Riktlinje för säkerhetskrav vid upphandling av IT-stöd

1. Inledning

Detta dokument redogör för vissa grundläggande säkerhetskrav som bör ställas i samband med anskaffning eller utveckling av IT-stöd. Med begreppet IT-stöd avses alla typer av IT-system och applikationer (fortsättningsvis även kallat ”systemet” eller ”applikationen”) som används för att hantera information inom Örebro kommun, inklusive gränssnitt ut mot externa parter, såsom ex. medborgare. De krav som redovisas är hämtade från vad som anses vara ”Best Security Practice”[1], ISO/IEC 17799 samt OWASP (Open Web Application Security Project) Testing Guide. Beroende på system och informationens känslighet kan det vara nödvändigt att komplettera dessa krav.

Säkerhet i IT-stöd skall åstadkommas genom tidig bedömning av vilka åtgärder som behöver vidtas för att skapa önskad skyddsnivå. De säkerhetskrav som ställs på IT-stödet skall spegla värdet av de informationstillgångarna och den potentiella skada för verksamheten som kan bli resultatet av felaktigheter i eller brist på säkerhet. Som bilaga till denna riktlinje finns ett förslag på arbetsgång för att hantera säkerhetsfrågorna vi upphandling av ett IT-stöd.

För att definiera säkerhetskrav för den information som skall hanteras i IT-stödet ska alltid en riskanalys genomföras. Denna analys ska dokumenteras! De säkerhetskrav som ställs skall beakta riktighet, sekretess, tillgänglighet samt spårbarhet.

Grundläggande krav som skall analyseras är bland andra:

- möjlighet till åtkomststyrning
- möjlighet till spårbarhet och loggning av händelser
- validering av indata, intern bearbetning och utdata
- placering i olika tekniska miljöers påverkan för skyddsnivå
- användbarhet (brister kan ge säkerhetsproblem).

I samband med framtagning av kravspecifikationer kan man utgå från exemplen i detta dokument för att vidare tydliggöra vilka krav och förväntningar som ställs på leverantören samt leveransen. Det är dock viktigt att detta arbete utgår från en tidigare genomförd och beskriven riskanalys. Annars är risken stor att säkerhetsnivån sätts antingen för högt eller för lågt.

Innan ett IT-stöd tas i bruk ska samtliga etablerade säkerhetsåtgärder verifieras och godkännas av systemägaren.

I anslutning till de olika avsnitten som beskriver krav finns ett avsnitt som benämns ”Övrigt att beakta”. Detta avsnitt beskriver framför allt viktiga aspekter på säkerhet i vår egen hantering av det nya IT-stödet.

---

[1] Best Security Praxis eller god sed är ett samlingsbegrepp för en rad olika källor, exempelvis olika leverantörers säkerhetsrekommendationer, allmänna råd och beskrivning kopplade till standarder, rekommendationer från statliga myndigheter avseende säkerhet osv.

2. Säkerhetskrav

2.2. Krav på leverantören, testning och leverans

Säk -1.	**Krav:** Leverantören ska ha en policy som beskriver hur de bedriver säkerhetsarbete i såväl den operativa verksamheten som kompetensutveckling avseende säker systemutveckling. Denna policy ska kunna bifogas.
Säk -2.	**Krav:** Leverantören skall tillämpa en vedertagen modell för systemutveckling samt projektarbete. **Beskriv** vilken/vilka modeller som tillämpas.
Säk -3.	**Krav:** Om tredjepart används för programutveckling ska ett avtal som reglerar både affärsmässighet och säkerhet tecknas. Avtalet ska bifogas. Följande punkter skall beaktas avseende säkerhet: • hur de rättsliga kraven skall uppfyllas, exempelvis rörande lagstiftning om sekretess och personuppgifter • vilka åtgärder som skall vidtas för att säkerställa att alla berörda parter, inklusive underleverantörer, är medvetna om sitt säkerhetsansvar, licensieringsarrangemang, äganderätt till koden och upphovsrätt • säkerställande av utfört arbetes kvalitet och noggrannhet; depositionsarrangemang för programkod om inte tredjepart kan fullgöra sin uppgift.
Säk -4.	**Krav:** Under utvecklingsfasen skall aktiviteter för säkerhetstestning och kvalitetsgranskning av kod finnas inplanerade. **Beskriv** hur dessa aktiviteter genomförs och på vilket sätt.
Säk -5.	**Krav:** Leverantören ska innan leverans till Örebro kommun bekosta säkerhetstestning av systemet och ingående systemkomponenter. Testet ska genomföras av tredje part anvisad av Örebro kommun.
Säk -6.	**Krav:** Leverantören ska på egen bekostnad åtgärda eventuella säkerhetsbrister som Örebro kommun identifierar i samband med acceptanstest och/eller leveranskontroll.

Övrigt att beakta

- Avtal skall omfatta tydliggörande av fördelning av ansvar för säkerhet och säkerhetsfunktioner mellan leverantören och beställaren. Avtalet bör bland annat beakta vem som ansvarar för implementation av säkerhetsfunktioner samt vem som ansvarar för testning och verifiering av säkerhet. I det fall tredje part anlitas för testning och verifiering skall det vara tydligt vilken av parterna som står för denna kostnad.
- Vid leverans och installation av IT-stödet får ej test- eller utvecklingsversioner placeras i produktionsmiljö, se även beskrivning av driftsättningsprocessen.
- I det fall IT-stödet omfattar komponenter utöver applikation, exempelvis webservrar, applikationsservrar, databaser eller liknande så skall dessa vara konfigurerade utifrån säkerhetssynpunkt respektive härdade.
- Testdata bör skyddas och kontrolleras. System- och acceptanstest kräver normalt avsevärda mängder testdata som är så snarlika produktionsdata som möjligt. Att använda produktionsdatabaser med bland annat persondata bör undvikas. Om sådana data ändå behöver används, bör följande uppfyllas:

    - de bör först anonymiseras
    - rutiner för styrning av åtkomst som tillämpas för produktionssystem skall också gälla vid test av sådana system
    - behörighet skall ges särskilt varje gång produktionsdata kopieras till ett testsystem
    - produktionsdata skall genast raderas från testsystem efter avslutad test
    - kopiering av produktionsdata skall loggas för att erhålla spårbarhet.
- Vid användning av testdata som ej är anonymiserat skall säkerhetsnivå och skyddsmekanismer aktiveras för testsystemet motsvarande produktionssystemet där informationen normalt förvaras.
- Information som omfattas av sekretesskrav bör ej ingå i testdata.

2.3. Krav för behörighetssystem och behörighetskontroller

Säk -7.	**Krav:** System skall i första hand konstrueras så att systemet använder till användaridentiteten knuten behörighet för att avgöra vilka funktioner inom systemet användaren skall ha tillgång till. Åtkomst i fleranvändardatabas skall göras med för systemet särskilt anordnad åtkomstidentitet. **Beskriv** hur dessa funktioner har implementerats.
Säk -8.	**Krav:** Känslig information för behörighetssystemet, såsom ex. lösenord, får ej lagras i klartext i applikationen eller i databaser som används av applikationer. **Beskriv** hur detta hanteras.
Säk -9.	**Krav:** Lösenord skall lagras på sätt som skyddar det mot avläsning. **Beskriv** hur detta hanteras.
Säk -10.	**Krav:** Systemets källkod får ej innehålla behörighetsinformation såsom användarnamn och lösenord för systemkonton.
Säk -11.	**Krav:** Behörighetssystemet skall tillåta att särskilda behörigheter, såsom administratörsbehörigheter, kan tilldelas utpekade användare.
Säk -12.	**Krav:** Så kallad ”grupp-login” får ej förekomma.
Säk -13.	**Krav:** Kontroller av lösenordskvalitet skall finnas. Däribland möjlighet att specificera lösenordslängd, intervall för byte och återanvändning av lösenord, komplexitetskrav, funktion för att styra bort olämpliga lösenord samt funktion för tvingande byte av temporära lösenord. (För utförligare beskrivning av kraven, se avsnitt 7.3 i Örebro kommuns riktlinjer för informationssäkerhet.) Dessa kontroller skall standardmässigt vara aktiverade. **Beskriv** hur detta hanteras.
Säk -14.	**Krav:** Behörigheter för interna systemkonton skall vara utformade enligt principen där minsta möjliga behörighet tilldelas. Detta gäller även konton som används vid kommunikation mellan systemkomponenter, exempelvis mellan applikation och databas. **Beskriv** hur detta hanteras.
Säk -15.	**Krav:** De delar av systemet som skyddas av behörighets- eller åtkomstkontroller skall ej vara direkt adresserbara för obehöriga användare.

Säk -16.	**Krav:** Funktioner för utloggning i systemet skall rensa all behörighets- och sessionsinformation som lagras i temporära filer i användarens dator.
Säk -17.	**Krav:** Behörighetsinformation får ej lagras i klartext i temporära filer som skapas i användarens arbetsstation när systemet används.
Säk -18.	**Krav:** Behörighetsinformation får ej sändas i klartext mellan server och arbetsstation.
Säk -19.	**Krav:** Användarbehörigheter skall tilldelas enligt principen där minsta möjliga behörighet tilldelas. **Beskriv** hur detta hanteras.

2.4. Krav för kontroller av data

Säk -20.	**Krav:** Utformningen av IT-stöd bör säkerställa att restriktioner är införda för att minimera risken för bearbetningsfel som leder till riktighetsförlust. **Beskriv** hur detta hanteras.
Säk -21.	**Krav:** I system där manuell inregistrering förekommer skall relevanta indata- och valideringskontroller finnas. Dessa kontroller skyddar mot så kallade ”injectionattacker” exempelvis Cross-Site Scripting och SQL-Injection. Valideringskontrollen kontrollerar inmatad data och ska upptäcka avsiktlig förvanskning eller förvanskning till följd av bearbetningsfel. **Beskriv** hur detta hanteras.
Säk -22.	**Krav:** Överföring över allmänna datanätverk skall vara skyddad genom teknik som säkerställer att information överförs oförvanskad. Även Örebro kommuns administrativa datanät ska jämföras med ett allmänt datanätverk. **Beskriv** hur detta hanteras.
Säk -23.	**Krav:** Systemet skall ej lämna detaljerade felmeddelanden som avslöjar information om systemets uppbyggnad eller ingående komponenter.
Säk -24.	**Krav:** Systemet ska ej ha debug-funktioner aktiverade.
Säk -25.	**Krav:** Sessionsidentiteter som används i systemet skall genereras slumpmässigt på så sätt att det ej är möjligt att enkelt konstruera eller härleda giltiga sessionsidentiteter. **Beskriv** hur detta hanteras.
Säk -26.	**Krav:** Vid överföring av information till/från externa system skall avsändaren verifieras. Beroende på hur känslig information som hanteras kan olika krav ställas på hur användaren verifieras. **Beskriv** hur detta hanteras.

Övrigt att beakta
De kontroller som krävs beror på tillämpningens art och vilken inverkan en förvanskning av data kan ha på verksamheten.

Exempel på kontroller som kan införas:

- validering av systemgenererade data

- kontroll av riktigheten hos data eller program, ner- eller uppladdade mellan centrala och anslutna datorutrustningar
- checksummor för poster eller filer
- kontroller för att säkerställa att tillämpningsprogram körs vid rätt tidpunkt
- kontroller för att säkerställa att program körs i rätt ordning, avslutas vid eventuellt fel och fortsatt bearbetning inte sker förrän problemet har lösts.

2.5. Krav för spårbarhet och loggning

Säk -27.	**Krav:** Vid IT-system med personuppgifter skall spårbarhet kunna medge uppgift om vem som behandlat uppgiften, tidpunkt, vilken uppgift som varit föremål för behandlingen och vad behandlingen bestod av. **Beskriv** hur detta hanteras.
Säk -28.	**Krav:** Loggningsfunktioner och historik skall finnas för användares in- och utloggningar i systemet samt även felaktiga/misslyckade inloggningar. **Beskriv** hur detta hanteras.
Säk -29.	**Krav:** Loggningsfunktioner skall finnas för säkerhetsrelaterade händelser, exempelvis felaktiga inloggningar, förändring av behörigheter, otillåten anslutning, överträdelser mot behörigheter etc. **Beskriv** hur detta hanteras.