Rutin

Gäller för: Västra Götalandsregionen
Innehållsansvar: Irja Burhöi, (irjbu1), Regionutvecklare
Granskad av: Anders Andersson, (andan18), Enhetschef
Godkänd av: Mariana Vikström, (marvi36), Direktör

Giltig från: 2026-09-21
Giltig till: 2030-12-31

Personrelaterade säkerhetsåtgärder för informations-säkerhet

Regional rutin 2026-2030

Ledningssystem för informationssäkerhet och dataskydd

VÄSTRA GÖTALANDSREGIONEN

Innehållsförteckning

.

1.Inledning

HR har en central roll i att säkerställa att Västra Götalandsregionen (VGR) har medarbetare och annan personal är medvetna, har vilja och förutsättningar för att agera informationssäkert.

HR-processerna för anställning och avslut av tjänst samt hantering vid bristande följsamhet till ledningssystemet är viktiga förutsättningar för en god informationssäkerhet inom VGR. HR-direktören ansvarar för att det finns rutiner samt att rutinerna efterlevs i VGR.

Syftet med rutinen är att tydliggöra vilka delar HR ansvarar för att ta fram styrning för personrelaterade säkerhetsåtgärder som har en påverkan på VGR:s informationssäkerhet.

2.Kontroll inför anställning

Kontroller inför anställning, exempelvis av meritförteckning, legitimering och referenstagning, ska utföras för den kandidat som avses erbjudas anställning eller uppdrag innan de blir en del av organisationen. Förnyad kontroll ska även göras vid förändrad tjänst eller uppdrag inom VGR.

Kontroll inför anställning ska utföras på alla medarbetare, inklusive heltids- och deltidsanställda samt visstidsanställda. Omfattning och nivå på kontrollen ska stå i proportion till den tilltänkta rollens ansvar, åtkomst till information och identifierade risker. Om dessa personer kontrakteras via tjänsteleverantörer, ska kraven på kontroll stå med i avtal mellan VGR och leverantör.

HR-direktör ansvarar för att det finns rutin för kontroll inför anställning vid all rekrytering för VGR:s räkning, som ska säkerställa följsamhet till relevant lagstiftning och tillämpliga delar av avsnitt 6.1 Bakgrundskontroll i ISO/IEC 27002:2022.

Chef ansvarar för att framtagna rutiner har följts vad gäller kontroll i samband med intervju, referenstagning och anställning samt vid behov stämma av checklista för säkerhetsprövning.

3.Anställningsvillkor

Medarbetarens och VGR:s ansvar för informationssäkerheten ska anges i anställningsavtal i syfte att säkerställa att medarbetaren förstår sitt informationssäkerhetsansvar vad gäller de roller som de är aktuella för.

Medarbetarens avtalsenliga skyldigheter ska spegla VGR:s ledningssystem för informationssäkerhet och dataskydd.

HR-direktör ansvarar för att anställningsavtal innehåller information om medarbetarens informationssäkerhetsvillkor i enlighet med avsnitt 6.2 Anställningsvillkor i ISO/IEC 27002:2022.

Chef ansvarar för att säkerställa att medarbetaren har godkänt anställningsavtal med tillhörande anställningsvillkor innan anställning påbörjas.

4.Påminnelse om sekretess

Inom den offentliga sektorn är sekretess för de anställda reglerat i lag. Sekretessförbindelse är därför inte möjlig att använda, utan ersätts av en påminnelse om sekretess. Vid anställning ska medarbetaren skriva under att man mottagit påminnelse om sekretess, där det framgår vilka delar som gäller även efter att anställning eller uppdrag har upphör. Medarbetare kan inte avkrävas någon tystnadsplikt utöver vad som anges i offentlighets- och sekretesslagen (SFS 2009:400) samt yttrandefrihetsgrundlagen (SFS 1991:1469).

Personal som inte har en anställning i VGR, exempelvis studerande, konsulter och andra som använder regionens resurser för informationsbehandling och kommer i kontakt med sekretessbelagd information, ska också informeras om och skriva under påminnelse om sekretess.

HR-direktör ansvarar för att det finns rutin avseende påminnelse om sekretess som ska säkerställa följsamhet till relevant

lagstiftning och tillämpliga delar av avsnitt 6.6 Avtal om konfidentialitet eller sekretess i ISO/IEC 27002:2022.

Chef ansvarar för att säkerställa att medarbetare och annan personal så som studerande och konsulter har skrivit under påminnelse om sekretess innan denne kommer i kontakt med sekretessbelagd information.

5.Disciplinär åtgärd

Det ska finnas en formell och kommunicerad disciplinär process för medarbetare och annan personal som nyttjar regionens informationsbehandlingsresurser som inte följer VGR:s ledningssystem för informationssäkerhet och dataskydd.

HR-direktör ansvarar för att det finns rutin avseende disciplinär process som ska säkerställa följsamhet till relevant lagstiftning och tillämpliga delar av avsnitt 6.4 Disciplinär process i ISO/IEC 27002:2022.

Chef ansvarar för att initiera disciplinär process vid misstänkt eller konstaterad överträdelse enligt fastställd rutin.

6.Vid avslut eller ändring av tjänst

Ansvar och skyldigheter för informationssäkerhet som fortsätter att gälla efter att en anställning upphör eller ändras ska definieras, tillämpas och kommuniceras till medarbetare och annan personal.

Processen för att hantera upphörande eller byte av anställning ska ange vilket ansvar och vilka skyldigheter avseende informationssäkerheten som fortsätter att gälla efter att anställningen hos VGR upphört eller ändrats. Detta kan exempelvis omfatta sekretess för information, immateriell äganderätt och annan kunskap som inhämtats.

HR-direktör ansvarar för att det finns rutin avseende ansvar efter upphörande eller ändring av anställning som ska säkerställa följsamhet till relevant lagstiftning och tillämpliga delar av avsnitt

6.5 Ansvar efter upphörande eller ändring av anställning i ISO/IEC 27002:2022.

Chef ansvarar för att säkerställa att medarbetare och annan personal så som studerande och konsulter har blivit informerad om ansvar och skyldigheter för informationssäkerhet vid avslut eller ändring av tjänst.

7. Relaterade dokument

- Termbank för informationssäkerhet - nationell terminologi för informations- och cybersäkerhetsområdet Termbanken för Informationssäkerhet
- Informationssäkerhet och dataskydd - Regional riktlinje 2023 – 2027 (dnr RS 2023-02811)
- Regiondirektörens fördelning av ansvar inom Koncernkontoret (diarienummer: RS 2023-05437)
- ISO/IEC 27002:2022 Informationssäkerhet, cybersäkerhet och integritetsskydd – Kontroller av informationssäkerhet

Information om handlingen

Handlingstyp: Rutin

Gäller för: Västra Götalandsregionen

Innehållsansvar: Irja Burhöi, (irjbu1), Regionutvecklare

Granskad av: Anders Andersson, (andan18), Enhetschef

Godkänd av: Mariana Vikström, (marvi36), Direktör

Dokument-ID: RS10162-1596316381-388

Version: 2.0

Giltig från: 2026-09-21

Giltig till: 2030-12-31