VÄSTRA GÖTALANDSREGIONEN

Version:	Status:	Sida:
1.1	Fastställd	1(5)

Utfärdat av:	Utfärdandedatum:	Diarienummer:
Henrik Tuneberg	20141023	

Anvisning

Gemensamma konton GIT

Beslutad:

Datum:

Underskrift säkerhetsdirektör VGR

Beslutad:

Datum:

Underskrift objektägare IT arbetsplats

Innehållsförteckning

0.1 Versionshistorik

Datum	Version	Utfärdare	Förändringsorsak
20131205	0.80	Henrik Tuneberg	Utkast
20131213	0.96	Henrik Tuneberg	Ändringar efter genomgång med verksamhet, informationssäkerhet och VGR IT
20140114	0.98	Henrik Tuneberg	Ändringar efter genomgång med verksamhet, informationssäkerhet och VGR IT
20140413	0.99	Henrik Tuneberg	Ändring efter synpunkter från SU och stegvis impelmentation
20140904	1.0	Henrik Tunerberg	Tillägg automatisk inloggning
20141022	1.1	Henrik Tuneberg	Ändring punkter 1.2.8 och 1.5

0.2 Referenser

Här anges alla de dokument som det hänvisas till i underlaget

Datum	Version	Förkortning	Utfärdare	Dokumentnamn

1 Inledning

Detta är en anvisning kring hantering av gemensamma inloggningskonton i VGR. Dokumentet är upprättat utifrån riktlinjer kring informationssäkerhet.

Det beskriver enhetliga krav på gemensamma konton – benämns vidare i dokumentet GK för gemensamma Konton och UK för Utbildningskonton.

1.1 Bakgrund

Inom vården och i andra verksamheter i VGR saknar personal ofta ”egna” datorer. Man delar istället dator med varandra. Oftast använder personal datorer beroende på var man befinner sig för tillfället, på expeditionen eller inne hos en patient. Att då behöva logga in och ut på datorn med personligt konto varje gång skulle ta alltför lång tid.

De datorer som har ett grupplogin är som regel ”navet” på en verksamhet och tillgänglighetskraven är mycket höga. Att ha snabb åtkomst till en startad och inloggad dator är jätteviktigt. Täta lösenordbyten på PC som delas av många, ibland ett 40-tal personer, skapar ett stort problem ute i verksamheten.

GK/UK är endast avsett för inloggning på datorn. För inloggning i verksamhetens IT-stöd (t ex Melior, Elvis, Heroma) krävs alltid att varje personal använder sina personliga konton.

IT-säkerhet bygger på att möta hot med olika medel. GK/UK är en säkerhetsrisk bl.a. med tanke på svårigheten att följa upp och koppla eventuella säkerhetsincidenter till person. Datorerna står ofta inloggade i ett oövervakat utrymme vilket kan ge patienter eller anhöriga obehörig tillgång till dessa. Därför krävs att GK/UK behörighet begränsas till de absolut nödvändigaste funktionerna på datorn.

1.2 Regler för GK och UK-konto

1. GK/UK består av namn och tillhörande lösenord och ska begränsas till personal och gemensamma datorer tillhörande en och samma klinik/avdelning. GK/UK är endast avsett för inloggning på datorn och skall bara ge åtkomst till det absolut nödvändigaste.

2. Endast behörig person kan beställa konton. Behörig person är linjechef, verksamhetschef eller person som fått delegation av denne chef.

3. För varje GK/UK ska finnas utsedd ansvarig kontaktperson som beskrivs ihop med beställningen. Denne ansvarar för att korrekt hantering av gemensamma kontot sker. Här ingår bl.a. att tala om vilka PC som skall ha specifikt GK/UK. Att tillse att lösenord till GK/UK byts årligen och att berörd personal får nödvändig information om hur kontot fungerar inklusive lösenordsbyte. Kontaktperson kan endast byta lösenord på de GK/UK som man står som registrerad ansvarig för.

4. Lösenordet till ett GK/UK ska endast vara känt av personal på en klinik/avdelning/enhet och av utsedd kontaktperson. Lösenordet får endast användas av personal på kliniken/avdelningen.

5. Lösenordet till GK/UK ska vara ett starkt lösenord och följa samma regler som för personliga lösenord i VGR.

6. Lösenordet till ett GK/UK ska inte göras tillgängligt för andra utanför kliniken/avdelningen. Vid misstanke att så skett ska lösenordet omedelbart ändras.

7. Lösenordsbyte övervakas och GK/UK som inte ändrat lösenord under ett år kommer att inaktiveras, varvid personal istället får använda personliga konton på de gemensamma datorerna. Endast ansvarig person/er som beskrivs under punkten 1.2.2 och 1.2.3 kan aktivera kontot igen.

8. GK/UK ger i grunden ingen behörighet till verksamhetens/klinikens gemensamma mappar/share, om sådana finns. Läs och/eller skrivbehörighet till dessa är en option som beställs på samma sätt som konton (se punkt 1.2.2). Bedömning av behov och säkerhet görs av informationsägare/verksamhetschef och lokalt informationssäkerhetsansvarig.

9. Åtkomst till internet kräver inloggning med användarens personliga inloggning till operativsystemet (detta för att åtkomst till resurser på internet ska kunna vara spårbart och kunna följas upp vid misstanke om missbruk). Kommer att hanteras i steg 2 enligt handlingsplan.

10. Det skall finnas en lista med betrodda websidor (vitlista) som verksamheten behöver komma åt och som man inget behöver logga in till internet för att nå. Lokalt säkerhetsansvariga ihop med informationssäkerhet ansvarar för att listan är riktig utifrån behov och säkerhet.

11. Ett GK/UK konto skall låsas till specifik dator/datorer (host). Datornamn rapporteras in i av ansvarig kontaktperson i samband med beställning.

12. VGR IT har rätt att ändra datornnamn (hostnamn) i en GK, UK grupp vid datorutbyte. Detta har även IT ansvarig vid PC utbyte samt ansvarig kontaktperson som beskrivs under punkten 1.2.2 och 1.2.3

1.3 Särskilda regler för GK-konto med automatisk inloggning

När ett GK konfigureras för automatisk inloggning via GPO och lösenordet inte är känt av någon person behöver inte skrivning om lösenordsbyte tillämpas. För dessa konton tillämpas en längre lösenordskonstruktion och de låses vid fem avvikande inloggningsförsök.

1.4 Ansvar och efterlevnad

Ansvaret att följa ovanstående regelverk och se till att personal som använder GK känner till denna anvisning ligger på respektive förvaltning hos verksamhetschef/linjechef och där utsedda kontaktpersoner.

Ansvarig kontaktperson kan vara samma som beställare (punkt 1.2.2) eller t.ex. LITA, IT samordnare, områdeskontakt och/eller av verksamhetschef/linjechef utsedd person.

1.5 Avsteg ifrån beslutad rutin och förändring av funktion

Om det finns specifika behov av ny GK-funktionalitet kopplat till system eller behörigheter hanteras detta enligt följande.

1. Informationsägare, verksamhetschef, chef beskriver behovet ihop med SIS. Behovet bedöms sedan ihop med lokal/regional informations-säkerhetsansvarig beroende på omfattning.

2. Om OK ur säkerhetssynpunkt skickar SIS funktion via Clarity Demand till berört systemobjekt. Märks ”Ny funktionalitet GK…”

3. Berört objektet ihop med VGR IT bedömer omfattning, möjligheter, tidplan och ev. kostnader och återkopplar till SIS. Vid samsyn läggs samlad beställning till VGR IT på hela förändringen.