

# Före – Under – Efter

**Sammanfattning av policy, ramverk och strategi  
för säkerhetsarbete i Västra Götalandsregionen**

**Handledning för chefer hur säkerhetsarbete  
ska bedrivas i VGR**

2008-06-01

## Innehållsförteckning

<b>Säkerhet Västra Götalandsregionen</b>	3
<b>1. Policy</b>	4
Följande principer ska därför vara vägledande i säkerhetsarbetet	4
Säkerhetsarbetets mål	4
Ansvar	5
<b>2. Säkerhetsstrategi 2008–2011 – 7 strategiska mål</b>	6
<b>3. Skyddsåtgärder – för att skapa en god säkerhet</b>	7
<b>4. Ramverk och riktlinjer – grunden i säkerhetsarbetet</b>	9
Steg 1 – Vad är skyddsvärt	9
Steg 2 – Säkerhetsprocessen	9
Steg 3 – Utbildning	9
<b>Mall för nämndens/styrelsens årliga redovisning till regionstyrelsen</b>	10
<b>Regionstyrelsen skall årligen rapportera</b>	11

## Säkerhet Västra Götalandsregionen

Säkerhetsstrategiska avdelningen ansvarar för utveckling av risk och krishantering utifrån regional policy, ramverk och strategi för säkerhet

### Före

Risk- och sårbarhetsanalys, genomföra skyddsåtgärder, planera/öva, organisera riskhanteringsgrupp.

### Under

Åtgärda det akuta, bedöm läget, aktivera operativ plan, aktivera kommunikationsplan avvikelshantering

### Efter

Samla in och analysera data, återkoppla analysera, åtgärda, återkoppla, normalisera, kommunicera, stöd anställda, utvärdera och dra lärdom



Risk och krisorganisation i respektive förvaltning

## 1. Policy

Västra Götalandsregionen ska värna människor, egendom, verksamheter och miljö, samt grundläggande värden som demokrati, jämlikhet, rättvisa, integritet och förtroende, mot hot och faror.

Västra Götalandsregionen är en del av rikets krishanteringsorganisation.

Samhällsviktig verksamhet ( i princip hela regionen) som hälso- och sjukvård och dess stödfunktioner, teknisk infrastruktur, person- och godstransporter samt flöden av varor och tjänster får inte bryta samman.

Det ska finnas god förmåga i Västra Götalandsregionen att hantera krissituationer. Den ska byggas på den ordinarie verksamhetens krav på säkerhet och uthållighet.

### **Följande principer ska därför vara vägledande i säkerhetsarbetet:**

**Ansvarsprincipen** Den som ansvarar under normala förhållanden ansvarar även under kris.

**Närhetsprincipen** Krisen ska hanteras där den inträffar och av närmast berörda.

**Likhetsprincipen** Innebär att en verksamhets lokalisering och organisation så långt som möjligt ska vara densamma under fred, kris och krig.

### **Säkerhetsarbetets mål**

Patienter, resenärer, besökare, studerande, personal och förtroendevalda ska vara trygga i regionens lokaler och verksamheter.

Rätt och riktig information ska nå rätt mottagare i rätt tid.

Regionens verksamheter ska vara robusta och ha god beredskap och förmåga för att hantera kriser, extraordinära händelser och dess konsekvenser.

God säkerhetskultur och en gemensam säkerhetsprocess i regionens verksamheter ska underlätta samverkan i säkerhetsarbetet över organisatoriska gränser.

*Policy, ramverk och riktlinjer samt säkerhetsstrategi, Dnr RSK 636:2006.*

## Information från Regionkansliet

### Ansvar

**Regionstyrelsen** ansvarar för att god säkerhet upprätthålls i regionen.

**Nämnder, styrelser och bolag** har det yttersta ansvaret för säkerheten inom respektive verksamhetsområde och ska se till:

- att säkerhetsarbetet fastställs i en plan som utgår från verksamhetens mål, skyddsvärda objekt och regionala direktiv
- att utbildning, risk- och sårbarhetsanalyser och övningar genomförs
- att resultatet av arbetet rapporteras till regionstyrelsen årligen.

**Förvaltningschef eller VD** ska upprätta en organisation för ett systematiskt säkerhetsarbete, som beaktar alla områden.

**Chef** ansvarar för säkerheten på den egna enheten och för att personalen är informerad.

**Varje medarbetare** ansvarar för att arbeta aktivt för ökad säkerhet och för att påpeka brister i säkerheten till närmsta chef.

### **2. Säkerhetsstrategi 2008–2011 – 7 strategiska mål**

**Mål 1.** Att förebygga mänskligt lidande, skador, skadeverkningar och kostnader förorsakade av skador, förluster, olyckor och andra oönskade händelser.

**Mål 2** Att säkerhetsarbetet i regionens verksamheter blir en ledningsfråga och kopplas till en tydlig politisk beslutsordning.

**Mål 3** Att Västfastigheter ansvarar för fastighetsbunden teknisk säkerhet (exvis; tekniska skyddsåtgärder avseende brand, inbrott, kameraövervakning med mera) samt kontinuiteten och säkerheten i medieförsörjningen till verksamheten (exvis; el, vatten, värme, gas med mera i regionens och i externt hyrda lokaler.

**Mål 4** Att Regionservice ansvarar för tekniska skyddsåtgärder och kontinuiteten, som inte västfastigheter har ansvar för, i regionens och i externt hyrda lokaler exvis inom IT-området.

**Mål 5** Att alla bolag och förvaltningar etablerar en ändamålsenlig risk- och krishanteringsorganisation och upprättar handlingsplaner för att uppnå en relevant säkerhetsnivå.

**Mål 6** Att säkerhetskulturen förbättras och utvecklas i regionens verksamheter.

**Mål 7** Att rätt och riktig information till rätt mottagare i rätt tid.

***Målen kommer årligen att följas upp och ligga till grund för den fortsatta planeringen av regionens säkerhetsarbete. Se mall sid 7 och 8.***

### 3. Skyddsåtgärder – för att skapa en god säkerhet

**Risk- och sårbarhetsanalyser** – Regionen och dess verksamheter ska kontinuerligt analysera risker och sårbarheter i verksamheten på lämpligt sätt.

**Fysiskt skydd** – huvudsakligen omfattande brand, tillträdesskydd och skydd mot yttre påverkan – ska etableras med utgångspunkt från identifierade hot och risker.

**Skydd av teknisk drift** – gäller alla tekniska system. Rutiner ska vara dokumenterade och även innefatta ändringshantering, avvikelsehantering, skydd av datamedia och skydd mot skadlig programkod.

**Databehandlingsresurser, inklusive datakommunikation, ska godkännas** i överenskommelse mellan aktuell systemägare, funktionsområdesansvarig, driftansvarig, eller motsvarande, innan de tas i drift.

#### **Åtkomst- och behörighetsstyrning**

Formella rutiner för tilldelning, förändring, upphörande och uppföljning av åtkomst ska finnas.

**Systemförändringar** – Särskild uppmärksamhet ska läggas på att verksamhetens säkerhetskrav beaktas vid utveckling, anskaffning och avveckling av informationsbehandlingsresurser. Etablerade säkerhetsåtgärder ska verifieras och godkännas av befattningshavare med motsvarande ansvar, före driftsättning

**Kris- och kontinuitetsplanering** – Åtgärdsplan ska säkerställa att verksamheten ska kunna bedrivas kontinuerligt. Planerna ska hållas uppdaterade och övas så att de blir ett naturligt inslag i ledning av arbetet. Planen ska omfatta beslutad krisorganisation och återgång till normal drift.

**Granskning och uppföljning** – Relevans och nytta av vidtagna åtgärder ska utvärderas genom regelbunden granskning och uppföljning

**Organisationsförändring** – Vid utredningar inför organisationsförändringar, där verksamhetsansvar förs över till annan förvaltning, bolag eller annan juridisk person, ska risk- och konsekvensanalyser genomföras för att säkerställa att säkerhetsbrister inte uppkommer.

## Information från Regionkansliet

**Ansvar för avtal med extern part** – Den som ingår avtal med extern part ansvarar för att risker relaterade till uppdraget analyseras, att kraven på riskhantering och säkerhet specificeras i avtalet och att uppföljning av avtalade skyddsåtgärder sker. Sekretessavtal ska tecknas med alla ingående parter.

**Rapportering av avvikelser och incidenter** – En samordnad avvikelse- och incidentrapportering är ett medel för varje verksamhets bedömning av effektiviteten i säkerhetsarbetet och en övergripande analys av förebyggande åtgärder. Vid större händelser eller olyckor inom regionens verksamheter ska en oberoende utredning genomföras.

**Dokumentation** – Uppkomna skador eller incidenter ska dokumenteras på ett systematiskt sätt för uppföljning och förbättring. I VGR ska vi använda MedControl.

***Ta hjälp av din säkerhetsfunktion.  
Där finns expertkunskapen om skyddsåtgärderna!***



Filmer/interaktiva  
utbildningsprogram

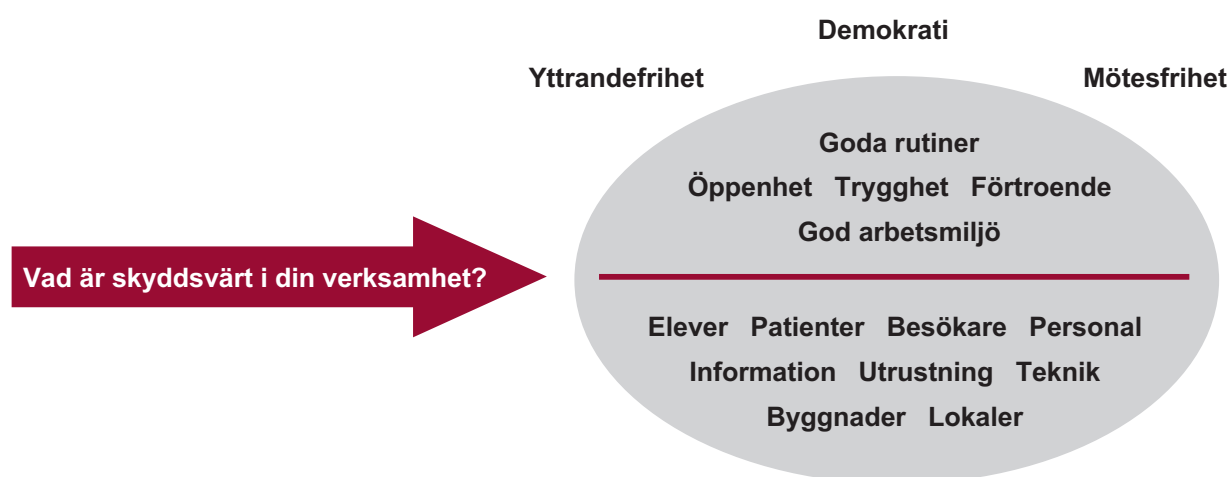
***På regionens hemsida finns ytterligare stöd i form av regelverk, mallar,  
verktyg och metoder. Se [intra.vgregion.se/sakerhet](http://intra.vgregion.se/sakerhet)***



## 4. Ramverk och riktlinjer – grunden i säkerhetsarbetet

### Steg 1 – Vad är skyddsvärt

Säkerhetsarbetet inom regionen ska omfatta allt från vardagssäkerhet till den stora krisen och utgå från det som betraktas som skyddsvärt.



### Steg 2 – Säkerhetsprocessen

Säkerhetsprocessen handlar om att arbeta i ett före, under och efterperspektiv.

FÖRE	UNDER	EFTER
<b>Förebyggande:</b> risk- och sårbarhetsanalys, genomför skyddsåtgärder	<b>Vardagsolycka:</b> åtgärda det akuta, avvikelserrapportera	<b>Fakta:</b> samla in och analysera data, återkoppla
<b>Förberedande:</b> planera, organisera riskhanteringsgrupp, öva	<b>Allvarlig händelse:</b> åtgärda det akuta, avvikelserrapportera	<b>Orsak:</b> analysera, åtgärda, återkoppla
	<b>Kris eller extraordinär händelse:</b> bedöm läget, aktivera operativ plan, aktivera kommunikationsplan	<b>Efterfas:</b> normalisera, kommunicera, stöd anställda, utvärdera och dra lärdom

### Steg 3 – Utbildning

Regionfullmäktige har i säkerhetspolicyn slagit fast att säkerhetsfrågor ska vara ett återkommande inslag i regionens/verksamhetens utbildningsinsatser för medarbetare, chefer och förtroendevalda, särskilt inom chefsutbildningen.

## Information från Regionkansliet

**Säkerhetsarbetet** ska revideras varje år inom respektive nämnds, styrelses eller bolags verksamhet. Resultatet ska redovisas i respektive årsredovisning, samt till regionstyrelsen enligt mall nedan.

**Samtliga nämnder och styrelser** får i uppdrag att årligen, i samband med ekonomisk redovisning, till regionkansliet inkomma med en översikt av läget i deras säkerhetsarbete, enligt punkt 1.8 i ramverk för säkerhetsarbete. Dnr RSK 636-2006

### Mall för nämndens/styrelsens årliga redovisning till regionstyrelsen

<p><b>Rött/DÅLIGT:</b> Vi är långt ifrån att nå uppsatta mål. Mycket arbete återstår.  <b>Orange/VARNING:</b> Vi är inte riktigt nära att nå målen. En hel del arbete återstår.  <b>Gult/OK:</b> Vi är på gång att nå våra mål. Vi är på rätt väg.  <b>Ljusgrönt/BRA:</b> Vi bedömer att vi når våra mål.  <b>Mörkgrönt/UTMÄRKT:</b> Vi överträffar våra mål. Våra resultat är utmärkta.</p>	 <p>Markera med pil enligt balanserat styrkortsmetodik</p>				
1 (Mål 1). Har din förvaltning en fungerande avvikelshantering.					
2 (Mål 1). Redovisas kostnader för inträffade händelser till förvaltningsledningen.					
3 (Mål 1). Är behovet av personer utbildade i riskanalys, sårbarhetsanalys eller händelseanalys tillgodosett.					
4 (Mål 2). Har förvaltnings-/bolagsledning säkerhetsfrågorna regelbundet på agendan.					
5 (Mål 3). Har Västfastigheter fått ett utökat ansvar för fastighetsbundna säkerhetsanläggningar					
6 (Mål 4). Har Regionsservice ansvar för tekniska skyddsåtgärder som inte Västfastigheter ansvarar för (inkl. IT-säkerheten)					
7 (Mål 5). Har förvaltningen en risk - och krishanteringsorganisation( IT, tele, el, vatten etc.)					
8 (Mål 5). Finns en handlingsplan fastställd av nämnden/styrelsen för säkerhetsarbetet.					
9 (Mål 6). Genomförs mätningar av säkerhetskulturen.					
10 (Mål 7). Är förvaltningsövergripande processer och digitala informationsmängder klassificerade utifrån sekretess, riktighet, tillgänglighet, spårbarhet.					
11 (Mål 7). Tillämpas regelverk som beskriver regionala krav på hur IT-stödet ska utvecklas i perspektiven verksamhet, informatik, teknik och säkerhet.					

## Information från Regionkansliet

Regionstyrelsen skall årligen rapportera till den myndighet som regeringen utser, om vilka åtgärder som vidtagits för att minska risker och sårbarheter och därmed förbättrat krishanteringsförmågan inom regionen, därför ska även nedanstående redovisas årligen till regionstyrelsen.

1. Vilka granskningar, risk- och sårbarhetsanalyser, och skyddsåtgärder av större betydelse har utförts avseende säkerheten och vilka förbättringsåtgärder har genomförts.
2. De övergripande och gemensamma risker som behöver hanteras över förvaltnings- och bolagsgränserna inom VGR.
3. Bedömning av aktuellt läge för er organisations krishanteringsförmåga  
Använd mallen nedan.

Strategisk Ledning	Samverkan med andra aktörer	Extern information/kommunikation	Intern information/kommunikation	Operativ ledning
Långsiktig planering. Prioritering av resurser Förtroendefrågor osv.	Andra förvaltningar, kommuner, polis räddningstjänst, etc.			I förväg planerad och övad kris/katastrofledning

<b>1</b> Inga tydliga brister/problem	<b>2</b> Oklarheter/osäkerheter	<b>3</b> Tydliga brister/problem
--	------------------------------------	-------------------------------------

Regionen har inledningsvis valt att använda MVA-metoden\* som ett verktyg för att genomföra risk och sårbarhetsanalyser. En genomförd analys ger svar på förvaltningens krishanteringsförmåga. Metodledare finns utbildade och i mån av behov kommer flera att utbildas.

\* **MVA** är en processinriktad metod för att analysera verksamhetens, förvaltningens och funktionens sårbarhet ur ett brett perspektiv. Utvecklad vid Lunds Universitet.

