UTFÄRDARE Ali Ababneh			DOKUMENTTYP Policy	
BESLUTAD AV KOMMUNFULLMÄKTIGE	DIARE NUMMER	DATUM	VERSION 1.0	DOKUMENTIDENTIFIKATION

Haparanda kommuns riskpolicy

PROGRAM
Uttrycker värdegrund och önskvärd utveckling av verksamheten.

POLICY
Uttrycker ett värdegrundsbaserat förhållningssätt och principer för vägledning.

STRATEGI
Konkretiserar ett program eller en policy och utgör en grund för prioritering.

HANDLINGSPLAN
Beskriver konkreta mål och åtgärder.

RIKTLINJER
Säkerställer ett riktigt agerande och en god kvalitet vid handläggning och utförande.

1. Syfte

Risk definieras som ”möjligheten av en avvikelse från det förväntade”. Risker kan inte undvikas utan måste hanteras där syftet med en etablerad process för riskhantering är att:

- att stödja Haparanda stad verksamhet genom att på ett strukturerat och effektivt sätt kunna identifiera och hantera risker gällande informationssäkerhet.
- stödja informationsägaren med kunskap på området.

2. Mål

Målet med riskhantering är att minska konsekvensen och sannolikheten av informationssäkerhetsrisker som kan orsaka skada på Haparanda stads verksamhet och invånare, i linje med de risker och behov som kommunen har identifierat. Vidare är ett huvudsakligt mål att alltid sträva efter att få risker som möjligt kopplade till informationssäkerhet förbises och att säkerhetsarbetet integreras med kommunens befintliga sätt att leda och styra sin verksamhet.

3. Omfattning

Processen för riskhantering är avsedd att utföras inom ledningssystemet för informationssäkerhets omfattning. En risk som anses påverka informations konfidentialitet, riktighet eller tillgänglighet omfattas av riskhanteringen. Detta innebär att informationssäkerhetsrisker identifieras samt klassificeras utifrån sannolikhet och påverkan på information, data, processer, system, rykte och/eller IT-infrastruktur.

Processen omfattar nedan moment:

- Genomförande av riskworkshops och dokumenterade riskanalyser.
- Hantering av identifierade risker.
- Åtgärd och acceptans av risker.
- Kontinuerlig uppföljning.

Riskanalyserna inom informationssäkerhet utgår från genomförda informationssäkerhetsklassificeringar. Klassificeringsmatrisen för informationssäkerhet återfinns i ”instruktion för hantering av tillgångar”.

4. Riskaptit

Då risker värderas används en riskmatris där sannolikheten för, och konsekvensen av, identifierade händelser graderas från 1–5. Utifrån sannolikhet och konsekvens ett riskvärde fram. Beroende på hur högt eller lågt riskvärdet är genereras en färg, antigen grön, gul, orange eller röd. Färgen indikerar huruvida risken faller inom ramen för Haparanda stads risktolerans eller inte.

- Risker som får ett riskvärde över 16 hamnar i det röda området ska prioriteras först och måste åtgärdas eller undvikas.
- Risker som hamnar i det orangea området. Betydande men tolerabel risk och ska prioriteras efter röda området
- Gula risker (5–10) ska övervakas för eventuella förändringar och kontroll ska dokumenteras.
- Gröna risker (0–4) kan accepteras och behöver ingen vidare åtgärd.

Ej tolerabel risk	**Röd**
Betydande men tolerabel risk	**Orange**
Tolerabel risk	**Gul**
Acceptabel risk	**Grön**

5. Riskanalysprocessen

Varje verksamhet ska genomföra och dokumentera analyser avseende vilka risker som ka påverka informationssäkerheten, och utifrån dessa analyser vidta lämpliga skyddsåtgärder.

5.1 Informationsobjekt

Processen för genomförande av en riskanalys gällande informationssäkerhet består av fem steg som genomförs under ett år. Risker identifieras utifrån kända informationsobjekt i Haparanda stads kritiska processer. Informationsobjekt har identifierats av verksamheten som kritiska för att processerna eller innehåller information som anses känslig och är extra skyddsvärd.

5.2 Informationsklassificering

Innan riskidentifieringen påbörjas ska en informationssäkerhetsklassificering av identifierade informationsobjekt ska ha genomförts. Informationsklassificeringen genomförs enligt ”instruktion för hantering av tillgångar”. Resultatet från informationssäkerhetsklassificeringen dokumenteras i riskanalysdokumentationen.

5.3 Riskworkshop och identifiera risker utifrån scenarion

5.3.1 Deltagare

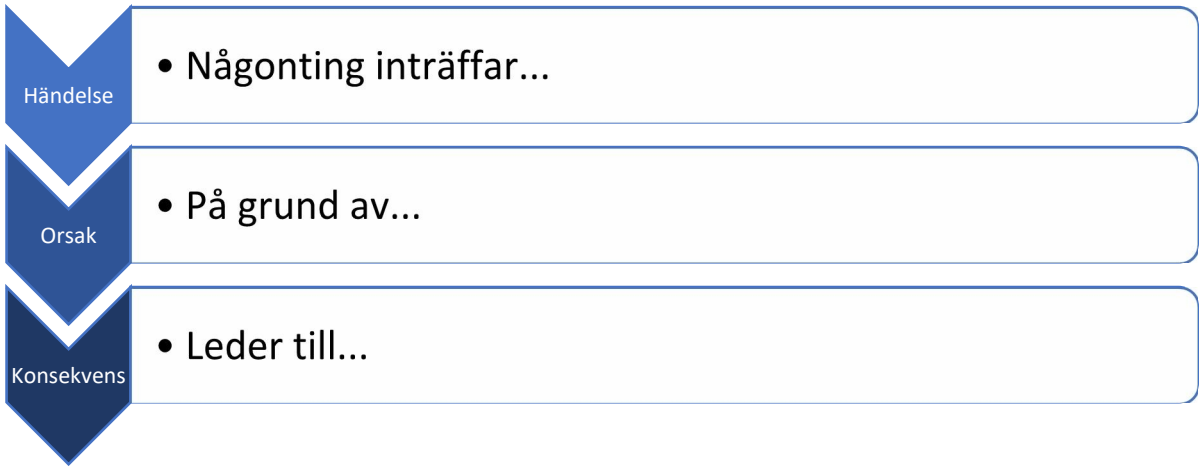
Riskworkshops genomförs en gång per år eller vartannat år tillsammans med utvalda intressenter i verksamheten. Riskworkshops utgår från Haparanda stads kritiska processer och dess identifierade skyddsvärda informationsobjekt. Ansvarig för respektive process ska närvara vid genomförande av riskworkshopen. Vidare bör en eller flera utvalda från som jobbar nära verksamhetsområdet medverka i syfte att bidra med expertkompetens.

5.3.2 Riskworkshop

Riskanalyserna kommer utgå från scenarion på något sätt påverkar informationssäkerheten (konfidentialitet, riktighet, tillgänglighet) av identifierade informationsobjekt. Det är viktigt att medverkande under riskanalysen förstår dess omfattning och i vilken kontext verksamheten agerar. För att säkerställa att samtliga personer som deltar under riskanalysen utgår från samma syfte och mål är det viktigt att detta kommuniceras.

5.3.3 Dokumentera risker

Utifrån beskrivna scenarion identifieras risker under riskworkshopen där deltagarna tillsammans diskuterar och kommer överens om relevanta risker. Dessa ska dokumenteras under riskworkshopen.



5.3.4 Bedöma och klassificera risker

Samtliga risker som identifieras under workshopen ska vid tillfälle i nära anslutning till genomförd workshop, bedömas och klassificeras utifrån sannolikhet och påverkan. Värdet av sannolikheten och påverkan resulterar i ett riskvärde som ligger inom tolerabel nivå eller utanför.

5.3.5 Riskägare

Riskägare har som ansvar att dokumentera åtgärdshantering för den risk som denne ansvarar för om denna riskvärdet överskrider tolerabel nivå.

5.3.6 Uppföljning

Det första steget består av att genomföra en informationssäkerhetsklassificering av informationen i en process eller ett system. Därefter definieras scopet för riskbedömningen. Detta följs av genomförandet av identifiering av risker, analys av dessa, utvärdering och hantering av riskerna. Hantering och genomförandet av åtgärderna följs därefter upp i uppföljningsfasen. Riskbedömningen och riskhantering ska vara en kontinuerlig process och stödja informationssäkerhetsarbetet. Riskbedömningar ska revideras när förutsättningar väsentligen förändras.

5.3.7 Lagring

Genomförd informationsklassificering, riskbedömning och riskhanteringsbeslut ska lagras på plats som anvisas av riskägare.