Rutin

Gäller för: Säkerhet och beredskap
Innehållsansvar: Robert Kielén, (robki1), Regionutvecklare
Godkänd av: Johan Flarup, (johfl), Direktör

Giltig från: 2025-10-01
Giltig till: 2029-12-31

Åtkomst till information och relaterade tillgångar

Regional rutin 2025 – 2029

Ledningssystem för informationssäkerhet och dataskydd

VÄSTRA GÖTALANDSREGIONEN

Innehåll

Inledning 4
Termer och begrepp 5
1 Åtkomstkontroll 8
1.1 Begränsning av åtkomst 8
1.2 Dynamisk åtkomstkontroll 8
1.2.1 Informationsägarens ansvar 8
2 Identitetshantering 9
2.1 Kategorier av användare 9
2.2 Ägare av IS/IT-tjänsts ansvar 9
3 Autentiseringsinformation och bärare 10
3.1 Ägare av IS/IT-tjänsts ansvar 10
3.2 Användarens ansvar 11
3.3 System med lösenordshantering 12
3.3.1 Ägare av IS/IT-tjänsts ansvar 12
3.4 Biometriska uppgifter 12
4 Behörighetshantering 13
4.1 Informationsägarens ansvar 13
4.2 Krav på process 13
4.3 Privilegierade åtkomsträttigheter 14
4.4 Krav på process 14
5 Säker autentisering 15
5.1 Tillitsnivåer 15
5.2 Ägare av IS/IT-tjänsts ansvar 15
6 Datamaskning 16
6.1 Informationsägarens ansvar 17
7 Tillgång till källkod 17
7.1 Krav på process 17
8 Förhindrande av dataläckage 18
8.1 Informationsägarens ansvar 18
9 Användning av privilegierade verktygsprogram 18

9.1 Ägare av IS/IT-tjänsts ansvar 18
10 Relaterade dokument 19
Bilaga 1..... 20

Inledning

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

Rutinen har utgångspunkt i *riktlinje för informationssäkerhet och dataskydd (RS 2023–02811)* där det beskrivs att *all åtkomst ska styras så att endast behöriga får tillgång till informationstillgångar*.

Rutinen beskriver krav för åtkomst till information men också relaterade tillgångar, det vill säga de resurser och tillgångar som gör det möjligt att hantera och skydda information. Rutinen omfattar bland annat säkerhetsåtgärder för identitetshantering, autentisering, hantering av autentiseringsinformation, hantering av behörigheter och åtkomsträttigheter, datamaskning, åtkomst till källkod och åtgärder för att förhindra dataläckage. Rutinen riktar sig till och betonar ansvaret som informationsägare, ägare av IS/IT-tjänst och användare har, samt behovet av kontinuerlig översyn och anpassning av säkerhetsåtgärder och utgör en central del i arbetet med informationssäkerhet och dataskydd.

Regional rutin - åtkomst till information och relaterade tillgångar är styrande för alla förvaltningar och bolag i Västra Götalandsregionen och ingår som en del i ledningssystemet för informationssäkerhet och dataskydd (LISD).

Termer och begrepp

Anonymisering	Personuppgifter ändras på ett oåterkalleligt sätt, så att den registrerade inte längre är direkt eller indirekt identifierbar.
Användare	Mänsklig eller icke-mänsklig entitet som nyttjar informationstillgångar.
Autentisering	Verifiering av ett påstående, exempelvis verifiering av en användares uppgivna identitet.
Behörighet	Tilldelade rättigheter att använda en informationstillgång på ett specificerat sätt.
Bruteforce	Användning av massor med tid och resurser för lösning av ett problem (i stället för en mer intelligent metod). Till exempel att pröva alla tänkbara lösningar i tur och ordning.
CAPTCHA	Förkortning av Completely Automated Public Turing test to tell Computers and Humans Apart som används för att avgöra om en användare är en människa eller inte.
Datamaskning	Omfattar ett antal metoder för att dölja, ersätta eller maskera känsliga uppgifter.
Dynamisk åtkomstkontroll	Metod för att hantera åtkomsträttigheter till resurser (som filer, system eller tjänster) där beslut om åtkomst baseras på flera variabler och görs i realtid. Till skillnad från statisk åtkomstkontroll, som bygger på fasta regler eller listor tar dynamisk åtkomstkontrollhänsyn till kontextuell information. Detta möjliggör mer flexibel och situationsanpassad säkerhet, särskilt i komplexa och föränderliga IT-miljöer.
Entitet	Objekt som är tydligt urskiljbart och som är av relevans för syftet med verksamheten inom ett område.

Exekverings-åtkomst	Styr om något kan köras (filer) eller nås (kataloger).
Hashning	Användning av funktion som avbildar en godtyckligt lång datasträng till en datasträng med fast längd, s.k. hashvärde.
Identifiering	Process vari en identitet som angivits av en användare eller en resurs verifieras.
Identitet	Entydigt bestämd person eller visst entydigt bestämt objekt. Det som gör en entitet unik.
Identitets-federation	Samverkan gällande systematiserat informationsutbyte mellan säkerhetsdomäner rörande användaridentiteter och användarattribut för att möjliggöra åtkomst till resurser i flera domäner.
Identitets-beteckning	Unik beteckning för en viss entitet (person, process, fysisk enhet eller liknande) i ett visst system eller inom en viss domän.
Immateriella-rättigheter	Juridiska rättigheter som skyddar skapandet av sinnet – det vill säga icke fysiska tillgångar som idéer, uppfinningar, konstnärliga verk, varumärken, design och programvara.
Informations-tillgång	Information och informationsbehandlande resurser som är av värde för en organisation.
Privilegierade-verktygsprogram	Verktygsprogram som har förmåga att kringgå säkerhetsåtgärder i system och applikationer.
Pseudonymisering	Processen för att uppnå pseudonymitet.
Pseudonymitet	Tillstånd i vilket användaren presenterar en annan identitetsbeteckning än identiteten.
Smarta saker	Omfattar olika typer av enheter (saker / ting) som har behov av att identifiera sig inom den digitala infrastrukturen. Exempel på saker som inkluderas i är till exempel robotar (AI, RPA

	m.m.) och uppkopplade saker (IoT - Internet of Things).
Tillitsnivåer för e-legitimering	Nivå av säkerhet för e-legitimation.
Åtkomst	Interaktion mellan en användare och en resurs som resulterar i överföring av information dem emellan eller utnyttjande av resurser.
Åtkomstkontroll	Funktioner i ett system som syftar till att reglera och kontrollera en användares åtkomst till information och resurser.
Åtkomsträttighet	En användares behörighet uttrycks i tilldelade åtkomsträttigheter. Dessa åtkomsträttigheter definierar vilka operationer en användare har rätt att utföra till exempel läsa, söka, skriva, radera, skapa och exekvera.

1 Åtkomstkontroll

Åtkomstkontroll omfattar en eller flera funktioner i ett system som syftar till att reglera och kontrollera användares åtkomst till information och resurser. Det kan exempelvis handla om administrativa funktioner som implementeras i processer eller tekniska funktioner som implementeras i programvara, applikation eller IS/IT-tjänster.

Åtkomstkontroll kan tillämpas på olika detaljnivå och kan täcka allt från hela nätverk eller system till specifika datafält. Åtkomstkontroll kan även omfatta egenskaper som användarens plats eller vilken typ av nätverksanslutning som används för åtkomst.

För att säkerställa en säker identitets och behörighetshantering ska åtkomst över organisationsgränser i första hand göras med hjälp av identitets- och behörighetsfederation. Samma sak gäller för åtkomst till andra organisationers tillgångar.

1.1 Begränsning av åtkomst

Åtkomst till information och andra relaterade tillgångar ska begränsas för att inte ge okända användaridentiteter eller anonyma aktörer åtkomst. Öppen eller anonym åtkomst kan ges till lagringsplatser där åtkomsten inte innebär informationssäkerhetsrisk. Åtkomst ska kontrolleras för att styra vilka uppgifter som kan nås av en viss identitet samt vilka identiteter eller grupper av identiteter som har vilken åtkomst, till exempel läs-, skriv-, raderings- och exekveringsåtkomst.

1.2 Dynamisk åtkomstkontroll

Åtkomstkontroll kan innehålla dynamiska element, till exempel funktion för utvärdering av tidigare åtkomst, egenskaper om användarens plats eller vilken typ av nätverksanslutning som används för åtkomst.

1.2.1 Informationsägarens ansvar

För att skydda information och relaterade tillgångar med stort värde ska dynamisk åtkomstkontroll användas när informationsägaren:

1 har behov att mer ingående styra vem som kan få åtkomst till samt under vilken period och på vilket sätt,

2 vill dela information med stort värde med personer utanför organisationen och ha fortsatt styrning över vem som kan få tillgång till den,

3 vill ha en dynamisk hantering i realtid av hur information med stort värde används och distribueras,

4 vill skydda information med stort värde mot obehörig ändring, kopiering och distribution (inklusive utskrifter),

5 vill övervaka hur information med stort värde används,

6 vill registrera eventuella ändringar av information med stort värde som utförs om en eventuell utredning krävs i framtiden.

2 Identitetshantering

Identiteter måste hanteras under hela livscykeln för att möjliggöra unik identifiering och tilldelning av åtkomsträttigheter. Bristfällig hantering kan leda till obehörig åtkomst, dataintrång och identitetsstöld, vilket hotar informationssäkerheten och den personliga integriteten.

2.1 Kategorier av användare

Två huvudsakliga kategorier av användare är mänskliga och icke-mänskliga. Syftet med att dela upp användare i kategorier och typer är att kraven på identitetshantering, autentisering och hantering av åtkomsträttigheter och autentiseringsinformation för olika användartyper skiljer sig åt.

Mänskliga användare:

- Medarbetare - personer som utför arbete i VGR:s namn, detta kan vara anställda, inhyrd personal, praktikanter osv.
- Leverantörer och partners - personer som företräder organisationer VGR arbetar tillsammans med. Det kan vara personer hos företag som förvaltar utrusning åt VGR eller kommuner, regioner, myndigheter som samarbete sker med.
- Privatpersoner – Personer som använder VGR:s tjänster, exempelvis patienter, resenärer och studerande.

Den andra kategorin, icke-mänskliga användare är under snabb utveckling och sammanfattas därför generellt in i:

- Maskiner och programvara - datorer, skrivare, telefoner, servrar och annan infrastruktur, smarta saker, programvarutjänster, mm.
- Annat - det finns andra icke-mänskliga entiteter som identitetshantering behövs för men som är utanför omfattningen av denna rutin, exempelvis organisationer och djur.

2.2 Ägare av IS/IT-tjänsts ansvar

Ägare av IS/IT-tjänst ska säkerställa att:

1 identiteter som tilldelas mänskliga entiteter är unika och personliga,

2 en identitet kopplas till en entitet, duplicerade identiteter för samma entitet får inte förekomma inom samma kontext i samma IS/IT-tjänst, om inte syftet är att separera åtkomsträttigheter,

3 identiteter som tilldelas flera entiteter, exempelvis gemensamma användarkonton endast tilldelas om det är absolut nödvändigt för verksamhets- eller driftsskäl, ska godkännas av informationsägare och dokumenteras, inklusive ansvar för identiteten,
4 identiteter som tilldelas icke-mänskliga entiteter, ska godkännas av informationsägare och dokumenteras, inklusive ansvar för identiteten,
5 identiteter ska avaktiveras utan dröjsmål om de inte längre behövs,
6 händelser rörande hantering av identiteter loggas,
7 identiteter som tillhandahålls eller utfärdas av tredje part uppfyller den tillitsnivå som krävs, tillitsnivån ska dokumenteras och kunna visas upp,
8 identiteter i identitetsfederationer hanteras av respektive användarorganisation,
9 tilliten till identiteten dokumenterats, exempelvis tillitsnivån för det identitetsbevis som använts vid grundidentifieringen av entiteten.

3 Autentiseringsinformation och bärare

Korrekt tilldelning och hantering av information och bärare av information som används för att styrka en identitet behövs för att motverka och förhindra obehörig åtkomst.

Det finns flera typer av autentiseringsinformation, lösenord och PIN-koder men även kryptografiska nycklar och biometrisk information omfattas. Bärare av autentiseringsinformation kan vara både fysiska och logiska, några exempel är smarta kort, USB-token, mobiltelefon, OTP-dosa, digitala certifikat.

Verktygsstöd för lösenordshantering som hjälper användare att lagra och fylla i lösenords eller annan autentiseringsinformation minskar mängden autentiseringsinformation som användare behöver skydda och kan därmed leda till att denna säkerhetsåtgärd blir mer verkningsfull. Samtidigt kan dessa verktyg också förstärka följderna av att autentiseringsinformation röjs och ska därför skyddas på ett sätt som minskar denna risk.

3.1 Ägare av IS/IT-tjänsts ansvar

Vid tilldelning av autentiseringsinformation ska ägare av IS/IT-tjänst säkerställa att:

1 lösenord och pinkoder som genereras automatiskt vid registrering av nya användare, som tillfällig och hemlig autentiseringsinformation, inte

går att gissa och är unika för varje användare, samt att lösenord och pinkoder måste ändras efter första användningen,

2 identiteten är korrekt före ny, förnyad eller tillfällig autentiseringsinformation tilldelas,

3 autentiseringsinformation och bärare överförs till användare på ett säkert sätt,

4 autentiseringsinformation som är förinställd eller tillhandahålls av leverantören ändras omedelbart efter installation,

5 händelser som rör tilldelning och hantering av autentiseringsinformation och bärare dokumenteras eller loggas.

3.2 Användarens ansvar

Användare ska:

1 hålla autentiseringsinformation såsom lösenord och PIN-koder konfidentiellt,

2 skydda bärare av autentiseringsinformation från obehöriga,

3 personlig autentiseringsinformation inte får delges någon annan,

4 personliga bärare av autentiseringsinformation inte får användas av någon annan,

5 autentiseringsinformation som används av icke-personliga entiteter enbart delges behöriga personer,

6 byta avslöjad eller misstänkt avslöjad autentiseringsinformation omedelbart,

7 omedelbart spärra bärare av autentiseringsinformation vid förlust,

8 välja starka lösenord i enlighet med följande rekommendationer:

- 8.1 lösenordet inte bygger på något som lätt kan gissas eller fås fram med hjälp av personrelaterad information (till exempel namn, telefonnummer och födelsedatum),
- 8.2 använda lösenfraser som är lätta att komma ihåg och helst omfattar bokstäver, siffror (alfanumeriska tecken) samt specialtecken,
- 8.3 lösenordets minimilängd är 14 tecken,

9 inte använda samma eller liknande lösenord för olika tjänster eller programvaror,

3.3 System med lösenordshantering

System med lösenordshantering omfattar system inklusive applikationer, IS/IT-tjänster och programvaror som används för eller hanterar lösenord.

3.3.1 Ägare av IS/IT-tjänsts ansvar

Ägare av IS/IT-tjänst ska säkerställa att systemet:

1 tillåter användare att välja och ändra sina lösenord,
2 innehåller funktionalitet för att motverka inmatningsfel,
3 lösenord och PIN inte visas i klartext vid manuell inmatning, användare ges möjlighet att visa manuellt inmatat lösenord i klartext,
4 tvingar mänskliga användarna att ändra lösenord vid första användning,
5 kräver att lösenord ändras efter en säkerhetsincident,
6 förhindrar att tidigare använda lösenord återanvänds,
7 förhindrar användning av vanliga och sårbara lösenord,
8 överför lösenorden på ett säkert sätt,
9 inte kräver lösenordsbyten utan anledning (för identiteter som används för systemadministration och tilldelas privilegierade åtkomsträttigheter kan lösenordsbyte krävas, men inte oftare än halvårsvis),
10 inte kräver speciell teckenuppsättning, till exempel minst en versal, gemen, siffra och specialtecken,
11 kräver 14 tecken som minimilängd för mänskliga identiteter och 30 tecken för icke-mänskliga,
12 använder bästa praxis för lagring lösenord som bland annat omfattar att aldrig lagra lösenord i klartext, använda modern hashfunktion som är designad för att motstå bruteforce-attacker och möjliggöra uppdatering av hashing-algoritmen,

Rekommendation

Genomför regelbundna tester av lösenordsstyrka, huvudsakligen för identiteter som tilldelats privilegierad åtkomsträttighet i säker, kontrollerad och separat avskild IT-miljö. Detta kan göras exempelvis med attacker som password spray (autentiseringsförsök med vanligt förekommande lösenord, ett åt gången på en större mängd identiteter) eller bruteforce-attack.

3.4 Biometriska uppgifter

Biometrisk identifiering innebär verifiering av en identitet genom exempelvis en medarbetares fingeravtryck, handgeometri, ögonbottenmönster, regnbågshinna,

ansikte, röst eller beteende. Dessa uppgifter är känsliga personuppgifter enligt dataskyddsförordningen och utgångspunkten är därför att det inte är tillåtet att behandla sådana uppgifter, eftersom behandlingen normalt innebär ett allt för stort intrång i den personliga integriteten och ett tungt vägande skäl krävs för behandling av dessa uppgifter.

Det finns situationer i arbetslivet där biometrisk upplåsning av exempelvis en mobiltelefon kan anses tillåten. Detta gäller om funktionen erbjuds som ett frivilligt alternativ och medarbetaren själv väljer att använda den, utan att arbetsgivaren på något sätt behandlar uppgifterna eller gör användningen obligatorisk.

4 Behörighetshantering

En användares behörighet uttrycks i tilldelade åtkomsträttigheter.

4.1 Informationsägarens ansvar

Vid tilldelning och borttagning av åtkomsträttigheter ska informationsägare:

1 genomföra behovs- och riskanalys före tilldelning av åtkomsträttigheter,
2 granska och vid behov tilldela, ändra eller ta bort åtkomsträttigheter löpande,
3 bedöma informationssäkerhetsrisker när befattning, roll, anställning eller annan position ändras eller avslutas, i bedömningen ta hänsyn till vem som initierade ändringen, medarbetarens ansvar samt värdet av medarbetarens tillgängliga informationstillgångar. Anledningen är att om exempelvis uppsägning initieras av chefen så kan detta leda till missnöje eller upplevelse om orättvis behandling vilket kan medföra risker för informationssäkerheten.

4.2 Krav på process

Processen för att tilldela och ta bort tilldelade åtkomsträttigheter ska:

1 omfatta beslut från informationsägaren för tilldelning, beslutet kan ske i förväg genom definierade kriterier, eller via delegerat ansvar för beslutet,
2 omfatta att behörigheter i behörighetsfederationer hanteras av respektive användarorganisation,
3 skilja på rollerna för att godkänna och tilldela åtkomsträttigheter,
4 omfatta att tilldelade åtkomsträttigheter tas bort när de inte längre behövs,

5 omfatta tidsbestämda åtkomsträttigheter, särskilt för medarbetare med tidsbestämd anställning samt för åtkomsträttigheter som behövs tillfälligt,
6 säkerställa att åtkomsträttigheter inte aktiveras före eventuella tillstånd är klara,
7 upprätthålla en central förteckning över identiteters logiska och fysiska åtkomsträttigheter samt förändringar av dessa,
8 omfatta förändring av åtkomsträttigheter för medarbetare som bytt befattning, roll, anställning eller annan position,
9 förhindra kloning eller kopiering av åtkomsträttigheter från en identitet till en annan,
10 i första hand och där det är lämpligt använda definierade verksamhetsroller, där en eller flera åtkomsträttigheter samlas,
11 vid tilldelning beakta tilliten till identiteten i förhållande till det tilldelningen avser.

4.3 Privilegierade åtkomsträttigheter

Privilegierade åtkomsträttigheter är åtkomsträttigheter som gör det möjligt att utföra särskilda aktiviteter, exempelvis krävs normalt privilegierade åtkomsträttigheter för systemadministratörsfunktioner. Privilegierade åtkomsträttigheter gör att användare kan kringgå säkerhetsåtgärder och är en stor bidragande faktor till fel eller intrång.

4.4 Krav på process

Utöver ovanstående krav på processen för att tilldela och ta bort åtkomsträttigheter, ska processen för privilegierade åtkomsträttigheter:

1 omfatta individuell bedömning,
2 dokumentera motivering av behov för tilldelningen,
3 beakta om användaren har nödvändig kompetens,
4 ta hänsyn till om särskild användarklient, utrustning eller gränssnitt krävs för åtkomsten,
5 ta hänsyn till om stärkt autentisering krävs för tilldelningen,
6 omfatta inbyggda privilegierade identiteter i programvaror så som root- och administratörs-identiteter,
7 tilldelas tidsbestämt,
8 tilldelas identiteter som används för systemadministration och inte identiteter som används för allmänna arbetsuppgifter.

5 Säker autentisering

Autentisering är processen där en angiven identitet bevisas och är en del av identifieringsprocessen. Säker autentisering är avgörande för att förhindra obehörig åtkomst och identitetsstöld.

Autentiseringens tillitsnivå baseras på tre huvudsakliga faktorer:

- tilliten till entitetens identiteten
- utfärdandeprocessens säkerhet
- säkerheten hos autentiseringsmetoden

5.1 Tillitsnivåer

För att beskriva tillitsnivån eller säkerhetsnivån vid autentisering ska tillitsramverket för svensk e-legitimation på nivåerna 2 till 4 användas i de fall där ramverket är tillämpbart, exempelvis när mänskliga användare loggar in med e-legitimation. I situationer där tillitsramverket inte är tillämpbart, till exempel vid autentisering av system, tjänster eller icke-mänskliga användare – används i stället tillitsnivåerna enligt SS-ISO/IEC 29115:2023, det vill säga Level of Assurance (LoA) 1–4.

Denna uppdelning garanterar att tillitsnivån alltid anpassas efter den aktuella autentiseringssituationen och typ av användare.

5.2 Ägare av IS/IT-tjänsts ansvar

För att uppnå säker autentisering ska ägare av IS/IT-tjänst vid implementation av inloggningsfunktioner i programvara säkerställa att:

1 lösenord som autentiseringsmetod undviks,

2 känslig information inte avslöjas förrän inloggningsprocessen har slutförts,

3 inte hjälpmeddelanden tillhandahåller hjälp för obehöriga entiteter (exempelvis ange vilken del av inloggningsinformation som är rätt eller fel),

4 inloggningsinformation valideras först när all inloggningsinformation har angivits,

5 skydd finnas mot bruteforce-inloggningsförsök för användarnamn och lösenord (till exempel genom att använda CAPTCHA, begära lösenordsåterställning eller blockera identiteten efter ett på förhand fastställt antal misslyckade inloggningsförsök),

6 misslyckade inloggningsförsök och lyckade inloggningar loggas,

7 lösenord och PIN inte visas i klartext vid inmatning, mänskliga användare ges möjlighet att visa inmatat lösenord i klartext,
8 autentiseringsinformation (exempelvis lösenord) som överförs över datanätverk krypteras ändamålsenligt,
9 inaktiva sessioner avslutas automatiskt efter angiven period av inaktivitet, perioden ska baseras på risk,
10 en för mänskliga användaren tydlig utloggningsfunktion finns,
11 autentiseringsinformation som utfärdats för privat användning (exempelvis e-legitimation), undviks för åtkomst i arbetet.

Ägare av IS/IT-tjänst ska även baserat på eventuella informationssäkerhetsrisker överväga om:

12 en säkerhetshändelse ska registreras om det upptäcks att någon har försökt eller lyckats göra ett intrång, till exempel genom att skicka en varning till användaren eller systemadministratörer efter ett visst antal felaktiga lösenordsförsök,
13 följande information ska visas eller skickas via separat kanal efter en godkänd inloggning:
    13.1 datum och tid för den förra godkända inloggningen.
    13.2 detaljuppgifter om misslyckade inloggningsförsök sedan den senaste godkända inloggningen,
14 allmänt varningsmeddelande ska visas som informerar om att programvaran är avsedd för behöriga användare.

6 Datamaskning

Datamaskning handlar om att med olika metoder dölja och begränsa exponeringen av känsliga data, inklusive personuppgifter, samt att uppfylla legala- och avtalskrav.

Metoder som pseudonymisering eller anonymisering kan dölja personuppgifter, den registrerades verkliga identitet eller annan känslig information, samt bryta kopplingen mellan personuppgifter och den registrerades identitet eller kopplingen till annan känslig information. Behovet av datamaskning för personuppgifter och andra känsliga uppgifter ska utvärderas av informationsägaren.

Personuppgifter i resursidentifierare och deras attribut, till exempel filnamn eller webbadresser (URL) ska undvikas eller döljas på lämpligt sätt. För att maskningen ska ha verkan bör samtliga delar av den känsliga informationen beaktas, om så inte sker kan det leda till att en person kan identifieras, även om direkt identifierande uppgifter om personen har maskats. Det beror på att andra data kan finnas som möjliggör en indirekt identifiering.

6.1 Informationsägarens ansvar

Vid införande av datamaskning ska informationsägare beakta:

1 vilken metod för datamaskning som är mest lämplig, exempelvis pseudonymisering, anonymisering, kryptering, hashning, radering av tecken eller substitution,
2 datamaskningens omfattning, beroende på hur de uppgifter som behandlas används,
3 åtkomstkontroller för behandlade uppgifter,
4 behov av förbud mot att sammanställa behandlade uppgifter och annan information i syfte att identifiera den registrerade,
5 eventuella legala krav, exempelvis krav på att betalkortsinformation ska maskas vid behandling eller lagring, krav på maskning av uppgifter för personer med skyddad identitet.

7 Tillgång till källkod

För att förhindra införande av obehörig funktionalitet i programvara, undvika oavsiktliga eller skadliga ändringar samt upprätthålla konfidentialitet för immateriella rättigheter behöver källkod och utvecklingsverktyg hanteras på lämpligt sätt. Detta omfattar åtkomst till källkod och utvecklingsverktyg inklusive designdokumentation, specifikationer, testplaner för verifiering och validering, kompilatorer, integrationsverktyg, testplattformar och testmiljöer.

7.1 Krav på process

Processer som hanterar källkod eller använder utvecklingsverktyg ska:

1 använda styrd central lagring i ett system för hantering av källkod,
2 vid uppdatering av källkod och dylikt, bevilja åtkomst till källkod i enlighet med regional rutin säker drift samt säker utveckling samt att uppdatering eller dylikt görs först efter att lämpligt godkännande har erhållits,
3 inte ge utvecklare direkt åtkomst till källkodskatalogen, utan via utvecklarverktyg med kontroll av aktiviteter och godkännanden vad gäller källkod,
4 förvara programförteckningar i en säker miljö, där läs- och skrivåtkomst hanteras och tilldelas på lämpligt sätt,
5 föra en granskningslogg över alla åtkomster och alla källkodsändringar,

6 om avsikten är att offentliggöra källkoden identifiera om ytterligare säkerhetsåtgärder behövs för att försäkra sig om källkodens integritet, exempelvis digital signering.

8 Förhindrande av dataläckage

För att upptäcka och förhindra att personer eller system utan behörighet röjer och extraherar information behöver åtgärder tillämpas på system, programvara, nätverk och andra resurser som behandlar, lagrar eller överför information.

8.1 Informationsägarens ansvar

Informationsägare ska baserat på risk för dataläckage bedöma behov av:

1. funktionalitet för att förhindra att information kopieras, klistras in, eller laddas upp till tjänster, enheter och lagringsmedier utanför organisationen,
2. programvara för att upptäcka om känslig information finns i ostrukturerade data,
3. programvara för att blockera användaråtgärder eller nätverksöverföringar, exempelvis kopiering från databas till kalkylblad eller överföring via e-post,
4. möjlighet för informationsägare att godkänna dataexport, exempelvis databaskopia,
5. att begränsa möjlighet till och införa användarvillkor för skärmdumpar eller skärmbilder.

9 Användning av privilegierade verktygsprogram

För att säkerställa att användning av verktygsprogrammen inte har skadlig inverkan på säkerhetsåtgärder som avser informationssäkerhet behöver användning av dessa begränsas och styras. Det beror på att verktygsprogrammen kan ha förmåga att kringgå säkerhetsåtgärder.

9.1 Ägare av IS/IT-tjänsts ansvar

Ägare av IS/IT-tjänst ansvarar för att privilegierade verktygsprogram:

1. begränsas till minsta möjliga antal betrodda och behöriga användare,

2. inte är tillgängliga för användare som har åtkomst till programvara i system där uppdelning av arbetsuppgifter och ansvar krävs och verktygsprogrammet kan kringgå systemets säkerhetsåtgärder,
3. som inte är nödvändig, tas bort eller avaktiveras,
4. begränsas till den tid då en godkänd ändring utförs,
5. loggar användning.

10 Relaterade dokument

- Riktlinje för informationssäkerhet och dataskydd (RS 2023–02811)
- Informationsklassning - regional vägledning säkerhetsåtgärder (rs14241-846171542-9)
- Informationssäkerhet, cybersäkerhet och integritetsskydd – Informationssäkerhetsåtgärder (ISO/IEC 27002:2022, IDT)
- Informationsteknik – Säkerhetstekniker – Assuransramverk för entitetsautentisering (ISO/IEC 29115:2013, IDT)
- Termbank för informationssäkerhet - nationell terminologi för informations- och cybersäkerhetsområdet (https://termbanken.informationssakerhet.se)
- Integritetsskyddsmyndigheten (IMY) - Biometriska uppgifter i arbetslivet | IMY
- Svenska tillitsnivåer - Tillitsnivåer för e-legitimering | Digg

Bilaga 1

Nedanstående tabell ger vägledning för vilka autentiseringsmetoder som kan vara lämpliga för olika typer av användare samt nivå av tillit till användarens identitet som kan vara möjlig med metoden. Dokumentet *Informationsklassning - regional vägledning säkerhetsåtgärder* beskriver vilken nivå av tillit till användarens identitet som ska väljas beroende på den informationsklass autentiseringen gäller för.

För att välja rätt autentiseringsmetod behöver även följande beaktas:

- Styrkan till användarens identitet vid utfärdandet,
- Tilliten till utfärdandet av autentiseringsinformationen,
- Process eller sammanhang som autentiseringen sker i,
- Eventuella legala och avtalskrav.

Användare	Tillit till användarens identitet	Autentiseringsmetod	Faktor
Medarbetare	LoA1 (LoA2 möjligt)	Lösenord, PIN-kod	Kunskapsbaserad
	LoA3 möjligt	Hårdvarudosa med engångskod + PIN-kod, Engångskod via SMS, e-post eller mobilapp + Lösenord,	Kunskap + innehavsbaserad
	Tillitsnivå 3	Svensk e-legitimation – tillitsnivå 3 (anskaffas via arbetsgivare), Europeisk e-legitimation – tillitsnivå väsentlig,	
	LoA2	Engångskod via SMS eller e-post	Innehavsbaserad
Leverantörer och partners	LoA1 (LoA2 möjligt)	Lösenord, PIN-kod	Kunskapsbaserad
	LoA3 möjligt	Hårdvarudosa med engångskod + PIN-kod, Engångskod via SMS, e-post eller mobilapp + Lösenord	Kunskap + innehavsbaserad
	Tillitsnivå 3	Svensk e-legitimation – tillitsnivå 3 (anskaffas via arbetsgivare), Europeisk e-legitimation – tillitsnivå väsentlig,	
	LoA2	Engångskod via SMS eller e-post	Innehavsbaserad

Privat-personer	LoA1 (LoA2 möjligt)	Lösenord, PIN-kod	Kunskapsbaserad
	LoA2	Engångskod via SMS eller e-post	Innehavsbaserad
	Tillitsnivå 3	E-legitimation - tillitsnivå 3 (anskaffas privat), Europeisk e-legitimation - tillitsnivå väsentlig	Kunskap + innehavsbaserad
Maskiner och programvara	LoA1 (LoA2 möjligt)	Applikationslösenord (ex. client secret, API-nyckel)	Kunskapsbaserad
	LoA2 (LoA3 möjligt)	Ömsesidig TLS med klient/servercertifikat (egenhändigt signerat), SSH public key, Private Key JWT	Innehavsbaserad
	LoA3 (LoA4 möjligt)	Ömsesidig TLS med klient/servercertifikat (betrodd certifikatutfärdare)	

Information om handlingen

Handlingstyp: Rutin

Gäller för: Säkerhet och beredskap

Innehållsansvar: Robert Kielén, (robki1), Regionutvecklare

Godkänd av: Johan Flarup, (johfl), Direktör

Dokument-ID: RS10162-1596316381-366

Version: 1.0

Giltig från: 2025-10-01

Giltig till: 2029-12-31