerhetskrav.

Användardokumentation kan med fördel integreras i aktuellt IT-system eller vara tillgänglig via Intranätet.

6.2.1 Utbildning i informationssäkerhet

Verksamhetsansvarig chef skall tillse att berörd personal ges möjlighet att genomgå utbildning i informationssäkerhet.

Anvisningar

6.2.1.1 *Anvisningar för användarutbildning [Appendix A]*

6.3 Säkerhetsincidenter och funktionsfel

Rutin skall finnas för hantering av incidenter och funktionsfel.

6.3.1 Rapportering

Incidenter och säkerhetsmässiga svagheter skall snarast möjligt rapporteras för att initiera nödvändiga åtgärder för att minimera skada, åtgärda brister och utreda eventuell brottslighet.

Anvisningar

6.3.1.1 *Anvisningar för incidenthantering [Appendix A]*

6.4 Överträdelser

Överträdelser av stadens/bolagets säkerhetsregler hanteras av verksamhetsansvarig chef.

7 Fysisk och miljörelaterad säkerhet

Stadens säkerhetspolicy [1993-09-06], som Brandförsvaret har förvaltningsansvar för, reglerar övergripande den fysiska säkerheten vid Stockholms stads bolag/förvaltningar.

7.1 Säkrade utrymmen

Åtgärder skall vidtas för att förhindra obehörigt tillträde till utrymmen med informations-tillgångar samt att förhindra skador och störningar där dessa tillgångar är placerade.

7.1.1 Skalskydd och tillträde

För verksamheten kritiska eller viktiga informationstillgångar skall inrymmas i säkrade utrymmen inom ett avgränsat skalskydd med lämpliga spärrar och tillträdeskontroller.
Nivån på skalskyddet fastställs med hjälp av riskanalys.
Installationer av tillträdesskydd, inbrottslarm och brandlarm skall grundas på auktoriserad organisations normer om sådana finns.

Tillträdeskontroll skall tillämpas för att säkerställa att endast behörig personal får tillträde till säkrade utrymmen.

Anvisningar

7.1.1.1 *Anvisningar för skalskydd och tillträde [Appendix A]*

7.2 Skydd av utrustning

Åtgärder skall vidtas för att förhindra förlust, skada eller åverkan på utrustning samt förhindra avbrott i verksamheten.

7.2.1 Fysiskt skydd, elförsörjning och kablageskydd

Beroende av placering av utrustning krävs olika typer av fysiskt skydd.
Eventuella miljörisker skall speciellt beaktas.

Anvisningar

7.2.1.1 *Anvisningar för placering och skydd av utrustning [Appendix A]*

7.2.2 Säkerhet för utrustning utanför egna lokaler

Utrustning som används utanför egna lokaler skall skyddas så att samma säkerhetsnivå, som om den används i de egna lokalerna, uppnås.
Särskild hänsyn skall tas mot risk för stöld och informationsåtkomst.

Anvisningar

7.2.2.1 *Anvisningar för distansarbete [Appendix A]*
7.2.2.2 *Anvisningar för mobil datoranvändning [Appendix A]*

7.2.3 Avveckling/återanvändning av utrustning

Avveckling/återanvändning av utrustning som innehåller lagrad information skall ske så att obehörig informationsåtkomst förhindras.

Anvisningar

7.2.3.1 *Anvisningar för avveckling/återanvändning av utrustning [Appendix A]*

7.3 Allmänna åtgärder

Informationstillgångar skall skyddas både genom personalens agerande och tekniska åtgärder.

7.3.1 Publika miljöer

Skalskydd skall anordnas med särskilt beaktande av den publika miljön.
Åtgärder skall vidtas för att motverka anonym användning av datorer som staden upplåter publikt.

Anvisningar

7.3.1.1 *Anvisningar för datorer i publik miljö [Appendix A]*

8 Styrning av kommunikation och drift

Gjord informationsklassificering styr säkerhetskraven för ledning och drift av IT-system och kommunikationsutrustning.

8.1 Driftrutiner och driftansvar

IT-chef eller motsvarande är ansvarig för ledning och drift av gemensamma informationstillgångar.
Skriftlig driftdokumentation med ansvarsfördelning skall finnas.

8.1.1 Dokumenterade driftrutiner

Driftrutiner skall vara dokumenterade och hållas aktuella. Ändringsrutin för driftdokumentation skall tillämpas.

I drift- och/eller förvaltningsåtagande för IT-system skall anvisningar finnas för att regelbundet kunna ta del av leverantörers systemrevisioner. Samtliga uppdateringar skall värderas utifrån ett säkerhetsperspektiv och de uppdateringar som innebär minskning av riskkostnaden skall införas.

Anvisningar

8.1.1.1 *Anvisningar för Informationsklassificering [Appendix A]*
8.1.1.2 *Anvisningar för driftdokumentation [Appendix A]*
8.1.1.3 *Anvisningar för säkerhetsuppdateringar (patchar) [Appendix A]*

8.1.2 Styrning av ändringar i driftmiljö

Förändringar i driftmiljö, utrustning och rutiner skall styras via befintliga anvisningar, ex.vis
- identifiering och registrering av större ändringar;
- konsekvensanalys av sådana ändringar;
- godkännande/beslutsform för ändringar;
- informationskrav till verksamheten;
- rutin för avbrytande av och återställande av misslyckade ändringar.

Fastställda processer för hantering av förändringar i IT-system skall alltid följas.
Process för ändringshantering skall följas även för åtgärder som är av rent infrastrukturell karaktär. Motsvarande process skall följas när det gäller IT-system som anskaffas från extern leverantör.
Samtliga ändringar skall kunna härledas till en ansvarig beställare.

Anvisningar

8.1.2.1 *Anvisningar för ändringar i driftmiljö [Appendix A]*

8.1.3 Uppdelning av arbetsuppgifter

Arbetsuppgifter och ansvarsområden skall delas upp så att möjligheter till obehörig förändring eller missbruk av information eller tjänster minskas.

8.1.4 Uppdelning av utvecklings- och driftresurser

Utvecklings-, test- och driftmiljö skall utformas så att risk för sammanblandning minimeras.
Åtgärderna skall medge att:
- utvecklings- och driftprogram kan köras i skilda tekniska miljöer;
- utvecklings- och testarbete kan åtskiljas;
- utvecklingspersonals åtkomst till driftmiljön kan regleras.

8.1.5 Hantering av externa resurser

Användning av extern leverantör för drift av IT-system skall föregås av och beslutas med en riskanalys som grund.
Följande frågeställningar skall bl.a. behandlas:
- identifiering av kritiska tillämpningar som hellre bör hållas inom den egna verksamheten;
- godkännande av systemägarrepresentant;
- påverkan på avbrottsplan;
- säkerhetsregler och sätt att kontrollera efterlevnad;
- övervaknings- och uppföljningsnivå;
- incidenthanteringsformer - ansvar, rapportering och rutiner.

Driftpersonal skall vara medveten om gällande säkerhetsregler och sekretessbestämmelser. Detta regleras i sekretessavtal som upprättas individuellt.

8.2 Driftgodkännande och planering

Skriftlig rutin för driftgodkännande av IT-system skall finnas.
Rutin för bedömning av framtida kapacitetsbehov skall finnas.

8.2.1 Driftgodkännande

Driftgodkännande skall föregås av en definierad testfas.

Anvisningar

8.2.1.1 *Anvisningar för driftgodkännande och planering [Appendix A]*
8.2.1.2 *Anvisningar för driftdokumentation [Appendix A]*

8.3 Skadliga program

Åtgärder skall införas i upptäckande och förebyggande syfte för att skydda mot skadlig programkod. Detta skall också innefatta lämpliga rutiner för att göra användarna uppmärksamma på risker och gällande anvisningar.

8.3.1 Skydd mot skadliga program

Användare skall vara medvetna om att datorer skall användas i enlighet med verksamhetens syfte och fastställda anvisningar.

Anvisningar

8.3.1.1 *Anvisningar för åtgärder mot skadliga program [Appendix A]*

8.4 Ordning och reda

Åtgärder skall vidtas för att säkerställa informationens riktighet och tillgänglighet i enlighet med stadens krav. Åtgärderna omfattar säkerhetskopiering, loggning av händelser och fel, övervakning av utrustning samt anvisningar för återställning.

8.4.1 Säkerhetskopiering

Utrymme där säkerhetskopior eller skåp som innehåller säkerhetskopior förvaras skall brandskyddas i enlighet med gällande lagstiftning samt eventuella normer från försäkringsinstitut. Kritiska säkerhetsfunktioner som återställning av säkerhetskopior skall övas och kontrolleras.

Anvisningar

8.4.1.1 *Anvisningar för säkerhetskopiering [Appendix A]*

8.4.2 Loggar

Kritiska händelser i drift och datakommunikation skall vara spårbara. Detta bör i första hand åstadkommas med automatiska loggningsfunktioner. Alternativt redovisas händelser skriftligt. Loggning bör inriktas på drift-, transaktions- och säkerhetshändelser.

Anvisningar

8.4.2.1 *Anvisningar för logghantering [Appendix A]*

8.5 Styrning av nätverk

Skydd av stadens egna nätverk för informationsöverföring skall ta hänsyn till krav utifrån organisationsavgränsning och kopplingar mot externa datanät. Hantering av säkerheten för nätverk, som kan sträcka sig över organisationsgränserna, kräver särskild uppmärksamhet.

Kompletterande åtgärder kan krävas för skyddet av känsliga data som sänds via allmänna nät.

Följande skall särskilt beaktas:

- ansvar och anvisningar skall fastställas för hantering av all ingående utrustning i nätverk
- särskilda åtgärder avseende informationens behov av skydd gällande åtkomstbegränsning och riktighet när data passerar allmänna nät liksom skydd mot anslutna IT-system.

8.5.1 Nätverk

Anvisningar och instruktioner skall finnas för att uppnå och vidmakthålla fastställd säkerhetsnivå i stadens nätverk.

Anvisningar

8.5.1.1 *Anvisningar för säkerhetsuppdateringar (patchar) [Appendix A]*

8.5.1.2 *Anvisningar för säkerhetsarkitektur nätverk [Appendix A]*

8.6 Mediahantering och mediasäkerhet

Skyddsrutiner skall finnas för att skydda pappersdokument, datamedia, in- och utdata samt systemdokumentation från skada, stöld och obehörig åtkomst.

8.6.1 Avveckling av media

Lagringsmedia skall avvecklas på ett säkert sätt när de inte längre behövs.

Följande skall särskilt beaktas:

- lagringsmedia som innehåller känslig information destrueras alternativt raderas på ett säkert sätt
- av spårbarhetsskäl skall det dokumenteras hur känsligt material avvecklas.

Anvisningar

8.6.1.1 *Anvisningar för avveckling av media [Appendix A]*

8.6.2 Säkerhet för systemdokumentation

Systemdokumentation skall skyddas i enlighet med aktuell säkerhetsprofil.

Anvisningar

8.6.2.1 *Anvisningar för systemdokumentation [Appendix A]*

8.7 Utbyte av information och program

Allt utbyte av information mellan organisationer skall styras och upprättas enligt gemensamma bedömningar avseende informationens behov av skydd gällande åtkomstbegränsning och riktighet samt krav på tillgänglighet.
Ansvarsförhållanden skall vara klarlagda på lämpligt sätt.

8.7.1 Säkerhet i elektronisk handel

Regleras i avtal mellan berörda parter.

Anvisningar

8.7.1.1 *Anvisningar för elektronisk handel [Appendix A]*

8.7.2 Säkerhet i elektroniskt offentliggjord information

Åtgärder skall vidtas för att skydda riktigheten hos elektroniskt offentliggjord information.

Anvisningar

8.7.2.1 *Anvisningar för elektroniskt offentliggjord information [Appendix A]*

8.7.3 Annat informationsutbyte

Anvisningar skall finnas för att skydda informationsutbyte vid användning av röst-, fax- och videokommunikationsutrustning.

Anvisningar

8.7.3.1 *Anvisningar för annat informationsutbyte [Appendix A]*

9 Styrning av åtkomst

Åtkomst till IT-system och nätverk skall styras utifrån verksamhetsbehov och säkerhetskrav.

9.1 Verksamhetskrav på styrning av åtkomst

Genomförd informationsklassificering avgör åtkomst till information.

9.2 Styrning av användares åtkomst

Användares åtkomst till informationstillgångar skall styras genom en kombination av tekniska och administrativa åtgärder.

9.2.1 Behörighetsadministration

Hantering av behörigheter skall ske enligt gällande anvisningar.

Anvisningar

9.2.1.1 *Anvisningar för hantering av behörighetsadministration [Appendix A]*

9.2.2 Behörighetskontroll

För användare skall åtkomst till informationstillgångar ske via behörighetskontrollsystem där användaren har en unik identitet och lösenord eller eventuellt en rolltillhörighet.

Anvisningar

9.2.2.1 *Anvisningar för behörighetskontroll [Appendix A]*

9.3 Styrning av åtkomst till nätverk

Interna och externa nätverk betraktas som informationstillgångar varför åtkomst styrs enligt gällande riktlinjer för åtkomst.
Stadens nätverk skall vara tydligt avgränsat mot omvärlden genom lämplig teknik.

9.3.1 Utnyttjande av nätverkstjänster

Konsulters och andra leverantörers utrustning får inte anslutas till stadens nätverk utan tillstånd.

Anvisningar

9.3.1.1 *Anvisningar för nätverksanslutning [Appendix A]*
9.3.1.2 *Anvisningar för säkerhetsarkitektur nätverk [Appendix A]*

9.4 Styrning av åtkomst till operativsystem

Operativ- och behörighetskontrollsystem skall utformas och utnyttjas för att åstadkomma styrning av användares inklusive administratörers åtkomst till informationstillgångar.

9.4.1 Åtkomst till operativsystem

Systemadministratörer skall kunna identifieras och styras vad gäller åtkomst till operativsystem.

Anvisningar

9.4.1.1 *Anvisningar för åtkomst till operativsystem [Appendix A]*

9.5 Styrning av åtkomst till tillämpningar

En fastställd katalogstruktur med hänsyn till verksamhetens organisation och ansvarsförhållanden skall tillämpas.

9.5.1 Åtkomst till tillämpningar

Säkerhetsåtgärder skall vidtas för att styra åtkomst till tillämpningar.
Systemägarrepresentant skall besluta om ett IT-systems information skall vara externt åtkomlig.

Anvisningar

9.5.1.1 *Anvisningar för åtkomst till databaser [Appendix A]*
9.5.1.2 *Anvisningar för kryptering [Appendix A]*

9.6 Övervakning av systemåtkomst och systemanvändning

Övervakningsinformation kan indikera avvikelser samt utnyttjas för utredning av incidenter.

9.6.1 Loggning av händelser

Loggar som registrerar avvikelser och andra säkerhetsrelevanta händelser skall finnas och bevaras under fastställd tid.

Anvisningar

9.6.1.1 *Anvisningar för logghantering [Appendix A]*

9.7 Mobil datoranvändning och distansarbete

Informationssäkerheten skall tryggas vid användning av mobil utrustning och vid distansarbete.

9.7.1 Mobil datoranvändning

Den ökade säkerhetsrisk som föreligger vid mobil datoranvändning skall beaktas i Anvisningar och Instruktioner.

Anvisningar

9.7.1.1 *Anvisningar för mobil datoranvändning [Appendix A]*

9.7.2 Distansarbete

Samma säkerhetsnivå skall gälla för distansarbetsplats som för ordinarie arbetsplats.

Anvisningar

9.7.2.1 *Anvisningar för distansarbete [Appendix A]*

10 Systemutveckling/-anskaffning och systemunderhåll

Systemutveckling skall alltid bedrivas i enlighet med fastställda modeller och metoder.

För samtliga informationstillgångar skall säkerhetskrav sammanställas med genomförd riskanalys och informationsklassificering enligt kapitel 5.2 som grund.

10.1 Säkerhetskrav på IT-system

Beaktande av säkerhetskrav skall ske redan från början i processen för systemutveckling/-anskaffning samt vara en del av förvaltningsansvaret avseende informationstillgångar.

10.1.1 Analys och specifikation av säkerhetskrav

Säkerhetskrav skall vara åtgärdade innan driftgodkännande kan ges.

Anvisningar

10.1.1.1 *Anvisningar för driftgodkännande och planering [Appendix A]*

10.1.1.2 *Anvisningar för Informationsklassificering [Appendix A]*

10.2 Säkerhet i tillämpningar

Utifrån fastställda säkerhetskrav skall införda säkerhetsåtgärder verifieras och godkännas av systemägarrepresentanten innan driftgodkännande.

10.2.1 Informationskvalitet

Kontrollmekanismer skall finnas så att förväntad informationskvalitet garanteras.

Anvisningar

10.2.1.1 *Anvisningar för användardokumentation [Appendix A]*

10.2.1.2 *Anvisningar för informationssäkerhet vid utveckling och tillämpning av Internettjänster [Appendix A]*

10.2.2 Elektronisk signatur

I de fall riktigheten vid informationsutbyte måste garanteras skall rekommenderad teknisk lösning användas.

Anvisningar

10.2.2.1 *Anvisningar för elektronisk signering [Appendix A]*

10.3 Säkerhet i databaser och program

Säkerhet i databaser under utvecklings- och förvaltningsskedet skall säkerställas genom tydliga anvisningar för åtkomst till databaser samt en dokumenterad metod för kvalitetssäkring för att tillgodose krav på riktighet.

10.3.1 Styrning av säkerhet i databaser och program

Hantering av databaser och program skall ske enligt fastställd systemutvecklings-/förvaltningsmodell.

Anvisningar

10.3.1.1 *Anvisningar för hantering av testdata och program [Appendix A]*

11 Kontinuitets- och avbrottsplanering

Kontinuitets- och avbrottsplanering är förmågan och beredskapen att hantera störningar/avbrott i en organisations verksamhet.

11.1 Aspekter på kontinuitetsplanering

En kontinuitetsplaneringsprocess upprättas för att minska den skada som förorsakas av olika allvarliga störningar/avbrott. Processen skall omfatta en kombination av förebyggande och återställande säkerhetsåtgärder.

I kontinuitetsplaneringen ingår att löpande identifiera och minska risker om inte detta gjorts i särskild riskanalys.

11.1.1 Processen kontinuitetsplanering

Processen skall fokusera på aktuell verksamhets viktigaste mål/uppgifter.

Anvisningar

11.1.1.1 *Anvisningar för processen kontinuitetsplanering [Appendix A]*

11.2 Aspekter på avbrottsplanering

Avbrottsplan skall upprättas för att säkerställa att berörda informationstillgångar kan återställas inom angiven maximal avbrottstid.

11.2.1 Processen avbrottsplanering

Processen skall fokusera på återstart av IT-system enligt fastställd prioritetsordning.

Anvisningar

11.2.1.1 *Anvisningar för processen avbrottsplanering [Appendix A]*

11.3 Riskanalyser

11.3.1 Processen riskanalys

Processen skall fokusera på aktuell verksamhets viktigaste mål/uppgifter.

Anvisningar

11.3.1.1 *Anvisningar för processen riskanalys [Appendix A]*

12 Efterlevnad

En väl fungerande informationshantering bidrar till att staden kan fullgöra sina uppgifter. Det är därför viktigt att tillämpliga lagar och förordningar samt aktuella regelverk efterlevs för att störningar ej skall uppstå.

12.1 Identifiering av tillämpliga bestämmelser

12.1.1 Lagar och förordningar

Minimikraven avseende informationssäkerhet fastställs genom lagar och förordningar.
Tryckfrihetsförordningen ställer krav på att allmän handling skall vara tillgänglig.

Anvisningar

12.1.1.1 *Förteckning över gällande lagar och förordningar [Appendix A]*

12.1.2 Immaterialrätt

Programvaror skall användas i enlighet med gällande avtal och licensregler.

12.1.3 Skydd av personuppgifter

Hantering av personuppgifter skall dokumenteras och anmälas till personuppgiftsombud.
Detta sker bland annat i samband med informationsklassificering av IT-system.

12.1.4 Reglering av kryptering

Kryptering får endast ske med av staden godkänd programvara.

12.2 Granskning av säkerhetspolicy, etik och teknisk efterlevnad

12.2.1 Kontroll av säkerhetspolicy och etik

Uppföljning av Internetanvändandet skall göras för att kontrollera om policies eller etiska normer efterlevs.
Uppföljning i övrigt kan ske på olika sätt beroende på typ av verksamhet.

Anvisningar

12.2.1.1 *Anvisningar för åtkomst till och användning av Internet [Appendix A]*

12.2.1.2 *Anvisningar för säkerhetsuppföljning [Appendix A]*

12.2.2 Kontroll av teknisk efterlevnad

Den använda tekniken skall kontrolleras utifrån ett säkerhetsperspektiv.
Exempelvis kan penetrationstester göras för att kontrollera IT-systemets åtkomst- och kommunikationsskydd.

12.3 Hänsynstaganden vid revision av IT-system

12.3.1 Styrning av revision av IT-system

IT-systeminriktad revision skall planeras, överenskommas och regelbundet genomföras för att minska risken för störningar i verksamhetsprocesserna.