Retningslinjer for brug af IT for ansatte og studerende

Rapportering af brud på persondatasikkerheden

SDU

Trusselsvurdering af den danske universitetssektor

Trusselsvurdering

Truslen fra cyber-spionage mod dansk forskning og universiteter

1. udgave september 2021

"Meget høj betyder, at der er aktører, der kan og vil løbende forsøge at angribe Danmark. Både cyberkriminelle og medarbejdere hos statslige aktører arbejder systematisk, vedholdende og målrettet på at ramme Danmark"

Center for Cybersikkerhed

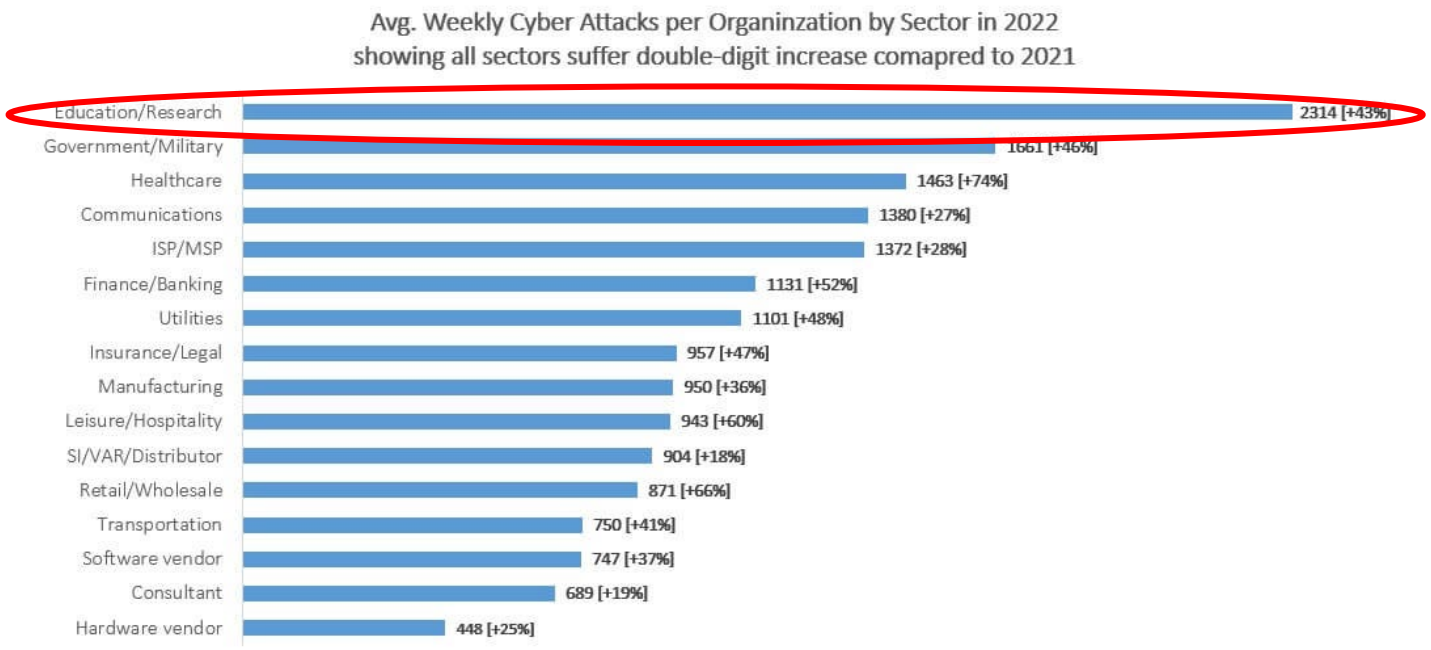
- Danske universiteter og forskningsinstitutioner er udsat for en MEGET HØJ trussel fra cyberspionage.
- Truslen kommer fra flere fremmede stater, der angriber forskning verden over.
- Danske universiteter og forskningsinstitutioner er også udsat for en MEGET HØJ trussel fra cyberkriminalitet. Universiteter kan f.eks., ligesom mål i mange andre sektorer, blive ramt af målrettede ransomware-angreb.
- Hackere forsøger ofte at få adgang til universiteters tværgående it-netværk, såsom mailsystemer. Det giver dem mulighed for at spionere mod flere fagområder inden for de enkelte universiteter på samme tid.

***Cyberspionage** betyder i praksis, at fremmede stater løbende forsøger at stjæle værdifuld information fra Danmark.*

***Cyberkriminalitet** er i denne vurdering en fællesbetegnelse for handlinger, hvor hackere bruger cyberangreb til at begå kriminalitet, der er motiveret af økonomisk berigelse.*

SDU

Gennemsnitlig ugentlige angreb per organisation fordelt per sektor i 2022



https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/

- → Stigning i globale angreb på 38% i 2022 sammenlignet med 2021.
- → Gennemsnitlig ugelige angreb pr. organisation var 1168 på verdensplan i Q4 2022.
- → Uddannelses sektoren havde gennemsnitlig 2314 angreb per organisation om ugen i 2022
- → stigning på 43% i 2022 i forhold 2021

(Foto: Foto: Thomas Hjort Jensen)

Hackere trængt ind i DTU's it-systemer: Op mod 25.000 brugere skal straks ændre adgangskoder

Hackere er trængt ind i DTU's systemer. Op mod 25.000 brugere skal omgående skifte deres adgangskoder.

24. august 2022 kl. 06.39

SDU

WANTED BY THE FBI

RUSSIAN FSB CENTER 16 HACKERS

Conspiracy to Commit Computer Intrusions; Conspiracy to Commit Wire Fraud; Wire Fraud; Computer Fraud – Unauthorized Access to Obtain Information from Protected Computers; Aggravated Identity Theft; Aiding and Abetting

PAVEL ALEKSANDROVICH AKULOV
(Павел Александрович Акулов)

MIKHAIL MIKHAILOVICH GAVRILOV
(Михаил Михайлович Гаврилов)

MARAT VALERYEVICH TYUKOV
(Марат Валерьевич Тюков)

CAUTION

On August 26, 2021, a grand jury sitting in the United States District of Kansas indicted three Russian Federal Security Service (FSB) officers for their alleged involvement in computer intrusion, wire fraud, and aggravated identity theft offenses. These officers were members of Center 16, an FSB component also known as Military Unit 71330, and were part of a team within Center 16 known by cybersecurity researchers as "Dragonfly," "Energetic Bear," and "Crouching Yeti." As alleged in the indictment, the three FSB officers, Pavel Aleksandrovich Akulov, Mikhail Mikhailovich Gavrilov, and Marat Valeryevich Tyukov, knowingly and intentionally conspired with each other, and with persons known and unknown, to obtain and maintain unauthorized persistent access ("hacking") to victim computer networks, belonging to companies and other entities in the global energy sector, including their power generation facilities, thereby enabling the Russian government to disrupt and damage such systems, if it wished. The defendants and their coconspirators targeted hundreds of American and international energy sector companies. Also targeted were over 380 foreign companies based in 135 countries including Albania, Australia, Belgium, Brazil, Canada, China, Croatia, Denmark, Finland, France, Germany, Hungary, India, Ireland, Italy, the Netherlands, Norway, Pakistan, Singapore, Slovakia, South Africa, South Korea, Spain, Sweden, Switzerland, and the United Kingdom. These companies included global oil and gas firms, utility and electrical grid companies, nuclear power plants, renewable energy companies, consulting and engineering groups, and advanced technology firms.

SHOULD BE CONSIDERED AN INTERNATIONAL FLIGHT RISK

If you have any information concerning this case, please contact your local FBI office or the nearest American Embassy or Consulate.

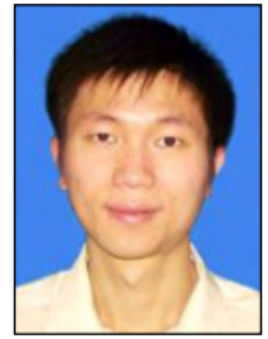
Field Offices: Portland, Richmond

www.fbi.gov

WANTED BY THE FBI

APT 40 CYBER ESPIONAGE ACTIVITIES

Conspiracy to Damage Protected Computers and Commit Economic Espionage; Criminal Forfeiture



Zhu Yunmin

Wu Shurong

Ding Xiaoyang

Cheng Qingmin

CAUTION

On May 28, 2021, a federal grand jury in the United States District Court for the Southern District of California returned an indictment against four People's Republic of China (PRC) citizens for their alleged roles in a long running campaign of computer network operations targeting trade secrets, intellectual property, and other high value information from companies, universities, research institutes, and governmental entities in the United States and abroad, as well as multiple foreign governments. The indictment alleges that Zhu Yunmin, Wu Shurong, Ding Xiaoyang, and Cheng Qingmin targeted the following sectors: aerospace/aviation, biomedical, defense industrial base, healthcare, manufacturing, maritime, research institutes, transportation (rail and shipping), and virus research from 2012 to 2018, on behalf of the PRC Ministry of State Security. Additionally, the indictment alleges the use of front companies by the PRC Ministry of State Security to conduct cyber espionage.

The four individuals are identified as:

ZHU Yunmin 朱允敏 (STC Codes: 2612/0336/2404) Alias: Zhu Rong

WU Shurong 吴淑荣 (STC Codes: 0702/3219/2837) Aliases: goodperson, ha0r3n, Shi Lei

DING Xiaoyang 丁晓阳 (STC Codes: 0002/2556/7122) Aliases: Ding Hao, Manager Chen

CHENG Qingmin 程庆民 (STC Codes: 4453/1987/3046) Alias: Manager Cheng

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

Field Office: San Diego

www.fbi.gov

Agenda

Retningslinjer for brug af IT for ansatte og studerende

SDU

Rapportering af brud på persondatasikkerheden

SDU

Find hjælp på databeskyttelse og informationssikkerheds siderne

https://sdunet.dk/da/servicesider/digitalisering-og-it/databeskyttelse

SDU


Serviceside

Digitalisering og IT

Databeskyttelse og informationssikkerhed på SDU

→ Administration

→ Forskning

→ Undervisning

SDU

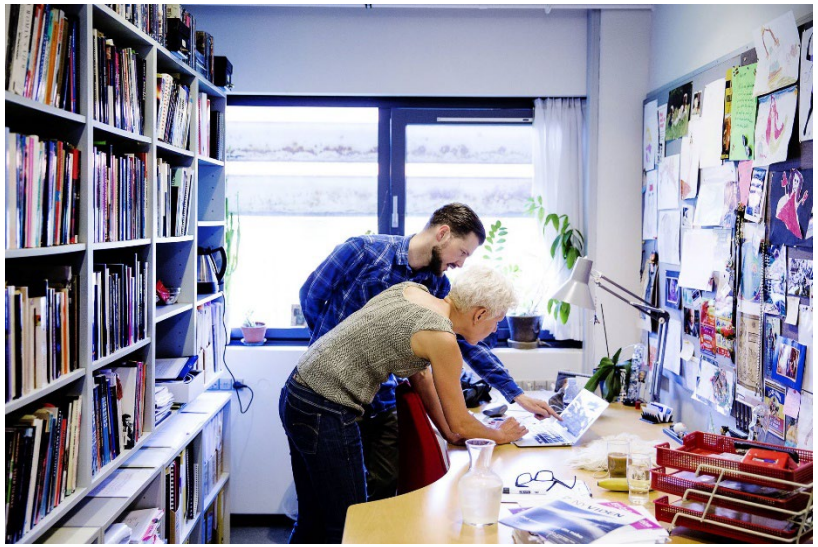
Retningslinjer for brug af IT for ansatte og studerende

SDU

Retningslinjer for brug af IT - ansatte

→ Revidering de personalepolitiske retningslinjers afsnit om it-anvendelse medførte, at Udvalget for Informationssikkerhed og Databeskyttelse (UID) i 2022 godkendte udmøntningen af politikken.

→ Retningslinjer for brug af IT for ansatte kan nu findes i en brugerrettet version på SDUnet.



Retningslinjer for brug af IT for ansatte

Du skal som ansat følge SDU's retningslinjer for brug af IT. Du kan i retningslinjerne finde mere om, hvad der er tilladt og hvad der ikke er tilladt, når du anvender SDU's udstyr, netværk og systemer.

Retningslinjerne gælder alle ansatte, og du kan løbende holde dig opdateret på SDUnet. IT omfatter udstyr, netværk, systemer, programmer mv.

Du er godt på vej, hvis du lærer nedenstående 10 bud for brug af IT. Du skal/må:

1. Anvende IT under iagttagelse af almindelig sund fornuft og under hensyntagen til studerende, ansatte og andre samarbejdspartnere.
2. Sikre at anvendelse ikke skader SDU's omdømme.
3. Ikke overlade udstyr, systemer mv. stillet til rådighed af SDU til børn, venner eller samlivspartner.

https://sdunet.dk/da/servicesider/digitalisering-og-it/databeskyttelse/sikkerhed/it-regler-for-ansatte

Uddrag fra retningslinjerne - ansatte

3. Ikke overlade udstyr, systemer mv. stillet til rådighed af SDU til børn, venner eller samlivspartner.

4. Som udgangspunkt kun anvende IT til løsning af arbejdsopgaver for SDU.

7. Som udgangspunkt ikke behandle oplysninger, der tilhører SDU, i systemer der ikke er godkendt af SDU IT. Hvis du undtagelsesvist installerer software som lokaladministrator, skal du selv sikre, at der er den fornødne licens og eventuel databehandleraftale.

10. Overveje hvilke private elementer, du opbevarer på din SDU-mail eller øvrige opbevaringsløsninger, da SDU er pålagt at have overblik over, hvilke aktiviteter der er på SDU's netværk, systemer mv.

→ Hvis du lader andre bruge SDU's installation af fx Word, får de også adgang til alle de data, du har adgang til i OneDrive, Teams og Sharepoint.
→ Der er i retningslinjerne eksempler på hvilken begrænset privat anvendelse, der findes acceptabelt. Fx at du bruger din PC til at tage referat til et møde i den lokale fodboldklub.
→ Der følger et ansvar med, hvis du benytter dig af muligheden for at bruge lokaladministratorrettigheder til at installere software bl.a. sikring af lovlighed og sikkerhedsopdateringer. Vær særligt opmærksom, hvis du behandler andres personoplysninger i softwaren.
→ SDU er forpligtet til at sikre, at systemerne ikke kan tilgås af uvedkommende, og at der er styr på hvem, der tilgår fx ansatte og studerendes personoplysninger.




SDU

Retningslinje for brug af IT - studerende

Retningslinjerne har været omkring Uddannelsesrådet og er nu tilgængelig i en brugerrettet version på MitSDU.

I tilfælde af overtrædelse af retningslinjerne eller forsøg herpå:

→ Sagen oplyses bedst muligt og forelægges relevant ledelseslag på fakultetet, som tager stilling til, om overtrædelsen skal håndteres efter regler om disciplinære foranstaltninger.

→ Såfremt det er tilfældet, sendes sagen til Juridisk Kontor (jura@sdu.dk).

→ Juridisk Kontor kan med fordel inddrages tidligere i forløbet, såfremt det findes relevant.

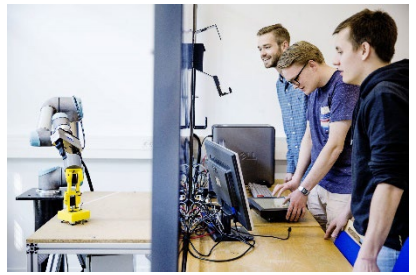
Retningslinjer for brug af IT for studerende

—

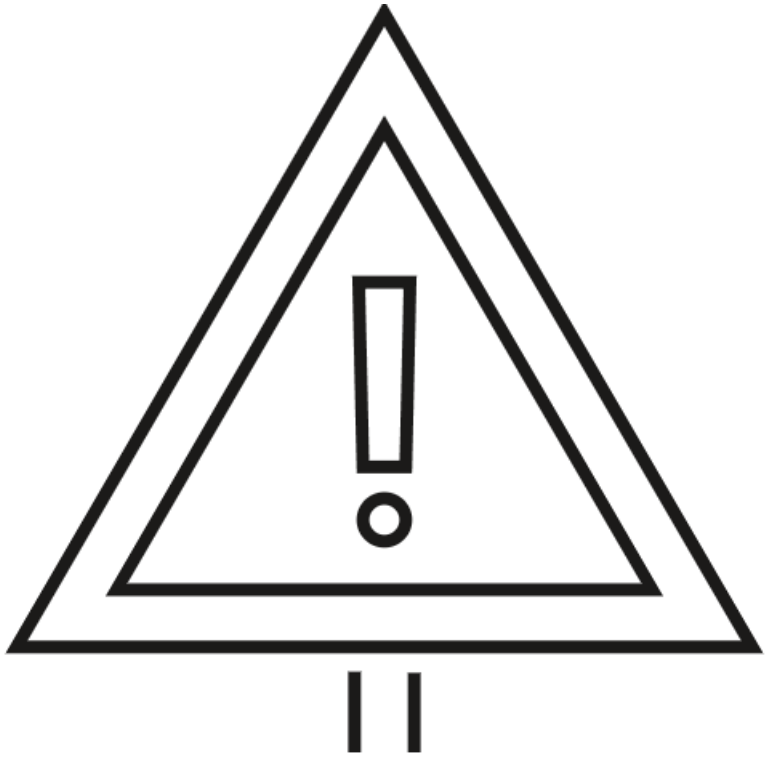
Du skal som studerende følge SDU's retningslinjer for brug af IT. Du kan i retningslinjerne finde mere om, hvad der er tilladt og hvad der ikke er tilladt, når du anvender SDU's udstyr, netværk og systemer.

Retningslinjerne gælder alle studerende, og du kan løbende holde dig opdateret på MitSDU. IT omfatter udstyr, netværk, systemer, programmer mv.

https://mitsdu.dk/da/mit_studie/kandidat/jura/vejledning-og-support/studerendeoggdpr/itreglerforstuderende



Rapportering af brud på persondatasikkerheden



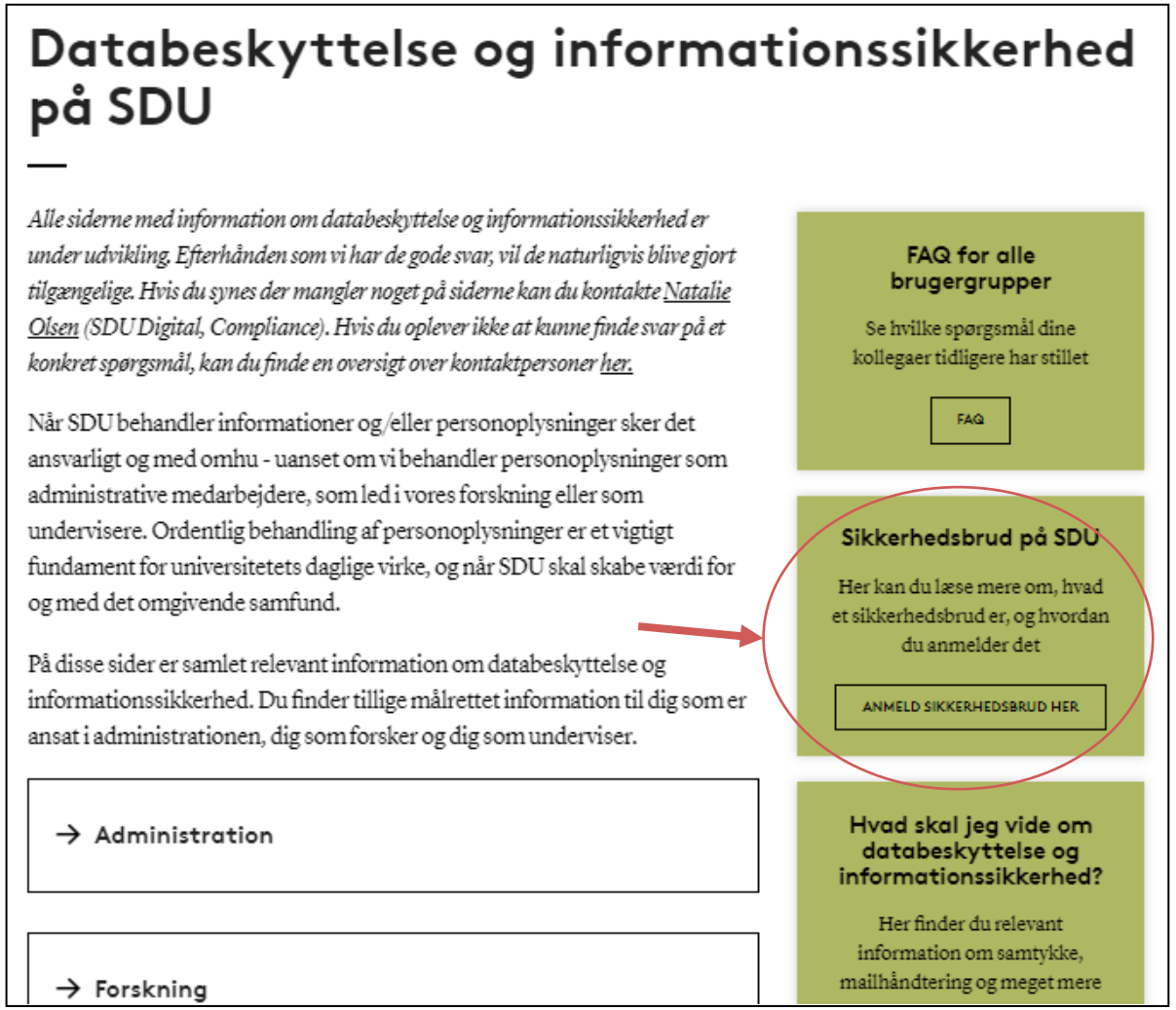
SDU

Ny proces for håndtering af brud på persondatasikkerheden

→ UID har godkendt en ny overordnet retningslinje for håndtering af brud på persondatasikkerheden

→ Formålet har været at:
- → Sikre ensartethed og smidighed i behandlingen af brud på tværs af organisationen.
- → Øge awareness omkring sikkerhed ift. SDU ejede informationer herunder personoplysninger.
- → Øge compliance i forhold til krav i GDPR om, at alle brud på persondatasikkerheden som udgangspunkt skal registreres.
- → Implementere en "lærende tilgang" til sikkerhedsbrud mhp. at kunne forebygge lignende hændelser i fremtiden.
- → Imødekomme kritik fra Datatilsynet i forbindelse med tidligere indmeldte brud.

https://sdunet.dk/da/servicesider/digitalisering-og-it/databeskyttelse

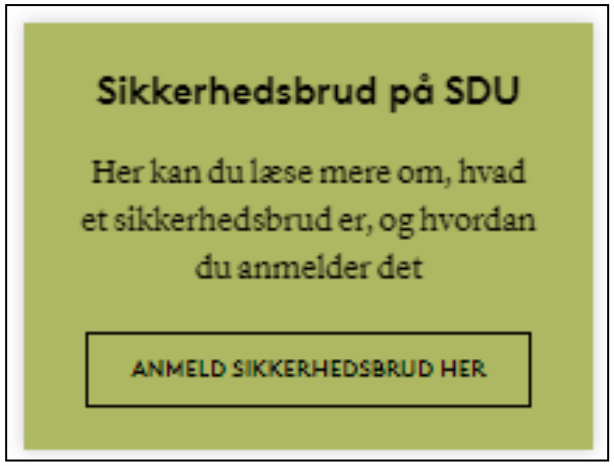


Hvornår skal jeg indrapportere et brud?

→ Der er som tidligere nævnt et krav i GDPR om, at alle brud på persondatasikkerheden skal registreres.

→ Hvornår er der tale om et brud på persondatasikkerheden?
  → Hændelig eller ulovlig tilintetgørelse, tab eller ændring af personoplysninger
  → Uautoriseret videregivelse eller adgang til personoplysninger (fx fejlforsendelser eller mangelfuld adgangsstyring)
  → Manglende tilgængelighed, som kan betyde en ulempe for brugeren (fx man ikke kan logge ind på digital eksamen)

→ Er du i tvivl, så meld hellere bruddet ind, så det kan blive vurderet.
→ Den som opdager et brud eller potentielt brud melder den ind via formularen på SDUnet.
→ SDU IT laver de første indledende undersøgelser fx undersøger om fejlsendt mail kan trækkes tilbage.
→ SDU RIO laver den juridiske vurdering om, der er krav om anmeldelse til Datatilsynet og underretning af de(n) registrerede.
→ SDU Digital Compliance sørger for opsamling og læring af hændelserne.



SDU

Vent ikke med at lave indberetningen

Krav om indberetning til Datatilsynet indenfor 72 timer
→ Hvis der er risiko for fysiske personer kan lide et tab eller ulempe fx:
  → Tab af kontrol med egne data
  → Risiko for identitetstyveri eller diskrimination
  → Tab af fortrolighed af data, der fx kan medføre skade på omdømme
  → Anden væsentlig økonomisk eller social ulempe for den registrerede

https://www.datatilsynet.dk/sikkerhedsbrud/omfattet-af-sikkerhedsbrud

Vi har en lærende tilgang til sikkerhedshændelser
→ Der er ingen, der laver fejl med vilje
→ Det skal være trygt at dele hændelser i afdelingen
→ Fokus på at forebygge, at det ikke sker igen fx for din kollega
→ Det er ledelsens ansvar, at der bliver skabt den nødvendige psykologiske tryghed, så medarbejdere åbent kan dele hændelser og lære af dem.
→ Det er en rigtig god idé at orientere din leder, hvis du oplever et brud på persondatasikkerheden.
→ Som indberetter af et brud vil man naturligt blive inddraget i udredningen, hvis der er brug for flere oplysninger.
→ Ved alvorlige brud, hvor der skal ske indberetning til Datatilsynet vil ledelsen i den ansvarlige afdeling og den systemansvarlige blive inddraget mhp. at skabe den nødvendige ledelsesmæssige forankring i forhold til læring af hændelsen.

SDU

Find hjælp på databeskyttelse og informationssikkerheds siderne

https://sdunet.dk/da/servicesider/digitalisering-og-it/databeskyttelse

Serviceside

Digitalisering og IT

Databeskyttelse og informationssikkerhed på SDU

Alle siderne med information om databeskyttelse og informationssikkerhed er under udvikling. Efterhånden som vi har de gode svar, vil de naturligvis blive gjort tilgængelige. Hvis du synes der mangler noget på siderne kan du kontakte Natalie Olsen (SDU Digital, Compliance). Hvis du oplever ikke at kunne finde svar på et konkret spørgsmål, kan du finde en oversigt over kontaktpersoner her.

Når SDU behandler informationer og/eller personoplysninger sker det ansvarligt og med omhu - uanset om vi behandler personoplysninger som administrative medarbejdere, som led i vores forskning eller som undervisere. Ordentlig behandling af personoplysninger er et vigtigt fundament for universitetets daglige virke, og når SDU skal skabe værdi for og med det omgivende samfund.

På disse sider er samlet relevant information om databeskyttelse og informationssikkerhed. Du finder tillige målrettet information til dig som er ansat i administrationen, dig som forsker og dig som underviser.

→ Administration

→ Forskning

→ Undervisning

FAQ for alle brugergrupper

Se hvilke spørgsmål dine kollegaer tidligere har stillet

FAQ

Sikkerhedsbrud på SDU

Her kan du læse mere om, hvad et sikkerhedsbrud er, og hvordan du anmelder det

ANMELD SIKKERHEDSBRUD HER

Hvad skal jeg vide om databeskyttelse og informationssikkerhed?

Her finder du relevant information om samtykke, mailhåndtering og meget mere

SE HER

→ GDPR-kursus for ansatte

→ Udvalget for informationssikkerhed og databeskyttelse

SDU

Spørgsmål?

SDU