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	2015-11-09	Anvisning för fysisk och miljörelaterad säkerhet, RSK 265-2003

VGR-RIKTLINJE FÖR FYSISK SÄKERHET

Mål

Västra Götalandsregionens information samt övriga informationstillgångar, som exempelvis lokaler och den utrustning som används för informationshantering, ska skyddas på en nivå som identifierats genom informationsklassificering.

Ur Riktlinjer för informationssäkerhet i Västra Götalandsregionen

Utgångspunkt

Kraven på fysisk säkerhet finns beskrivna i *VGR-riktlinje för fysisk säkerhet* och ska tillämpas för alla lokaler där information hanteras, samt för all utrustning som används för informationshantering. Information och utrustning ska skyddas på ett likvärdigt sätt, oavsett om den hanteras innanför eller utanför regionens lokaler. Utöver ovanstående riktlinje ska Arkivnämndens regler och rekommendationer iakttas för lokaler som förvarar arkivmaterial.

Ur Riktlinjer för informationssäkerhet i Västra Götalandsregionen

1 Omfattning

Information och utrustning ska skyddas på ett likvärdigt sätt oavsett om den hanteras innanför eller utanför regionens lokaler.

Lokal där information förvaras eller hanteras ska klassificeras utifrån informations skyddsvärde.

Förutom det skydd som kan skapas genom exempelvis kontrollerad inpassering, gemensamma rutiner, har varje medarbetare som arbetar i regionen ansvar för att känslig information inte finns tillgänglig för obehöriga.

2 Fysiskt skydd av lokaler

Fysiskt skydd består av:

- Yttre skalskydd (Mekaniskt skydd i en byggnads omslutningsytor, vars funktion är att förhindra eller fördröja intrång och åverkan.)
- Inre skalskydd (Mekaniskt skydd i en lokals anslutningsytor, vars funktion är att förhindra eller fördröja intrång och åverkan.)
- Kablageskydd
- Bevakning
- Inbrottslarm (Teknisk installation, vars funktion är att upptäcka intrång eller åverkan.)
- Passagekontrollsystem
- Byggnadstekniskt brandskydd (Konstruktions- och installationsskydd som förhindrar och fördröjer brand- och brandgasspridning samt tekniska installationer som upptäcker brand och brandgaser.)

2.1 Skalskydd

Skalskyddet ska ses som en helhet med en enhetlig skyddsnivå, fastställd genom en riskanalys. Dess funktion är att förhindra, fördröja och upptäcka intrång eller åverkan.

Skalskydd (mekaniskt eller tekniskt skydd) ska användas för att skydda utrymmen där information och informationsbehandlingsresurser finns. Krav på fysiskt skydd ställs av informationsägaren genom informationsklassificering. I anslutning till det mekaniska skyddet ska teknisk installation för upptäckt av obehörigt intrång eller åverkan finnas, exempelvis inbrottslarm, kameraövervakning.

Ansvaret för att upprätta och under hålla skalskyddet ska fastställas i samverkan mellan den lokalt fastighetsansvarige och verksamhetens säkerhetsansvarige eller av denne utsedd person. Gränsdragningslista ska upprättas, där det tydligt framgår vem som ansvarar för de olika delarna av skalskyddet.

2.1.1 Tillträde och identifiering

Inpassering till lokaler som inte betraktas som allmänna, ska utformas så att den utgör en tydlig avgränsning, som möjliggör att fysiskt utestänga obehöriga besökande.

Endast medarbetare och besökare med besökskort ska få tillträde till lokaler som inte betraktas som allmänna. För studerande gäller att verksamhetschef ansvarar för att de får tillträde till de lokaler som är nödvändiga.

Inom hälso- och sjukvård ansvarar verksamhetschef för att det finns regler för hur patienter och besökande har tillträde till lokaler som inte betraktas som allmänna.

2.2 Inte allmänna lokaler

Tillträdesgräns upprättas där det finns behov av behörighetskontroll. Dessa ska finnas i det yttre och inre skalskyddet samt i övriga fysiska gränser, där det finns behov av behörighetskontroll. Tillträdesgränser kontrolleras med hjälp av organisatoriska åtgärder, exempelvis bemannad reception och/eller teknisk installation som lås, passagekontrollsystem.

Innanför tillträdesgränsen kan det finnas behov av att förstärka skyddet ytterligare – skyddsvärda lokaler – med hänsyn till informationsklassificering och informationens omfång.

2.2.1 Skyddsvärd lokal

I regionens lokaler hanteras informationstillgångar med olika grad av skyddsbehov. Därför måste administrativa lokaler få ett kompletterande skydd, som motsvarar skyddsnivåerna i informationsklassificeringen. Som skyddsvärd lokal räknas bland annat administrativa lokaler.

Huvudprincipen är att endast behöriga medarbetare får vistas i skyddsvärd lokal. Extern servicepersonal, som utför arbeten i skyddsvärd lokal, ska få instruktioner om vilka rutiner som gäller för vistelsen. Ansvarig för att så sker är den som anlitar utomstående leverantör.

Kompletterande skydd ska användas då informationsklassificeringens hanteringsregler kräver detta.

2.2.2 Mycket skyddsvärd lokal

Kritiska eller känsliga informationstillgångar ska inrymmas i mycket skyddsvärd lokal med lämpliga säkerhetsavspärrningar. Mycket skyddsvärd lokal ska, för att säkerställa att endast behörig personal får tillträde, skyddas genom lämpliga tillträdeskontroller.

Som mycket skyddsvärd lokal räknas bland annat:

- Infrastrukturrum data (centralt och lokalt)
- Arkivlokaler
- Infrastrukturrum tele
- Utrymmen för korskoppling

Medarbetare ska ha kunskap om de rutiner och regler som gäller för att vistas och utföra arbetet i mycket skyddsvärd lokal.
Den befattningshavare som är ansvarig för verksamheten som bedrivs i mycket skyddsvärd lokal har ansvar för att ta fram en rutin för hur arbetet i respektive lokal får bedrivas.

2.2.3 Allmänna tillträdes-, leverans- och lastutrymmen

Platser för tillträde som t ex leverans- och lastutrymmen och andra platser där obehöriga personer kan komma in i lokalerna bör övervakas och ska avskärmas för att undvika obehörigt tillträde.

3 Skydd av utrustning

Den utrustning Västra Götalandsregionen använder för sin informationshantering ska i möjligaste mån skyddas, så att den inte förloras, stjäls eller skadas. Det primära syftet är att skydda lagrad information.
Som utrustning räknas bl.a. läsplattor, telefoner och USB-minnen. Även fysiska dokument ska hanteras på motsvarande sätt.

3.1 Placering och skydd av utrustning

Inredning av lokaler och placering av utrustning ska ske på ett sådant sätt, att utrustningen skyddas mot fysiska och miljömässiga hot. Skydd ska även finnas mot otillbörlig åtkomst.

Kring särskilt skyddsvärd utrustning ska lämpligt skydd vidtas i enlighet med informationsklassificeringens krav.

3.2 Kraftförsörjning och andra stödjande funktioner

För att utrustningen ska kunna fungera på avsett sätt, krävs ett antal stödjande funktioner som kraftförsörjning, klimatanläggningar, ventilation m.m. Dessa stödjande funktioner ska vara utformade på ett adekvat sätt och även regelbundet granskas, så att de uppfyller de krav på funktion som ställs av verksamheten.
Informationsklassificering ska utgöra stöd för de krav som ska ställas på till exempel redundans, reservkraft och kablageskydd.
Telekommunikationsutrustningar bör anslutas via minst två olika kommunikationsvägar.

3.3 Skydd av kablar

Kablar som används för datatrafik och telekommunikation ska skyddas mot avlyssning och åverkan. Skydd mot åverkan gäller även kablar som används för elförsörjning till utrustning för informationstjänster.

3.4 Underhåll och reparation av utrustning

Underhåll och reparation av utrustning ska ske enligt regionens regelverk och tillverkarens anvisningar och får endast utföras av auktoriserade reparatörer.

Särskilda regler ska utformas, för reparation av utrustning som innehåller känslig information.

3.5 Brandskydd

Arbetet med brandskydd ska bedrivas systematiskt. Brandskyddet ska, utöver gällande grundnivåer i lagstiftningen, ta hänsyn till behovet av skydd för verksamhet och informationstillgångar.

3.6 Bevakning och larm

Bevakning och larm är ett komplement till övriga skyddsåtgärder och ska, efter riskbedömning, användas där extra skydd är motiverat. Rutin för hanteringen ska finnas.

3.7 Säkerhet för utrustning utanför egna lokaler

Säkerhet beträffande utrustning utanför egna lokaler ska utformas med hänsyn till de olika risker, som är förknippade med att arbeta utanför organisationens lokaler. Samma skyddskrav gäller oavsett om utrustningen förvaras i regionens lokaler eller utanför dessa.

3.8 Extern användning av regionens egendom

Utrustning, information eller programvara får inte avlägsnas från regionens lokaler utan tillstånd.