S

Informationsklassning

Inledning
Data som lagras och bearbetas i stadens IT-system bildar information som representerar stora värden. För att få en heltäckande uppfattning om säkerhetskraven i dessa IT-säkerhetssystem måste hänsyn tas till följande faktorer:

- krav på informationens riktighet
- krav på tillgänglighet
- krav på åtkomstbegränsning
- krav på spårbarhet

När kraven är identifierade kan rätt skyddsnivå fastställas för det aktuella informationssystemet/databasen.
De system som är väsentliga för verksamheten skall informationsklassas vartannat år.
Vid nyutveckling/anskaffning av informationssystem skall informationsklassning ske i ett tidigt skede. Avdelningschef/enhetschef ansvarar för att detta genomförs.

Definition
Med informationsklassning avses en metod att indela informationen med hänsyn till vilken skyddsnivå systemägaren kräver, när det gäller
Riktighet, Tillgänglighet, Åtkomstbegränsning och Spårbarhet.

Genomförande
Deltagare vid ett klassningstillfälle bör vara, förvaltningens systemrepresentant, användare, system/driftstekniskt ansvarig samt IT-säkerhetssamordnare i rollen som klassningsledare. Vid klassning av lokala system bör systemförvaltaren för lokala system deltaga.

Vid tillfället ges en kort information om IT-säkerhet och var klassningen kommer in i enlighet med förvaltningens och stadens IT-säkerhetsregler.
Därefter görs en beskrivning av systemet genom att blanketten ”Protokoll för klassificering av IT-system” fylls i.

Efter detta går man igenom klassificeringsmatrisen och kommer överens om vilken klass systemet skall ha.

Grundnivå (klass 3)
Förhöjd nivå (klass 2)
Högsta nivå (klass 1)

När man enats om en klassificering dokumenteras detta i protokollet.

Nästa moment är att kontrollera att den satta klassificeringen överensstämmer med nuläget när det gäller erforderlig säkerhetsnivå.
För varje klassificeringstal finns ett antal åtgärder beskrivna i åtgärdskatalogen.
Efter genomförd kontroll skall de åtgärder som är kvar
att genomföra förtecknas i prioriteringsordning på en bristlista och undertecknas av systemägarrepresentanten.
Efter en lämplig tid görs en ny kontroll och eventuella brister prioriteras.

Åtgärdskatalog

För klass 3 behöver inga specifika åtgärder vidtas. De generella bestämmelser som gäller för IT-säkerheten i staden måste givetvis följas.

RIKTIGHET

Klass 2	Klass 1	
+	+	Rimlighetskontroller för data som ger önskad informationskvalité skall finnas *Kommentar: kontrollera att det finns stöd i programmet för automatiska kontroller av viktiga inmatade uppgifterna t ex datumformat, obligatoriska fält, felaktiga slutsummor, spärr mot orimligt höga summor etc*
+	+	Rutiner för datainsamling skall vara sådana att störningar minimeras *Kommentar: kontrollera befintliga pappers- kontorsrutiner i det flöde som sker innan uppgifterna matas in i programmet. Titta även på samma rutiner sedan programmet lämnat ifrån sig uppgifter*
+	+	Utbildningsplan för personal skall fastläggas och genomförandet säkerställas *Kommentar: se till att introduktionsutbildning och fortutbildning finns att tillgå i samband med köpet av programmet. Tänk på behovet av utbildning av nyanställd personal.*
+	+	Erforderlig dokumentation skall upprättas och a-jourhållas
+	+	Samtliga tester som systemutvecklingsmodellen kräver skall genomföras
+	+	Övriga kvalitetssäkrings- och sårbarhetsanalyser som erfordras enligt utvecklingsmodellen skall genomföras
-	+	Regelbunden dialog med systemets samtliga intressenter skall etableras *Kommentar: intressenter kan exempelvis vara andra systemägare som har gränssnitt mot det klassade*

- \+ Systemägaren skall garantera datas riktighet genom undertecknad kvalitetsdeklaration

- \+ Systemutvecklingsarbetet skall bedrivas mot fastställda ändringsterminer, s.k releaser

- \+ Rutiner för datainsamling skall vara sådana att störningar minimeras

TILLGÄNGLIGHET

Klass 2	Klass 1	
+	+	Behov av klimatanläggning (kyla, fukt) och skydd mot gas- och vätskeutströmning skall prövas utifrån den aktuella situationen i serverrummet.
+	+	Avbrottsfri kraft (UPS) skall alltid finnas.
+	+	Operatörskonsol skall skyddas med lösenord.
+	+	Rutiner för säkerhetskopiering skall fastställas efter aktuell verksamhets behov. Dock bör alltid backup på data tas minst en gång per vecka.
+	+	Rutiner för märkning av backup-media skall fastställas
+	+	Återläsningsrutiner (Restore) skall testas regelbundet.
+	+	Säkerhetskopia skall förvaras i arkiv med brandklass motsvarande 120 minuter enligt Statens Provningsanstalts kriterier i annan byggnad än driftstället.
+	+	Åtskild test- och produktionsmiljö skall finnas för att undvika driftstörningar.
+	+	Beroende av nyckelpersonal skall minimeras
+	+	Funktion för användarstöd skall finnas etablerad. *Kommentar: kan vara help-desk, jourtelefon, korridorstödsfunktion etc*
+	+	Avtal om service på utrustning skall finnas.
-	+	Tillträde till driftlokaler skall kunna loggas
-	+	Alternativ driftcentral skall finnas tillgänglig
-	+	Den alternativa driftcentralen skall kunna användas även under icke avbrottstid.

- + Spegling av diskar skall fungera kontinuerligt

- + Personella och administrativa rutiner skall upprättas för att kunna hantera alternativ driftcentral.

- + Möjlighet till alternativa datakommunikationsvägar skall finnas och arrangeras efter verksamhetens behov

ÅTKOMSTBEGRÄNSNING

Klass 2	Klass 1	
+	+	För aktuell systemmiljö godkänt behörighetskontrollsystem skall användas
+	+	Detaljerade rutiner för behörighetsadministrationen skall upprättas
+	+	Användarstöd skall ges möjlighet till support för viss lösenordshantering
+	+	Om betalningsförmedling sker skall elektroniskt sigill användas.
+	+	Om betalningsförmedling sker skall digital signatur användas när denna tjänst fått standardiserad utformning.
+	+	Beroende av nyckelpersonal skall minimeras
+	+	Eventuellt behov av destruktion av lagringsmedia skall beaktas
-	+	Kryptering av lagrat och överfört data skall ske i enlighet med stadens standard då sekretessbelagd information hanteras i IT-system
-	+	Destruktion av lagringsmedia skall ske på godkänt vis *Kommentar: MFO har avtal med destruktionsföretag*
-	+	Behörighetskontrollsystem för operativsystemet skall finnas

SPÅRBARHET

Klass 2	Klass 1	
+	+	System- och applikationsloggar skall alltid vara påslagna
+	+	Detaljerade rutiner för loggning och uppföljning skall fastställas
-	+	Speciella funktioner skall byggas om inte applikationen stöder verksamhetens och revisionens krav

Protokoll för klassificering av IT-system

ALLMÄNNA UPPGIFTER

System
Datum för klassificering

Beskrivning

Avgränsning

Närvarande Namn	 Roll

REDOVISNING AV RESULTAT

Förvaltningsorganisation

Roll	Organisation

Legala krav

Lag	Tillämpbar	Uppfylld	Kommentar
Tryckfrihetsförordningen			
Sekretesslagen			
Bokföringslagen/ Lagen om kommunal redovisning			
Lagen om Upphovsmannarätt			
Arkivlagen			
Lagen om skydd av företagshemligheter			
Personuppgiftslagen			
Socialtjänstlagen			
Säkerhetsskyddslagen			

Särskilda uppgifter för system som innehåller personuppgifter

Ändamål med behandlingen
Kategori av personer som berörs av behandlingen
Personuppgifter som skall behandlas
Mottagare till uppgifterna
Säkerhetsåtgärder
Överföring till tredje land (Internet)

KLASSIFICERING

	Riktighet	Tillgänglighet	Åtkomstbegränsning	Spårbarhet
Klass				

Kommentarer till klassificeringen

UNDERSKRIFT

Protokollet skall undertecknas av klassningsledaren. Systemägaren för de lokala systemen alternativt förvaltningens representant för de övergripande systemen fastställer klassificeringen och de övriga förhållanden som försättsbladet och bristlistan redovisar genom att justera detta protokoll.

_____
(ort, datum)

_____
(klassningsledare)

_____
(namnförtydligande)

Justeras:

_____
(ort, datum)

_____
(Systemägarrepresentant för de lokala systemen/Systemrepresentant för övergripande system)

_____
(namnförtydligande)