Dokumentnamn: Grundläggande informationssäkerhet för studenter och elever		Revision: 04
Dokumenttyp: 8.4.1.1.1-4 utbildningsmaterial	Dokumentnummer: 21-345	
Detta dokument gäller för: Region Blekinge	Funktionsområde: Informationssäkerhet	
Dokumentansvarig: Informationssäkerhetsstrateg	Beslut av: Säkerhetschef	
Beslut datum: 2023-05-25	Nästa revidering: 2024-05-30	

Grundläggande informationssäkerhet för studenter och elever

Innehållsförteckning

Informationssäkerhet

Ansvarig chef för studenter ska säkerställa att de tar del av framtagen grundläggande information gällande informationssäkerhet. Ansvarig chef ska bedöma om ytterligare kunskap behövs för att den externa användarens ansvar och uppgift ska kunna utföras på ett säkert sätt.

Mer information om gällande regelverk och riktlinjer för informationssäkerhet finns på Intranätet Ledning och styrning/Arbetssätt/Säkerhet/Informationssäkerhet/Introduktion till informationssäkerhet

Samtycke till studentmedverkan

När en student eller elev ska delta i vårdarbetet av en patient skall samtycke alltid inhämtas. En patient har rätt att säga nej till att studenten medverkar.

Medlyssning

Medlyssning innebär att en student i lärandesyfte lyssnar på ett samtal mellan vårdpersonal och patient. Det gäller både via fysiska möten, telefonrådgivning samt chatt. Samtycke till medlyssningen ska alltid inhämtas och dokumenteras i journalen, även om studenten inte medverkar i samtalet.

Sekretess och Tystnadsplikt

Alla som arbetar inom hälso- och sjukvården, både offentlig och privat, arbetar under sekretess och tystnadsplikt. Det innebär att alla uppgifter som rör patientens personliga förhållanden skyddas av sekretess och får enbart lämnas ut efter särskild prövning.

Brott mot sekretess och tystnadsplikt kan få rättsliga påföljder. Den som bryter mot tystnadsplikten kan dömas i domstol eller på andra sätt bli föremål för åtgärder av de myndigheter som har tillsyn över vården.

Sekretess

Sekretess innebär förbud att röja eller utnyttja uppgift. Förbudet gäller oavsett om det sker muntligen, skriftligen eller på något annat sätt. Sekretessen gäller både mot enskild och andra myndigheter. Sekretessen regleras av offentlighets- och sekretesslagen (2009:400)

Tystnadsplikt

Den som arbetar, praktiserar eller på annat sätt har uppdrag inom Region Blekinge har tystnadsplikt. Tystnadsplikten gäller samtliga verksamheter och innebär att man inte får lämna ut särskild information om det inte finns lagstöd för detta. Tystnadsplikten gäller även efter avslutat uppdrag och resten av livet. Tystnadsplikt regleras i patientsäkerhetslagen (2010:659)

Rent skrivbord och tom skärm

Det är inte tillåtet att lämna en dator olåst utan uppsyn.
Det är inte tillåtet att låta någon annan använda din dina inloggningsuppgifter.
Lämna ingen känslig information synlig för obehöriga.

Informationshantering

Informationsklassning – lagring och delning av information

Information som lagras, oavsett plats, behöver klassas så att du som användare vet var och hur informationen får hanteras och lagras samt om informationen får delas med någon annan utomstående. På Region Blekinge klassar vi informationen i nedan beskriva nivåer.

Öppen information

Allmänna offentliga handlingar och information avsedd att spridas externt. Får inte innehålla personuppgifter.

Intern information

Arbetsmaterial och information skapad i det dagliga arbetet och avsedd för internt bruk. Kan innehålla personuppgifter enligt dataskyddsförordningen. Det får inte innehålla känsliga personuppgifter (se definition för känsliga personuppgifter under rubriken sekretessbelagd information).

Personuppgifter är enligt dataskyddsförordningen all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet, t.ex. adress eller en mailadress.

Konfidentiell information

Information som är avsedd att hållas konfidentiell inom en viss grupp av personer och inte avsedd att göras allmänt känd. Exempel på konfidentiell information är t.ex. ekonomisk rapport, tekniska beskrivningar och systemdokumentation på hög nivå, lösenord, HSA-id och användar-id som är kopplat till enskild individ.

Konfidentiell information kan också t.ex. vara löneuppgifter, uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler, uppgifter om sociala förhållanden.

Sekretessbelagd information

Uppgifter eller annan information som är sekretessbelagd enligt offentlighets- och sekretesslagen eller känsliga personuppgifter enligt dataskyddsförordningen.

Exempel på sekretessbelagd information är fastighetsritningar över t.ex. vatten- och el-försörjning, beskrivning av infrastruktur, nätarkitekturskisser, säkerhetsanalyser, tekniska beskrivningar och systemdokumentation på detaljnivå, domänadministratorslösenord.

Ett annat exempel är upphandlingsdokumentation som är sekretessbelagd under upphandlingsfasen, och därefter offentlig handling.

Exempel på sekretessbelagd information som kan gälla enskild person är uppgifter rörande sjuk- och hälsovård, tillstånd för färdtjänst, omplacering av anställd och anställdas privata uppgifter kring adress, telefonnummer mm, skyddade personuppgifter, forskningsresultat kring enskilda. Folkhögskolan omfattas även av sekretess avseende studie- och yrkesvägledning och elevvårdande verksamhet i övrigt. Det kan också vara förberedelser inför revision eller annan granskning, säkerhets- och bevakningsåtgärder.

Exempel på känsliga personuppgifter kan vara etniskt ursprung, politisk åsikt, religion, facktillhörighet, uppgifter om hälsa t.ex. biometriska och genetiska uppgifter, patientuppgifter, sexualliv eller sexuell läggning.

Säkerhetsskyddsklassad information

Information med högt skyddsvärde som rör Sveriges säkerhet.

Aggregerad information

Aggregerad information betyder att flertalet olika typer av uppgifter samlas och tillsammans utgör ett nytt skyddsvärde. Tänk på att till exempel många detaljerade tekniska beskrivningar eller detaljerade fastighetsritningar blir aggregerad information som klassas som högt skyddsvärde, det vill säga Säkerhetsskyddsklassad information och ska hanteras därefter.

Hantering av information
Konfidentiell och sekretessbelagd information får endast delas med begränsad grupp medarbetare inom Region Blekinge eller med betrodda parter utifrån tilldelade arbetsuppgifter.

Konfidentiell och sekretessbelagd information ska lagras på ett sådant sätt att inte obehöriga kan ta del av dem. Sekretessbelagd information får inte hanteras (lagras, delas) i molntjänster.

Riktlinjer för lagring och delning av information.

Informationsklassning och dokumentskydd
I Word, Excel och Powerpoint ska du ange vilken känslighet informationen i dina filer har och skydda dem beroende på vilken klassning du har kommit fram till att de ska ha. Du kan bestämma vilka som ska få läsa eller ändra i filen, för obehöriga är filen låst, oläsligt och krypterat. Välj mellan klassningen öppen, intern, konfidentiell och sekretess.

I verktygsfältet ikon **Känslighet** väljer du vilken nivå som dokumentet ska ha. Väljer du inte någon specifik känslighet blir dokumentet automatiskt klassat som intern.

E-post
Region Blekinges e-postsystem är ditt verktyg för kommunikation. Var restriktiv med vilken information du skickar i e-post.
Du är skyldig att följa de riktlinjer och rutiner som är beslutade i Region Blekinge.

Du får skicka konfidentiell och sekretessbelagd information internt inom regionen. Konfidentiell och sekretessbelagd information ska skickas krypterat utanför Region Blekinges domän.
Kopior till mottagare (CC) ska användas restriktivt för att minska risken för spridning.
Automatisk vidarebefordran är inte tillåten.

Klicka aldrig på länkar i e-post där du inte är säker på vem som är avsändaren. Lämna heller aldrig ut inloggnings- eller kontouppgifter.

Misstänker du att din dator drabbats av skadlig kod så kontakta IT Service Desk eller mejla spam@regionblekinge.se

Lär mer:
Riktlinjer för e-post

Användning av sociala medier, foto, filmning

Sociala medier
Region Blekinge närvarar i sociala medier för att möta Blekinges invånare, anställda i verksamheten och andra som är intresserade av den information som Region Blekinges olika konton förmedlar. Syftet med kanalerna att nå ut med budskap i form av inlägg kopplat till viktig information, arbetsgivarvarumärke och varumärkeskännedom. Delning i Region Blekinges sociala medier ska ske i enlighet med styrande dokument.

Känslig information i strid med svensk lag, Region Blekinges riktlinjer eller värdegrund får inte kommuniceras i sociala medier.

Du får inte publicera uppgifter som är konfidentiella eller sekretessbelagda. Du får inte heller dela uppgifter i privata meddelande, slutna grupper eller liknande.

Foto och film
Det är inte tillåtet att utan tillstånd fota eller filma inom Region Blekinges lokaler.

Känslig information i strid med svensk lag, Region Blekinges riktlinjer eller värdegrund får inte kommuniceras i sociala medier.

Du får inte publicera uppgifter av känslig karaktär. Du får inte heller dela uppgifter i privata meddelande, slutna grupper eller liknande.

Privat mobiltelefon
Privat mobiltelefon får som regel inte användas i lokaler där det bedrivs hälso- och sjukvård samt tandvård.

Dataintrång
Att ta del av patientjournal i annat syfte än vad som framgår av Patientdatalagen är i tillåtet. Du får endast ta del av uppgifter i Region Blekinges digitala system om det är uppenbart arbetsrelaterat.
Loggning av aktivitet i digitala system sker och granskas kontinuerligt.
Dataintrång kan leda till arbetsrättsliga åtgärder samt polisanmälan

Internetbaserad kommunikation
För användningen av Internetbaserad kommunikation, exempelvis röst- eller videosamtal, chatt och videomöte används bl.a. Microsoft Skype, Teams och Zoom. Var noga med att kontrollera vilken information som får delas och lagras. Se till så att ingen obehörig kan överhöra dina samtal.

Riktlinjer kring vad som får delas och lagras i internetbaserad kommunikation finns i dokumentet Riktlinjer för lagring och delning av information.

Incidenter
En oförutsedd händelse eller informationssäkerhetsincident kan vara avsiktlig eller oavsiktlig. Det kan vara allt från att någon obehörig tar del av regionens information till att du får ett virus som påverkar regionen eller att något verkar vara misstänkt och avvikande.

Om något oförutsett inträffar i IT-miljö ska du anmäla det till IT Service Desk (tfn 0455-73 62 00).

Du ska alltid anmäla informationssäkerhetsincidenter omgående till informationssakerhet@regionblekinge.se

Vid avslutat uppdrag
Region Blekinge äger arbetet och resultatet. Samtlig information (insamlad information, rådata, arbetsmaterial samt framställd rapport och kopior) ska lämnas över till ansvarig chef när avtalstiden/uppdraget avslutas och därefter raderas från studentens/elevens enhet.