# Rutin – Loggkontroll i Viva

## 1. Referenser

| Nr | Dokument | Lagringsplats |
|---|---|---|
| **1.** | Rutin för sekretessbrott | Ägs av Personalavdelningen. Under utveckling. |
| **2.** | Blankett för uppföljning av loggkontroll i Viva | V:\SOC\VERKSAMHETER\ADM\ Kvalitetssystem\3 Utveckling\Pågående projekt\Verksamhetssystembyte\VIVA införande\Loggkontroll\Checklista-loggkontroll-viva.docx |

## 2. Begrepp och förkortningar

| Nr | Begrepp/körkortning | Betydelse |
|---|---|---|
| **1.** | Viva | Journalhanteringssystem använt inom Socialförvaltningen Piteå |
| **2.** | ILAB | Det företag som äger, utvecklar och tillhandahåller systemet Viva. |
| **3.** | Användare | Syftar på personer som jobbar i Viva-systemet. Inkluderar handläggare, omvårdnadspersonal, administratörer o dyl. |
| **4.** | Ärende | Post i Viva-systemet på vilken behörigheter sätts och accesser loggförs. Är föremål för loggkontrollen. Beroende på syfte och om ärendet läggs upp av Myndighet eller Verkställighet kan det i verksamheten kallas ärende, åtagande eller uppdrag. |
| **5.** | VO | Verksamhetsområde |
| **6.** | HSL | Hälso- och sjukvårdslagen |
| *7.* | MAS | Medicinskt ansvarig sjuksköterska |

# 3. Varför gör vi loggkontroll

Loggkontrollen utförs för att värna den enskildes integritet. Kontroller sker för att undersöka ifall det förekommit sekretessbrott, det vill säga om någon läser i ärenden i Viva vilken den inte är behörig att läsa.

# 4. Vad är tillåtet

Följande regler beskriver under vilka förutsättningar man har rätt att ta del av informationen i en brukares akt.

***Regler för sekretess i verksamhetssystemet – handläggare (Myndighet)***

- Du endast har rätt till ärenden som man själv är handläggare eller medhandläggare i.
- Du har rätt till ärenden där ordinarie handläggare är frånvarande, kortare eller längre tid, och du är utsedd att handlägga ärendet åt honom/henne.
- Du har vid förfrågningar/anmälningar rätt att gå in i *klientbilden* i Viva och se om klienten/klienterna har ett ärende och vem som är handläggare.

***Regler för sekretess i verksamhetssystemet – Omsorgspersonal, behandlande personal och HSL-personal (Verkställighet)***

- Du har rätt till ärenden och annan dokumentation i de klientärenden där du har en direkt och aktuell vård- eller omsorgsrelation eller en behandlande relation.

# 5. Vilka kontroller kan göras?

Kontroller kan initieras och utföras av flera olika orsaker och sätt.

***Typer av kontroller***

| | |
|---|---|
| Planerad kontroll | Kontrollen utförs regelbundet utifrån ett urval användare där det undersöks vilka brukares ärenden dessa användare har öppnat i Viva. |
| Kontroll av särskild användare | Vid misstanke om att en särskild användare gjort obehöriga läsningar av ärenden i Viva. Sker på initiativ från berörd arbetsledare. |
| Kontroll av särskild brukare | Vid misstanke om att uppgifter om en särskild brukare har varit föremål för obehörig läsning från användare. Sker på initiativ från berörd arbetsledare. |
| Kontroll när brukare begär det | Brukaren själv kan begära att en loggkontroll för att få veta vilka användare som har tagit del av dess ärenden. |

# 6. Planerad kontroll

Som nämnts är det användarna som står i fokus för den planerade loggkontrollen för att undersöka ifall de haft behörighet att öppna de ärenden de har öppnat i Viva. Användarna delas in i grupper efter riskbedömning och loggkontrollen är uppdelad efter dessa grupper på flera tillfällen spridda över året.

## Hur ofta sker kontrollen?

Grupperingen av användare är konstruerade så att varje användare är medlem i en användargrupp som utsätts för granskning under 2 kontrollperioder per år. Varje kontrollperiod är 2 veckor lång, dvs kontrolldata (loggar) plockas från denna period.
Spridningen över året för kontroll av grupperna beskrivs i tabellen **Storlek och Schemaläggning av loggkontroller**.

## Hur sker urvalet, riskbedömning?

### Riskfaktor

I Viva, där det inte finns några avgränsningar i systemet med avseende på lagrum, är den enskilt största riskfaktorn antalet brukare/brukaregrupper en användare har tilldelats behörighet till. Ju fler tilldelade behörigheter, desto högre risk för felaktiga accesser till ärenden.

### Riskprofiler

Vid riskprofileringen grupperas användarna efter sina arbetsuppgifter/roller in i två huvudgrupper, *Myndighet* och *Verkställighet*. Ur riskperspektiv är en skillnad mellan dessa två grupper antalet tilldelade behörigheter i Viva.
Användare som jobbar inom Myndighet har generellt ett stort antal behörigheter då de alla jobbar med många brukare.
Användare inom Verkställighet jobbar med ett avgränsat antal brukare och har enbart behörighet tilldelat till dessa brukare. Därmed har dessa ett mer begränsat antal behörigheter tilldelade.
Användare som chefer, administration och IT-personal sorterar in i gruppen för Myndighet. De har liknande vidspännande behörigheter som normala användare inom Myndighet och får därmed en likande riskprofil.

### Urval

*Myndighet*
Gruppen Myndighet är en ur riskbedömningsperspektiv en homogen grupp där de flesta användare har många behörigheter tilldelade. Därmed betraktas de som en gemensam användargrupp med hög procentsats för hur många användare som skall plockas ut för loggkontrollerna.

*Verkställighet*
Till skillnad från användare i gruppen Myndighet har användarna inom Verkställighet sinsemellan ett varierande antal tilldelade behörigheter. De delas in i tre undergrupper, *låg-, medel- & högrisk*, utefter hur många behörigheter en användare har tilldelats. Ju fler behörigheter, desto högre riskgrupp.
Undergrupperna har sedan olika procentsatser för hur många användare ur respektive undergrupp som ska tas ut för loggkontroll.
I gruppen högrisk hamnar merparten av sjuksköterskorna och i grupperna låg- och medelrisk hamnar merparten av vikarierna. För att få en kontroll av vikarierna är kontrollperioderna 2 och 3 schemalagda under sommarperioden (se tabellen Storlek och Schemaläggning av loggkontroller).

Grupperna med urvalsstorlekar beskrivs i tabellen Storlek och Schemaläggning av loggkontroller.

### Storlek och Schemaläggning av loggkontroller

Under året finns fyra kontrollperioder fördelade enligt:

| Kontrollperiod | Kontrolldata tas från |
|---|---|
| **1** | 2 första hela veckorna i februari |
| **2** | 2 sista hela veckorna i juni |
| **3** | 2 sista hela veckorna i juli |
| **4** | 2 första hela veckorna i november |

Storlek på urvalgrupperna och fördelning på kontrollperioder enligt:

| Gruppering | Andel (%) per kontrolltillfälle | Kontrollperioder |
|---|---|---|
| **Myndighet** | | |
| Samtliga | 15 | 1 & 3 |
| **Verkställighet** | | |
| Högrisk<br>>15 behörigheter | 10 | 1 & 3 |
| Medelrisk<br>6-15 behörigheter | 6 | 1 & 3 |
| Lågrisk<br>1-5 behörigheter | 4 | 2 & 4 |

## Ansvarsfördelning

Följande ansvarsfördelning gäller för den planerade loggkontrollen.

| Roll | Arbetsuppgift/ansvar |
|---|---|
| Systemadministratör för Viva | Initierar att kontrollen startas och att VO-cheferna får sina listor med utvalda användare för vidare kontroll. Kontrollen av de som tagit del av akterna avser en månad tillbaka från kontrolltillfället. |
| VO-cheferna | Ansvarar för att kontrollerna utförs av lämplig chef. Ansvarar för att återrapportera till IT-strateg |
| IT-strateg | Sammanställer resultatet av granskningarna och presenterar detta för politik och förvaltningsledning. |

## Hur sker den planerade kontrollen?

Kontrollen kan beskrivas i följande huvudmoment;

1. Systemansvarige tar fram en lista över vilka användare som varit inloggade under kontrollperioden.
2. Utifrån grupperingarna och procentsatserna för urvalsgrupperna (se **Storlek och Schemaläggning av loggkontroller**) skapas listor med användare utvalda för loggkontroll från listan med aktiva användare.
3. Systemansvarige delar upp de utvalda användarna i listor efter VO och kompletterar listorna med de ärenden varje användare har öppnat i Viva under kontrollperioden. Dessa listor lämnas till respektive VO-chef.
4. VO-chefen ansvarar för att respektive användares chef går igenom att listorna för att kontrollera (se Granskning) att användarna haft tillbörlig behörighet på de ärenden de har öppnat enligt listan. För bedömning se Vad är tillåtet.
5. VO-cheferna rapporterar resultatet av granskningarna till IT-strateg genom att skicka in checklistorna för de olika användarna.

6. IT-strategen sammanställer resultaten och presenterar det först för arbetsutskottet och sedan vidare till socialnämnden.

### Granskning av åtkomster, beskrivning

Granskning av vilka ärenden en användare har öppnat sker av chefen för aktuell användare. Det är chefen som kan bedöma om användaren har haft korrekt behörighet att läsa i de akter användaren öppnat.
Om användaren läst ett ärende utan korrekt behörighet är det chefen som gör en initial utredning om varför användaren obehörigt har läst i aktuellt ärende. I denna utredning kan chefen vid behov få stöd från MAS och/eller Kvalitetscontroller. Om den initiala utredningen visar att det inte finns giltiga skäl att läsa i akten är det att betrakta som sekretessbrott och ska då hanteras enligt rutinen för sekretessbrott (se 9 Vad händer vid sekretessbrott).

***Checklista kontroll av behörighet***

| | |
|---|---|
| 1. Användaren behörig? | Har användaren behörighet till alla akter/journaler denne tagit del av? Om inte, gå till steg 2. |
| 2. Om nej, finns godtagbar förklaring? | Prata med användaren som varit inne i akten och fråga varför detta skett. En godtagbar förklaring är exempelvis att man tagit fel på person när man sökt i Viva. Om ingen godtagbar förklaring finns, gå till steg 3. |
| 3. Om nej, är det dataintrång? | Finns ingen godtagbar förklaring måste frågan ställa om det har varit frågan om dataintrång. Exempel på dataintrång är nar man tagit del av akten för att få information om en granne, släkting el dyl. för sin egen privata räkning. |

## 7. Kontroll av särskild anställd/brukare

Detta initieras av aktuell arbetsledare. Kontrollen innehåller följande moment:
1. Kontakt tas med systemansvarig för Viva för att få fram underlag för loggkontroll.
2. Arbetsledaren informerar närmsta överordnad samt MAS eller Kvalitetscontroller (beroende på lagrum) att en särskild kontroll ska ske.
3. Arbetsledaren genomför loggkontrollen.
4. Arbetsledare rapporterar resultatet till närmsta överordnad, MAS eller Kvalitetscontroller (beroende på lagrum) samt IT-strateg.
5. IT- strategen sammanställer resultatet och presenterar det för individutskottet och vid behov sedan (avidentifierat) vidare till socialnämnden.
6. Vid sekretessbrott vidtar arbetsledaren åtgärder enligt rutinen för sekretessbrott (se Referenser 1).

## 8. Brukaren själv begär en loggkontroll

För att vara säker på att personen är den som den utger sig för att vara är det alltid bäst att denna begäran sker i ett personligt möte. Går inte det så är det den som lämnar ut logguppgifterna som ska försäkra sig om att materialet lämnas till rätt person. Kontrollen hanteras av arbetsledaren enligt följande moment:
1. Kontakt tas med systemansvarig för Viva för att få fram en logg som visar de personer som tagit del av ärendet/ärendena.
2. Arbetsledaren boka möte med brukaren där arbetsledaren tillsammans med brukaren går genom loggrapporten för att hjälpa brukaren att utläsa den då det

ibland kan vara svårt för en utomstående att själv tolka informationen i loggrapporten.
3. Om ett möte ej är möjligt lämnar arbetsledaren över loggrapporten till brukaren och försöker samtidigt förklara hur man läser den.
4. Vid sekretessbrott vidtar arbetsledaren åtgärder enligt rutinen för sekretessbrott (se Referenser 1).

# 9. Vad händer vid sekretessbrott

Misstänkta sekretessbrott tecknas ner på blankett (se Referenser 2) för vidare uppföljning och utredning enligt rutinen för sekretessbrott (se Referenser 1).
Om det vid den uppföljande granskningen framkommer att en anställd obehörigt har läst ett ärende i Viva utan godtagbar orsak kan det finnas grund för att vidta arbetsrättsliga åtgärder som korrigerande samtal, varning eller uppsägning. Även polisanmälan kan bli aktuell. För vidare hantering i dessa fall kontaktas personalavdelningen för att få hjälp med att bedöma eventuella rättsliga åtgärder.

# 10. Redovisning

Resultatet från varje separat loggkontrollstillfälle rapporteras till socialchefen som är systemägare. En årlig sammanställning görs under januari månad påföljande år för att redovisas hela årets loggkontroller till socialförvaltningens ledning och till socialnämnden.
Eventuella sekretessbrott tecknas ner på blankett för uppföljning (se Referenser 2) och redovisas direkt till socialchef och vidare enligt rutinen för sekretessbrott (se Referenser 1).