LEDNINGSKANSLIET

2015-05-13 Dnr C2015/303

Regler för fjärranslutning till Karlstads universitets datanät

Syfte

Reglernas syfte är att klargöra de styrande principerna och definitionerna som gäller för fjärranslutning av digitala enheter (datorer, surfplattor och smarta telefoner) till Karlstads universitets datanät. Reglerna är framtagen i enlighet med *Tillåten användning/etiska regler för Sunet (http://www.sunet.se/Om-sunet/Policyfragor/Tillaten-anvandning.html)*.

Reglerna har arbetats fram av It-styrningsfunktionen på Ledningskansliet. Synpunkter har inhämtats från It-avdelningen och reglerna har diskuterats i It-beställarrådet.

Dokument

- Policy för fjärranslutning till Karlstads universitets datanät
- Regler för fjärranslutning till Karlstads universitets datanät
- Handläggningsordning för fjärranslutning till Karlstads universitets datanät

Beslut	CB 6/15	Dnr.	C2015/303	Ersätter	C2008/13
Giltighet fr.o.m.	2015-05-13	t.o.m.	tillsvidare	Handläggare	Claes Asker

Regler för fjärranslutning till Karlstads universitets datanät

Termer

- Digital enhet
  Med digitala enheter menas datorer, läsplattor och mobiltelefoner, men även framtida enheter som kan konsumera information över internet
- VPN
  VPN (Virtuellt Privat Nätverk) är en lösning som innebär att en säker förbindelse över Internet sätts upp mellan en digital enhet och det lokala nätverket och med vars hjälp det är möjligt att nå lokala system från annan plats utanför universitetets nätverk.
- Kau-dator:
  En dator som konfigurerats och preparerats av Karlstads universitets systemspecialister inom It-arbetsplats, för att följa en särskild specifikation. Benämndes tidigare DGD-dator.
- KauID
  En digital identitet som används för många system vid universitetet.
- GFS
  En systemförvaltningsmodell (Gemensam förvaltningsstyrning) som delar in universitetets system i samlande systemgrupper, beskriver organisation, planer och rutiner för systemgrupperna samt de samordnande funktionerna.
- DDM
  Ett system för DDM (Digital device management) hanterar digitala enheter i en organisation. Det gäller funktioner för hantering av installerad mjukvara, säkerhetsinställningar, lokalisering, backup mm.

Krav på anslutningen

Fjärranslutningen ska ske med hjälp av tekniken VPN och vara både krypterad och autentiserad. Anslutningen hamnar i ett relevant lokalt datanät som ger åtkomst till fastställda tjänster.

Alla anslutningstillfällen ska registreras för att kunna spåra otillåten anslutning till universitetets datanät. Den enda information som ska registreras för ändamålet är:

- En identifikator för den digitala enheten.
- En identifikator för användaren.
- Tidpunkter för då anslutningen startas och avslutas.
- IP-adressen från vilken anslutningen genomförs.

Krav på autentisering

All fjärranslutning till universitetets datanät ska ske med den digitala identiteten KauID och följa *Regler för digitala enheter vid Karlstads universitet (Dnr C2014/59)*.

Krav på digitala enheter

Skydd

Samtliga digitala enheter som fjärransluter till universitetets datanät ska, där så är möjligt, ha ett adekvat skydd aktiverat, så som anti-virus, brandvägg samt lösenkodslås.

Tekniska krav

En förutsättning för anslutning med VPN är att den tekniska lösningen som universitetet valt för VPN-tjänst fungerar på den anslutande digitala enheten.

Kau-dator

En Kau-dator har alltid korrekt skydd aktiverat och användaren är autentiserad mot universitetets användarregister. Därmed förutsätts en Kau-dator alltid följa gällande regler och kan därför ges samma åtkomst till tjänster då den fjärransluts som då den fysiskt befinner sig i universitetets datanät.

Övriga digitala enheter ägda av Karlstads universitet

Övriga digitala enheter som ägs av Karlstads universitet, så som Mac- och Linuxdatorer, suftplattor och mobiltelefoner, kan fjärransluta via VPN till universitetets datanät under förutsättning att enheten är korrekt skyddad enligt rubriken *Skydd* ovan. Den digitala enheten ska även vara registrerad och aktiv i något av universitetets DDM-system.

Åtkomst till interna tjänster är beroende av vilken användare som ansluter med den digitala enheten.

Anställdas privata digitala enheter

För privata digitala enheter gäller samma regler som för övriga digitala enheter ägda av Karlstads universitet, med skillnaden att enheten inte ska registreras i ett DDM-system.

Anställdas enheter har endast åtkomst till fastställda bastjänster.

It-konsulters digitala enheter

För it-konsulters digitala enheter gäller samma regler som för övriga digitala enheter ägda av Karlstads universitet, med skillnaden att enheten inte ska registreras i ett DDM-system.

It-konsulters enheter har endast åtkomst till utvalda specifika tjänster.

Krav på användaren

Anställda

Om den anställde misstänker att VPN-anslutningen missbrukas av någon annan eller om den digitala enheten har förkommit ska detta omgående anmälas till It-avdelningens grupp för incidenthantering, med fördel via e-postadressen irt@kau.se.

Anställda som inte använder Kau-dator måste säkerställa att skyddet på den digitala enheten fortsatt är det samma som då VPN aktiverades.

It-konsulter

It-konsulter som får en VPN-anslutning ska alltid teckna en individuell sekretess- och ansvarsförbindelse för användning av universitetets it-resurser.

Om it-konsulten misstänker att VPN-anslutningen missbrukas av någon annan eller om den digitala enheten har förkommit ska detta omgående anmälas till It-avdelningens grupp för incidenthantering, med fördel via e-postadressen irt@kau.se.

Tjänster via VPN

Med åtkomst till universitetets datanät ges också åtkomst till digitala tjänster, system och applikationer, som normalt inte görs tillgängliga utanför universitetets datanät. Tjänsterna är indelade i tre kategorier.

Bastjänster

Bastjänster är tjänster som alla anställda har åtkomst till via VPN-anslutning. Exempel på det är lagring, egenrapportering och intranätet. Aktuella bastjänster ska alltid finnas angivna på webbplats för medarbetare.

Specifika tjänster

GFS-tjänster

Systemspecialister och it-specialister ska alltid ges möjlighet att ansluta via VPN till relevanta tjänster för att utföra sina arbetsuppgifter på distans. Arbetsuppgifterna ska vara relaterade till de system och applikationer som är definierade inom respektive GFS-systemgrupp.

För VPN-åtkomst till GFS-tjänster krävs att den anslutande digitala enheten ägs av universitetet.

Tjänster för it-konsulter

Där så är nödvändigt ska it-konsulter ges VPN-åtkomst till digitala tjänster på universitetets datanät. Tjänsterna ska vara explicita och avgränsade till konsultens uppdrag och åtkomsten ska avslutas i anslutning till att uppdraget avslutas.

Övriga tjänster

Åtkomst till övriga tjänster sker på individuell basis och ska alltid godkännas av förvaltningsledare It-arbetsplats. Exempel på detta kan vara en forskares behov att åtkomst till ett system som används inom ett forskningsprojekt.

För åtkomst till övriga tjänster krävs att den anslutande digitala enheten ägs av universitetet.