Riktlinjer för IT-säkerhet

1. Syfte

Dessa riktlinjer utgör tvingande regler för användande av IT-resurser inom Svenska Röda Korset (nätverk, skrivare, smartphones, servrar, klienter) samt för handhavande av sekretessbelagd information. Riktlinjerna syftar till att upprätthålla önskad administrativ och teknisk säkerhetsnivå.

2. Avgränsning

Dessa riktlinjer avser säkerheten i Svenska Röda Korsets IT-infrastruktur samt elektronisk meddelande- och dokumenthantering. Riktlinjerna är styrande för säkerhetsarbetet inom hela organisationen.

Dessa riktlinjer reglerar inte personskydd.

3. Regler

- IT-verksamheten ska tillhandahålla en katastrofplan som garanterar korrekt hantering av incidenter som drabbar Svenska Röda Korsets verksamhets-kritiska IT-system.
  (Beskrivs i dokumentet *Katastrofplan*)

- IT-säkerhetsansvarig på Svenska Röda Korset är direkt underställd IT-chefen och ansvarar för uppföljningen av och arbetet med IT-säkerhet.
  (Beskrivs i dokumentet *IT-säkerhetsansvarig*)

- Samtliga Svenska Röda Korsets IT-system innehållande affärs- och verksamhetsinformation, ska ha dokumenterad backuphantering som förhindrar förlust av data.
  (Beskrivs i dokumentet *Backuphantering*)

- Svenska Röda Korsets IT-system ska ha ett digitalt skalskydd, som skyddar från externa attacker.
  (Beskrivs i dokumentet *Digitalt skalskydd*)

- IT-verksamheten ska säkerställa att det finns en standard, som styr hur klienter anslutna till Svenska Röda Korset ska vara konfigurerade.
  (Beskrivs i dokumentet *Anslutna klienter)*

- Svenska Röda Korsets IT-system ska vara tillgängliga enligt tjänsteavrop beslutat av systemägaren i samråd med IT-chefen.
  (Beskrivs i dokumentet *Tillgänglighet)*

- Samtliga Svenska Röda Korsets IT-system ska ha dokumenterad behörighetshantering som garanterar att endast behöriga användare har åtkomst till given data.
  (Beskrivs i dokumentet *Behörighetshantering*)

- IT-verksamheten ska säkerställa att det finns ett dokumenterat arbetssätt som standardiserar och styr säkerhetsincidenthanteringen.
  (Beskrivs i dokumentet *IT-säkerhetsincidenthantering*)

- Rapportering av IT-verksamhetens arbete kring IT-säkerhet ska möjliggöra en ökad spårbarhet och uppföljning. Svenska Röda Korsets rapporter på området IT-säkerhet ska avläggas minst en gång per år.
  (Beskrivs i dokumentet *IT-säkerhetsrapportering)*

4. Ansvar

IT-säkerhetsansvarig för Svenska Röda Korset är samordningsansvarig för IT-säkerhetsarbetet inom organisationen, men respektive verksamhetsansvarig och regionansvarig ansvarar för att IT-säkerheten i den egna verksamheten efterlevs. Anställda vid Svenska Röda Korset samt anlitade konsulter och övriga användare av Svenska Röda Korsets IT-resuser ska följa regelverket i dessa riktlinjer. Ansvarsfördelningen ska finnas inskriven i IT-försäkran. IT-säkerhetsansvarig ska säkerställa att Svenska Röda Korset tillhandahåller relevant information kring IT-säkerhetsfrågor.

Specifik Riktlinje för kontinuitetsplan IT-drift

1. Syfte

IT-verksamheten skall tillhandahålla en kontinuitetsplan som garanterar korrekt hantering av incidenter som drabbar Svenska Röda Korsets IT-verksamhet.

Denna specifika riktlinje utgör tvingande regler för den kontinuitetsplan som skall styra hantering av allvariga incidenter i kritiska delar av IT-verksamheten.

2. Avgränsning

Denna specifika riktlinje avser kontinuitetsplanen för IT-verksamheten. Riktlinjen är styrande för kontinuitetsplanens innehåll. Kontinuitetsplanen reglerar inte personskydd.

3. Regler

- Kontinuitetsplanen beskrivs i rutinen *Kontinuitetsplan för IT-drift*. Syftet med rutinen är att beskriva tänkbara scenarier och hanteringen av dessa.

- Kontinuitetsplanen skall beskriva hantering av allvarliga incidenter vilka drabbar IT-verksamheten. Syftet är att möjliggöra en systematisk arbetsinsatts för att minimera skadepåverkan.

- Kontinuitetsplanen skall innehålla en beskrivning av den organisation som skall gälla vid hantering av inträffad katastrof. Syftet är att rätt person/personer snabbt skall kunna påbörja arbetet med att återställa och säkra driften av IT-miljön.

- Det skall finna en prioriteringslista över komponenter som innefattas av kontinuitetsplanen. Syftet är att tydliggöra kontinuitetsplanens omfattning, avseende mjukvara och hårdvara.

4. Ansvar

IT-säkerhetsansvarig ansvarar för att det finns en uppdaterad kontinuitetsplan.

Specifik Riktlinje för IT-säkerhetsansvarig

1. Syfte

IT-säkerhetsansvarig på Svenska Röda Korset är direkt underställd IT-chefen, och ansvarar för uppföljningen av, och arbetet med, IT-säkerhet.

Denna specifika riktlinje utgör tvingande regler för den som är IT-säkerhetsansvarig på Svenska Röda Korset. Riktlinjen syftar till att upprätthålla önskad nivå på styrningen av arbetet med IT-säkerhet.

2. Avgränsning

Denna specifika riktlinje avser endast rollen som IT-säkerhetsansvarig.

3. Regler

- IT-säkerhetsansvarig skall höja säkerheten inom Svenska Röda Korset, genom att driva arbetet med IT-säkerhet inom organisationen.
  Syftet är att aktivt utveckla IT-säkerhetsarbetet i takt med den föränderliga hotbilden.

- IT-säkerhetsansvarig skall kontinuerligt sammanställa och rapportera status på IT-säkerheten till IT-chefen.
  Syftet är att kontinuerligt följa upp IT-säkerhetsarbetet och möjliggöra avstämning mot rådande hotbild.

- IT-säkerhetsansvarig skall öka förståelsen för IT-säkerhet bland Svenska Röda Korsets anställda, genom att tydliggöra vilka specifika riktlinjer som organisationen har på området, samt hur de skall följas.
  Syftet är att höja IT-säkerheten inom Svenska Röda Korset.

- IT-säkerhetsansvarig skall säkerställa spårbarhet av arbetet med IT-säkerhet, genom att regelbundet (minst årligen) genomföra och till IT-chefen presentera en analys av Svenska Röda Korsets arbete på området. Rapporteringen skall ske i enighet med *Specifik Riktlinje Rapportering IT-säkerhet*.
  Syftet är att möjliggöra uppföljning av arbetet med IT-säkerhet.

4. Ansvar

Den IT-säkerhetsansvarige är direkt underställd IT-chefen, och ansvarar för Svenska Röda Korsets IT-säkerhet.

Specifik Riktlinje för backuphantering

1. Syfte

Samtliga Svenska Röda Korsets IT-system innehållande affärs- och verksamhetsinformation, skall ha dokumenterad backuphantering som förhindrar förlust av data.

Denna specifik riktlinje utgör tvingande regler för hur samtliga Svenska Röda Korsets IT-system innehållande affärs- och verksamhetsinformation skall hanteras med avseende på backuphantering.

2. Avgränsning

Denna specifika riktlinje avser samtliga Svenska Röda Korsets IT-system innehållande affärs- och verksamhetsinformation. Riktlinjen är styrande för dokumentationen av backuprutiner.

3. Regler

- Backup skall göras på samtliga system som driftas på servrar, enligt för varje tillfälle gällande backupschema.
  Syftet är att säkerställa att ingen data går förlorad.

- Det skall finnas en rutin för återläsning av data.
  Syftet är att möjliggöra åtkomst till förlorad data.

- Backupen skall göras i lösningar som tillgodoser hela Svenska Röda Korstes backupbehov.
  Syftet är att säkerställa att backup kan tas på alla organisationens system.

- Backupansvarig skall varje arbetsdag gå igenom skapade backup loggar för att säkerställa att en korrekt backup skett. Vid eventuella avvikelser skall backupansvarig vidta lämpliga åtgärder.
  Syftet är att möjliggöra kontroll och spårbarhet.

- Det skall finnas en rutin för regelbunden test av återläsning av data. Särskilt viktigt för data i verksamhetskritiskasystem.
  Syftet är att säkerställa att backup och återläsning fungerar.

4. Ansvar

Ansvaret för backuphanteringen ligger på backupansvarig.

Specifik Riktlinje för digitalt skalskydd

1. Syfte

Svenska Röda Korsets IT-system skall ha ett digitalt skalskydd, som skyddar från attacker initierade såväl utifrån som inifrån organisationen.

Denna specifika riktlinje utgör tvingande regler rörande digitalt skalskydd inom Svenska Röda Korset. Riktlinjen syftar till att styra arbetet med digitalt skalskydd, och därigenom säkerställa ett digitalt skalskydd som uppfyller organisationens behov.

2. Avgränsning

Denna specifika riktlinje avser IT-verksamhetens arbete med digitalt skalskydd inom Svenska Röda Korset.

3. Regler

- Det skall vid alla tillfällen finnas ett fungerande digitalt skalskydd för Svenska Röda Korsets IT-resurser.
  Syftet är att i största möjliga mån skydda organisationen mot externa, såväl som interna attacker.

- Digitalt skalskydd skall bygga på beprövade kunskaper och produkter. Kompetensen att hantera skalskyddet skall finnas inom Svenska Röda Korsets IT-verksamhet.
  Syftet är att säkerställa att Svenska Röda Korsets IT-verksamhet har kontroll över organisationens digitala skalskydd.

4. Ansvar

IT-säkerhetsansvarig är ansvarig för införandet och underhållet av det digitala skalskyddet inom Svenska Röda Korset.

Specifik Riktlinje för anslutna klienter

1. Syfte

IT-verksamheten skall säkerställa att det finns en standard som styr hur klienter anslutna till Svenska Röda Korset skall vara konfigurerade.

Denna specifika riktlinje utgör tvingande regler för inom Svenska Röda Korset anslutna klienter.

2. Avgränsning

Dessa specifika riktlinjer avser inom Svenska Röda Korset anslutna klienter. Riktlinjerna är styrande för konfigurering och hanteringen av anslutna klienter inom Svenska Röda Korset.

3. Regler

3.1 Klienter tillhörande Svenska Röda Korset

- Anslutna klienter inom Svenska Röda Korset skall vara konfigurerade i enlighet med det som för tillfället gäller för tjänsten *Standardarbetsplats*. Syftet är att standardisera konfigurationer rörande säkerhet, samt underlätta service och support av klienter.

- Extra konfigurering styrs av Servicedesk.
  Syftet är att kontrollera installationen av program som inte ingår i standardarbetsplatsen.

- Ingen förändring får göras på klienterna utan IT's uttryckliga godkännande, då detta kan bidra till ökade säkerhetsrisker.
  Syfet är att styra hur klienterna är konfigurerade.

3.2 Klienter ej tillhörande Svenska Röda Korset

- Externa klienter skall i huvudsak anslutas till Svenska Röda Korsets gästnät för internet åtkomst.
  Syftet är att för externa klienter möjliggöra säker åtkomst till internet utan att ge tillgång till Svenska Röda Korsets interna nät.

- Externa klienter som kräver anslutning till Svenska Röda Korsets IT-infrastruktur skall leva upp till den IT-säkerhetsnivå som är satt av IT-verksamheten.

Syftet är att klienter ej tillhörande Svenska Röda Korset inte skall skapa säkerhetsrisker.

4. Ansvar

Säkerställandet av att det finns rutiner för hantering av anslutna klinter inom Svenska Röda Korset ligger på IT-säkerhetsansvarig.

Specifik Riktlinje rörande tillgänglighet

1. Syfte

IT-verksamheten skall garantera att tillgängligheten av Svenska Röda Korsets IT-system lever upp det som överenskommits mellan systemägare och IT-chef.

Denna specifika riktlinje utgör tvingande regler rörande tillgänglighet av Svenska Röda Korsets IT-system. Riktlinjen är styrande för hur arbetet med tillgängligheten skall bedrivas.

2. Avgränsning

Denna specifika riktlinje avser tillgängligheten av samtliga Svenska Röda Korsets IT-system.

3. Regler

- Det skall för varje system finnas en överenskommelse mellan systemägaren och IT-chefen om hur tillgängligheten skall se ut.
  Syftet är att säkerställa att tillgängligheten är anpassad både till verksamhetens behov, samt till IT-verksamhetens resurser och möjligheter.

- Avtalet om tillgänglighet skall innehålla tider då systemet skall vara tillgängligt för användare. Både i normalfall, samt vid undantag från sådana.
  Syftet är att garantera en rimlig tillgänglighet, som hanterar undantag vilka kan vara periodiska över året, eller kunna avropas vid speciella tillfällen.

- För att garantera IT-verksamhetens möjlighet att genomföra uppgraderingar och underhåll av IT-system, skall servicefönster för Svenska Röda Korsets IT-system finnas tillgängliga enligt avtal mellan systemägare och IT-chef.
  Syftet är att möjliggöra uppgraderingar och underhåll under kontrollerade former.

- Ett IT-systems tillgänglighet skall regelbundet rapporteras till systemägaren.
  Syftet är att systemägaren skall kunna flagga för om tillgängligheten inte lever upp till verksamhetens behov.

- Det skall finnas ett övervakningssystem som uppmärksammar IT-verksamheten på störningar som kan leda till avtalsbrott rörande tillgänglighet av Svensak Röda Korsets IT-system.
  Syftet är att möjligöra för IT-verksamheten att planera in stop i driften.

- Driftsättningar av nya eller uppgraderingar av existerande system skall ske enligt gällande driftsättningsrutin.
  Syftet är att driftsättning av nya eller existerade system skall ske med minimal påverkan på verksamheten.

4. Ansvar

IT-chef ansvarar för tillgängligheten av samtliga Svenska Röda Korsets IT-system.

Specifik Riktlinje behörighetshantering

1. Syfte

Samtliga Svenska Röda Korsets IT-system skall ha dokumenterad behörighetshantering som garanterar att endast behöriga användare har åtkomst till given data.

Denna specifika riktlinje utgör tvingande regler rörande behörighetshantering inom Svenska Röda Korsets IT-system.

2. Avgränsning

Denna specifika riktlinje avser behörighetshanteringen inom Svenska Röda Korsets IT-system. Riktlinjerna är styrande för hur arbetet med behörighetshanteringen skall bedrivas.

3. Regler

- Katalogtjänst vald av Svenska Röda Korset (t ex Microsofts AD) ska vara det i huvudsak styrande behörighetssystemet för åtkomst till IT-resurser inom organisationen.
  Syftet är att reglera åtkomsten till IT-resurser.

- Behörighetsinformation i system som kräver egen behörighetshantering, skall i största möjliga utsträckning överensstämma med den information som finns i den valda katalogtjänsten.
  Syftet är att samtliga system i största möjliga mån skall ha överensstämmande behörighetsinformation.

- All behörighetshantering skall skötas av IT-verksamheten om inte annat överrenskommits med systemägaren.
  Syftet är att säkerställa vem som har ansvar för ett systems behörighetshantering.

- Användare av Svenska Röda Korsets IT-resurser är ansvariga för tilldelade behörighetsuppgifter. Detta innebär att det inte är tillåtet att dela med sig av sina behörighetsuppgifter till andra än personal inom IT-verksamheten.
  Syftet är att förhindra obehörigt eller felaktigt användande av behörighetsuppgifter.

- Användandet av annans behörighetsuppgifter är förbjudet.
  Syftet är att Svenska Röda Korsets medarbetare och extern personal skall vara begränsade till tilldelad behörighet.

- Det ska finnas en rutin för hantering av Svenska Röda Korsets medarbetare och externa resurser.
  Syftet är att förhindra användandet av behörighetsuppgifter som för tillfället inte skall används.

- Det skall finnas en rutin för hur frivilligas åtkomst till Svenska Röda Korsets IT-resurser skall hanteras.
  Syftet är att styra frivilligas användande av Svenska Röda Korsets IT-system, samt att förenkla administrationen av frivilligas behörighet.

4. Ansvar

IT-säkerhetsansvarig ansvarar för att rutiner rörande behörighetshantering inom samtliga Svenska Röda Korsets IT-resurser, motsvarar organisationens krav.

Specifik Riktlinje för IT-säkerhetsincidenthantering

1. Syfte

IT-verksamheten skall säkerställa att det finns ett dokumenterat arbetssätt som standardiserar och styr IT-säkerhetsincidenthanteringen.

Denna specifika riktlinje utgör tvingande regler rörande säkerhetsincidenthantering inom Svenska Röda Korset. Riktlinjen syftar till att styra arbetet med säkerhetsincidenthantering.

2. Avgränsning

Denna specifika riktlinje avser endast IT-säkerhetsincidenthantering inom Svenska Röda Korset, och berör enbart IT-verksamheten.

3. Regler

- Dokumenterad IT-säkerhetsincidentshanteringsrutin skall finnas och efterföljas.
  Syftet är att standardisera hanteringen av IT-säkerhetsincidenter.

- Rapportering av IT-säkerhetsincidenter skall beskrivas i IT-säkerhetshanteringsrutinen. Rutinen skall beskriva vilka säkerhetsincidenter som skall rapporteras, och hur de skall rapporteras.
  Syftet är att effektivisera rapportering av inträffade säkerhetsincidenter, och möjliggöra spåbarhet.

4. Ansvar

IT-säkerhetsansvarig är ansvarig för IT-säkerhetsincidenthanteringen inom Svenska Röda Korset.

Specifik Riktlinje Rapportering IT-säkerhet

1. Syfte

Rapportering av IT-verksamhetens arbete kring IT-säkerhet skall möjliggöra en ökad spårbarhet och uppföljning. Svenska Röda Korsets rapporter på området IT-säkerhet skall avläggas enligt fastslagna intervall.

Denna specifika riktlinje utgör tvingande regler för all rapportering rörande IT-säkerhet inom Svenska Röda Korset. Dokumenterade rapporteringsrutiner skall finnas och efterlevas.

2. Avgränsning

Denna specifika riktlinje avser endast rapportering gällande IT-säkerhet inom Svenska Röda Korset. IT-säkerhetsrapporteringen består av fyra rapporter;

- Sårbarhetsanalys (IT-säkerhetsansvarig till IT-chef)
- Lägesrapport IT-säkerhet (IT-säkerhetsansvarig till IT-chef)
- IT-säkerhet infrastruktur (Infrastrukturansvarig till IT-säkerhetsansvarig)
- IT-säkerhet servicedesk (Servicedeskansvarig till IT-säkerhetsansvarig)

3. Regler

- Dokumenterad IT-säkerhetsrapportering skall finnas och efterföljas.

- IT-säkerhetsansvarig ansvarar för att det regelbundet (minst årligen inför verksamhetsplaneringen) genomförs och till IT-chefen presenteras en sårbarhetsanalys av företagets IT-miljö. Formatet för sårbarhetsanalysen skall finnas beskriven i en rutin.

- IT-säkerhetsansvarig ansvarar för att det regelbundet (en gång per tertial) genomförs och till IT-chefen presenteras en lägesrapport för IT-säkerheten. Formatet för *Lägesrapport IT-säkerhet* skall finnas beskriven i en rutin.

- IT-säkerhetsansvarig ansvarar för att rapporten *IT-säkerhet infrastruktur* regelbundet (en gång per tertial) skrivs av ansvarig för Infrastruktur. Formatet för rapporten *IT-säkerhet infrastruktur* skall finnas beskriven i en rutin.

- IT-säkerhetsansvarig ansvarar för att rapporten *IT-säkerhet servicedesk* regelbundet (en gång per tertial) skrivs av ansvarig för Servicedesk. Formatet för rapporten *IT-säkerhet servicedesk* skall finnas beskriven i en rutin.

IT-säkerhetsansvarig ansvarar för IT-säkerhetsrapporteringen till IT-chefen.