VÄSTRA GÖTALANDSREGIONEN

Koncernkontoret
Enhet säkerhet

| Dokumenttyp | Övergripande dokument | Version |
|---|---|---|
| VGR-riktlinje | Riktlinjer för informationssäkerhet | 1.0 |
| Dokumentansvarig | Kontaktperson | Dnr |
| Valter Lindström | Monika Göransson | RS 129-2015 |
| Beslutad av | Giltig från | Ersätter |
| Valter Lindström, koncernsäkerhetschef | 2015-12-18 | Regional anvisning för styrning av åtkomst och behörighet, RSK 265-2003 |

# VGR-RIKTLINJE FÖR ÅTKOMST TILL INFORMATION

**Mål**

Användare ska ha tillgång till rätt information på rätt sätt för sin arbetsuppgift och vara medveten om sitt personliga ansvar.

Lämpliga krav på spårbarhet ska finnas omsatta i all informationshantering, samtidigt som den personliga integriteten värnas.

*Ur Informationssäkerhetspolicy för Västra Götaland*

***Utgångspunkt***

Åtkomst till information ska ges enligt klart definierade principer, tydliga ansvarsförhållanden och enhetliga metoder. Det ska finnas ansvar, rutiner och tekniska skyddsåtgärder som styr användares åtkomst till information och IS/IT-tjänster. Detta gäller även för externa IS/IT-tjänster och mobil utrustning.

Informationsklassificering styr vilka krav på identifiering och behörigheter som ska ställas. Se *VGR-rutin för klassificering av informationstillgångar*.

Västra Götalandsregionens grundläggande värderingar bygger på god etik och moral, vilket innebär att det inte är tillåtet att besöka sidor som innehåller pornografiskt material, hot, förtal, våld, terror, rasism, hets mot folkgrupp, mobbning, brott mot diskrimineringslagen eller uppmaning till droganvändning.

Samma begränsning gäller för besökare, patienter, studerande och andra användare som ges tillgång till regionens nät

Kraven för åtkomst till information finns beskrivna i *VGR-riktlinje för åtkomst till information* och ska tillämpas för all hantering av åtkomst till information.

*Ur Riktlinjer för informationssäkerhet i Västra Götalandsregionen*

## *1 Behörighet*

Informationsägaren/vårdgivaren ansvarar för att det finns villkor och rutiner för vilka som får behörighet för åtkomst till data och information. Reglerna ska omfatta vad som krävs, av vem och hur beslut fattas samt när uppföljning av behörigheter ska ske.

Det ska säkerställas att behörigheter tilldelas, ändras och tas bort på ett kontrollerat sätt.

Grundprincipen vid bedömning av tilldelning av behörigheter är, att den ska styras av behovet av tillgång till information och informationsbehandlingsresurser, för att arbetet ska kunna utföras på ett adekvat sätt. För att varje användare ska få rätt behörighet måste ansvarig beslutsfattare först ha genomfört behovs- och riskanalyser. Dessa ska ta hänsyn till vilka behov av åtkomst en användare har samt vilka risker det kan innebära om personen har för lite eller för mycket tillgång till olika uppgifter. Detta gäller för behörigheter på alla nivåer inom VGR, det vill säga även så kallade höga behörigheter.

### 1.1 Digital identitet

Personliga och unika elektroniska användaridentiteter ska användas av alla medarbetare i Västra Götalandsregionen och tilldelas genom en tydlig rutin.

### 1.2 Granskning av användarrättigheter

Ansvarig chef/uppdragsgivare ska, med stöd av utdrag från behörighetsadministrationen, årligen granska, och vid behov revidera, sina medarbetares åtkomsträttigheter.

### 1.3 Förändring av anställning

Chef/uppdragsgivare är också ansvarig för att avsluta behörigheter och att utrustning återlämnas. Den nya chefen/uppdragsgivaren ansvarar för att beställa nya behörigheter och utrustning.

### 1.4 Avslut av användarkonto

Alla anställdas, uppdragstagares och tredjepartsanvändares rättigheter till informationen, IS/IT-system och lokaler ska dras in när anställningen/avtalet/överenskommelsen upphör eller förändras. Informationen i e-postlåda, hemkatalog eller liknande ska gallras för avslut av anställning. Ansvarig chef avgör till vem behövlig information ska överlämnas. Eventuell kvarvarande information ska vara åtkomlig för ansvarig chef under det aktuella kalenderåret plus tolv månader. Därefter fattar ansvarig chef beslut om gallring och arkivering.

### 1.5 Behörighet för admin- och root-konton

Särskilda rättigheter, som exempelvis administratörsrättigheter, ska endast delas ut där så är uttryckligen nödvändigt och då ska rättigheterna vara tidsbegränsade och personliga. För varje resurs ska det vara beslutat vem som granskar dessa behörigheter och detta ska vara en del av systemdokumentationen. Särskilda rättigheter ska följas upp minst två gånger per år.

### 1.6 Inloggningsmetod

I första hand ska inloggning ske med tvåfaktors autentisering, t ex TjänsteID+. Där så inte är möjligt, ska lösenord konstrueras så att en tillräcklig god kvalitet, efter systemets möjligheter och säkerhetsbehov, uppnås.

På grund av risken för avlyssning är det inte tillåtet att välja samma användaridentitet eller lösenord som används inom VGR:s IT-system vid användning av internetbaserade informationstjänster.

## 2 Information om säkerhetssystem

Information och data som rör säkerhets- eller bevakningsåtgärder med avseende regionens fysiska infrastruktur, ska hanteras så att obehöriga inte kan ta del av den.

## 3 Åtkomst till information och IS/IT-tjänster

### 3.1 Privat användning

Västra Götalandsregionens informationsbehandlingsresurs är avsedda för arbetsrelaterade uppgifter. Användningen av utrustningen ska präglas av användarens goda omdöme, så att den inte innebär säkerhetsrisker för regionens IS/IT-miljö, stör regionens verksamhet eller påverkar VGR:s rykte negativt. Respektive chef avgör i vilken utsträckning utrustningen får användas för privat ändamål.

### 3.2 Internet

Arbetsrelaterat undantag från regeln att vissa sidor är förbjudna att besöka kan beviljas. Ansvarig chef anmäler till VGR IT:s Service Center.

Om patienter ges möjlighet att använda regionens tekniska utrustning för internetuppkoppling, ska begränsningar göras för att skydda produktionsmiljö och utrustning.

Representerar en person Västra Götalandsregionen på sociala nätverk eller liknande, har hen ett ansvar att regionens regelverk, etik och god sed följs. Mer information finns hos regionkansliets kommunikationsavdelning. Användaren ska också vara medveten om att besök på webbplatser lämnar elektroniska spår efter sig och med dessa kan andra registrera vilka webbplatser regionens medarbetare besökt.

### 3.3 Åtkomst till regionens informationstillgångar över internet

Åtkomst till regionens interna informationstillgångar över internet eller andra externa nät, får endast ske genom säker uppkoppling, vilket innebär behörighetskontroll och skyddad överföring, t ex VPN. Styrning av åtkomsten bör kunna ske, så att den begränsas till nödvändiga IS/IT-system.

IS/IT-direktören ansvarar för att IS/IT-tjänsten ”säker uppkoppling” uppfyller informationsägarens krav i informationsklassificering och är en del av tjänsteportföljen.
Informationsägare tar beslut om det ska vara tillåtet att använda IS/IT-systemet på distans (utanför VGRnet). Säkerhetskraven i gällande regelverk om informationssäkerhet ska vara uppfyllda. Ansvarig chef beslutar om distansåtkomst för den enskilde medarbetaren. En behovs-/riskanalys ska ligga till grund för beslutet.

### 3.4 Skicka känslig information

När användare försöker skicka känslig information okrypterat över öppna nät (Internet, Sjunet mm) bör det finnas en funktion som varnar användaren,

## 4 Säkerhetskrav avseende patientinformation

Vid hantering av patientinformation inom Västra Götalandsregionen ska Patientdatalagen och Socialstyrelsens föreskrift *Informationshantering och journalföring i hälso- och sjukvården* följas. Tillämpning av dessa beskrivs i *Regionövergripande villkor för behörighet, spärr och logg*, RSK 771-2008.

### 4.1 Överföring av och åtkomst till patientuppgifter

Västra Götalandsregionens tekniska nätverk är att betrakta som ett öppet nätverk. Detta innebär att patientuppgifter inte får kommuniceras utan godtagbart skydd. Olika tekniska skyddsåtgärder ska användas, som exempelvis kryptering, digital signatur och stark autentisering.

### 4.2 Kommunikation med medborgare/patient om person- och patientinformation

Om information kommuniceras elektroniskt mellan medborgare/patient och vårdgivare ska:

- Samtycke att förmedla patient- och personuppgifter elektroniskt inhämtas från patient/medborgare
- Patienten/medborgaren entydigt identifieras
- Teknik för skydd (kryptering) av kommunikation användas

### 4.3 Patientåtkomst till egen journal

Patienter får ges direktåtkomst till sin journal, om säkerhetskrav enligt Socialstyrelsens föreskrifter tillämpas. Detta kräver stark autentisering, vilket innebär att vårdgivaren använder inloggningslösningar som ställer krav på att identiteten säkerställs genom en tvåfaktorslösning samt att kommunikationen krypteras.

### 4.4 Rättelse, blockering och utplånande av personuppgifter

IS/IT-system i Västra Götalandsregionen ska, enligt bestämmelser i personuppgiftslagen och Patientdatalagen, vara utformade så att rättelse, blockering och utplånande av personuppgifter är möjlig.

## 5 Spårbarhet

Spårbarhet är väsentlig för att genomföra åtkomstkontroll. Det ska entydigt gå att härleda aktiviteter i ett IS/IT-system till en identifierad användare eller process.

### 5.1 Åtkomstkontroll

Loggning är kontinuerligt insamlande av information om de aktiviteter som utförs i ett IS/IT-system. Utöver lagreglerade krav ska informationsägarens krav på spårbarhet ligga till grund för vad och hur mycket som ska loggas.

Aktiviteter som genomförs av admin i centrala tjänster och funktioner i IS/IT-miljöer ska vara spårbara i förhållande till informationens skyddsbehov.

### 5.2 Granskning av loggar

Vårdgivare ansvarar för att det inom hälso- och sjukvårdens ledningssystem finns rutiner som säkerställer hantering av loggar.

I andra verksamheter ansvarar informationsägaren för en löpande granskning av loggar.

### 5.3 Gallringstid och hantering av loggar

Gallringstid av loggar styrs av berörd lagstiftning och verksamhetens behov av att kunna spåra aktiviteter i IS/IT-system.

## 6 Hantering av skyddade personuppgifter

Vid utveckling av IS/IT-system ska särskild hänsyn tas till att ett adekvat skydd för personer med skyddade personuppgifter säkerställs och omfattar såväl anställda som patienter, elever osv. Se Riktlinjer för hantering av personer med skyddade personuppgifter, RSK 265-2003.

## 7 Arkivering

Arkiverad data eller information ska lagras i ett sådant format, att de är möjliga att läsa under hela bevarandetiden. Krav på tidsbestämt långtidsbevarande av information finns i exempelvis Patientdatalagen, Bokföringslagen och Arkivlagen. Dessa krav kan komma att ändras över tiden. Informationsägaren ska alltid samråda med Regionarkivet och tillämpa gällande arkivreglemente och övriga föreskrifter från Arkivnämnden.