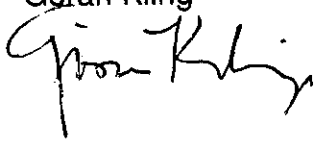
Säkerhets-handbok

Volvo Data

Gäller endast Sverige

Utgiven:	1997.01.31
Utgåva:	3
Ersätter:	1994.12.01
Distribution:	Alla anställda i Sverige
Utfärdare:	Sune Johansson Säkerhetschef
Fastställd:	Göran Kling



INNEHÅLL

POLICY

ALLMÄNT

Företagande medför risker. Riskerna är av väsentligen två slag :

- affärsrisker
- skaderisker

Till skillnad från affärsriskerna, som kan ge både positiva och negativa utfall, är skaderiskerna enbart negativa för företaget och dess medarbetare.

Inom Volvokoncernen skall eftersträvas att skaderisker

* elimineras
  alternativt
* förebygges
* begränsas
  och/eller
* kompenseras

genom medvetet och organiserat arbetarskydd respektive säkerhetsskydd och risk management.

Medan arbetarskydd inriktas på åtgärder mot ohälsa och olycksfall bland medarbetarna avser säkerhetsskydd åtgärder mot brottslig och obehörig verksamhet liksom andra hot mot medarbetare och tillgångar, såväl egendom som kunskap, information och goodwill.

SÄKERHETSPOLICY FÖR VOLVO DATA AB

Alla anställda inom Volvo Data har ansvar för att skydda de tillgångar företaget förvaltar mot skada, missbruk eller förlust.

Volvo Data har ett ansvar mot sina huvudmän att skydda företagets tillgångar. Gentemot de anställda finns ansvar för deras säkerhet. Företaget har också påtagit sig ansvar gentemot sina kunder att handha deras databehandling i överenskommen omfattning med betryggande säkerhet.

Fastställd 1997.01.31

Göran Kling

INLEDNING

BAKGRUND

Inom Volvo utvecklas, drivs och förvaltas ett stort antal informationssystem. Dessa representerar stora värden för de olika Volvoföretagens verksamhet. De flesta av dessa informationssystems bearbetning och lagring av data sker på Volvo Data. De olika Volvoföretagen har därför rätt att ställa höga krav på säkerheten gentemot Volvo Data för dessa system, både vad gäller kontinuitet i bearbetningen och möjligheter att förhindra och stoppa oauktoriserad hantering.

Företagsledningen vid Volvo Data AB beslutar om företagets säkerhetspolicy och säkerhetsregler. Verkställande direktören för Volvo Data är ytterst ansvarig för all säkerhet inom Volvo Data. Till sin hjälp har VD en säkerhetsorganisation med chefen för stabsenheten Säkerhet direktrapporterande till sig.

De överordnade säkerhetsbestämmelser som är utfärdade av koncernledningen gäller övergripande för alla företag inom koncernen.

Förteckning över publikationer inom säkerhetsområdet finns som bilaga i slutet av denna handbok.

SYFTE

Denna säkerhetshandbok syftar till att skapa förutsättningar för Volvo Datas olika enheter och staber att fungera på ett ur säkerhetssynpunkt tillfredsställande sätt.
I alla delar av verksamheten ställs krav på säkerhet i olika former. Säkerhetshandboken skall förmedla kunskap om säkerhetsområdet samt kunna fungera som uppslagsverk för alla anställda.

VEM GÖR VAD?

Det åligger **samtliga chefer** att känna till och informera sina medarbetare om Volvo Datas regler. Tystnadsplikt gäller till exempel för all Volvoanställd personal.
Information till olika media skall kanaliseras genom Informationsavdelningen, avd 2030.
Det åvilar **samtliga anställda** inom Volvo Data att vara uppmärksamma på och informera Säkerhetsavdelningen, 2010, eller säkerhetsansvarig på övriga orter, när man upptäcker något som kan vara en säkerhetsbrist.
Rapport kan ske antingen direkt (personligt , telefon osv) eller med hjälp av formaterat memo: "Rapport om säkerhetshändelse", i AT **VDSECURA** i Memo.

VEM RIKTAR HANDBOKEN SIG TILL?

Handboken riktar sig till **samtliga anställda** inom Volvo Data. Den berör alla delar av verksamheten och är ett styrmedel för effektiv säkerhet.

Denna handbok innehåller Volvo Datas överordnade regler, oberoende av ort. De specifika regler, som gäller på orter utanför Göteborg, finns i bilagorna A, B, C och D. Bilaga A för Skövde, B för Köping, C för Eskilstuna och D för Olofström.

För Volvo Datas verksamhet utanför Sverige finns Säkerhetshandboken i en engelsk version. I denna version är bilagorna A - D (Skövde, Köping, Eskilstuna, Olofström) ersatta med vad som gäller på de utländska orterna, Gent, Lyss, Daventry och Greensboro.

I den engelska versionen är de svenska lagarna och avtalen utbytta mot vad som gäller i respektive land.

HANDBOKENS INDELNING

Denna handbok är indelad i kapitel över olika säkerhetsområden.

Första kapitlet : **Organisation**. Hur säkerhet är organiserad inom dels Volvo dels Volvo Data.

Andra kapitlet : **Informationssäkerhet**. Här behandlas regler för behandling av information, säkerhetsklassificering mm.

Tredje kapitlet : **Kontinuitetsplanering**. Innehåller regler för vad som gäller vid ett avbrott och återgång till normala rutiner.

Fjärde kapitlet : **Personsäkerhet**. Detta tar upp hur man förfar vid brand och vad man bör tänka på vid tjänsteresa mm.

Femte kapitlet : **Fysisk säkerhet**, där det beskrivs allmänt vad som gäller för tillträde till Volvo Datas lokaler.

Sjätte kapitlet : **Fysisk säkerhet, tillträde till lokal** beskriver hur tillträde fås till Volvo Datas lokaler på de olika orterna inom Sverige.

Sjunde kapitlet : **Säkerhetsrutiner** vid besök, fotografering osv.

Åttonde kapitlet : **Tips i det dagliga arbetet** .

Bilagor A, B ,C och D : **Särskilda regler för de svenska orter utanför Göteborg, där Volvo Data har verksamhet.**

Nästa bilaga är : **Datalagen**. Licens och tillstånd.
Här finns regler för vad som fordras för att få registrera personinformation.

Näst sist i handboken finns en bilaga med uppgifter om vilka **publikationer**, som finns på Volvo inom säkerhetsområdet.

Sist i handboken finns 'Regler för **informationsklassning**'. Detta är ett utdrag ur Säkerhetsbestämmelser inom Volvokoncernen.

ORGANISATION

VOLVOKONCERNEN

Inom Volvokoncernen finns en gemensam bas för hur säkerhetsarbetet skall bedrivas. Dessa finns utgivna i publikationen "Säkerhetsbestämmelser inom Volvokoncernen".
Denna publikation har tilldelats cheferna på Volvo Data enligt organisationsplan och tilldelas fortlöpande nya chefer. Innehållet i denna publikation finns beskrivet i bilaga i slutet av denna handbok.

VOLVO DATA

Volvo Data har sin verksamhet på flera orter. Oberoende av ort gäller de överordnade "Säkerhetsbestämmelserna inom Volvokoncernen" och Volvo Datas Säkerhetshandbok.
Företagsledningen är den instans som anger inriktning och omfattning för säkerhetsarbetet. Företagsledningen avsätter resurser och medel för beslutade säkerhetsåtgärder. Säkerhetsaktiviteter följs upp av chef som avrapporterar till säkerhetschef. De säkerhetsåtgärder, som planeras men inte genomförs, skall ej komma till allmän kännedom.
Interna säkerhetsregler som har beslutats av Volvo Datas Säkerhetsråd finns antingen beskrivna i anslagstavla VDSECURA eller annars finns det i VDSECURA angivet var det går att finna informationen.

Chef skall informera sin personal så att de säkerhetsföreskrifter som finns i denna handbok efterlevs.

Varje anställd i företaget skall efterleva de säkerhetsbestämmelser som är fastställda. Denna Säkerhetshandbok tilldelas samtliga anställda inom Volvo Data.

Säkerhetschefen utarbetar säkerhetspolicy och säkerhetsplaner samt medverkar i olika uppdrag inom säkerhetsområdet. Tillsammans med Volvo Datas övriga organisation införs de olika säkerhetsskydden.

Säkerhetsavdelningen på Volvo Data

Säkerhetsavdelningen, 2010, är företagsledningens verkställande organ när det gäller säkerhet. Hur säkerheten skall vara utformad beskrivs i riktlinjer, regler och rekommendationer.

Ett led i detta arbete är att utarbeta och underhålla en **säkerhetshandbok**, som skall överensstämma med Volvo Datas säkerhetsplan.

Säkerhetsavdelningen ansvarar för såväl fysisk som logisk säkerhet. Avdelningen har också möjlighet att kontrollera att säkerhetsreglerna följs.

Säkerhetschefen rapporterar till verkställande direktör på Volvo Data.

Lokala säkerhetsansvariga

Inom de lokaler där central hårdvara är placerad och på de orter utanför Göteborg där Volvo Data har verksamhet, finns det lokala säkerhetsansvariga. De lokala säkerhetsansvariga ansvarar för att säkerheten fungerar enligt de regler som Säkerhetsavdelningen, 2010, utarbetar och enligt lokala regler. Årlig kontroll skall göras av avd. 2010.

Platschefen är ytterst ansvarig för säkerheten inom dessa lokaler.

Chef

Chef inom Volvo Data skall beakta säkerheten inom sitt ansvarsområde ur bland annat följande aspekter :

- Personalen skall informeras om gällande säkerhetsbestämmelser
- Personalen skall känna till utrymningsvägar och samlingsplats
- Personalen skall erhålla den behörighet som krävs för att kunna utföra sitt arbete.

När personal byter arbetsuppgift skall befogenhet till dataåtkomst och utrymmen ändras så att dessa stämmer med de nya arbetsuppgifterna. När Volvo Dataanställd personal slutar skall tillgång till datorer och tillträde till lokaler stoppas.

Rapporteringsansvar

Om något onormalt inträffar i säkerhetshänseende meddelas detta till säkerhetsavdelningen och rapporteras till närmaste chef.
För att underlätta rapporteringen finns det ett formaterat memo, Rapport om säkerhetshändelse i anslagstavla **VDSECURA,** som kan användas.

INFORMATIONSSÄKERHET

ALLMÄNT

Nedan beskrivs vad som gäller för Volvo Data, Göteborg.
För övriga orter inom Sverige, där Volvo Data har verksamhet, finns det som avviker beskrivet i bilagorna A - D.

VAD ÄR INFORMATIONSSÄKERHET

Begreppet informationssäkerhet omfattar behandling, lagring och arkivering av all information oberoende av media.

All information i lagrad form, oberoende av i vilken form den är lagrad, skall vara klassificerad så att det går att avgöra hur den skall behandlas eller arkiveras. Den information som inte har någon klassning anses som fri att användas inom företaget av alla anställda, men får **inte lämna företaget** utan medgivande av chef.

INFORMATIONSKLASSIFICERING

Inom Volvo tar Koncernsäkerhetsrådet, där Volvo Data är representerat, fram de regler som gäller för klassificering av information. Dessa utarbetade regler ges sedan ut i publikationen "Säkerhetsbestämmelser inom Volvokoncernen" och gäller som bas för alla bolag inom koncernen.

Definition av de tre informationsklasserna finns i bilaga i slutet av denna handbok.

Ansvar för klassificering

Den som är ägare till information ansvarar också för att denna klassificeras efter de regler som finns angivna.

I de fall Volvo Data förvaltar kunders information gäller den klassificering av information som kunden har gjort. Om ett specifikt säkerhetsavtal har skrivits, skall reglerna finnas angivna i detta.

När information omklassas bestäms det också från vilket datum den nya klassens regler gäller för handhavande och arkivering.

På den information som inte skall vara tillgänglig för alla anställda skall det klart och tydligt framgå vilken klassifieringsnivå som gäller.
Stämplar för klassificering av pappersinformation finns hos enhetssekretariaten.

Alla regler, som du behöver för hur information skall behandlas på ett godtagbart sätt, finns i Volvos telefonkatalog.
Dessutom finns dessa regler som bilaga i denna handbok.

LAGRAD INFORMATION, DATAMEDIA

Datorbaserad information skall skyddas av ett av Volvo godkänt säkerhetssystem. Om det rör sig om information som är klassad som kvalificerat företagshemlig, skall den också vara krypterad. Detta gäller oberoende av datortyp och media (hårddisk, diskett, tape, disk etc). Om disketter eller magnetband förvaras i datorhallar jämställs detta med låst utrymme. Om förvaring sker utanför dessa utrymmen bör speciella datamediaskåp användas. Dessa skåp skyddar också informationen om brand uppstår.

Bearbetning och lagring av personinformation får endast göras inom de regler som Datalagen ger. För närmare information se bilagan 'Datalagen. Licens och tillstånd' i slutet av denna handbok.

KUND- OCH LEVERANTÖRSINFORMATION

Vi får mycket information från kunder och leverantörer. Oftast är den inte offentlig och vi har därför ett ansvar att inte sprida den vidare. Sådan information skall betraktas som konfidentiell och behandlas på samma sätt som egen konfidentiell information. Ett sekretessavtal mellan Volvo Data och den andra parten är lämpligt för att reglera vad som skall gälla.

UTLÄMNANDE OCH MOTTAGANDE AV KONFIDENTIELL INFORMATION

Vid utlämnande av konfidentiell information skall det klart framgå för mottagaren vilken klassning som gäller och vad detta innebär ifråga om handhavande, arkivering osv. När konfidentiell information lämnas till person eller företag utanför Volvo Data, skall en sekretessförbindelse upprättas, där det specificeras vilka regler som gäller.

När konfidentiell information mottas av anställd på Volvo Data, skall det också klart framgå hur informationen skall handhas. Konfidentiell information från annat bolag inom Volvo följer de säkerhetsregler, som är uppsatta för koncernen. För konfidentiell information från externa företag eller personer skall det framgå genom avtal eller annan överenskommelse vilka regler som gäller.

Regler och blankettförslag för sekretessförbindelser finns i Säkerhetsbestämmelser inom Volvokoncernen. Mall för säkerhetsavtal finns på Volvo Datas Säkerhetsavdelning.

SKROTNING ELLER FÖRSÄLJNING AV PERSONDATORER.

När en persondator försäljs eller skrotas skall den information som är lagrad på hårddisken förstöras.
Vid skrotning skall hårddisken plockas ur och förstöras innan datorn lämnar företaget.
När datorn säljs skall hårddisken överskrivas så många gånger att det är mycket svårt för köparen att återfinna den lagrade informationen.
Rutiner för hur detta skall göras finns i anslagstavla VDSECURA.

HUR SÄKRAS INFORMATION

I denna handbok finns de överordnade reglerna för hur information skall hanteras ur säkerhetssynpunkt.

De hjälpmedel (t ex program, krypteringsutrustning, smartcard) som behövs för ADB-baserad säkerhet kommer att finnas angivna i AT **VDSECURA** i Memo.

Under ovan nämnda anslagstavla kommer antingen hjälpmedlet vara beskrivet eller vem/vilken instans som ansvarar och ger stöd.

GRANSKNING OCH REVISION

För att säkerställa att de olika verksamheterna inom Volvo Data följer de regler och riktlinjer, som dels är beskrivna i detta kapitel, dels i publikationen Säkerhetsbestämmelser inom Volvokoncernen, utför Säkerhetsavdelningen granskning och revision.

Denna granskning och revision består av:

Att systemutveckling i AU-modellens olika faser (förstudie, projektering, genomförande och förvaltning) väljer rätt skydd för information samt att lagar och förordningar följs.

Att vid överföring av information de regler som finns angivna i Säkerhetsbestämmelser inom Volvo koncernen samt externa krav (t ex Tullen, banker) följs.

Att dataregister har backupdata om den datorhall som produktion normalt körs i blir utslagen.

Att konfidentiell information hålls inlåst när den ej används.

Att behörighets- och accessregler är rätt uppdaterade.

Att påpekade brister blir åtgärdade.

I bilaga H finns beskrivning över arbetsgången vid säkerhetsrevisioner inom Volvo Data.

INFORMATIONSBEHANDLING

Nedan följer exempel på hur informationen skall behandlas i enlighet med den klassning som har gjorts och som fordras för att säkerställa behandling av information.

Arbetsplats

Lås in konfidentiell information innan du lämnar arbetsplatsen. Informationen kan vara i pappersform eller på databärande media.

Lösenord

Lösenord får inte förvaras synligt, i olåsta skrivbord, under skrivbordsunderlägg, på skärmar etc. Det är **förbjudet** att koda in lösenord på funktionstangenter eller i program.

Datalistor

Information från skrivare skall hämtas till arbetsplatsen och inte ligga kvar till allmänt beskådande. Vi har idag inte någon speciell kontroll av vem som är behörig att komma in i printerrum etc. Alla som har tillträde till Volvo Datas lokaler har i regel också tillträde till de ut rymmen, där skrivarna står. "Tänk efter före" om du skriver ut konfidentiell information! Kontrollera att hela dokumentet har skrivits ut!

Inter-/IntraNet

Information med informationsklass "Kvalificerad företagshemlig" eller "Företagshemlig" får inte lagras så att den är åtkomlig från Internet eller Intranet förrän av Koncernsäkerhetsrådet godkänt behörighetssystem eller godkänd krypteringsmetod har installerats.

Inkommande/utgående post

Information, som sänds inom och utom företaget, skall behandlas enligt de regler som framgår av Säkerhetsbestämmelser inom Volvokoncernen. Dessa finns även beskrivna i Volvos telefonkatalog.

Om du väntar konfidentiell information via postdistribution, hämta in denna så snart som möjligt. Det har hänt att ankommande post som innehållit programvara eller delar till persondatorer har "försvunnit" så var uppmärksam. Tyvärr är dessa paket ofta märkta på utsidan med både leverantör och vad innehållet är.

Lägg inte konfidentiell information i avgående post efter det att sista hämtningsturen gått för dagen och speciellt inte vid veckoslut.

Vid elektronisk överföring av information skall de regler följas som finns i Säkerhetsbestämmelser inom Volvokoncernen.

Distribution

De bestämmelser som finns för distribution av sekretessbelagd information finns dels i "Säkerhetsbestämmelser inom Volvokoncernen" dels i Volvos telefonkatalog.

Arkivering

Konfidentiell information skall alltid förvaras inlåst i godkända skåp när den ej används.

Makulering

Information som inte är klassad som konfidentiell kan makuleras i de öppna containers som finns utplacerade. Övrig information skall läggas i de låsta sekretesscontainers som är avsedda för makulering av konfidentiell information.

Telefax	Mottagning av dokument som kommer med telefax skall hållas under uppsikt. Sändning av dokument skall vara bevakad. Kvalificerat företagshemliga dokument får endast sändas med godkänd krypterad telefaxmetod.
Terminaler	Logga av eller sätt terminal eller arbetsstation i Stand-by när du lämnar arbetsplatsen och slå alltid av strömmen vid arbetsdagens slut. Säkerhetsrutiner och viruskontroller skall följas enligt de rekommendationer som finns.
Distansarbete	Säkerhetsregler finns angivna i AT VDSECURA i Memo.
Kryptering	Regler finns i AT VDSECURA i Memo.

PERSONAL SOM INTE ÄR ANSTÄLLD PÅ VOLVO DATA

I samband med att personer, icke Volvo Data-anställda (t ex praktikanter och konsulter), börjar sitt arbete skall de skriva på en Sekretessförbindelse. När det gäller personal från externt företag skall det finnas en sekretessförbindelse påskriven av VD för företaget eller av honom utsedd representant. Dessa förbindelser specificerar vilka regler som gäller för den information de får ta del av under arbetstiden på Volvo Data.

En skriven sekretessförbindelse ger möjlighet att lagligt kräva ersättning om någon bryter mot dessa regler.

Blankett och regler för sekretessförbindelse finns i "Säkerhetsbestämmelser inom Volvokoncernen". Dessa blanketter kan rekvireras från Säkerhetsavd. 2010.

De användaridentifikationer som lämnas ut till tillfällig personal skall begränsas till den period, anställningen är avsedd att vara. Användarid får maximalt gälla ett år. Om behov kvarstår efter denna tid skall tillstånd förnyas av den chef som ansvarar för personen.

Vid arbetsperiodens slut skall användarid och behörighet tas bort.

Det åligger chef att, innan den tillfälligt anställdes uppdrag påbörjas, tillsammans med denne ha en genomgång av de säkerhetsregler som gäller satta i relation till kommande arbetsuppgifter.
Efter att arbetsuppgiften är slutförd och den tillfälligt anställde lämnar företaget skall chef se till att lagrad information tas till vara eller rensas bort. Chefen skall också gå igenom vilken information som ej är tillåten att föra vidare utanför Volvo Data.

ANSVARIG FÖR DATAANLÄGGNING

Med en dataanläggning menas här allt från en stordatoranläggning till en enmans arbetsstation.

På en större datacentral är det normalt chefen för anläggningen som ansvarar för säkerheten. På en mindre anläggning (t ex en persondator) bär användaren ansvaret.
Dock har varje anställd skyldighet att rapportera upptäckta säkerhetsbrister och ansvar för att erhållen information ej kommer i orätta händer.

Om satta regler inte efterlevs, innebär ansvaret rapportskyldighet till både chef och säkerhetschef.

DATAVIRUS

Akut

Om du misstänker någon form av datavirus, kontakta ditt **Närstöd** (gäller alla typer av persondatorer). Om du har en dator som är hopkopplad med andra inom ett nätverk, gör ingenting förrän du fått hjälp, för att förhindra att viruset sprider sig till de andra datorerna inom nätet.
Sänd alltid information om det inträffade till memo **VD.VIRUS**.
För senaste information om hur du skall förfara se Anti Virusgruppens information i IntraNet:
ftp://nike.volvo.se/VirusProtection/DrSolomon/cmd/virus1.htm
eller i anslagstavla VDSECURA.

Förebyggande

De som har en mindre anläggning typ persondator skall följa de regler, som finns utgivna för hur förekomst av datavirus upptäcks och hur man skyddar sig mot det. **Kontakta alltid ditt Närstöd innan du installerar ett nytt program!**

KONTINUITETSPLANERING

ALLMÄNT

Varje verksamhetsområde skall ha dokumenterat i en handlingsplan vad som skall göras i det fall något inträffar, allt från en mindre skada till en allvarlig kris.

Denna handlingsplan eller kontinuitetsplan förvaras brandsäkert, eller i två oberoende lokaler, så att den alltid är tillgänglig.

Syftet med kontinuitetsplanen är att det skall finnas dokumenterat:

- Vem som ansvarar för olika delar av uppbyggnadsarbetet (telefonnummer etc).
- Vem som är ställföreträdare och var dokumentationen finns när ordinarie ansvarig inte är anträffbar. Ställföreträdare skall vara väl förtrogen med kontinuitetsplanen
- Leverantörer av mjukvara och hårdvara.
- Vad som behöver göras för att komma tillbaka till normala rutiner efter en skada
- Var det går att anskaffa ersättningsresurser
- Hur utrustning som är av vital betydelse går att ersätta så att verksamheten inte äventyras

Målet är att komma igång så fort som möjligt.

REGLER

Målet med planen är att verksamheten skall komma igång inom den tid som avtalats med kund och att rätt data finns tillgänglig.

Kontinuitetsplanering är ett verksamhetsansvar och varje avdelning och stab på Volvo Data skall medverka i framtagning av plan, som täcker allt ifrån normala rutiner till rekonstruktion av resurser i ett nödläge.

Varje chef skall hålla kontinuitetsplanen uppdaterad i enlighet med sitt verksamhetsområde.

Inom respektive verksamhetsområde skall finnas en handlingsplan för hur den egna verksamheten skall återskapas efter skada.

Alla kontinuitetsplaner har informationsklass : "Företagshemlig" och skall behandlas enligt regler för denna klass.

För dataregister som är av vital betydelse för Volvos överlevnad och som förvaltas av Volvo Data skall backup finnas. Denna backup skall förvaras på ett sådant sätt att även om en datorhall slås ut skall backupdata finnas.

PRIORITERING

Om någon av datacentralerna havererar eller någon av datorerna slås ut skall det finnas avtalat med kunderna i vilken ordning applikationssystemen skall återstartas. Denna uppstartsordning kan variera beroende på tidpunkt.

Ett system finns (benämnt KOPLA) för prioritering av resurser.

HAVERIORGANISATION

I Volvo Datas överordnade kontinuitetsplan finns en haveriorganisation som har till uppgift att leda arbetet för att komma tillbaka till normal verksamhet.
I denna organisation finns representanter från företagsledningen och de olika enheterna. I detta överordnade organisationsarbete ingår bl a att anskaffa maskiner, lokalyta, el, kyla och kommunikationslinjer. Tillsammans med kunder bestäms i vilken ordning de prioriterade systemen skall startas.
I denna organisation ingår ej att kontrollera att applikationsdata finns tillgänglig.

Igångsättning

Varje verksamhetsområde skall definiera vilka regler som skall gälla för igångsättande av sin haveriorganisation och sitt restaureringsarbete.

AVVIKELSE

Alla förändringar som görs i Volvo Datas verksamhet och som påverkar kontinuiteten skall vara omhändertagna ur kontinuitetssynpunkt.

Är förändringen ej kontinuitetsplanerad vid införandet skall Företagsledningen skriftligt ha givit tillstånd att avvikelse får ske.

PERSONSÄKERHET

Det finns en hel del vi skall göra för att stärka personsäkerheten på Volvo Data. Här har vi delat upp ämnet i fem områden:

Arbetsplatssäkerheten,
Säkerhet vid resor,
Säkerhet vid möten och konferenser,
Akut sjukdom eller olycksfall
Övrigt.

Beroende på ort, där Volvo Data har verksamhet, gäller olika telefonnummer, samlingsplatser etc. Nedan beskrivs vad som gäller Volvo Data, Göteborg.
För de övriga orterna Skövde, Köping, Eskilstuna och Olofström finns det som avviker beskrivet i bilagorna A, B, C och D.

ARBETSPLATSSÄKERHETEN

På en arbetsplats kan många olyckor inträffa. Det finns mycket, som du själv kan göra, som t ex hålla ordning på sladdar och kablar. De utgör stor risk för snubbling om de inte hålls undan från ytor där vi går. Elkablar kan bli deformerade och förorsaka brand eller personskador vid överslag.

Papper, kartonger, plaster och annat som inte behövs i det dagliga arbetet skall städas bort då de kan vara till hinder vid utrymning. De ger också näring till en eventuell brand.

På varje våningsplan finns det en utrymningstavla som ger dig information om utrymningsvägar och samlingsplats.
Gör dig familjär med dessa utrymningsvägar **innan något händer.** Den gång du måste komma ut kan det vara för sent.

Om det brinner

I de flesta av Volvo Datas utrymmen finns det branddetektorer. Automatiska brandlarm, som avger signal och varnar oss om att brand har uppstått, saknas dock på många ställen.

Om brand uppstår gäller : **Rädda liv - Varna andra - Stäng dörrar - Försök släcka.**
Kontrollera alla utrymmen och informera om vad som hänt. Glöm ej meddela sekretariatet, som sprider informationen vidare till övriga våningsplan. Det åligger chef att informera sina anställda om vilken typ av brandlarm som finns på arbetsplatsen.

Larma brandkår och vakt. Beroende på ort gäller olika telefonnummer. Dessa telefonnummer skall finnas uppsatta på telefon (etiketter) och finns i Volvos internkatalog. **Om du är osäker på telefonnumret, använd 00112**
Obs ! 00 först, externnummer.

Använd brandlarm om det finns, eftersom det går snabbare än att telefonera. Stanna om möjligt kvar vid brandlarmet eller möt brandkåren och visa vägen.

Brandlarm, där sådana finns, är en pulserande eller långt utdragen ringsignal, som skall göra oss uppmärksamma på att brand har uppstått.
Släck eller förhindra brandens spridning - **Tag inga onödiga risker !**

Se till att dörrar och fönster stängs så att branden inte sprider sig.

Om utrymning krävs gäller följande:

- Utrym lokalerna enligt bestämda utrymningsvägar, om ej annat meddelas. Utrymningsplan finns på varje våningsplan.
- Gå till angiven samlingsplats (markerad på utrymningstavlan).
- Se till att du blir registrerad på samlingsplatsen.
- Chef kontrollerar om någon saknas och anmäler detta till brandbefäl.
- Stanna kvar på samlingsplatsen för vidare information.

Vid utrymning: ANVÄND ALDRIG HISS !

Utrymningsvägar får inte blockeras. Detta gäller även de gångar, som leder till och från arbetsplatsen.

SÄKERHET VID RESOR

Volvo Data-anställda med unik kompetens inom samma område bör inte resa tillsammans. Om de råkar ut för en olyckshändelse medför detta förutom den personliga skadan även att Volvo kan komma att skadas.

Lämna aldrig ut till någon om att medarbetare är bortrest utan ge endast uppgift när han/hon är tillbaka på arbetsplatsen. Dina uppgifter kan dels leda till inbrott i bostaden dels är vi alla lite sårbarare när vi är hemifrån.

För att skydda dig när du är ute och reser kan du före resan låna en "Reseskyddskudde" som innehåller bl a brandvarnare, täcktape, ljusstav och skyddshandskar.
Reseskyddskudden lånar du av avd. 2010.

Företagsinformation skall alltid förvaras under uppsikt. Vid förlust av information skall enhetschef och säkerhetsavdelning kontaktas. Det är viktigt att du vet vilken information du har förlorat, så att åtgärder kan vidtas för att förhindra skada.

Utlandsresa

Innan du reser tänk på att du har möjlighet till att få hjälp av säkerhetsansvarig med:

- Råd till utlandsplacerade
- Omvärldsanalyser
- Aktuell risksituation i respektive land
- Dagsaktuell information vid resans start

Var noga med att beställa biljett av auktoriserad resebyrå. Innan du reser - se alltid till att du har utländsk valuta samt resecheckar med dig. **Växla aldrig pengar på gatan**. Undvik att visa dina pengar. Använd helst kontokort/kreditkort. Lär dig att använda mynttelefonapparater och bär på dig

nödvändiga växelmynt eller betalkort. Bär på dig en lista över lokala telefonnummer till polis, sjukhus, brandkår, företagets lokala representant, konsulatet etc.

Var vaksam så att inte du eller ditt bagage blir ofrivilliga bärare av sådant som kan medföra straff tex sprängämnen eller narkotika. Ha dina förvaringsutrymmen och väskor låsta samt under uppsikt. Bär aldrig annans bagage genom tullen.

Vid resor utanför Norden kan du kontakta Säkerhetsavdelningen, 2010, för råd beträffande resmålet.

För sin egen säkerhet bör varje enskild person, som skall ut och resa ta med sig personlig skyddsutrustning. I broschyren "Volvos säkerhetsråd till utlandsresenärer" finns tips som du kan ha nytta av.

Om något händer

Om något oförutsett skulle inträffa under resan kan du förutom vad som anges i "Volvos säkerhetsråd till utlandsresenärer" kontakta Volvo Datas Säkerhetschef:
Tefonnummer till ansvariga går att få genom:

- Vakten PV-porten tfn 031-599000.
- Volvos Växel tfn 660000 eller 590000.
- Volvo Datas Helpdesk tfn 667060.

SÄKERHET VID MÖTEN OCH KONFERENSER

Vid möten förlagda **utanför** Volvos områden kan säkerhetsansvarig kontaktas för hjälp med:

- utvärdering av platsen ur säkerhetssynpunkt
- avlyssningsrisker
- bevakningsförfarande
- personskydd

Ta för vana att alltid ta med dig allt material tillbaka, gäller även det du skrivit på blädderblock etc. Om du använder "svarta tavlan", torka av den innan du lämnar lokalen.

AKUT SJUKDOM ELLER OLYCKSFALL

Vid akut sjukdom eller olycksfall och hjälp behövs, skall **alltid** vakten PV-porten kontaktas, **telefon 99000**. Meddela vakten vad som har hänt så sköter de om att sjukvårdspersonal och ambulans kallas.
Vakten visar vägen för ambulansen till olycksplatsen.

ÖVRIGT OM PERSONSÄKERHET

Vid hot, telefonterror eller kidnappning, kontakta:

- Larmtelefon 031- 59 90 00
- Volvo Datas säkerhetschef via Volvos telefonväxel.
- Gör egna iakttagelser som t ex dialekt, bakgrundsljud, röstläge, mans-/kvinnoröst.

FYSISK SÄKERHET

ALLMÄNT

Volvo Datas säkerhet skall vara sådan att anställda, kunder och leverantörer känner förtroende för den. Anställda skall känna att de har en säker arbetsplats.

Kunderna skall lita på att Volvo Data tar hand om deras information på ett professionellt och säkert sätt.

Leverantörer skall känna förtroende för oss så att Volvo Data får vara uttestare av kommande produkter, som gör att Volvo-koncernen tidigt kan använda dessa och därigenom få konkurrensfördelar.

Allt mer av koncernens information lagras på datamedia. Volvo Data har genomfört en omfattande konsolidering av koncernens datacentraler. Detta innebär en koncentration av datorkraften till ett fåtal platser. Samtidigt ökar kraven på att säkerhetsfrågorna löses på ett betryggande sätt såväl inom datacentralerna som för kommunikation till och från dem. Detta ställer krav på oss och vi måste alla hjälpa till så att Volvo Data kan erbjuda en hög säkerhet.

Upptäcker du brister i vårt säkerhetsskydd, meddela säkerhetsavdelningen eller din chef! Misstanke om brott, t ex stöld, måste alltid rapporteras.

Varje enskild medarbetare har ett ansvar för att Volvo Datas säkerhetsbestämmelser följs.

Vid nyanställning eller då anställd byter arbetsplats åligger det chef på berörd avdelning att visa utrymningsvägar och samlingsplats. Detta gäller också då den anställde skall ha tillträde till utrymmen utöver arbetsplatsen.

För ej Volvo Data-anställd, som fått eget passerkort till Volvo Datas lokaler, är det **tillståndsgivarens ansvar** att informera om och visa utrymningsvägar och samlingsplats. Tillståndsgivare måste tillhöra befogenhetsgrupperad personal.

Besöksmottagare ansvarar för sina besökare under tiden besöket varar, dvs från hämtning till avlämning i reception/utgång.

ID-KORT

Volvo Data-anställd.

Samtliga Volvo Data-anställda erhåller ett personligt ID-kort med foto (passerkort) till Volvo Data i Göteborg.

När anställning upphör **skall** kortet lämnas till Personalavdelningen. Detta är ett chefsansvar.

Pensionär.

Pensionärer har samma typ av ID-kort som övriga anställda. Dessa kort kan dock inte användas i kortläsare då de saknar kod. Innehavaren kan endast få tillträde genom reception.

Mot uppvisande av detta kort kan pensionärer utnyttja de rabatter, i olika affärer, som kommer Volvo-anställda till del.

Dessa ID-kort utdelas i samband med pensionering.

Familjemedlemmar/barn

Anställd som vill ha med sig familjemedlemmar till arbetsplatsen skall ha tillstånd av chef. Att ta med barnen till arbetsplatsen sker på den anställdes egen risk. Om en olycka sker har Volvo Data inga försäkringar som gäller barnen.
Sjuka barn bör ej tas med till arbetsplatsen.

Sekretesserinran

Vid kvittering av ID-kort skall samtidigt blanketten **Sekretesserinran ID-kort Volvo Data** undertecknas. I denna sekretesserinran finns information om vad som gäller för ID-kort.

Blankett Sekretesserinran finns återgiven på nästa sida.

Sekretesserinran ID-kort Volvo Data

Efter att ha skrivit under denna sekretesserinran, får du ett ID-kort som är personligt och som samtidigt är ett passerkort till Volvo Datas lokaler.

Du påtar Dig också ett ansvar för :

- Att endast använda ID-kortet för egen passage och för sådana personer, som Du säkert vet har tillträde till Volvo Datas lokaler. Kortet får användas för insläpp av egen/egna gäst(er). Du är ansvarig för gästen under tiden besöket varar.

- Att endast vistas i de lokaler som det finns tillbörlig anledning till
- Att förvara ID-kortet så att det inte kommer i orätta händer

- Att inte skriva upp eventuell kod på kortet

- Att bära kortet väl synligt i de lokaler där detta påfordras och visa upp kortet utan anmaning för receptionist eller vakt
- Att omedelbart anmäla förlust av ID-kortet till:
  Vakt PV tfn 031-599000. Gäller hela dygnet alla dagar året runt

- Att i direkt anslutning till att Din tjänst vid Volvo Data upphör, lämna ID-kortet till Din personalkontakt eller chef. För icke Volvo Dataanställd personal återlämnas ID-kortet till utfärdaren.

- Att Du följer gällande säkerhetsföreskrifter, sekretessbestämmelser och skyddsbestämmelser

- Att ej fotografera inom Volvos område utan tillstånd

Jag är införstådd med ovanstående och att överträdelser kommer att beivras.

.....den / 199

.....
namn avd anstnr

När du kvitterat denna Sekretesserinran skall du ha en kopia, som du skall spara, så du vet dels vilket ansvar du har påtagit dig dels vad du skall göra om ditt ID-kort förkommer.

Var rädd om Ditt ID-kort, eftersom det finns personuppgifter på det, som om de missbrukas kan orsaka dig personlig skada.

FYSISK SÄKERHET, TILLTRÄDE TILL LOKAL

ALLMÄNT

Beroende av ort inom Sverige, där Volvo Data har verksamhet, är det olika regler som gäller för tillträde till lokaler. Nedan beskrivs de regler som gäller för Volvo Data, Göteborg. För de övriga orterna, Skövde, Köping, Eskilstuna och Olofström finns det som avviker beskrivet i bilagorna A, B, C respektive D.

TILLTRÄDE TILL LOKALER

För att skydda Volvo Datas verksamhet är de flesta lokaler utrustade med passagekontrollsystem. Alla anställda har ett **personligt** ID-kort (passerkort) med foto. Detta passerkort ger tillträde till Volvo Datas lokaler genom att visa det för vakt/receptionist eller genom validitetskontroll i kortläsare.

Volvo Datas interna utrymmen är indelade i olika zoner beroende på vilken verksamhet som bedrivs där. Tillträde till de olika zonerna bestäms av arbetsuppgiften. Tillträde till driftsavdelningen fordrar utöver passerkort även en kod. Till dessa utrymmen har, **när arbetet så fordrar**, de anställda, servicepersonal från hårdvaruleverantör samt underhållspersonal för kyla, el, vatten etc, tillträde.

Samtliga Volvo Datas utrymmen räknas som interna områden förutom de lokaler som användes för utbildningsändamål i DABV.

I de utrymmen där det finns automatisk sprinkleranläggning får **inte** någon form av sändande utrustning användas. Dessa kan utlösa sprinklersystemet. Se även under rubrik "Sändande utrustning" i kapitel Säkerhetsrutiner.

Generellt gäller att tillträde till datorhallar eller andra utrymmen, som har automatisk eldsläckningsanläggning, fordrar att man genomgått en speciell brandskyddsutbildning. Denna får ej vara äldre än tre år vid tillståndsgivningen. Sådana kurser anordnas varje år.

ID-KORT

Volvo Data-anställd.

Beroende på arbetsuppgifterna får den anställde tillgång till olika utrymmen.

Volvo Data-anställd, som glömt att ta med sitt ID-kort till arbetet, kan låna ett temporärt kort av receptionen, DABV. Detta kort ger tillträde till den egna arbetsplatsen, men inte till övriga utrymmen.

Tjänstledig

Chef avgör om en tjänstledig medarbetare skall ha tillgång till sin arbetsplats under tjänstledigheten. Om **inte** skall detta meddelas Receptionen DABV, som ombesörjer att passerkortet spärras.

Volvo-anställd

De Volvo-anställda, som har täta kontakter med Volvo Data eller genom sin befattning (t ex AU-ansvarig) behöver komma in på Volvo Data, kan få personliga ID-kort (med foto). Dessa kund-ID-kort ger tillträde till Volvo Datas kontorsutrymmen vardagar klockan 08.00-16.30. (Tiden kan förlängas om speciellt behov finns).

Vissa Volvo-anställda, som för sitt arbete behöver komma in i Volvo Datas lokaler, har tillträde dygnet runt. Detta gäller för tex dem, som utför biltransporter. För dessa gäller att de endast får komma in i den zon som är lägst klassad. Ett undantag är de från Underhållsavdelningen som sköter kyla, el, vatten etc. De har tillträde till samtliga utrymmen i VAK, DA, DB, Buss, VTV och PVSV. För alla ej Volvo Dataanställda gäller att tillträde endast får ske när arbetet så fordrar.

Konsulter m fl

Konsulter, entreprenörer, praktikanter och leverantörer som utför arbete i Volvo Datas lokaler skall ha samma typ av ID-kort som Volvo Data-anställd om arbetet omfattar mer än 14 dagar. För arbeten mindre än 14 dagar kan temporärt kort lånas av reception, DABV, efter det att chef på berörd avdelning gett tillstånd. Tillståndsgivare måste tillhöra befogenhetsgrupperad personal. (Se vilka krav som ställs under **ALLMÄNT** i början av detta kapitel).

Beställning av ID-kort

Framställning av underlag till ID-kort för icke Volvo Data anställd personal, sker genom att kopiera från AT VDSECURA i Memo "Ansökan tillfälligt ID-kort".

I ansökan om ID-kort skall följande information lämnas:

- Vilket företag som konsult, entreprenör etc kommer från
- Namn och personnummer.
- Hur länge ID-kortet skall gälla (max 1 år med möjlighet till förlängning om behov finns)
- Till vilka utrymmen kortet skall gälla

När underlaget är klart meddelar utfärdaren den som skall ha ID-kort att komma till Receptionen DABV för fotografering. Efter det att fotograferingen är klar skall kortet förses med kod, registreras och inplastas. Detta tar 2-3 dagar och sedan finns det för avhämtning i Receptionen DABV.
Det är tillståndsgivarens skyldighet att se till att ID-kortet återlämnas när arbetet upphör.

Kategorier av ID-kort

I nedre högra delen av ID-kortet anges innehavarens typ av kontakt med Volvo Data t ex pensionär, konsult, leverantör, entreprenör, kund etc.

Besökare

Varje Volvo Data anställd har rätt att ta emot besökare i tjänsten. Om besök sker dit inte alla Volvo Data anställda har tillträde fordras chefs tillstånd.

Besök i datorhallar och modemrum är inte tillåtet utan tillstånd av enhetschef på driftsavdelningen eller av företagsledningen. Det finns ett bildspel, som visar hur det ser ut i dessa utrymmen. Om du är intresserad av att visa dina besökare detta bildspel, kontakta avd. 2170.

Den som tar emot besök är också ansvarig för den besökande. Besökare hämtas och lämnas vid receptionen.

SÄKERHETSRUTINER

ALLMÄNT

Nedan beskrivs vad som gäller för Volvo Datagruppen. Dessutom finns det för övriga orter inom Sverige, där Volvo Data har verksamhet, beskrivet det som avviker i bilagorna A - D.

Behörighet

Som medel att skydda vår verksamhet finns bl a tekniska hjälpmedel såsom TV-övervakning, passagekontrollsystem, inbrottslarm och behörighetskontrollsystem.

Även om vi har många hjälpmedel beror det "till syvende och sist" på oss anställda, om vi skall ha en bra säkerhet.

Det är förbjudet att släppa in obehöriga personer till Volvo Data.

Det är förbjudet att använda nödvred eller att ställa upp dörrar och fönster, som ingår i brand- eller tillträdesskydd. Nödvred får självfallet endast användas i nödsituationer.

Det är förbjudet att bereda sig, eller försöka bereda sig, tillgång till konfidentiell information och data, som inte behövs för att utföra arbetsuppgifterna.

Arbetsplatsen

Den tid som tillbringas på arbetsplatsen är inte mer än 25 - 30 % av årets timmar. Om du lämnar din terminal, arbetsstation eller andra elektriska apparater med strömmen på när du inte är här kan de utgöra en brandrisk. En annan orsak att slå av strömmen är att vi alla måste vara rädda om vår miljö och även kostnaden för företaget. En persondator har en effekt på ca 500 W, vilket innebär att den på en helg kan förbruka 30 kWh.

Slå alltid av strömmen på de apparater du har hand om när du lämnar arbetsplatsen för dagen

Nyanställning

Vid nyanställning skriver den nyanställde på **Tystnadsplikt**, vilket innebär ett åtagande att följa gällande regler rörande sekretess.

Studiebesök

Tillstånd söks och utfärdas av informationsavdelningen, avd 2030.

Fotografering och kameror

För att få fotografera inom Volvo Datas lokaler erfordras tillstånd från Informationsavdelningen 2030. Kamera får ej medföras om tillstånd saknas.

Sändande utrustning

I datorhallar och modemrum får ej sändande utrustning användas eftersom det finns risk att bland annat släckningsanordningar kan utlöses, vilket leder till driftavbrott.

För att få **använda mobiltelefon** oberoende av typ (NMT 450, NMT 900 och GSM) inom Volvo Datas lokaler **fordras tillstånd av chef** på den avdelning du vistas.
Dessa mobiltelefoner har en uteffekt av 1W eller däröver och följande skador har rapporterats inom Volvokoncernen:

- o felaktiga värden på elektriska instrument och givare
- o störning på provutrustning
- o störd Memo-kommunikation
- o falska brandlarm utlösta p g a störda detektorer
- o reläskydd i ställverk utlöst med fabriksstillestånd som följd

En mobiltelefon är **alltid** aktiv när den är påslagen d v s den sänder för att hålla kontakt med radionätet, även när man inte pratar i telefonen.

Från avdelning 2010 kan beställas en broschyr över vilka regler som gäller för sändande utrustning.

Köp eller lån av inventarier

För att få ta ut inventarier tillhörande Volvo Data skall tillstånd av ägaren finnas.
Blankett TY 1001-8 skall användas. Denna blankett finns under AT, VDSECURA, i Memo. På blanketten anges om objektet är **köpt eller lånat.**
Detta gäller även när bärbar terminal, telefon etc lånas vid jour eller om arbete skall utföras utanför Volvo Datas utrymmen. Om ingen lånehandling finns, gäller ej Volvo försäkring (enligt Volvos Risk Manager).

Ett alternativt handlingssätt är att inventarieägaren tecknar en egen försäkring på inventariet. Denna försäkring tecknas tillsammans med Säkerhet, avd. 2010. Kostnaden för försäkringen betalas av inventarieägaren.

Stöld

Stöld av **personlig egendom** skall omedelbart anmälas till polismyndighet. Spärrning av kontokort av olika slag bör ske så snart som möjligt. Stölden skall så snart som möjligt även anmälas till säkerhetschef, avd 2010, som med hjälp av PVs utredningsavdelning gör utredning.

Volvo Data ansvarar ej för anställdas personliga egendom.
Ersättning för stulen egendom, som tillhör företagets anställda, kan ej fås av Volvo Data.
Det är med andra ord upp till var och en att se till sin egendom och sitt försäkringsskydd.

Stöld av Volvo Datas egendom skall snarast rapporteras till kostnadsställeansvarig och säkerhetschef.
För att förhindra att stöldbegärliga varor stjäls skall dessa före de tas i bruk märkas med **'Volvo Data'** eller på annat sätt som visar att de tillhör företaget (t ex företagets juridiska nummer). Typ av stöldbegärliga varor är bärbar dator, PC, Macintosh, TV-monitor, sändande utrustning, video och stereo. För att göra det möjligt att få tillbaka stöldgods skall tillverkningsnummer och fabrikat noteras vid uppacknings/installationstillfället.

Om din terminal eller persondator har ett ID för att kommunicera med övriga datorer inom Volvokoncernen, se till att detta ID snarast blir spärrat om maskinen blir stulen.

Vapen

Vapen får **ej** tas med eller förvaras i Volvo Datas lokaler.

Alkoholhaltiga drycker och narkotiska preparat

Alkoholhaltiga drycker får ej tas med till Volvo Datas lokaler utan tillstånd från Volvo Datas Säkerhetschef.
Narkotiska preparat får inte förekomma inom Volvo Datas lokaler.

Rökning

Rökning inom Volvo Datas utrymmen är endast tillåten i de pausutrymmen, som är märkta "Rökning tillåten" I alla övriga lokaler är rökning förbjuden under alla tider på dygnet.

Bilparkering

Parkering av bilar får endast ske på de platser som är markerade. Det är förbjudet att parkera på tillfartsvägar. Dels försvåras framfart för eventuella utryckningsfordon dels uppstår onödiga krockar och eventuellt personskador. Samma lagar som gäller ute i samhället gäller naturligtvis inom Volvo.

Händelserapport och åtgärd

När något misstänkt eller oegentligt upptäcks, såsom uppställda fönster, dörrar, personer som inte bör vistas i vissa utrymmen etc, skall detta snarast rapporteras till vakten PV-porten, telefon 99000 och under kontorstid även till säkerhetschef Volvo Data.

TIPS I DET DAGLIGA ARBETET

Till sist kommer några praktiska tips i det dagliga arbetet.

Lås in och håll tyst

Konfidentiell information, som lagras i datorsystem, skall skyddas mot obehörig åtkomst och bör vara krypterad. Om informationen är 'kvalificerad företagshemligt' skall den alltid vara krypterad. Konfidentiella handlingar skall förvaras inlåsta i säkerhetsskåp eller motsvarande. Kontrollera att du inte har hemlig information liggande framme när du lämnar arbetsplatsen. Tänk på vad du berättar för utomstående, vänner och bekanta. Samtala inte om konfidentiella uppgifter på sådan plats där andra lätt kan ta del av samtalet.
Telex, telefax och biltelefon får inte användas för konfidentiell information om inte kryptering användes.

Skydda försändelser

Interna konfidentiella försändelser skyddas mot obehörig läsning genom att läggas i kuvert, som förseglas med speciell säkerhetstejp eller speciella kuvert som du kan rekvirera från Sekretariat HD3N. Beroende på vilken typ av handling (kvalificerat företagshemligt, företagshemligt eller företagsintern) som skall distribueras gäller olika tillvägagångssätt. I Volvos interna telefonkatalog finns en förteckning över hur du skall göra i de olika fallen.

Tänk på vad du kastar

Konfidentiella handlingar får inte läggas i papperskorg utan skall förstöras i pappersdestruktör eller läggas i låsbara sekretesscontainers. Detta gäller även karbon, disketter etc.

Arbetsstation

Konfidentiell information får inte lämnas kvar synligt på bildskärmen. Logga av eller använd passwordskyddad skärmsläckare, när du lämnar din arbetsplats. Datamedia med konfidentiell information skall förvaras i säkerhetsskåp eller helst i datamediaskåp som tål brand. Tänk igenom din backup situation för data och program. Är du osäker på hur du skall göra med back-up, ta kontakt med ditt Närstöd (gäller alla typer av persondatorer).

Kopior

Konfidentiell information får kopieras först efter utfärdarens medgivande.

Skydda lösenord och koder

Dina personliga lösenord skall hanteras som konfidentiell information. De får inte noteras så att obehöriga kan ta del av dem. Du ansvarar för användningen av dina användaridentiteter.

Om du har kod till ditt passerkort skall även denna kod behandlas som konfidentiell information.

Personliga ägodelar

Personliga tillhörigheter kan vara attraktiva för tjuvar. Håll därför dina värdesaker under uppsikt och förvara dem säkert. Beträffande ersättning se Stöld under kapitel Säkerhetsrutiner.

Möte eller konferens

Gå igenom vad som får och vad som skall sägas i förväg. Tänk på att den besökande kan sitta hos våra konkurrenter nästa dag. Kom ihåg att efter sammankomsten:

- o påminna deltagarna om sekretessbestämmelserna om ni gått igenom konfidentiella saker på mötet
- o rengöra tavlor
- o riva av papper på blädderblock och tag med dig dessa
- o ta med överbliven dokumentation

Enkäter och information

Du skall inte besvara externa enkäter om Volvo eller ge information om företaget till utomstående. Hänvisa i första hand till Informationsavdelningen. Rapportera sedan till din chef.

Vem var det här?

Alla, som har tillträde till Volvo Data, har fått ett ID-kort. De, som har fått tillträde till datacentralerna, skall alltid bära sina ID-kort väl synliga i dessa byggnader.

Observera att besökare **alltid** skall hämtas och lämnas vid reception/utgång. Du har ansvar för den besökande så länge besöket varar. Om du släpper in en person i samband med att du själv går in genom entrén, är det **du** som bär ansvaret för personen i fråga.

Var vaksam mot personer du inte känner igen - särskilt om de saknar ID-kort. Fråga efter vem som söks och om du kan hjälpa till. Var inte godtrogen, fråga hellre en gång för mycket. Besökare på "villovägar" skall vänligt men bestämt hjälpas tillrätta. Påträffar du person du misstänker är obehörig, meddela säkerhetsansvarig eller vakt. Alla anställda och besökare måste kunna styrka sin identitet på begäran av bevakningspersonal /receptionspersonal.

Fotografering

Inom företagets lokaler råder generellt fotograferingsförbud. Tillstånd erfordras från Informationsavdelningen på Volvo Data.

Trivselanordningar

Kaffebryggare och dylikt får endast finnas i godkända utrymmen och skall vara inkopplade till sådana eluttag som styrs av timer. Levande ljus får inte lämnas obevakade och får endast finnas i pausutrymmen. Rökning är endast tillåten i pausutrymmen märkta "Rökning tillåten".

BILAGA A. SÄRSKILDA REGLER, SKÖVDE

INFORMATIONSBEHANDLING

Makulering

Information som inte är klassad som konfidentiell kan makuleras i de öppna gallercontainers som finns i pappersarkivet. Övrigt material tuggas i befintlig papperstugg som finns placerad i DC:s pappersarkiv. Varje medarbetare ansvarar själv för makulering av sitt material.

DATAVIRUS

Akut

Om du misstänker någon form av datavirus, kontakta Kundstöd tfn 5150 (gäller alla typer av datorer). Om du har en dator som är hopkopplad med andra inom ett nätverk, gör ingenting förrän du fått hjälp, för att förhindra att viruset sprider sig till de andra datorerna inom nätet. Kundstöd informerar i sin tur säkerhetsansvarig.

Förebyggande

De som har en mindre anläggning typ persondator skall följa de regler, som finns utgivna för hur förekomst av datavirus upptäcks och hur man skyddar sig mot det. Innan du installerar ny programprodukt på din arbetsstation eller ny version av befintlig programprodukt skall du ta kontakt med memoid : VK.SWR. Denna grupp står också till förfogande vid frågor/information om bl a datavirus.

PERSONSÄKERHET

ARBETSPLATSSÄKERHETEN

Om det brinner

Vid utrymningslarm gäller :

- o Utrym lokalerna enligt bestämda utrymningsvägar. Dessa framgår av utrymningsplan som finns anslagna på varje våningsplan.
- o Gå till angiven samlingsplats (Entrén övre planet).
- o Anmäl dig till tjänstgörande enhetschef för att bli registrerad.
- o Om någon som vistats i lokalen saknas, anmäls detta av registrerande enhetschef till räddningsledningen, som ansvarar för allt fortsatt arbete.
- o Stanna kvar på samlingsplatsen för vidare information

Vid utrymning: ANVÄND ALDRIG HISS !
Utrymningsvägar får inte blockeras. Detta gäller även de gångar, som leder till och från arbetsplatsen.

FYSISK SÄKERHET, TILLTRÄDE TILL LOKAL

TILLTRÄDE TILL LOKALER

För personal, anställda på VDS (Volvo Data Skövde), gäller dessutom personligt ID-kort, med foto, utfärdat av VLK (Volvo Lastvagnar Komponenter AB) i Skövde som har ortens bevakningsansvar. Detta kort berättigar till inträde inom området genom uppvisande för vakt och/eller genom validitetskontroll i kortläsare vid befintliga grindar.

VDS interna utrymmen är indelade i olika zoner beroende på vilken verksamhet som bedrivs där. Tillträde till de olika zonerna bestäms av arbetsuppgifterna.

Tillträde till den yttre zonen är tillåten vardagar 07.00 - 17.00 för personer med gällande ID-kort.

På övrig tid är tillträde tillåten enbart för personal och då tillsammans med kod. Tillträde till driftsutrymmen fordrar alltid ID-kort och behörighetskod.

ID-KORT

Volvo Data anställd

Utlåning av temporärt ID-kort till VDS-anställd sker hos avd. 8702.

Pensionär

Pensionär får efter hänvändelse till A-port tillträde till området 07.00 - 17.00 vardagar och därmed tillträde till yttre zon under samma tidsperiod.

Volvo-anställd

Alla Volvo-anställda inom Skövde med gällande passagekort äger rätt till tillträde vardagar 07.00 - 17.00 till VDS yttre zon. Om behov finnes (vissa hantverkare såsom elektriker etc) för inpassering annan tid tilldelas dessa behörighetskod genom avd. 8702.

Konsulter m fl

Konsulter, entreprenörer, praktikanter och leverantörer som utför arbete för VDS skall ha samma ID-kort som övriga inom Skövde om arbetet omfattar mer än fyra veckor. För arbeten under kortare tidsperiod kan temporärt passagekort lånas hos avd. 8702. Passersedelsblankett (VS S20) användes för portpassage. Denna utfärdas av ansvarig chef inom VDS.

Besökare

Varje Volvo Data anställd har rätt att ta emot besökare i tjänsten. Besök skall anmälas till A-port. Besökare skall skriva in sig i A-porten hos tjänstgörande portvakt. Portvakten meddelar VDS-anställd om besökarens ankomst. Portvakten avgör om besökare skall hämtas/lämnas eller om vederbörande får förflytta sig själv inom Volvos fabriksområde.

Besök i datorhallar och modemrum är tillåtet för besökare efter tillstånd av avdelningschef, dennes ställföreträdare eller av avd. 8702.

SÄKERHETSRUTINER

Studiebesök

Tillstånd ges av enhetschef eller dennes ställföreträdare.

Fotografering och kameror

För att få fotografera inom VDS lokaler erfordras tillstånd av enhetschef eller dennes ställföreträdare.

BILAGA B. SÄRSKILDA REGLER, KÖPING

PERSONSÄKERHET

Om det brinner

I de flesta av Volvo Datas utrymmen finns det branddetektorer. Automatiska brandlarm, som avger signal och varnar oss om att brand har uppstått, finns i de flesta utrymmena.

Om brand uppstår gäller : **Rädda liv - Varna andra - Stäng dörrar** .
Det åligger chef att informera sina anställda om vilken typ av brandlarm och brandsläckare som finns på arbetsplatsen.

Larma vakten, telefon 2333 (hjälptelefon) som i sin tur larmar SOSAB (SOS alarmerings AB).
Brandlarmet går direkt till C-porten, därefter till SOSAB. Stanna om möjligt och möt brandförsvaret.

Brandlarm, där sådana finns, är en långt utdragen ringsignal.

Släck eller förhindra brandens spridning - **Tag inga onödiga risker !**

Se till att dörrar och fönster stängs så att branden inte sprider sig.

Om utrymning krävs gäller följande:

- Utrym lokalerna enligt utrymningsplan (finns på varje våningsplan)
- Gå till angiven samlingsplats (markerad på utrymningsplan).
- Se till att du blir registrerad på samlingsplatsen
- Chef kontrollerar om någon saknas och anmäler detta till brandbefäl
- Stanna kvar på samlingsplatsen för vidare information

Utrymningsvägar får inte blockeras. Detta gäller även de gångar, som leder till och från arbetsplatsen.

AKUT SJUKDOM ELLER OLYCKSFALL

Kontakta portvakt c-porten tel. 2333 (hjälptelefon) som kontaktar företagshälsovården och vid behov även ambulans. Vakten beskriver vägen till den drabbade utifrån var larmet kom ifrån.

ÖVRIGT OM PERSONSÄKERHET

Vid hot, t ex telefonterror, kontakta:

- Vakten i C-porten telefon 2153
- Volvo Datas säkerhetsansvarige telefon 2313
- Gör egna iakttagelser som t ex dialekt, bakgrundsljud, röstläge, man eller kvinna.

FYSISK SÄKERHET, TILLTRÄDE TILL LOKAL

ID-KORT

Tillträde till lokaler

För att skydda Volvo Datas verksamhet är VDKs lokaler utrustade med passagekontrollsystem. Alla anställda har ett personligt ID-kort (passerkort).Detta kort ger tillträde till VDKs lokaler genom validitetskontroll i kortläsare.

VDKs interna utrymmen är indelade i olika zoner beroende på vilken verksamhet som bedrivs. Tillträde till de olika zonerna bestäms av arbetsuppgiften.
Vissa tider krävs utöver giltigt passerkort även kod.

Tjänstledig

Chef avgör om tjänstledig medarbetare skall ha tillgång till sin arbetsplats under tjänstledigheten. Om *inte* skall kortet återlämnas samt säkerhetsansvarig 886x meddelas, som ombesörjer att passerkortet återlämnas

Volvo-anställd

De Volvo-anställda, som har täta kontakter med Volvo Data eller genom sin befattning behöver komma in på Volvo Data ofta, kan få behörigheter på sina egna kort att komma in till VDKs område.
Dessa kunders passerkort berättigar till tillträde vardagar mellan kl. 07.00 - 17.00.
Vissa Volvo-anställda som för sitt arbete behöver komma in i VDKs lokaler, t ex Underhållsavdelningen, gäller att de har tillträde till VDKs utrymmen dygnet runt.
För alla ej Volvo Data anställda gäller att tillträde endast får ske när arbetet så kräver.

Sändande utrustning

I maskinhall och LAN-rum är det generellt förbud mot medförande av mobiltelefon.
För att få använda mobiltelefon oberoende av typ inom dessa lokaler fordras tillstånd av chef 886x.

Konsulter m fl

Konsulter, entreprenörer, praktikanter och leverantörer som utför arbete i VDKs lokaler skall ha samma typ av ID-kort som Volvo Data-anställd om arbetet skall vara längre än 14 dagar. För arbeten mindre än denna tid kan lånekort fås från avd 6910.
När arbete upphör åligger det innehavaren till ID-kortet att återlämna detta till säkerhetsansvarig VDK.

De som önskar ID-kort kontaktar säkerhetsansvarig (tel. 2313) som avgör om ID-kort skall tilldelas den sökande.

ID-kort utlämnas av avd. 690002 enligt de uppgifter som ges av säkerhetsansvarig, Volvo Data.

När arbetet upphör åligger det innehavaren till ID-kortet att återlämna detta till säkerhetsansvarig, Volvo Data.

Besökare

Varje Volvo Dataanställd har rätt att ta emot besökare i tjänsten. Om besök sker dit inte alla Volvo Data anställda har tillträde fordras chefs tillstånd.

Besök i datorhallar och växelrum är ej tillåtet utan tillstånd av chef, avd. 8860 eller av enhetschef.

Den som tar emot besök är också ansvarig för den besökande.

SÄKERHETSRUTINER

Studiebesök

Tillstånd söks och utfärdas av enhetschef eller stf.

Fotografering och kameror

Tillstånd söks och utfärdas av enhetschef eller stf.

Stöld

Stöld av **personlig egendom** skall omedelbart anmälas till polismyndighet. Spärrning av kontokort av olika slag bör ske så snart som möjligt. Stölden skall så snart som möjligt även anmälas till säkerhetsansvarig, tel. 2313.

Köp eller lån av inventarier

Vid utförsel av utrustning som tillhör Volvo Data skall Formaterat memo i anslagstavla VDADM användas.. På blanketten skall anges eventuella serienummer eller tillverkningsnummer på varje del som skall föras ut från Volvo Data.

Detta gäller även när bärbar terminal, telefon etc lånas vid jour eller om arbete skall utföras utanför Volvo Datas utrymmen.

Om ingen lånehandling finns, gäller ej Volvos försäkring (enligt Volvos Risk Manager).

Tillstånd till utförsel ges av ägare till utrustning (chef).

Kopior av formaterat memo enl. nedan:

- 1 kopia till säkerhetsansvarig
- 1 kopia behålls av låntagaren
- 1 kopia behålls av chef tills utrustningen återlämnats, då kopian sändes till säkerhetsansvarig för avregistrering.

Händelserapport och åtgärd

När något misstänkt eller oegentligt upptäcks, såsom uppställda fönster, dörrar, personer som inte bör vistas i vissa utrymmen etc, skall detta snarast rapporteras till vakten i C-porten, telefon 2153 och under kontorstid även till säkerhetsansvarig på telefon 2313.

BILAGA C. SÄRSKILDA REGLER, ESKILSTUNA

PERSONSÄKERHET

Om det brinner

I de flesta av Volvo Datas utrymmen finns det branddetektorer. Automatiska brandlarm, som avger signal och varnar oss om att brand har uppstått, saknas dock på många ställen.

Om brand uppstår gäller : **Rädda liv - Varna andra - Stäng dörrar .**
Kontrollera alla utrymmen och informera om vad som hänt. Glöm ej meddela sekretariatet, som sprider informationen vidare till övriga våningsplan. Det åligger chef att informera sina anställda om vilken typ av brandlarm som finns på arbetsplatsen.

Larma vakten, telefon 1111 eller direkt till SOS alarmering på telefon 0 112

Använd brandalarm om det finns, eftersom det går snabbare än att telefonera. Stanna om möjligt kvar vid brandalarmet eller möt brandkåren och visa vägen.

Brandlarm, där sådana finns, är en pulserande eller långt utdragen ringsignal, som skall göra oss uppmärksamma på att brand har uppstått.

Släck eller förhindra brandens spridning - **Tag inga onödiga risker !**

Se till att dörrar och fönster stängs så att branden inte sprider sig.

Om utrymning krävs gäller följande:

- Utrym lokalerna via markerade utrymningsvägar, om ej annat meddelats.
- Gå till angiven samlingsplats (vid muren på HK:s parkering).
- Se till att du blir registrerad på samlingsplatsen
- Chef kontrollerar om någon saknas och anmäler detta till brandbefäl
- Stanna kvar på samlingsplatsen för vidare information

Vid utrymning: ANVÄND ALDRIG HISS !

Utrymningsvägar får inte blockeras. Detta gäller även de gångar, som leder till och från arbetsplatsen.

AKUT SJUKDOM ELLER OLYCKSFALL

Vid akut sjukdom eller olycksfall ring Vakten i Hällby, telefon 1111,
eller SOS Alarmering, telefon 0 112.

ÖVRIGT OM PERSONSÄKERHET

Vid hot, t ex telefonterror, kontakta:

- o Vakten i Hällby, telefon 1947
- o Volvo Datas säkerhetsansvarige, Sören Eidelöf, telefon 2456
- o Gör egna iakttagelser som t ex dialekt, bakgrundsljud, röstläge, man eller kvinna.

FYSISK SÄKERHET, TILLTRÄDE TILL LOKAL

ID-KORT

Volvo Data-anställd.

Volvo Data-anställd, som glömt att ta med sitt ID-kort till arbetet, kan låna ett temporärt kort av säkerhetsansvarig (Sören Eidelöf, tel. 2456). Detta kort ger tillträde till den egna arbetsplatsen, men inte till övriga utrymmen.

VCE-anställd

De VCE-anställda, som har täta kontakter med Volvo Data eller genom sin befattning (t ex AU-ansvarig) behöver komma in på Volvo Data får tillträde till Volvo Datas kontorsutrymmen, vardagar 0700 - 1800.

Vissa VCE-anställda (t ex underhållspersonal) får tillträde till alla av Volvo Datas utrymmen. Tillträde får då endast ske när arbetet så fordrar.

Konsulter m fl

Konsulter, entreprenörer, praktikanter och leverantörer som utför arbete i Volvo Datas lokaler kan få ett tillfälligt lånepasserkort. Detta kort utlämnas av säkerhetsansvarig (Sören Eidelöf, tel. 2456) efter det att chef på berörd avdelning lämnat tillstånd.
Det är ansvarig chefs ansvar att se till att låne-passerkortet återlämnas när arbetet upphör.

Besökare

Varje Volvo Data anställd har rätt att ta emot besökare i tjänsten. Om besök sker dit inte alla Volvo Data anställda har tillträde fordras chefs tillstånd.

Besök i datorhallar och växelrum är ej tillåtet utan tillstånd av avdelningschef på driftsavdelningen eller av enhetschef.

Den som tar emot besök är också ansvarig för den besökande. Besökare hämtas och lämnas vid entrén.

SÄKERHETSRUTINER

Studiebesök

Tillstånd söks hos och utfärdas av säkerhetsansvarig, (Sören Eidelöf, telefon 2456).

Fotografering och kameror

Tillstånd söks hos och utfärdas av säkerhetsansvarig, (Sören Eidelöf, telefon 2456).

Stöld

Stöld av **PERSONLIG EGENDOM** skall omedelbart anmälas till polismyndighet. Spärrning av kontokort av olika slag bör ske så snart som möjligt. Stölden skall så snart som möjligt även anmälas till säkerhetsansvarig (Sören Eidelöf, telefon 2456).

Händelserapport och åtgärd

När något misstänkt eller oegentligt upptäcks, såsom uppställda fönster, dörrar, personer som inte bör vistas i vissa utrymmen etc, skall detta snarast rapporteras till vakten i huvudporten, telefon 1947 och under kontorstid även till säkerhetsansvarig på VDE, (Sören Eidelöf, telefon 2456).

BILAGA D. SÄRSKILDA REGLER, OLOFSTRÖM

Inom Volvo Data i Olofström används för närvarande två skrifter som har framtagits i samband med ISO-certifieringen:

- Kvalitetsmanual administrativ utveckling
- Administrativ utveckling rutiner

Dessa innehåller även de lokala säkerhetsbestämmelserna och rutinerna.

Under 1997 kommer anpassning att göras till Volvo Datas Säkerhetshandbok.

BILAGA E. DATALAGEN. LICENS OCH TILLSTÅND

ALLMÄNT

De flesta som kommer i kontakt med datasystem känner till att Datalagen ställer krav på hur personinformation får föras i dataregister. Vad som gäller mera preciserat är dock oklart. Nedan följer en sammanfattning av vad som gäller för personregister inom Volvo Data.

DATAINSPEKTIONENS LICENS OCH TILLSTÅND

Varje företag skall ha en LICENS från Datainspektionen för att få registrera personinformation. Denna licens ger företaget rättighet att få registrera allmänna uppgifter. För att få registrera integritetskänsliga uppgifter fordras utöver licens även TILLSTÅND för varje register. Exempel på när tillstånd fordras är, uppgifter om sjukdomar, brott och straff, sexualliv, ras, politisk eller religiös uppfattning eller omdömen eller värderingar (s k mjukdata).

Licensen är utställd på en person inom företaget och denne skall föra en liggare över alla företagets register som innehåller personinformation.

Licensen på Volvo Data är utställd på dess Säkerhetschef avd. 2010. Före Du skapar ett nytt register eller ändrar i ett befintligt skall Säkerhetschefen informeras och han skall kontrollera registrets innehåll.

Register som Volvo Data handhar för övriga företag inom eller utanför koncernen fordrar att respektive företag har sin licens och eventuella tillstånd.

Datainspektionen har rätt att kontrollera att Datalagen följs och att liggare finns.

DEN REGISTRERADES RÄTT

Enligt Datalagen är företaget skyldigt att vid förfrågan kunna visa upp för den registrerade vilken information som finns om denne.

BILAGA F. FÖRTECKNING ÖVER PUBLIKATIONER INOM SÄKERHETSOMRÅDET

Inom säkerhetsområdet finns en hel del skrifter utgivna. Förteckningen nedan ger namnet på dem och en bild över vad de innehåller.

- **Säkerhetsbestämmelser inom Volvokoncernen**

  Skriften innehåller övergripande säkerhetsbestämmelser om säkerhetsskydd, skyddsobjekt, tillträdesskydd, behandling av hemliga handlingar, aktuella lagar, informationsskydd, fototillstånd mm, som är gemensamt för samtliga bolag inom Volvo-koncernen.
  Den utges av ansvarig för Juridik och Säkerhet i Koncernledningen.

- **Anslagstavla VDSECURA i Memo.**

  Här finns information om de säkerhetsregler och -rutiner som är beslutade av Volvo Datas Säkerhetsråd och inte finns beskrivna i Säkerhetshandboken.
  VDSECURA innehåller även formaterade memo som används i olika säkerhetsrutiner.

- **Kan du bevara en hemlighet?**

  Detta är en publikation, som vill ge råd om vad Volvoanställda bör tänka på, för att inte avsiktligt eller oavsiktligt sprida information, som inte bör vara känd utanför Volvo. Häftet är utgivet av Central säkerhetstjänst och lämnas till nyanställda på Volvo Data i Introduktionspärmen.

- **Volvos interna telefonkatalog**

  Den innehåller regler för hur information skall utväxlas vid olika typer av kommunikation t ex hur "kvalificerat företagshemlig" information skall hanteras.

- **Säkerhetspolicy**

  Detta är en övergripande beskrivning av hur säkerheten skall fungera inom Volvo Data. En mer detaljerad beskrivning finns i Volvo Datas säkerhetshandbok.

- **ACF2 Behörighetshandbok**

  Detta är en handbok, som beskriver organisation och regler för säkerhetssystemet ACF2 i stordatorvärlden. Ansvarig utgivare är Säkerhetschef Volvo Data.
  Den går att beställa från avdelning 2170.

- **Volvos IT-säkerhetshandbok**

  Denna bok beskriver de regler som gäller inom data-/informationsbehandlingsområdet. Bland annat ingår de regler som gäller som lägsta säkerhetsnivå (MSB). Boken omarbetas och kommer efter remissbehandling att fastställas av Koncernsäkerhetsrådet. Den kommer därefter att finnas för utlåning på Säkerhetsavdelningen.

- **Volvo Lastvagnars Riktlinjer För Säkerhetsskydd**

  Denna bok kommer troligen att ersätta "Säkerhetsbestämmelser inom Volvokoncernen" (Se ovan).
  Här finns många goda råd att ta del av. Exempelvis: råd vid kidnappning, checklista vid telefonhot, råd vid resor och mycket annat.
  Boken finns för utlåning på Säkerhetsavdelningen, 2010

- **Säkerhet vid mobil kommunikation**.

  Broschyr med regler för sändande utrustning och telfonnummer att kontakta vid problem.

- **Säkerhetsregler för anställda.**

  Vikblad med säkerhetsregler för Volvo Dataanställda.
  Kan beställas hos Säkerhetsavdelningen eller receptionen DA.

- **Säkerhetsregler för leverantörer och entreprenörer till Volvo Data.**

  Vikblad med säkerhetsregler för **icke** Volvo Dataanställda.
  Kan beställas hos Säkerhetsavdelningen eller receptionen DA.

- **Videoband med säkerhetsinformation.**

  Volvo har tillsammans med andra företag sammanställt en vido som innehåller information om säkerhet. Denna kan tillsammans med instruktioner lånas av Informationsavdelningen, 2030.

BILAGA G. REGLER FÖR INFORMATIONSKLASSNING

Nedan återges vad som gäller för de olika informationsklasserna enligt publikationen "Säkerhetsbestämmelser inom Volvo koncernen".

- **KVALIFICERAT FÖRETAGSHEMLIG**

  Information av sådan karaktär att den ger företaget ett betydande försteg framför sina konkurrenter, eller vars avslöjande, spridning, användning eller ändring skulle kunna medföra synnerligen allvarliga skadeverkningar för företaget.

  Exempel på sådan information kan vara samlade uppgifter om företagets strategiska planer, nytt produktprojekt, lönsamhet, större investeringar och produktionsplaner, köp och försäljning av företag etc.

- **FÖRETAGSHEMLIG**

  Information av sådan karaktär att den ger företaget ett klart försteg framför sina konkurrenter, eller vars avslöjande, spridning, användning eller ändring skulle kunna medföra betydande skadeverkningar för företaget

  Exempel på sådan information kan vara utveckling, formgivning, provning, tillverkning, marknadsplaner, produktionsuppgifter, kostnader/intäkter, anställningshandlingar och betyg m fl personuppgifter

- **FÖRETAGSINTERN**

  Information av sådan karaktär att dess spridning, användning eller ändring skulle kunna medföra begränsad, mindre skada för företaget. Sådan information är uteslutande avsedd för anställda inom företaget och för samarbetspartners

Bilaga H. Säkerhetsrevisioner.

Allmänt

Ett effektivt ADB-säkerhetsarbete förutsätter kunskap om de svagheter som finns samt utarbetande av förslag till hur dessa ska undanröjas. I det följande beskrivs huvuddragen i den arbetsgång som ska gälla inom Volvo.

Sårbarhetsanalys.

För att kunna uppnå planerad säkerhetsnivå är det viktigt att riskerna - såväl sannolikheter som skadekostnader - bedöms på ett systematiskt sätt.
Riskbedömningen har till syfte:

- att bedöma vilka kostnader som kan uppstå vid störningar i ADB-verksamheten
- att klarlägga vilka skyddsåtgärder som krävs för att förhindra störningar eller minska skadeverkningar
- att minimera kostnaderna för skydd

Sårbarhetsanalysen bygger på att man identifierar tänkbara negativa händelser såsom:

- försening, avbrott, förlust av data
- obehörig användning
- bristande kvalitet

och redovisar de negativa konsekvenser som kan uppstå om händelserna inträffar.

Genomförande av sårbarhetsanalyser

Inom Volvo bör Volvo-metoden användas vid riskanalyser.

Volvo-metoden består av ett datasystem för PC som framtagits och underhålls fortlöpande. Systemet omfattar 14 avsnitt som i stort sett täcker ett företags totala säkerhet inom IT-området. Metoden täcker följande avsnitt:

1. Organisation/ansvar
2. Personal
3. Tillgänglighet/tillförlitlighet
4. Kringmiljö
5. Tillträde
6. Försörjning
7. Brandskydd
8. Skydd mot vattenskador
9. Systemsäkerhet
10. Nätverk/telekommunikation
11. Systemutveckling
12. Persondatorer
13. Säkerhetskopiering/arkivering
14. Katastrofplanering

Resultat i form av rapporter från genomförd utredning är företagshemlig information.

Riskbedömningen kan kompletteras med SBA eller annan metod om detta bedöms vara önskvärt.

Arbetsgång.

Normalt går en sårbarhetsanalys med Volvometoden till på följande sätt:

1. Tillsammans avgör controller och ansvarig för reviderat objekt:
   - vilka avsnitt enligt ovan som skall behandlas
   - tid för kontrollen och vilka som skall deltaga
2. Controller tar fram checklistor från systemet för de utvalda avsnitten samt läser in ev inhämtad information om revisionsobjektet.
3. Gemensamt ifylls checklistor, ev med inkallade experter på olika avsnitt.
4. Resultatet registreras i systemet och output utgörs av säkerhetsnivå, bristrapport och åtgärdslista. Controller tar även fram ett redovisningspaket, bestående av overheadbilder, som kan användas för information om analysen.
5. Ansvarig för det reviderade objektet går igenom åtgärdslista och sätter tider och kostnader för en åtgärdsplan.
6. Åtgärdslista och handlingsplan utgör underlag för de årliga säkerhets revisionerna.

Årlig uppföljning.

För att kunna upprätthålla den fastställda säkerhetsnivån inom Volvo är det nödvändigt att arbetet med ADB-säkerhetsfrågorna bedrivs kontinuerligt.
I samband med budgetprocessen ska för det kommande året fastställas en tidsatt åtgärdsplan inom varje bolag för att säkerställa önskad ADB-säkerhetsnivå. Rapport skall också göras över det gångna årets ADB-säkerhetsarbete, varav framgår eventuella avvikelser från åtgärdsplan.