IT-STYRNING

2022-04-25 Dnr C2015/643

Allmänna regler för informationssäkerhet vid Karlstads universitet

Syfte

Syftet med de allmänna reglerna är att beskriva det alla verksamma vid Karlstads universitet ska känna till för att kunna bidra till en god säkerhetskultur och att skydda verksamhetens information. Handledningen är framtagen i enlighet med MSBFS 2009:10.

Arbetet med dokumentet har skett i Informationssäkerhetsgruppen. Synpunkter har inhämtats från It-avdelningen och systemförvaltningsorganisationen samt via remiss till fakulteterna, Lärarutbildningen och Centrala stöd.

Dokument

- Policy för informationssäkerhet vid Karlstads universitet
- Allmänna regler för informationssäkerhet vid Karlstads universitet

Dokumenthistorik

Datum	Förändring
2016-01-11	Första utgåvan. Arbetades fram av It-styrningsfunktionen på Ledningskansliet. Synpunkter hämtades från It-avdelningen och It-säkerhetssamordnaren.
2022-04-25	Anpassningar för ansökan om Swamid Assurance Level 3: Tillägg om andra faktorer under *Åtkomst och användaridentitet*.

Allmänna regler för informationssäkerhet vid Karlstads universitet

För att upprätthålla en tillräcklig skyddsnivå för information och systemmiljö måste vi arbeta gemensamt och kontinuerligt. Uppsatta säkerhetsregler och styrdokument inom it-området[1] ska tillämpas och efterlevas av samtliga verksamma inom Karlstads universitet, de vill säga alla medarbetare, studenter, partners och konsulter i verksamheten.

Information – oavsett om det är muntlig, skriftlig, i elektronisk form, alla former av forskningsmaterial, tentamina med mera – är en tillgång som i likhet med personal och fysisk egendom är avgörande för vår verksamhet. Myndigheten för samhällsskydd och beredskap anger därför i föreskriften MSBFS 2009:10 hur svenska myndigheter ska arbeta med informationssäkerhet. Med informationssäkerhet menas säkerhet för informationstillgångar avseende förmågan att upprätthålla önskad konfidentialitet, riktighet, tillgänglighet och spårbarhet.

Samtliga verksamma ansvarar för att känna till och följa gällande regler för informationssäkerhet inom Karlstads universitet.

Hantering av känslig information

Med känslig information menas exempelvis information som omfattas av eller kan komma att omfattas av sekretess eller som av andra skäl ej bör spridas till obehöriga.

Vid hantering av känslig information måste du tänka på att:

- Du bara får ta del av den känsliga informationen som du behöver för att kunna utföra ditt arbete.
- Känslig information i pappersform ska låsas in när den inte används så att obehörig åtkomst förhindras[2].
- Känslig information endast får skickas i krypterad form när den skickas via e-post. Kontakta It-supporten för hjälp.
- Känslig information aldrig får diskuteras på allmän plats eller om risk finns att obehöriga kan ta del av uppgifterna.
- Då känslig information visas på bildskärm får skärmen inte vara synlig för obehöriga. Kontakta It-supporten för tips om hjälpmedel.

Incidentrapportering

Incidentrapportering är en viktig del av Karlstads universitets informationssäkerhetsarbete. Du som användare ska hjälpa till genom att:

- Snarast möjligt rapportera incidenter som kan påverka informationssäkerheten.
- Rapportera incidenter till irt@kau.se eller anknytning 2525.
- Även rapportera misstankar om incidenter.

---

[1] Inslaget › It-styrning › Styrdokument för IT

[2] FB 35/14: Skydd av kontor för chefer

Exempel på informationssäkerhetsincidenter är:

- Felaktig, olovlig eller skadlig hantering av information som kan innebära negativ påverkan för Karlstads universitet.
- Information som kommit i orätta händer.
- Stöld av utrusning.
- Dataintrång.
- Skadlig kod (så som virus) eller skadlig programvara.
- Försök att vilseleda en användare att lämna ut personlig information, lösenord eller att klicka på osäkra länkar.

Användning av it-system

Användning av it-system, så som e-post, lärplattform, bibliotekssystem, reserapporteringssystem, fakturahanteringssystem, intranät, lagringstjänst etc, är till för verksamhetsrelaterade uppgifter. Grundregeln är att it-system inte får användas för privat bruk. Avsteg från grundregeln hantera av respektive it-systems förvaltningsorganisation[3].

It-utrustning och bärbar media

Vid hantering av it-utrustning och bärbar media ska du tänka på att:

- Universitets utrustning primärt ska användas för verksamhetsrelaterade ändamål.
- Det inte är tillåtet att använda universitetets utrustning i samband med bisysslor.
- Endast utrustning som är konfigurerad enligt av universitet definierad standard får kopplas upp mot nätverket[4].
- Arbetsrelaterad information på lokal hårddisk eller bärbar media alltid ska säkerhetskopieras och förvaras säkert. Där så är möjligt ska informationen sparas på angivna ställen (nätverksdiskar, diarium, Dokumenthörnan etc).
- Information i datorer, mobiltelefoner och på papper ska skyddas fysiskt, dvs de får inte lämnas obevakade.
- Bärbara datorer, mobiltelefoner, surfplattor etc alltid ska vara skyddade mot obehörig åtkomst genom användande av lösenord, pinkod eller motsvarande[5].
- Känslig information ska krypteras då den lagras på bärbar it-media. Kontakta It-supporten för hjälp.

Distansarbete

Vid arbete på distans ska du tänka på att:

- Fjärranslutning mot Karlstads universitets nätverk endast får ske genom godkända kommunikationslösningar för fjärranslutning[6].
- Endast utrustning som uppfyller Karlstads universitets säkerhetskrav får kopplas upp mot universitetets interna nätverk[6].
- Känslig information förvaras och hanteras på ett säkert sätt enligt gällande säkerhetskrav.

---

[3] Inslaget › It-styrning › Systemförvaltning

[4] Regler för fjärranslutning

[5] Regler för digitala identiteter

[6] Regler för fjärranslutning

- Känslig information alltid ska krypteras vid lagring på flyttbara medier så som bärbara datorer, usb-minne och mobiltelefoner. Kontakta It-supporten för hjälp.

Åtkomst och användaridentitet

Avseende åtkomst och användaridentitet ska du tänka på att:

- Dina åtkomsträttigheter är personliga och aldrig får delas med andra. Du är personligt ansvarig för de aktiviteter som utförs via dina inloggningsuppgifter.
- Dina användaridentiteter, lösenord, andra faktorer (inklusive e-legitimation för medarbetare) och passerkort är personliga och aldrig får lånas eller lämnas ut[7].
- Du omedelbart ska rapportera incident om du misstänker att någon obehörig känner till ditt lösenord eller om du tappat bort ditt passerkort. Byt även snarast ditt lösenord.

Loggning och logganalys

Avseende loggning och logganalys gäller följande:

- All internetanvändning loggas.
- För system som innehåller känsliga uppgifter genomförs loggning av alla användaraktiviteter, dvs allt vi gör i systemet.
- Syftet med loggningen är att kunna säkerställa att endast behöriga personer har tagit del av en viss information.
- Logganalys genomförs regelbundet.
- Loggar gallras enligt gällande föreskrifter.

6 saker att tänka på!

1. Tänk på i vilken miljö du befinner dig i när du hanterar och talar om känslig information.
2. Undvik att skicka känslig information via e-post. Om så sker ska den krypteras. Kontakta It-supporten för hjälp.
3. Lås eller logga ut från din digitala klientenhet när du går därifrån.
4. Skydda dina inloggningsuppgifter och lämna aldrig ut dem samt svara aldrig på e-postmeddelanden som frågar efter ditt lösenord.
5. Ladda inte ner filer och öppna inte bilagor eller länkar i e-post om du är osäker på vad de innehåller eller vem avsändaren är.
6. Se till att din information är säkerhetskopierad oavsett om den är lagrad på stationär dator eller bärbar it-media. Kontakta It-supporten för hjälp.

Vi har alla ett ansvar!

Informationssäkerhet baseras i huvudsak på sunt förnuft och gott omdöme, där ditt omdöme och ditt agerande är avgörande. Sammantaget är detta viktiga förutsättningar som bidrar till att upprätthålla förtroendet för vår verksamhet och säkerställa den information som vi hanterar.

---

[7] Regler för digitala identiteter