Informationssikkerhedspolitik for Roskilde Universitet

Informationssikkerhedspolitikken er gældende fra 1. oktober 2024 og revideres næste gang september 2025. Politiken er godkendt af Universitetsledelsen (UL) den 25. oktober 2024.

INDHOLD

1.Formål med informationssikkerhedspolitikken

Informationssikkerhed handler om at beskytte informationer, såsom data, informationer og viden mod misbrug, uautoriseret adgang, afbrydelse, eller ødelæggelse. Det defineres som de redskaber og processer, som RUC anvender for at beskytte vores informationer. Det omfatter alt fra fysisk sikkerhed, beskyttelse af digitale enheder (servere, computere, tablets, telefoner osv.), datakryptering til netværks- og infrastruktursikkerhed samt test og revision.

Det er et krav til universiteter at have en informationssikkerhedspolitik, som anviser, hvordan lovgivningen på området implementeres i organisationen. RUC's informationssikkerhedspolitik fastlægger, hvordan vi på RUC arbejder med informationssikkerhed, forstået som anvendelse og forvaltning af systemer, løsninger, projekter, data, informationer og viden. Data, informationer og viden kan optræde både digitalt og som udprint, håndskrevne noter eller på anden vis i fysisk form.

I informationssikkerhedspolitikken finder du blandt andet vores fælles hovedmålsætninger, som vi alle skal arbejde frem mod, samt beskrivelse af - ansvar, god adfærd og de foranstaltninger, forstået som de handlinger og redskaber, vi implementerer for at forhindre uautoriseret adgang, afbrydelse eller ødelæggelse. Politikken beskriver RUC's overordnede tilgang til informationssikkerhed og udgør grundlaget for ambitionen om at udbrede informationssikkerhed i den hele organisation og overfor eksterne partnere.

Informationssikkerhed på RUC har til formål at understøtte RUC's værdigrundlag, vision og strategiske mål, og gør det muligt for RUC at opretholde sit omdømme som en anerkendt uddannelses- og forskningsinstitution.

1.1 Læsevejledning

Formålet med Informationssikkerhedspolitikken er at formidle både rettigheder og pligter i forbindelse med informationssikkerhed på RUC. Politikken uddybes og konkretiseres i en række vejledninger. Vejledningerne er at finde på RUC's serviceportal og i læringsplatformen Moodle til de studerende.

1.2 Hovedmålsætninger

Informationssikkerhedspolitikken afspejler til enhver tid RUC's niveau for informationssikkerhed, som fastsættes med udgangspunkt i eksterne krav og interne behov, og herunder særligt efterlevelse af gældende lovgivning, myndighedskrav og aftaler samt beskyttelse mod aktuelle trusler og heraf afledte risici.

RUC følger en risikobaseret tilgang til informationssikkerhed med risikostyringsmodel, der er opbygget efter de kvalitetsstyringsprincipper, som er specificeret i ISO27001-standarden, og som det fællesstatslige sikkerhedsprojekt anbefaler benyttes.

1.2.1 Beskrivelse af hovedmålsætninger

I arbejdet med informationssikkerhed indgår tre hovedmålsætninger, som det er vigtigt, at alle på RUC kender og forstår: fortrolighed, integritet og tilgængelighed.

Fortrolighed handler om at sikre, at informationer og viden ikke gøres tilgængelige eller afsløres for uautoriserede personer eller processer. Formålet med fortrolighed er, at informationerne kun er synlige og tilgængelige for de personer, der ejer dem eller har et dokumenteret arbejds- eller studiebetinget behov og dermed er autoriseret til at have adgang.

Integritet skal sikre, at informationer og viden er nøjagtige og fuldstændige, så de er pålidelige og ikke ændres til noget forkert, hverken utilsigtet eller tilsigtet.

Tilgængelighed omhandler, at informationer og viden er tilgængelig og anvendelig ved anmodning fra en autoriseret person eller proces.

1.3 Omfang

Informationssikkerhedspolitikken gælder både for aktiviteter (f.eks. behandling af data), personer og aktiver (f.eks. software og hardware). De tre hovedmålsætninger, fortrolighed, integritet og tilgængelighed, skal altid konkretiseres i formelle aftaler og kontrakter over for f.eks. samarbejdspartnere og andre, hvor dette er relevant.

Informationssikkerhedspolitikken samt aktuelle retningslinjer og vejledninger skal altid respekteres og anvendes. Det kan f.eks. være ved indkøb, anskaffelse eller bortskaffelse af aktiver samt ved deltagelse i aktiviteter, hvor der behandles data, informationer eller viden.

1.3.1 Beskrivelse af omfang for hhv. aktiviteter, personer og aktiver

Informationssikkerhedspolitikken gælder for alle RUC's data- og informationsrelaterede *aktiviteter*, uanset om disse udføres af ansatte på RUC - herunder institutterne og biblioteket - eller af samarbejdspartnere eller andre personer, som har en tilknytning til RUC.

Politikken er således gældende for *personer,* forstået som alle ansatte og studerende på RUC, samt samarbejdspartnere eller andre personer, som har en tilknytning til RUC, som udfører arbejdsopgaver så vel som læser på et studie på RUC.

Politikken omfatter altså al anvendelse, vedligeholdelse og installation i forbindelse med RUC's data og informationsaktiver. Politikken gælder også for alle RUC's egne *aktiver* og aktiver, som er linket, forbundet eller hvor der foregår opbevaring eller udveksling af data til eller med RUC's organisation

2. Organisering og ansvar

Ansvaret for informationssikkerhedens udmøntning på RUC er altid placeret hos universitetets øverste ledelse, rektoratet. Rektoratet kan delegere opgaver på de enkelte funktionsområder, inklusive vejledning og instruktion af ansatte, studerende, samarbejdspartnere og andre, for hvem informationssikkerhedspolitikken er gældende. Gældende procedurer formuleres og kommunikeres af respektive data- information- eller systemejere og/eller dekaner eller institutledelser ud fra informationssikkerhedspolitikken og gældende retningslinjer samt vejledninger.

2.1 Interne organisatoriske forhold

Informationssikkerhedspolitikken aktiveres og anvendes i RUC's samlede organisations fortløbende arbejde. Informationssikkerhed skal indgå både på det *strategiske*, det *taktiske* og det *operationelle* plan i RUC's organisation, og der skal foregå løbende rapportering til ledelsesniveauer om, i hvilken grad de informationssikkerhedsmæssige standarder, retningslinjer og vejledninger efterleves.

2.1.1 Beskrivelse af organiseringen på det strategiske, taktiske, og operationelle

På *det strategiske plan* udstikker rektoratet den overordnede retning for informationssikkerhed på RUC og definerer dermed, hvad RUC's behov for informationssikkerhed er. Dette sker på baggrund af informationssikkerhedsmæssige analyser, vurderinger, evalueringer fra Informationssikkerhedschefen (CISO), Databeskyttelsesrådgiveren (DPO) og den fælles IT-afdeling på RUC, som skal besidde de faglige ressourcer til at udføre og vejlede om dette arbejde.

På *det taktiske plan* er det CISO, som formaliserer og kommunikerer, samt har ansvaret for at analysere, vurdere, evaluere og fremtidssikre informationssikkerheden på RUC. CISO udstikker den overordnede retning for informationssikkerhed på RUC og oversætter det til retningslinjer og vejledninger for, hvordan RUC's besluttede sikkerhedsniveau kan opfyldes.

På *det operationelle plan* har alle, der drifter en løsning eller et system (f.eks. systemejere og systemforvaltere), der anvendes til at opbevare eller behandle data, informationer eller viden, pligt til at designe og implementere disse løsninger og systemer på en måde, så de lever op til de på RUC aftalte retningslinjer og vejledninger for informationssikkerhed. Det er også et krav at der i den efterfølgende drift af f.eks. et system skal sikres en måde, hvorpå det løbende kan kontrolleres, at løsningen eller systemet lever op til de gældende standarder og retningslinjer for informationssikkerhed på RUC.

2.1.2 Beskrivelse af rapportering på efterlevelse af standarder og retningslinjer

Den driftsansvarlige (f.eks. systemejer eller forvalter) for en løsning eller et system har ansvar for løbende at indsamle og indberette resultater til CISO om, hvorvidt løsningen eller systemet lever op til RUC's standarder og retningslinjer for informationssikkerhed. CISO har ansvar for at samle de indberettede resultater i en rapportering, der gør det muligt at opretholde et samlet overblik og foretage periodisk ledelsesrapportering. Formålet med den periodiske ledelsesrapportering er, at rektoratet har mulighed for at agere og prioritere i forhold til informationssikkerhedsmæssige udfordringer på tværs af hele RUC.

2.2 Samarbejdspartnere og engagementer

Alle, der behandler data, informationer eller viden for RUC, skal efterleve RUC's krav til informationssikkerhed. Det gælder altså ikke kun ansatte og studerende på RUC, men også samarbejdspartnere (f.eks. leverandører, gæsteforskere mv.) og andre personer som er tilknyttet eller har en relation til RUC.

2.2.1 Beskrivelse af samarbejdspartnere og engagementer i relation til informationssikkerhed

Hvis data, informationer og viden opbevares eller behandles uden for RUC, f.eks. hos en ekstern samarbejdspartner, skal denne samarbejdspartner være informeret om og efterleve de samme krav til informationssikkerhed, som der stilles internt på RUC. Ligeledes gælder, at hvis ansatte, studerende, samarbejdspartnere eller andre personer, som er tilknyttet RUC, transporterer eller anvender data, informationer eller viden uden for RUC, skal kravene til informationssikkerhed fra RUC stadig efterleves.

3. Brugeradfærd

At udvise god informationssikkerhedsmæssig adfærd er ikke blot en forventning, men en pligt, uanset om du er ansat, studerende, samarbejdspartner eller på anden måde tilknyttet RUC. På RUC arbejder vi derfor efter en række adfærdsprincipper, som også er forankret i din relation til RUC gennem f.eks. dit ansættelsesforhold, din indskrivning på et studie eller via din samarbejdsaftale eller kontrakt med RUC. RUC bestræber sig på at stille de nødvendige faciliteter til rådighed (f.eks. sikker opbevaring af data, informationer og viden) i et rimeligt omfang. Ved data, informationer og viden med særlige krav eller af signifikant omfang påhviler faciliteringsopgaven i udgangspunktet dataejer.

3.1 Adfærdsprincipper

Det forudsættes, at alle ansatte, studerende, samarbejdspartnere eller andre personer, som er tilknyttet RUC, til enhver tid agerer professionelt og udviser sund fornuft. Til at understøtte

dette arbejdes der efter tre overordnede principper for brugeradfærd, nemlig *transparens, accept* og *ansvarlighed*.

3.1.1 Beskrivelse af adfærdsprincipper for informationssikkerhed

Transparens defineres som, at vi på RUC bestræber os på at skabe et informationssikkerhedsmiljø, der er tydeligt dokumenteret og kommunikeret i retningslinjer og vejledninger, hvilket giver os alle mulighed for at agere digitalt forsvarligt i dagligdagen.

Accept betyder, at med muligheden for adgang til RUC's data og informationer følger et ansvar for at overholde informationssikkerheden på RUC, som du skal forholde dig til, forstå og acceptere.

Ansvarlighed, beskriver hvordan du på RUC har ansvar for dine egne handlinger, samt at hvis du bliver opmærksom på et informationssikkerhedsproblem, er det dit ansvar at reagere og melde problemet videre til rette instans.

3.2 Ansættelses-, indskrivnings-, aftale- og kontraktforholdet

Adgang til data eller informationer på RUC baseres altid på et dokumenteret arbejds- eller studiebetinget behov, som skal godkendes både af nærmeste leder og af den enhed, der ejer ansvaret for de givne data eller informationer. I tilfælde af, at de gældende bestemmelser for informationssikkerheden ikke overholdes, vil der blive sanktioneret i overensstemmelse med aktuelle bestemmelser på RUC.

3.2.1 Beskrivelse af arbejdsbetinget behov og sanktioner

Der er altid krav om et arbejds- eller studiebetinget behov for at få eller forsat have adgang til data, informationer eller viden på RUC. Et arbejds- eller studiebetinget behov skal kunne dokumenteres, når de nødvendige og tilstrækkelige rettigheder skal tildeles. Sådanne adgange skal også løbende kontrolleres, hvis der stilles krav herom. Nærmeste leder skal løbende sikre, at adgangen afspejler det aktuelle behov. Ansatte, studerende, samarbejdspartnere eller andre personer, som er tilknyttet RUC, der bryder de gældende bestemmelser for informationssikkerhed på RUC, kan sanktioneres disciplinært. De aktuelle bestemmelser herom fastsættes i overensstemmelse med den gældende personalepolitik, kontrakter og formaliserede aftaler på RUC og gælder både ansatte, studerende og samarbejdspartnere samt andre der på anden vis er tilknyttet RUC.

4. Funktionsadskillelse

På RUC arbejder vi proaktivt både i forhold til at beskytte vores organisation mod tilsigtede eller utilsigtede hændelser som f.eks. misbrug, uautoriseret adgang, afbrydelse, eller ødelæggelse, samt for at beskytte dig som ansat, studerende, samarbejdspartner eller anden person med tilknytning RUC mod uberettiget mistanke om at have begået tilsigtede hændelser. I dette arbejde er funktionsadskillelse, hvor opgaver og ansvarsområder adskilles for at forhindre fejl og misbrug af f.eks. adgangsrettigheder essentielt. Alle på RUC, som varetager data eller systemer har ansvar for at sikre at funktionsadskillelse er implementeret, hvor nødvendigt.

4.1 Beskrivelse af Funktionsadskillelse

Funktionsadskillelse defineres som, at du ikke kan eller må godkende eller hemmeligholde dine egne handlinger på visse områder. Det konkrete og aktuelle omfang at funktionsadskillelse på RUC skal begrundes og dokumenteres med udgangspunkt i interne forretningsmæssige eller organisatoriske behov eller eksterne krav. RUC stiller en hjemmeside til rådighed hvor du kan finde specifik vejledning om, hvordan du skal forholde dig til funktionsadskillelse.

5. Klassifikation af informationer, data og systemer

Alle RUC's informationer, data og systemer har værdi i varierende grad og skal klassificeres for at sikre, at de behandles, opbevares og evt. videregives korrekt i forhold til gældende bestemmelser og lovgivning. Alle på RUC, som arbejder med eller opbevarer data eller drifter et system eller en løsning, har ansvar for at sikre, at data, informationer og viden er klassificeret korrekt.

5.1 Beskrivelse af klassifikation af informationer, data og systemer

Klassificering betyder, at informationer, data og systemer mærkes ud fra deres type. Det vil f.eks. sige, om der er tale om behandling af fortrolige eller følsomme oplysninger, og om der f.eks. er krav om pseudonymisering eller anonymisering, inden oplysningerne må behandles, eller hvis der er tale om et system, hvor der skal laves særlige foranstaltninger grundet den type data, information, eller viden der behandles i systemet. Ved at klassificere informationer, data og systemer synliggøres deres værdi på en systematisk måde, og dermed kan de beskyttes i nødvendig og tilstrækkelig grad på et ensartet grundlag. RUC stiller en hjemmeside til rådighed hvor du kan finde specifik vejledning om, hvordan du skal forholde dig til klassifikation af data, information, viden eller systemer

6. Risikovurdering og analyse

På RUC arbejder vi med informationssikkerhed ud fra risikovurderinger, hvilket betyder, at vi løbende og proaktivt identificerer, evaluerer og håndterer risici forbundet med brugen af systemer, løsninger, projekter, data, informationer og viden. En risikovurdering er en systematisk proces, som har til formål at forstå, hvilke trusler og sårbarheder der kan påvirke sikkerheden, samt hvad konsekvenserne af disse kan være. Alle på RUC har ansvar for at risikovurdere de systemer, løsninger, projekter, data, informationer og viden man drifter eller er ansvarlig leder for.

6.1 Beskrivelse af risikovurdering og analyse

Den proaktive identifikation, evaluering og håndtering af risici udføres ved at lave en risikovurdering og analyse af konkrete systemer, løsninger, projekter, data, informationer eller viden efter RUC's metode og anvisninger. Formålet med risikovurdering og analyse er, at man gør sig bekendt med de aktuelle informationssikkerhedsmæssige risici, som er til stede, så vi kan træffe effektive og informerede beslutninger om, hvordan vi bedst beskytter vores data, informationer, viden og systemer. RUC stiller en hjemmeside til rådighed hvor du kan finde specifik vejledning om risikovurdering inklusiv en beskrivelse af RUC's metode.

versionshistorik

Version	Dato
0.1	08.02.2024
0.2	09.08.2024
0.3	02.09.2024