

Yttrande angående KPMGS-rapport om granskning av behörighets- och loggkontroller

IT-enheten har tagit del av KPMG:s rapport angående den granskning av behörighets- och loggkontroller som genomfördes under hösten 2015.

Stora delar av de synpunkter och åtgärdsförslag som KPMG framför i sin rapport anser vi omfatta interna rutiner och arbetssätt inom socialförvaltningen, men det finns även ett antal punkter där IT har ett övergripande ansvar för att producera, dokumentera och kommunicera rutiner, policys och riktlinjer gällande det löpande informationssäkerhetsarbetet.

Nedan redogörs för de punkter som vi identifierat oss som ansvariga för med förslag på åtgärder, tidplan samt resurser involverade i detta arbete.

1. Slutföra arbetet med övergripande informationssäkerhetspolicy (Punkt 8.1)

Förslag på åtgärd:

Steg 1: Slutföra arbetet med en övergripande informationssäkerhetspolicy, tillse att den blir fastställd av kommunfullmäktige och utkommunicerad till verksamheterna.

Steg 2: Införa Ledningssystem för Informationssäkerhet (LIS), utgående från den modell som utarbetats av MSB med anpassning av tillämpliga delar.

Tidplan:

Steg 1: (Förslag på aktivitet)

Förslag på övergripande informationssäkerhetspolicy framtagen
Fastställd av KF
Information, utbildning verksamhet

Klart: (senast)
2016-03-31
2016-06-30
2016-12-31

Steg 2: (Förslag på aktivitet)

Införande ledningssystem för informationssäkerhet (LIS)

Klart: (senast)
2017-12-31

Resurser: (Både steg 1 och steg 2)

IT-enheten (och eventuellt konsultstöd)
IT-råd
Säkerhetssamordnare

2. Säkerhetskopiering av loggar (Punkt 8.3 samt 8.3.1)

Bakgrund: I dag tas det löpande backuper på Procapita HSL, och där ingår även transaktionsloggar. Hantering av dessa backuper följer de gängse rutiner som finns angående förvaring och skydd.

Förslag på åtgärd:

Förtydligande av krav samt rutiner för hantering av säkerhetskopior av HSL-logg över tid tas fram i samarbete med Socialförvaltningen.

Kommentar:

För att tillmötesgå kravet på tid (10 år), Tillgänglighet och Konfidentialitet och med tanke på att verksamhetssystemet kan bli utbytt under denna period, bör loggen på sikt kunna hanteras självständigt utan beroende/koppling till verksamhetssystemet och förslagsvis då i ett e-arkiv.

IT-enheten utför inga loggkontroller i Procapita HSL, detta ansvarar systemägarens interna förvaltningsorganisation för.

Tidplan:

Framtag rutiner för hantering av säkerhetskopior av HSL-logg över tid

Klart: (Senast)

2016-03-31

Resurser:

IT-enheten
Socialförvaltningen
Rapportering till IT-råd

3. Tilldelning av behörigheter (Punkt 8.4)

Förslag på åtgärd:

Fr.o.m 2016-01-01 finns en elektronisk blankett för beställning av användarkonto, denna beställningsblankett är behörighetssatt och endast chefer har möjlighet att göra beställning. Med denna blankett kan användarkonton beställas, ändras och avslutas.

När beställningen skickas går det ett mail från beställande chef till helpdesk, och det finns en spårbarhet i hela beställningsflödet. Detta är kommunicerat på kommunens intranät.

Tidplan:

Säkerställa processen för tilldelning av användarkonto (Användare)

Klart: (senast)

2016-02-28

Resurser:


IT-enheten
IT-rådet (Information 2015-12-18)

Kommentar:

Då samtliga användare, av spårbarhetsskäl, sparas i Procapita, men rensas i AD:et vid avslut kan det finnas avvikelser när man jämför Procapita-AD-PA-system. Användarnamn i Procapita återanvänds aldrig, av ovanstående skäl, men ett användarnamn i AD:et kan återanvändas om personens namnkonstruktion är snarlik någon tidigare anställd. Dock är det ett nytt konto och det finns ingen koppling till tidigare användare gällande behörighet etc.

Hantering med beställningsunderlag infördes för ca 10 år sedan, och då många arbetat inom kommunen längre än så, finns risk för att underlag för beställningen av användarkonto för vissa användare kan saknas.

IT-enheten 2016-01-13


Dan Malmberg Jansson
IT-chef