Gäller för: Västra Götalandsregionen
Innehållsansvar: Fredrik Almyren, (freal8), Regionutvecklare
Godkänd av: Johan Flarup, (johfl), Direktör

Giltig från: 2024-09-10
Giltig till: 2028-12-31

Säker utveckling

Informationssäkerhet & dataskydd vid verksamhetsutveckling

Regional rutin 2024 – 2028

Ledningssystem för informationssäkerhet och dataskydd

Innehållsförteckning

1 Sammanfattning

Informationssäkerhet och dataskydd ska genomsyra all verksamhetsutveckling inom Västra Götalandsregionen[1] oavsett om det handlar om att ta fram effektivare verksamhetsprocesser, systemstöd, bättre sängar, ändamålsenliga fastigheter, ny kollektivtrafik eller annan typ av utveckling.

Syftet med Regional rutin för informationssäkerhet och dataskydd vid verksamhetsutveckling är att tydliggöra vem som ansvarar för de olika delarna av informationssäkerhets- och dataskyddsarbetet under arbetet.

Huvudsaklig målgrupp för rutinen är informationsägare, projektägare och projektledare för alla typer av verksamhetsutveckling i alla förvaltningar och bolag som ingår i Västra Götalandsregionen.

Informationsägare eller dess företrädare, projektägare och projektledare ska fastställa vilka säkerhetsåtgärder inom informationssäkerhet och dataskydd som är relevanta för verksamhetsutvecklingen och säkerställa att dessa tas om hand i utvecklingsarbetet. Detta gäller även när hela eller delar av utvecklingen beställs från en extern part.

Regional rutin för informationssäkerhet och dataskydd i verksamhetsutveckling är styrande för alla förvaltningar och bolag som ingår i Västra Götalandsregionen och är en del i ledningssystemet för informationssäkerhet och dataskydd.

Ramarna för rutinen sätts av riktlinjen *Informationssäkerhet och dataskydd – Regional riktlinje 2023-2027* (RS 2023-02811) och innehållet utgår från SS-ISO/IEC 27002.

Rutinen ersätter den tidigare *VGR-riktlinje för styrning av utveckling och införande av IS/IT*.

Kompletterande säkerhetsåtgärder vid verksamhetsutveckling hittas även i *Regional rutin för inbyggt dataskydd och dataskydd som standard*.[2]

För verksamhetsutveckling som innefattar IS/IT-tjänster är Koncernstab digitalisering ansvariga för att ta fram, godkänna och tillämpa anvisningar specifika för utveckling av IS/IT-tjänster enligt beskrivningar i kapitel 5. Syftet med dessa rutiner är att ha kontroll över och skydda alla IS/IT-tjänster.

[1] Förkortas VGR
[2] Andra rutiner som är relevanta för informationssäkerhetsarbetet inom VGR kan hittas bland styrande dokument på VGR:s intranät.

2 Termer och begrepp

Huvuddelen av termer och begrepp är hämtade från MSB termbank för informationssäkerhet, Svensk kravterminologi, ISO/IEC 27000:2018, *Informationssäkerhet och dataskydd – Regional riktlinje 2023-2027* (RS 2023-02811) samt VGR:s projektstyrningsmodell Projektilen.

Dataskydd	Omfattar skydd för den personliga integriteten vid behandling av personuppgifter och är också det en del av informationssäkerhetsarbetet.
Informationssäkerhet[3]	Skydd av informationstillgångar avseende konfidentialitet, riktighet och tillgänglighet Informationssäkerhet kan uppnås genom en uppsättning säkerhetsåtgärder för bevarande av egenskaper som konfidentialitet, riktighet och tillgänglighet men även spårbarhet, autenticitet, ansvarsskyldighet, oavvislighet och auktorisation. Informationssäkerhet omfattar områdena organisatorisk säkerhet och teknisk säkerhet Informationssäkerhet innefattar cybersäkerhet och IT-säkerhet.
Informationssäkerhetskrav[4]	Krav som reglerar en eller flera aspekter av informationssäkerhet.

[3] MSB Termbank
[4] Svensk kravterminologi

Informationstillgång[5]	Information och informationsbehandlande resurser som är av värde för en organisation. Informationstillgångar kan vara av fysisk eller logisk karaktär, eller bådadera. *Exempel på informationstillgångar är: information, program, tjänster, datorer, nätverk, människor eller immateriella tillgångar.*
Informationsägare[6]	Alla informationstillgångar ska ha en informationsägare. Informationsägaren ansvarar för att säkerställa implementation och efterlevnad av säkerhetsåtgärder utifrån krav på skydd för informationstillgångarna. Grundprincipen är att informationsägarskapet följer det ordinarie verksamhetsansvaret. Detta gäller från ledning till enskilda medarbetare. Informationsägarskapet sammanfaller med ansvaret i verksamheten, till exempel ansvarar en avdelningschef för information inom avdelningen, eller en processägare för informationen inom processen. När informationstillgångarna ingår i regiongemensamma processer, regiongemensamma IS/IT- tjänster, projekt och/eller upphandlingar företräds flera myndigheters informationsägare av en regional processägare. Fördelning av processansvar följer av VGR:s processmodell (dnr nr RS 2022-05853).
Konfidentialitet[7]	Egenskap hos informationstillgång som innebär att den inte tillgängliggörs eller avslöjas för obehöriga individer, objekt eller processer

[5] MSB Termbank
[6] Informationssäkerhet och dataskydd – Regional riktlinje 2023-2027 (RS 2023-02811)
[7] MSB Termbank

LISD[8]	Ledningssystemet för informationssäkerhet och dataskydd på VGR är en del av verksamhetens ledningssystem. LISD inkluderar mål, styrdokument, organisation och processer för informationssäkerhet, dataskydd, cybersäkerhet och IT-säkerhet. Riktlinjen tar sin utgångspunkt i SS-ISO/IEC 27000-serien för informationssäkerhet och personlig integritet som en utgångspunkt för att bedriva ett systematisk och riskbaserat informationssäkerhetsarbete
Lösning	Avser nya, ändrade eller påverkade huvudprocesser eller stödprocesser samt tillhörande IS/IT-tjänster. En lösning kan också avse fysiska objekt som VGR utvecklar eller upphandlar, exempelvis sjukhussängar, fastigheter eller tåg.
Process[9]	Grupp av aktiviteter som samverkar eller påverkar varandra, och som omformar insatser till utfall.
Projekt[10]	Projekt är en arbetsform och ett verktyg för att genomföra uppgifter. Projekt kan nyttjas för att skapa fokus och kraft för en förbättring, utveckling eller förändring under en begränsad tid. Arbetsformen är flexibel och passar både mindre och större tillfälliga uppgifter som behöver vara färdiga inom en given tidsram.
Projektledare[11]	Projektledaren leder och koordinerar aktiviteter i ett projekt. *I denna rutin används begreppet projektledare för den person som är utsedd av projektägaren att leda en verksamhetsutveckling så att den infriar mål och håller tid och budget.*

[8] Informationssäkerhet och dataskydd – Regional riktlinje 2023-2027 (RS 2023-02811)
[9] ISO/IEC 27000
[10] VGR:s projektstyrningsmodell Projektilen
[11] VGR:s projektstyrningsmodell Projektilen

Projektägare[12]	Projektägare är den som äger projektet, har det övergripande ansvaret för projektet och har högsta beslutande mandat. Projektägarskapet kan inte delegeras vidare. *I denna rutin används begreppet projektägare för den person som av koncernstabschef, förvaltningschef eller VD fått uppdrag att styra en verksamhetsutveckling så att den når sitt mål inom tilldelat ramar*.
Riktighet[13]	Egenskap hos informationstillgång som innebär att den skyddas mot oönskad förändring.
Säkerhetsåtgärder[14]	Identifierad uppsättning åtgärder för att möta en organisations risker. Säkerhetsåtgärder för informationssäkerhet omfattar åtgärder inom det organisatoriska, personrelaterade, tekniska och fysiska säkerhetsområdet. Exempel på säkerhetsåtgärd: *Regelbunden säkerhetskopiering minst en gång per dygn*
Tillgänglighet[15]	Egenskap hos informationstillgång som innebär att den är åtkomlig och användbar inom förväntad tid och omfattning.

[12] VGR:s projektstyrningsmodell Projektilen
[13] MSB Termbank
[14] MSB Termbank
[15] MSB Termbank

Verksamhetsutveckling	En strukturerad och kontinuerlig process där en organisation arbetar för att förbättra sina affärsprocesser, resurser, och verksamhetsresultat för att nå sina strategiska mål. Detta innefattar en rad olika aktiviteter och metoder som syftar till att öka effektiviteten, produktiviteten, och kvaliteten inom organisationen. På VGR bedrivs ofta verksamhetsutveckling i projektform men även andra uppdragsformer kan tillämpas.
Ägare IS/IT-tjänst[16]	Ägare av IS/IT-tjänst har ansvar för att, utifrån de krav som ställs på tjänsten genom informationsklassningen och utifrån de risker som identifierats, att införa, förvalta, följa upp och utvärdera säkerhetsåtgärder i IS/IT-tjänsten så att adekvat skydd uppnås i tjänsten *Ägare IS/IT-tjänst motsvarar ofta rollen produktområdesansvarig, systemägare eller applikationsägare för enskild applikation, tjänst, plattform eller större system och plattformar.*

[16] Informationssäkerhet och dataskydd – Regional riktlinje 2023-2027 (RS 2023-02811)

3 Ansvar och roller

Verksamhetsutveckling drivs enligt regiondirektörens beslut om fördelning av ansvar på koncernkontoret[17]. Prioriteringen av och beslut om verksamhetsutveckling görs av en koncernstabschef på koncernkontoret baserat på detta beslut och tilldelat ansvar. Koncernstabschefen, eller någon av koncernstabschefen utsedd, utser projektägare för verksamhetsutveckling.

Förvaltningsspecifik verksamhetsutveckling prioriteras och beslutas av respektive förvaltningschef som också utser projektägare för verksamhetsutvecklingen.

Ansvar för informationssäkerhet definieras i kapitel 3 av riktlinjen *Informationssäkerhet och dataskydd, Regional riktlinje 2023 – 2027* (RS 2023–02811).

I den regionala riktlinjen tydliggörs sammanfattningsvis att:

- Förvaltningschef/VD ansvarar för tillämpning av LISD i den egna förvaltningen.
- Informationsägaren ansvarar för att den lagstiftning som gäller ägarens informationstillgångar efterlevs.
- Informationsägaren ansvarar vidare för att säkerställa implementation och efterlevnad av säkerhetsåtgärder utifrån krav på skydd för informationstillgångarna.
- När informationstillgångar ingår i regiongemensamma processer, IS/IT-tjänster, utvecklingsuppdrag och/eller upphandlingar företräds flera förvaltningars informationsägare av en regional processägare.
- Projektägaren ska säkerställa att informationssäkerhets- och dataskyddsarbetet genomförs vid verksamhetsutveckling. Detta gäller alla typer av verksamhetsutveckling oavsett komplexitet, omfattning, varaktighet, ämnesområde eller tillämpningsområde.
- Projektägaren ska i ett tidigt skede identifiera vem som är regional processägare eller informationsägare och som kan fatta beslut om informationen och dess säkerhet såväl när verksamhetsutvecklingen pågår som när den avslutats. Som stöd finns på varje förvaltning informationssäkerhetssamordnare och dataskyddssamordnare.

[17] Regiondirektörens fördelning av ansvar inom Koncernkontoret, RS 2023-05437

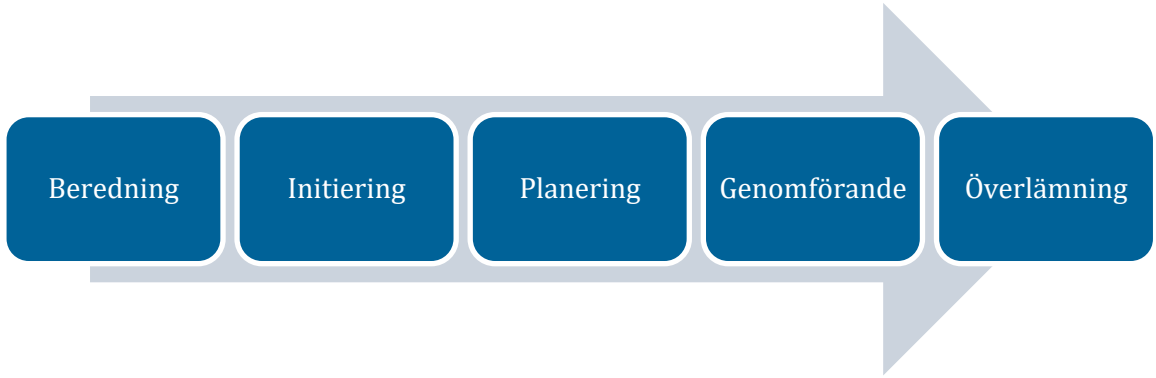
- Projektägaren är informationsägare för de informationstillgångar som krävs för att genomföra verksamhetsutvecklingen[18] och ska säkerställa att den som leder verksamhetsutvecklingen följer de säkerhetsåtgärder[19] som dessa informationstillgångar kräver.
- Informationssäkerhetssamordnare är ett stöd till verksamheten i dess informationssäkerhetsarbete och verkar för en regiongemensam tillämpning av interna styrdokument och regelverk i den egna verksamheten. Varje förvaltning ska ha en utsedd informationssäkerhetssamordnare.
- Dataskyddssamordnare är ett stöd till verksamheten i dess dataskyddsarbete och verkar för en regiongemensam tillämpning av interna styrdokument och regelverk i den egna verksamheten. Varje förvaltning ska ha en utsedd dataskyddsamordnare.
- Det operativa informationssäkerhets- och dataskyddsarbetet vid verksamhetsutveckling kan med fördel utföras av en informationssäkerhetssamordnare eller dataskyddssamordnare.
- Ägare av IS/IT-tjänst har ansvar för att införa, förvalta, följa upp och utvärdera säkerhetsåtgärder i IS/IT-tjänsten så att adekvat skydd uppnås i tjänsten.

[18] Exempel på informationstillgångar som krävs för ett utvecklingsuppdrag kan vara upphandlingsinformation, krav, lagringsytor (Sharepoint, G-disk…), kommunikationskanaler (Teams, e-post…) designlösningar, kod, testdata osv.
[19] Exempel på säkerhetsåtgärder i ett utvecklingsuppdrag kan vara att upphandlingsinformation ska hanteras med sekretess på sluten lagringsyta eller att verksamhetsdata för migrering ska hanteras med utökad behörighetskontroll separerat från testdata.

4 Informationssäkerhet vid verksamhetsutveckling

Informationssäkerhetsaspekter ska beaktas från början till slut vid verksamhetsutveckling och säkerhetsåtgärder ska integreras under hela utvecklingsarbetet, från kravställning till utrullning och förvaltning av den förändring som gjorts.

Informationssäkerhet och dataskydd ska hanteras, både för resultatet av verksamhetsutvecklingen och för arbetet som leder fram till den förändring som är syftet med verksamhetsutvecklingen.



Figur 1 Grundläggande steg vid verksamhetsutveckling.

Oavsett vilken utvecklingsmetodik som tillämpas ska VGR utifrån informationstillgångarnas ”värde” för verksamheten identifiera relevanta och tillräckliga administrativa, fysiska eller tekniska säkerhetsåtgärder.

I följande kapitel beskrivs de aktiviteter som, ur ett informationssäkerhets- och dataskyddsperspektiv, ska genomföras i samband med verksamhetsutveckling. Åtgärderna utgår ifrån VGR:s ledningssystem för informationssäkerhet och dataskydd samt avsnitt 5.8 *Informationssäkerhet i projektledning* samt avsnitt 8.25 *Säker utvecklingscykel* i SS-ISO/IEC 27002.

4.1 Beredning

Under den beredning som föregår en verksamhetsutveckling ska följande aktiviteter genomföras:

- Projektägaren ska identifiera vem som är informationsägare för de verksamhetsprocesser och informationstillgångar som omfattas av den önskade verksamhetsutvecklingen.

  Projektägaren kan, efter överenskommelse, företräda informationsägaren i informationssäkerhetsarbetet under genomförandet av utvecklingsarbetet.

- Projektägaren ska säkerställa att de informationstillgångar som kommer att omfattas av den önskade verksamhetsutvecklingen är klassificerade enligt *Informationsklassning – Regional rutin 2024-2028*.

  Klassningen resulterar i säkerhetsåtgärder som ska vidtas för den önskade verksamhetsutvecklingen.

- Projektägaren ska säkerställa att det finns ansvariga för att leda, övervaka och förvalta säkerhetsåtgärder genom hela verksamhetsutvecklingen.

- Projektägaren ska säkerställa att överväganden och aktiviteter som rör informationssäkerhet följs upp, vid på förhand fastställda stadier, av lämpade personer eller styrande forum, till exempel ett projekts styrgrupp.

-

4.2 Initiering

Under initieringen av en verksamhetsutveckling ska följande aktiviteter genomföras:

- Projektägaren ska säkerställa att potentiella risker och hot vad gäller informationssäkerhet avseende förändringen som verksamhetsutvecklingen innebär identifieras, bedöms och åtgärdas löpande enligt *Riskhantering för informationssäkerhet – Regional rutin 2024-2028*.

Här ingår också att utvärdera om den planerade förändringen påverkar andra informationsägares eller verksamheters informationssäkerhet och vid behov informera berörda om dessa risker.

- Informationsägaren eller dess företrädare kan, i samråd med informationssäkerhetssamordnare eller dataskyddssamordnare, besluta att acceptera risker avseende informationssäkerheten i lösningen inom dess verkställighetsansvar och regionens nivå för riskacceptans[20].

  Saknas realistiska säkerhetsåtgärder som leder till att riskerna kan undvikas, minskas eller överföras på ett effektivt sätt ska riskerna övervakas tills dess de hanterats till denna nivå.

  Risker som sträcker sig utanför verkställighetsansvaret ska eskaleras till den som har mandat, där risken ska hanteras på motsvarande sätt. Hantering av risker görs även då enligt *Riskhantering för informationssäkerhet – Regional rutin 2024-2028*.

- Projektägaren ska säkerställa att de informationstillgångar som är nödvändiga för arbetet med verksamhetsutvecklingen klassificeras enligt *Informationsklassning – Regional rutin 2024-2028*.

  Projektägaren är informationsägare för de informationstillgångar som uppstår under utvecklingsarbetet, exempelvis upphandlingsunderlag, krav, ritningar, systemdesign, programkod, testfall, avtal, mm.

  Informationsklassningen ligger till grund för de säkerhetsåtgärder som ska vidtas för att säkerställa informationssäkerheten under verksamhetsutvecklingsarbetet.

- Projektägaren ska säkerställa att potentiella risker och hot avseende informationssäkerhet under verksamhetsutvecklingen

[20] VGR har i *Riskhantering för informationssäkerhet – Regional rutin 2024-2028* definierat regionens riskacceptans. Riskacceptansen definierar vid vilken kombination av konsekvens och sannolikhet en risk kan accepteras, ska övervakas eller hanteras.

identifieras, bedöms och åtgärdas enligt *Riskhantering för informationssäkerhet – Regional rutin 2024-2028*.

- Informationsägaren eller dess företrädare kan besluta att acceptera risker avseende informationssäkerheten under verksamhetsutvecklingen[21] inom dess verkställighetsansvar och regionens nivå för riskacceptans.

  Saknas realistiska säkerhetsåtgärder som leder till att riskerna kan undvikas, minskas eller överföras på ett effektivt sätt ska riskerna övervakas tills dess de hanterats till denna nivå.

  Risker som sträcker sig utanför verkställighetsansvaret behöver eskaleras till den som har mandat där risken ska hanteras på motsvarande sätt. Hantering av risker görs enligt *Riskhantering för informationssäkerhet – Regional rutin 2024-2028*.

- Projektägaren ska säkerställa att en tröskelanalys genomförs enligt *Tröskelanalys avseende dataskydd - regional rutin 2024-2028*. Syftet är att klargöra om lösningen kommer att omfatta så pass känsliga personuppgifter att det finns ett behov av att genomföra en konsekvensbedömning.

- Projektägaren ska säkerställa att alla deltagare i utvecklingsarbetet får information om de krav på informationssäkerhet och dataskydd som gäller, varför det är viktigt att uppfylla dessa krav samt hur kraven ska uppfyllas i praktiken.

- Projektägaren ska, om personuppgifter hanteras i lösningen, säkerställa att personuppgiftsbiträdesavtal, PUB-avtal, tecknas med leverantörer som deltar i utvecklingsarbetet eller bidrar med lösningar.

  Koncerninköp ansvarar för att PUB-avtal tecknas. Den utpekade IS/IT-ägaren för lösningen ansvarar för att ta fram instruktioner

[21] Projektägaren är informationsägare för informationstillgångar som skapas i utvecklingsuppdraget och kan fatta beslut om att acceptera risker som rör dessa. Vissa informationstillgångar som hanteras i utvecklingsuppdraget, exempelvis skarpa data som ska migreras eller gemensamma IS/IT-tjänster, kan ha en annan informationsägare som då måste fatta beslut om att acceptera risker mot dessa informationstillgångar.

till leverantören som bilaga till PUB-avtalet. Den utpekade IS/IT-ägaren ska stå som dataskyddskontakt i PUB-avtalet.

4.3 Planering

Under planeringen av verksamhetsutveckling ska följande aktiviteter genomföras:

- Projektägaren ska, om tröskelanalysen resulterade i det, säkerställa att en konsekvensbedömning enligt *Konsekvensbedömning avseende dataskydd - regional rutin 2024-2028* genomförs. Syftet är, bland annat, att säkerställa att ytterligare säkerhetsåtgärder till skydd för personuppgifter identifieras.

- Projektägaren ska säkerställa att specifika krav vad gäller informationssäkerhet och dataskydd som uppstår på grund av att externa organisationer påverkas av en verksamhetsförändring, fångas upp under kravarbetet.

- Projektledaren ska säkerställa att de utifrån informationsklassningar, riskhantering, tröskelanalys och konsekvensbedömning identifierade säkerhetsåtgärderna är en integrerad del av planen för verksamhetsutvecklingsarbetet.

- Projektledaren ska säkerställa efterlevnaden av legala och avtalsmässiga krav vad gäller informationssäkerhet och dataskydd men också andra relevanta legala och avtalsmässiga krav.

- Om personuppgifter kommer behandlas i den planerade lösningen ska projektledaren säkerställa att processer och system är utformade så att inhämtande och behandling (inklusive användning, utlämnande, bevarande, överföring och destruktion) begränsas till det som är nödvändigt för det identifierade ändamålet.

- Om personuppgifter kommer att behandlas, i och med förändringen som utvecklingsarbetet resulterar i, ska projektledaren säkerställa att processer och IS/IT-tjänster är utformade på ett korrekt sätt. Detta innebär att de registrerade ska förses med lämplig information om behandlingen av deras

personuppgifter men också att andra eventuella tillämpliga förpliktelser gentemot de registrerade, i relation till behandlingen av deras personuppgifter, vidtas. Det kan exempelvis vara att få åtkomst till, korrigera och/eller radera personuppgifter.

- Projektledaren ska säkerställa att de definierade säkerhetsåtgärderna är tydliga, tillräckliga och genomförbara för implementation av förändringen samt efterföljande förvaltning.

- Projektledaren ska säkerställa att tydliga säkerhetskrav för utvecklingsarbetet och den planerade förändringen definieras baserat på säkerhetsåtgärderna.

  Säkerhetskraven ska utformas så att de är relevanta för den som ska genomföra utvecklingsarbetet till exempel en VGR-intern utvecklingsenhet eller en extern leverantör.

4.4 Genomförande

Under genomförandet av verksamhetsutveckling ska följande aktiviteter genomföras:

- Projektledaren ska säkerställa att de säkerhetskrav som definierats för verksamhetsutvecklingen och dess lösning implementeras och testas.

- Projektägaren ska säkerställa att relevanta tester, inklusive acceptanstester och säkerhetstester kopplat till tidigare definierade säkerhetsåtgärder, är genomförda och godkända före överlämning till den organisation som ska förvalta förändringen. Detta gäller oavsett om verksamhetsutvecklingsarbetet utförts av VGR eller av extern leverantör.

4.5 Överlämning

Inför överlämning av resultatet från en verksamhetsutveckling till förvaltning och drift, ska följande aktiviteter genomföras:

- Informationsägare eller dess företrädare ska godkänna eventuella avvikelser, exempelvis säkerhetskrav som inte har uppfyllts eller risker som inte åtgärdats, före överlämning till den organisation som ska förvalta förändringen.

- Projektledaren ska säkerställa att den information om förändringen som behövs för att förvalta och drifta den överlämnas till förvaltningsorganisationen.

  Informationsägarskapet för den information som behövs för förvaltning och drift övergår därmed till mottagande förvaltningsorganisation.

- Projektledaren ska säkerställa att den information som har använts under utvecklingsarbetet och som inte lämnas över till förvaltningsorganisationen hanteras enligt informationshanteringsplan för berörd förvaltning. Detta kan innebära att viss information ska diarieföras, viss information ska förvaltas inom ett visst produktområde och viss information ska gallras.

  Eventuella samarbetsytor som använts för verksamhetsutvecklingsarbetet ska avslutas.

5 Säkra IS/IT-tjänster

Vid utveckling av IS/IT-tjänster finns ytterligare säkerhetsåtgärder som ska vidtas för att säkerställa informationssäkerhet och dataskydd.

I digitaliseringsdirektörens ledningsansvar ingår att:

> *”…ta fram, besluta och förvalta rutiner för Västra Götalandsregionens verksamheter utifrån policys och riktlinjer som fastställts av regionfullmäktige och regionstyrelsen och som rör digitalisering, IT-system och digitala verktyg samt att i övrigt leda, utveckla och samordna arbetet inom området.”*

Koncernstab digitalisering, KSD, har därmed en central roll i att ta fram tillämpningsanvisningar, i enlighet med legala krav och ISO/IEC 27002, för att säkerställa informationssäkerheten och dataskyddet i IS/IT-tjänster samt ansvarar för att tillämpningsanvisningarna efterlevs i VGR.

Vid framtagning av tillämpningsanvisningar enligt ISO/IEC 27002 bör KSD ta hänsyn till den *Strategiska målarkitektur för Systemutveckling* samt involvera förvaltningarnas IT-organisationer i arbetet.

KSD ska också ta hänsyn till *Regional riktlinje - Egentillverkning av medicinteknisk produkt* och säkerhets- och prestandakrav beskrivna i *Regional rutin - Egentillverkning av medicinteknisk produkt*[22].

När tillämpningsanvisningar för respektive område tas fram ska vidare hänsyn tas till att vissa IS/IT-tjänster kan ha organisationer utöver VGR som användare. Detta kan ställa ytterligare krav på säkerhetsåtgärder för att säkerställa informationssäkerhet och dataskydd för VGR och berörda organisationer.

Kapitel 5.1 detaljerar de aktiviteter, utöver de generiska aktiviteter i kapitel 4, som ska utföras vid verksamhetsutveckling som innefattar en eller flera IS/IT-tjänster.

Kapitel 5.2-5.13 detaljerar sedan de områden i ISO/IEC 27002 där Koncernstab digitalisering har ansvar för att ta fram tillämpningsanvisningar som detaljerar de säkerhetsåtgärder som ska tillämpas vid ett utvecklingsarbete som omfattar IS/IT-tjänster.

[22] Riktlinjen och rutinen är giltig till 31 augusti 2024. Ersätts under 2024 med en ny rutin

5.1 Verksamhetsutveckling som omfattar IS/IT-tjänst

5.1.1 Planering

- Projektledaren ska säkerställa att kravarbetet för den eller de planerade IS/IT-tjänsterna tar hänsyn till VGR:s principer för Säkerhetskrav för applikationer enligt kapitel 5.2 nedan.

- Projektledaren ska säkerställa att designarbetet för den eller de planerade IS/IT-tjänsterna utgår ifrån VGR:s principer för Säker systemarkitektur och tekniska principer enligt kapitel 5.3 nedan.

5.1.2 Genomförande

- Projektledaren ska säkerställa att utvecklingsarbetet för den eller de planerade IS/IT-tjänsterna följer VGR:s principer för säker kodning enligt kapitel 5.4 och principerna för utkontrakterad utveckling enligt kapitel 5.8 nedan.

- Projektledaren ska säkerställa att testarbetet för den eller de planerade IS/IT-tjänsterna följer VGR:s principer för säkerhetstest enligt kapitel 5.5 till 5.7 nedan.

- Projektledaren ska säkerställa att den eller de planerade IS/IT-tjänsterna samt utvecklingen av dessa följer VGR:s principer för immateriella rättigheter enligt kapitel 5.9 nedan.

- Projektledaren ska säkerställa att hanteringen av informationssäkerhet i relation till leverantörer följer VGR:s principer för:
    - Informationssäkerhet i leverantörsrelationer enligt kapitel 5.10 nedan,
    - Hantering av informationssäkerhet inom leverantörsavtal enligt kapitel 5.11 nedan,
    - Hantering av informationssäkerhet i IKT-leveranskedjan enligt kapitel 5.12 nedan och,
    - Övervakning, granskning och ändringshantering av leverantörstjänster enligt kapitel 5.13 nedan

5.1.3 Överlämning

- Projektledaren ska säkerställa att den eller de planerade IS/IT-tjänsterna genomgår en IT-säkerhetsspecifikation enligt *IT-säkerhetsspecifikation – Regional rutin 2024-2028*. Syftet är att säkerställa att IS/IT-tjänsterna når upp till den informationsklass som fastställts för de informationstillgångar som ska hanteras i lösningen.

  IT-säkerhetsspecifikationen fungerar också som underlag om man i framtiden väljer att utnyttja IS/IT-tjänsterna till andra syften och andra informationstillgångar än de ursprungliga.

- Ägare IS/IT-tjänst ska säkerställa att de säkerhetsåtgärder som identifierats i informationssäkerhets- och dataskyddsarbetet har genomförts före överlämning till förvaltning och att detta finns dokumenterat, exempelvis i V-SAC[23] eller IT-SAC[24]. Här ingår exempelvis att dokumentera hur informationssäkerheten och dataskyddet hanterats.

[23] V-SAC beskriver ett antal grundläggande kriterier som bör vara uppfyllda för att projektresultat ska kunna överlämnas till beställare/uppdragsgivare för vidare förvaltning. Här ingår frågor om bland annat informationsklassning.
[24] IT-SAC betyder IT Service Acceptance Criteria och beskriver ett antal grundläggande kriterier som behöver vara uppfyllda för att en ny eller förändrad tjänst ska kunna överlämnas till koncernstab digitalisering (KSD) leveransorganisation. Här ingår detaljer som rör exempelvis backuper och behörighetshantering.

5.2 Säkerhetskrav för applikationer

VGR ska ställa informationssäkerhetskrav på IS/IT-tjänster, vilket kan inkludera krav på autentisering, behörighetskontroll, kryptering och hantering av känslig information. Andra exempel är kopplat till lagstiftning, exempelvis de krav som lagen för samhällsviktiga och digitala tjänster[25] definierar.

KSD ansvarar för att ta fram en tillämpningsanvisning, för all IS/IT-utveckling på VGR, som ska säkerställa följsamhet till relevant lagstiftning och tillämpliga delar av avsnitt 8.26 i ISO/IEC 27002.

5.3 Säker systemarkitektur och tekniska principer

VGR ska genom en säker systemarkitektur och tekniska principer, säkerställa att IS/IT-tjänsten är motståndskraftigt mot olika säkerhetshot, både vid design inom VGR och vid utkontrakterad design och utveckling. Detta område omfattar alla delar av utvecklingsarbetet och tar hänsyn till olika perspektiv såsom verksamhet, data, applikationer och teknik, inklusive den underliggande infrastrukturen som till exempel servrar, nätverk och andra tekniska resurser.

KSD ansvarar för att ta fram en tillämpningsanvisning, för all IS/IT-utveckling på VGR, som ska säkerställa följsamhet till relevant lagstiftning och tillämpliga delar av avsnitt 8.27 i ISO/IEC 27002.

5.4 Säker kodning

VGR ska tillämpa principer för säker kodning vid utveckling av IS/IT-tjänster, både inom VGR och vid utkontrakterad utveckling. Principerna ska, utöver egenutvecklade programvara, omfatta programvarukomponenter från tredjeparter och programvara med öppen källkod.

KSD ansvarar för att ta fram en tillämpningsanvisning, för all IS/IT-utveckling på VGR, som ska säkerställa följsamhet till relevant lagstiftning och tillämpliga delar av avsnitt 8.28 i ISO/IEC 27002.

[25] Den svenska lagen om informationssäkerhet för samhällsviktiga och digitala tjänster ställer krav på leverantörer att skydda sina nätverk och informationssystem från cyberhot och att rapportera allvarliga incidenter. Lagen är en implementering av EU:s Network and Information Systems Directive, NIS som under 2024 får en tillskärpning baserat på EU-direktivet NIS2.

5.5 Säkerhetstestning i utveckling och acceptans

VGR ska genomföra säkerhetstester under utvecklings- och acceptansfaser för att upptäcka och åtgärda säkerhetsbrister och sårbarheter. Detta gäller både nya IS/IT-tjänster och vid förändringar av befintliga IS/IT-tjänster, oavsett om design och utveckling sker inom VGR eller är utkontrakterad.

KSD ansvarar för att ta fram en tillämpningsanvisning, för all IS/IT-utveckling på VGR, som ska säkerställa följsamhet till relevant lagstiftning och tillämpliga delar av avsnitt 8.29 i ISO/IEC 27002.

5.6 Separation av utvecklings, test- och produktionsmiljöer

VGR ska i utvecklingsarbetet säkerställa en tydlig åtskillnad mellan olika IT-miljöer för att undvika oavsiktlig påverkan av produktionsmiljön från utvecklings- eller testaktiviteter. Detta gäller både nya IS/IT-tjänster och vid förändringar av befintliga IS/IT-tjänster, oavsett om design, utveckling och test sker inom VGR eller är utkontrakterad.

KSD ansvarar för att ta fram en tillämpningsanvisning[26], för all IS/IT-utveckling på VGR, som ska säkerställa följsamhet till relevant lagstiftning och tillämpliga delar av avsnitt 8.31 i ISO/IEC 27002.

5.7 Testinformation

VGR ska säkerställa att testdata och andra typer av information som används i utvecklings- och testprocessen hanteras på ett säkert sätt. Detta gäller både nya IS/IT-tjänster och vid förändringar av befintliga IS/IT-tjänster, oavsett om design, utveckling och test sker inom VGR eller är utkontrakterad.

Testinformation bör väljas för att säkerställa testresultatens tillförlitlighet och den berörda verksamhetsinformationens konfidentialitet. Känslig information (inklusive personuppgifter) bör inte kopieras in i utvecklings- och testmiljöer.

KSD ansvarar för att ta fram en tillämpningsanvisning, för all IS/IT-utveckling på VGR, som ska säkerställa följsamhet till relevant lagstiftning och tillämpliga delar av avsnitt 8.33 i ISO/IEC 27002.

[26] Idag finns Riktlinjer för test av informationssystem på VGR som täcker delar av detta.

5.8 Utkontrakterad utveckling

VGR ska vid utkontraktering, på samma sätt som vid egenutveckling, säkerställa att IS/IT-tjänster designas, implementeras och testas på ett säkert sätt för att därigenom minimera sårbarheter och säkerhetsproblem som kan utnyttjas av angripare.

KSD ansvarar för att ta fram en tillämpningsanvisning, för all IS/IT-utveckling på VGR, som vid utkontrakterad utveckling ska säkerställa följsamhet till relevant lagstiftning och tillämpliga delar av avsnitt 8.30 i ISO/IEC 27002 samt relevanta delar i del 1-4 av ISO/IEC 27036.

5.9 Immateriella rättigheter

VGR ska säkerställa efterlevnad av författningskrav och avtalskrav som rör immateriella rättigheter och användning av proprietära[27] produkter vid utveckling och användning av en IS/IT-tjänst. Här avses de delar som rör mjukvara och mjukvarulicenser under utveckling och användning.

KSD ansvarar för att ta fram en tillämpningsanvisning, för all IS/IT-utveckling på VGR, som ska säkerställa följsamhet till relevant lagstiftning och tillämpliga delar av avsnitt 8.32 i ISO/IEC 27002.

Vad gäller övriga immateriella rättigheter, exempelvis för video eller text, ska informationsägaren eller regional processägare säkerställa att de hanteras i enlighet med RS 2016-04284 Användning av upphovsrättsskyddat material (vgregion.se).

5.10 Informationssäkerhet i leverantörsrelationer

VGR ska säkerställa informationssäkerhet och dataskydd i leverantörsrelationer samt vid användning av produkter och tjänster som tillhandahålls av leverantörer. Detta gäller också när VGR använder resurser från leverantörer av molntjänster.

Styrningen för detta ska omfatta säkerhetsåtgärder som ska vidtas av VGR, och säkerhetsåtgärder som VGR kräver att leverantören ska vidta. Styrningen ska omfatta informationssäkerhet före, under och efter avslutad användning av en leverantörs produkter och tjänster.

KSD ansvarar för att ta fram en tillämpningsanvisning, för informationssäkerhet och dataskydd i leverantörsrelationer, som ska

[27] Äganderättsskyddade produkter vilket betyder att produkterna är skyddade av äganderätt, vilket omfattar immateriella rättigheter som patent, upphovsrätt, varumärken och andra typer av rättsligt skydd för intellektuell egendom.

säkerställa följsamhet till relevant lagstiftning och tillämpliga delar av avsnitt 5.19 i ISO/IEC 27002 samt relevanta delar i del 1-4 av ISO/IEC 27036.

5.11 Hantering av informationssäkerhet inom leverantörsavtal

VGR ska upprätta Leverantörsavtal för att säkerställa att VGR och leverantören har en klar bild av båda parters skyldighet att uppfylla relevanta informationssäkerhetskrav.

KSD ansvarar för att ta fram en tillämpningsanvisning, för hantering av informationssäkerhet inom leverantörsavtal, som ska säkerställa följsamhet till relevant lagstiftning och tillämpliga delar av avsnitt 5.20 i ISO/IEC 27002 samt relevanta delar i del 1-4 av ISO/IEC 27036.

5.12 Hantering av informationssäkerhet i IKT-leveranskedjan[28]

VGR ska utöver de allmänna informationssäkerhetskraven för leverantörsrelationer också säkerställa hanteringen av informationssäkerheten i processen för leverans, drift och underhåll av IT-system och tjänster. Detta gäller oavsett om VGR levererar IT-system och tjänster eller om andra leverantörer gör det för VGR:s räkning.

KSD ansvarar för att ta fram en tillämpningsanvisning, för Hantering av informationssäkerhet i IKT-leveranskedjan, som ska säkerställa följsamhet till relevant lagstiftning och tillämpliga delar av avsnitt 5.21 i ISO/IEC 27002 samt relevanta delar i del 1-4 av ISO/IEC 27036.

5.13 Övervakning, granskning och ändringshantering av leverantörstjänster

VGR ska ha en process för att hantera relationen mellan VGR och leverantören. Denna process ska bland annat säkerställa att informationssäkerhetsvillkoren och bestämmelserna i avtalen följs, att incidenter och problem som rör informationssäkerhet och dataskydd hanteras korrekt samt att ändringar i leverantörstjänster eller verksamhetsstatus inte påverkar tjänsteleveranser.

[28] IKT-leveranskedjan refererar till processen för att tillhandahålla och hantera informationsteknik (IKT) inom en organisation, inklusive leverans, drift och underhåll av IT-system och tjänster.

KSD ansvarar för att ta fram en tillämpningsanvisning, för Övervakning, granskning och ändringshantering av leverantörstjänster, som ska säkerställa följsamhet till relevant lagstiftning och tillämpliga delar av avsnitt 5.22 i ISO/IEC 27002 samt relevanta delar i del 1-4 av ISO/IEC 27036.

6 Relaterade dokument

- SS-EN ISO/IEC 27002:2022, Informationssäkerhet, cybersäkerhet och integritetsskydd[29]
- SS-ISO/IEC 27036, Informationsteknik – Säkerhetstekniker – Informationssäkerhet vid leverantörsrelationer[30]
    - Del 1: Översikt och begrepp
    - Del 2: Allmänna krav
    - Del 3: Riktlinjer för säkerhet i leveranskedjan för hårdvara, programvara och tjänster
    - Del 4: Riktlinjer för säkerhet vid molntjänster
- Termbank för informationssäkerhet - nationell terminologi för informations- och cybersäkerhetsområdet[31]
- Strategisk målarkitektur för Systemutveckling, Koncernstab digitalisering[32]
- RS 2016-04284 Användning av upphovsrättsskyddat material[33]
- Mall för V-SAC
- Mall för IT-SAC
- HS 2021-00795 Regional riktlinje - Egentillverkning av medicinteknisk produkt
- HS 2021-00796 Regional rutin - Egentillverkning av medicinteknisk produkt
- Policy - säkerhet och beredskap i Västra Götalandsregionen (dnr RS 2018-00129)
- Informationssäkerhet och dataskydd - Regional riktlinje 2023 – 2027 (dnr RS 2023-02811) [34]
- Informationsklassning – Regional rutin 2024 – 2028
- Riskhantering för informationssäkerhet – Regional rutin 2024 – 2028
- IT-säkerhetsspecifikation - Regional rutin 2024 – 2028
- Informationssäkerhet för extern molntjänst - Regional rutin 2024 – 2028

[29] SS-EN ISO/IEC 27002:2022 kan hittas på https://www.sis.se/ och finns gratis tillgängligt för VGR-anställda kopplat till VGR:s SIS-abonnemang.
[30] SS-ISO/IEC 27036 kan hittas på https://www.sis.se/
[31] Termbanken hittas på MSB:s hemsida
[32] ADD:n för Strategisk målarkitektur för Systemutveckling hittas på VGR:s iServer.
[33] Dokumentet hittas i VGR:s arkiv via https://hittaiarkivet.vgregion.se/
[34] Riktlinje och rutiner inom informationssäkerhet kan hittas under https://insidan.vgregion.se/stod-och-tjanster/sakerhet-och-krisberedskap/styrande-dokument-sakerhet-och-beredskap/ och rubriken *Informationssäkerhet*

Information om handlingen

Handlingstyp: Rutin

Gäller för: Västra Götalandsregionen

Innehållsansvar: Fredrik Almyren, (freal8), Regionutvecklare

Godkänd av: Johan Flarup, (johfl), Direktör

Dokument-ID: RS10162-1596316381-136

Version: 3.0

Giltig från: 2024-09-10

Giltig till: 2028-12-31