Koncernkontoret		
IT-avdelningen	**Datum**: 2011-06-29 Dnr:	
Dokumentförvaltare: Johan Åbrandt, Martin X Svensson Koncernkontoret, IT-avdelningen		**Dokumentets status**: Fastställd
Dokumentid: Åtkomst till Vårdtjänst via RSVPN **Dokumentformat:** A4	**Version:** 1.0	**Dokumenttyp:** Anvisning **Dokumentklass:** Styrande dokument **Ämne:** Ledningssystem för informationssäkerhet

Anvisning

Åtkomst till Vårdtjänst via RSVPN

Revisionshistorik

Datum	Ver.	Namn	Kommentar
2011-06-14	0.1	Johan Åbrandt	Upprättad
2011-06-29	1.0	Johan Åbrandt	Fastställd av tf Chef IT Avdelningen

Beslutad

Datum:	Datum:
----------	----------
Underskrift dokumentförvaltare	Underskrift Chef IT-avd
----------	----------
Namnförtydligande	Namnförtydligande

Innehållsförteckning

1. Bakgrund och syfte

Mot bakgrund av de förändringar och den utveckling som skett och sker vad gäller tillgång till olika typer av IT infrastruktur som andra huvudmän med en relation till Region Skåne har, krävs riktlinjer för hur olika frågor bör hanteras.

Tidigare har medborgarna i Hälsoval Skåne kunnat göra ett eget val av vård och till offentlig och privat vård. Där var målet är att enheterna som omfattas ska kunna använda de Region Skåne system som krävs för att ha tillgång till och lämna relevant information.

På liknande sätt har entreprenad lagts för andra typer av verksamhet där man på samma sätt har behov av olika form av informationsåtkomst.

Sedan flera år har olika arbeten bedrivits i syfte att få fram en teknisk plattform med vilken system på ett säkert och tryggt sätt ska kunna utbyta information, exempelvis med övriga vårdgivare.

Detta arbete är krävande och pågår fortfarande. Vissa system och informationsmängder kan idag hanteras via denna plattform på ett säkert sätt över Internet. Mycket arbete återstår dock och många av Region Skånes nuvarande IT system kan inte utnyttja plattformen utan man får avvakta en ny generation applikationer och system innan detta kan realiseras fullt ut.

Tillgång till IT tjänster som i sig själv inte har tillräcklig säkerhetsnivå för åtkomst över internet, kan under tiden erbjudas via Region Skånes tjänst för extern åtkomst, RSVPN. Detta dokument beskriver riktlinjer och begränsningar för åtkomst till tjänster via RSVPN.

2. Definitioner och förkortningar

RSVPN
Region Skånes Virtual Private Network. En tjänst med vilken en användare kan ansluta sig fjärrmässigt till Regionens nät. Använder sig av eID (SITHS) kort och kryptering för en hög säkerhet.

3. Avgränsningar

Detta dokument beskriver endast riktlinjer för utnyttjande av de tekniska möjligheter för åtkomst som ges av RSVPN. Regler och förutsättningar för anslutning till denna och andra tjänster regleras i Region Skånes Ledningssystem för informationssäkerhet (se särskilt 9.1.3 Utomstående parter och 9.2.2 Extern åtkomst).

Detta dokument ersätter inte regler gällande RSVPN, se http://www.skane.se/templates/Page.aspx?id=258676.

4. Anvisning

Åtkomst till tjänst via RSVPN kan ges på 3 olika sätt:

1. ***Åtkomst till webb tjänst via bokmärke i RSVPN portalen:*** Kan användas för tjänst som i sig själv stödjer åtkomst via http eller https. Trafiken tunnlas från klientens dator via en inbyggd proxy i RSVPN till definierad server tjänst.
2. ***Åtkomst till terminal server session via bokmärke i RSVPN portalen:*** Kan användas för tjänster som i sig inte stödjer åtkomst via http eller https, till exempel äldre klient-server baserade tjänster. Klienten installeras på en terminal server (Citrix eller annan motsvarande VDI lösning). Trafiken tunnlas via inbyggd proxy i RSVPN till definierad terminal server eller gateway.
3. ***Åtkomst till tjänst på Region Skånes interna nätverk via upprättande av nätverktunnel mellan klientdator och Region Skånes interna nätverk:*** En VPN tunnel på IP nivå skapas vilket innebär att nätverkstrafiken i detta alternativ inte tunnlas via inbyggd proxy i RSVPN. I detta alternativ så ansluts klientdatorn till Region Skånes interna nätverk vilket innebär väsentligt högre säkerhetsrisk än alternativ 1 och 2. Vid användning av detta alternativ så begränsas klientdatorns möjlighet till kommunikation med annat nätverk än Region Skånes (split tunneling tillåts inte), för att minimera risken för att den upprättade nätverkstunneln kan användas för riktade angrepp eller virusspridning mot Region Skåne.

RSVPN stödjer 2 inloggningsmetoder: Inloggning med eID kort och inloggning med engångslösenord via SMS. De olika inloggningsalternativen ger olika möjligheter till åtkomst:

- För åtkomst till system som behandlar patientinformation eller personuppgift gällande person som är patient eller vårdpersonal, så krävs inloggning med eID kort.
- För åtkomst till tjänst via bokmärke i RSVPN portalen (alternativ 2 och 3) så krävs inloggning med eID kort såvida tjänsten inte står på nätverk avskiljt från Region Skånes övriga interna nätverk (DMZ).
- För åtkomst till tjänst via upprättande av nätverkstunnel på IP nivå (alternativ 3) så krävs inloggning med eID kort. Detta eftersom denna åtkomstmetod exponerar Region Skånes interna nätverk för högre risk och därmed kräver en säkrare identifiering av användaren.

Åtkomst till tjänst via RSVPN ska i första hand ges genom alternativ 1 eller 2: Åtkomst till webb tjänst via bokmärke i RSVPN portalen eller Åtkomst till terminal server session via bokmärke i RSVPN portalen.

Åtkomst till tjänst på Region Skånes interna nätverk via upprättande av nätverktunnel mellan klientdator och Region Skånes interna nätverk (alternativ 3) ska endast användas i undantagsfall. Detta eftersom alternativ 3 dels innebär högre risk för Region Skånes interna nätverk, dels innebär att klientdatorns möjlighet att nå tjänster utanför Region Skånes interna nätverk begränsas (split tunneling tillåts inte). Detta kan till exempel innebära att användaren av klientdatorn inte har möjlighet att använda tjänster som normalt nås via det lokala nätverket (skrivare, administrativa system, vårdtjänster utanför Region Skånes nätverk) samtidigt som klientdatorn är ansluten till tjänst på Region Skånes nätverk.