REGION KRONOBERG

Krav på lösenord och användarkonto

Gäller för: Region Kronoberg

Innehållsförteckning

1 Inledning

En användares användarnamn och lösenord är personliga.

Det innebär att

- användaren är personligt ansvarig för de aktiviteter som sker ifrån användarens användarkonto och inloggning.
- användare är personligt ansvarig för de aktiviteter som sker i system/program, där användarens användarnamn och lösenord används.

Det är därför av största vikt att användaren använder sig av bra (starka) lösenord, så att det är svårt för någon obehörig att gissa dem.

2 Allmänna krav på användar-id och lösenord

2.1 Användarnamn (användar-id)

Användarnamn är en användares unika identitet i Region Kronberg.

- Användarnamn ska vara unikt och följa användaren.
- Användarnamn ska aldrig återanvändas till någon annan person.
- Användarnamn ska användas i alla system.

2.2 Lösenord

Ett lösenord ska vara lätt att komma ihåg, svårt att gissa och ska inte kunna kopplas till användaren.

2.2.1 Krav på lösenord

För att ha god informationssäkerhet inom Region Kronoberg, ställs minst följande krav på lösenord och hanteringen av dem.

- Lösenord är personliga och får inte överlåtas.
- **Ett lösenord ska vara komplext och bestå av minst åtta tecken och bestå av minst tre av de fyra teckenuppsättningarna.**
  Med teckenuppsättning menas:
  1. versaler (A B C)
  2. gemener (a b c)
  3. siffror (1 2 3)
  4. specialtecken (# & %)

  Använd inte nationella tecken såsom *å ä ö*.
- Lösenordet ska inte vara detsamma som användarnamnet eller bestå av delar av användarnamnet.
- Lösenordet ska inte vara knutet till personlig information som till exempel namn, personnummer och telefonnummer.
- Ett lösenord får inte vara en vanlig teckenkombination eller bestå av tecken som ligger i följd på tangentbordet till exempel: *qwerty* eller *1234*.

- Det ska inte vara ett ord eller en vanlig kombination av ord som finns i ordböcker eller används i dagligt språkbruk, oberoende av språk.
- Ett lösenord får inte vara ett ord som är skrivet baklänges.
- En användares lösenord som används inom organisationen får inte vara likadant som andra lösenord som används utanför organisationen.
- Lösenord bör bytas var tredje månad och bör inte vara likadant som ett tidigare använt lösenord.
- Lösenord bör inte skrivas ner. Om det finns behov av att göra det ska anteckningen om lösenordet behandlas som en värdehandling.

3 Användarens ansvar

3.1 Användarkonto

Den person som har ett användarkonto i Region Kronoberg ansvarar för:

- att ha ett komplext lösenord, vilket innebär en blandning av bokstäver, siffror och tecken
- att ha en lösenordsfråga registrerad
- att byta lösenord
- att lösenord inte sprids
- att byta lösenordet om en misstanke finns att någon obehörig kan ha fått tillgång till lösenordet
- att inte återanvända gamla lösenord

3.2 System och program

Kraven ovan gäller för samtliga program som används av personal inom Region Kronoberg som tillämpar inloggning med någon form av lösenord.

Undantag kan finns om aktuellt system inte erbjuder möjlighet till säker inloggning och det inte finns alternativa system. Undantag ska beslutas av VC.

3.3 Tips till användaren vid val av lösenord

För att uppfylla kraven på ett komplext lösenord, så kan detta vara ett tips för användaren.

- ✓ Tänk en hel mening, till exempel: ”***5*** ***F****ula* ***e****lefanter* ***f****lög* ***t****ill* ***d****e* ***7*** ***m****ånarna*”
- ✓ Använd de första bokstäverna i varje ord och siffrorna.
- ✓ Lösenordet blir: ***5Feftd7m***

Lösenordet blir då svårt att gissa för en utomstående, men lätt för innehavaren att komma ihåg.

3.4 Lösenordsfråga
Rutinen för lösenordfrågan ska följas.

3.5 Spärra eller glömt lösenord
Spärra - Om en användare har misstanke om otillåten användning av användarens inloggning, ska lösenordet omedelbart spärras och ersättas med ett nytt. Det kan bli aktuellt med en utredning om eventuellt dataintrång. Användaren ska vid behov kontakta aktuell supportorganisation eller systemförvaltare för berört system för att spärra och byta lösenord

Glömt - Om en användare har glömt sin inloggning ska användaren ska vid behov kontakta aktuell supportorganisation eller systemförvaltare för berört system för att spärra och byta lösenord

Supportorganisation eller systemförvaltare, ska säkerställa användaren genom att använda rutinen för lösenordsfrågan eller på annat sätt säkerställa identiteten.

4 Windowsinloggning

4.1 Användarkonto och lösenord vid Windowsinloggning
En användare ska ha ett användarkonto med ett unikt användarid (användarnamn) och lösenord.

Användarkontot ger användaren behörighet till dator, mappar och program som behövs för att utföra sitt arbete.

4.1.1 Lösenord till användarkonto
- **Lösenord ska vara komplext**, vilket innebär:
  - Bestå av minst åtta tecken
  - Bestå av minst tre av de fyra teckenuppsättningarna (se 3.2.1).
- Lösenord ska bytas var tredje månad.
- Det ska inte gå att återanvända ett tidigare använt lösenord.

4.1.2 Byta lösenord till användarkonto
För att byta lösenord till användarkontot (Windowsinloggning), ska användaren göra följande:

Tryck samtidigt Ctrl+Alt+Del. Därefter knappen "Ändra lösenord". Följ instruktionerna.

4.1.3 Spärra användarkonto
För att spärra ett användarkonto (Windowsinloggning) ska användaren ta kontakt med IT-supporten.

IT-supporten ska säkerställa användaren genom att använda rutinen för lösenordsfrågan.

4.2 Funktionskonto och lösenord vid Windowsinloggning

På arbetsplatser där flera användare delar på en dator, kan inloggningen till datorn (Windowsinloggning) ske med funktionskonto och lösenord. Denna möjlighet ska användas i undantagsfall. I första hand ska ”växla användare” användas.

Funktionskonto är en gruppinloggning, som inte får ge användare åtkomst till andra system eller mappar.

- I första hand ska ”växla användare” användas, om det inte fungerar så är det möjligt att använda funktionskonto.
- Funktionskonto ska endast delas av ett begränsat antal personer inom en enhet.
- Lösenordet till funktionskontot ska följa samma regler som ett personligt lösenord enligt ovan.
- Det bör finnas en person som ansvarar för att lösenordet ändras och ges till berörda.
- När inloggning sker med funktionskonto ska ingen åtkomst till andra system eller mappar vara möjligt.
- Vid misstanke om att det finns någon obehörig som kan ha fått tillgång till lösenordet ska lösenordet bytas. Tänk på att informera alla som behöver tillgång till datorn.

5 Stark autentisering krävs vid kommunikation av patientuppgifter över öppna nät

Socialstyrelsens föreskrift, SOSFS 2008:14, ställer krav på stark autentisering, om patientuppgifter ska kommuniceras över öppna nät, så som Internet och Sjunet.

- Vid överföring av patientuppgifter över öppna nät ska ingen obehörig kunna ta del av uppgifterna. Vilket innebär att kommunikationen ska vara krypterad.
- Åtkomsten till patientuppgifterna ska ske med stark autentisering*.

I Region Kronoberg har alla medarbetare e-tjänstekort (SITHS-kort) vilket kan möjliggör stark autentisering. Det finns även andra tekniska lösningar.

** Stark autentisering, innebär att identiteten kontrolleras på två olika sätt.*

6 Definitioner

Definitioner hämtade från **Terminologi för** informationssäkerhet (SIS-TR 50:2015)

SVENSK TERM	*ENGELSK TERM*	DEFINITION	DEFINITION
användare	*user*	individ eller system som nyttjar **informationstillgång**ar	Ofta avses en individ som direkt interagerar med ett datoriserat system. Här förutsätts som regel att användaren har **behörighet** att använda **informationstillgångar**na.
informations-system	*information system*	applikationer, tjänster eller andra komponenter som hanterar **information**	
Användaridentitet (även Användar-id, Användarnamn)	*user identity; user ID*	**identitetsbeteckning** för en **användare**	
autentisering	*authentication*	**verifiering** av ett påstående	Exempelvis verifiering av att en **användare** är den man påstår sig vara. Denna typ av verifiering, utförd av verifierande part, används t.ex. vid inloggning eller vid kommunikation mellan två system eller användare.
behörighet	*permission*	tilldelade rättigheter att an-vända en **informationstill-gång** på ett specificerat sätt	Rättigheter kan innefatta t.ex. rät-tigheten för en viss **användare** att ta del av innehållet i en databas eller att skriva ut på en viss skrivare.
e-legitimation; e-id	*e-Identification; eID*	identitetshandling i elektronisk form, som vid elektronisk kom-munikation används för legiti-mering, underskrift eller båda-dera	Termen är tekniskt en beteckning för ett **användarcertifikat** tillsam-mans med en samhörande **privat nyckel**.
engångslösenord	*one-time pass-word; OTP*	**lösenord** som bara kan användas en gång	**ring** används, är det bättre att använda engångslösenord vid oskyddad överföring än vanliga, statiska lösenord vilka lättare kan komma i orätta händer. En lista med slumpmässigt genererade engångslösenord distribueras på förhand till **användare**n. En **man-i-mitten-attack** är ett klassiskt **hot** mot engångslösenord.
lösenord	*password*	teckensträng som anges vid **behörighetskontroll** för att möjliggöra **identifiering** av **användare**	Används ofta i samband med in-loggning. Lösenordet kan vara ge-nererat av systemet, **användare**n eller (till skilda delar) av bägge och bör inte bestå enbart av bokstäver. Användning av lösenord kan inne-bära viss **risk**, t.ex. att en obehörig lyckas gissa eller avlyssna lösenor-det Jfr **lösenordsgissning**. Lösenord har därför normalt en viss, för systemet fastställd minimilängd och en begränsad giltighetstid. Jfr **autentisering**.

PIN-kod; PIN	*personal identifica-tion number; PIN*	**lösenord** bestående enbart av siffror	