Indhold

1. FORMÅL

Procedurer for sikker anvendelse af IT.

2. GYLDIGHEDSOMRÅDE

IT-sikkerhed for brugere er gældende for alle medarbejdere på Teknologisk Institut og datterselskaber samt enhver der gives adgang til Instituttets netværk, herunder eksterne konsulenter, vikarer, praktikanter og medhjælpere.

3. ANSVARSFORHOLD

IT er ansvarlig for IT-sikkerhed, administration af rettigheder m.m. Medarbejdere er ansvarlige at følge de udstukket retningslinjer.

4. IT-SIKKERHED FOR BRUGERE

4.1. Adgangsforhold

Kun medarbejdere med tildelte initialer og underskreven aftale kan få adgang til Instituttets netværk via et personligt login.

Netværksadgang er senest tildelt på medarbejderens første arbejdsdag. Alle tildelinger og ændringer håndteres af Personale og Udvikling. Periodiske rettighedstildelinger kan kun gives efter henvendelse i Personale og Udvikling.

Password til netværk er strengt personlige og må aldrig overdrages. Password skal skiftes periodisk (hver 3. måned). Det nye password skal være unikt og afvige væsentligt fra det tidligere anvendte, og må ikke følge en systematik.

Password oplyses til medarbejder ved henvendelse i IT-afdelingen. Password nulstilles og rettes ved første login. Brugerne må ikke gemme deres password elektronisk, notere det eller videregives det til andre. Benyttes samme password i flere systemer skal password skiftes samtidig i alle systemer.

Tildeling af fysiske nøgler, adgangskort, tokens og andet registreres centralt og administreres af Personale og Udvikling, og holdes ajour i takt med ændringer, samt i forbindelse med nye ansættelser, flytninger og fratrædelser.

Der er permanent overvågning af al trafik på nettet i form af logning.

En PC skal låses, når den forlades, så andre ikke kan benytte adgangen (login) ved fravær. Skulle medarbejder glemme at låse PC, vil dette ske automatisk efter 20 minutter uden aktivitet.

4.2. Omgang med IT-aktiver (definition)

Det er den enkelte medarbejders personlige ansvar og pligt, at betjene det udstyr der stilles til deres rådighed ifølge de retningslinjer, regler og forskrifter der gives fra systemansvarlige/IT-afdelingen. Medarbejderen skal omgående rapportere problemer og fejl til nærmeste leder eller til den systemansvarlige/IT-afdelingen.

Generelt gælder:

- IT-udstyr må ikke overdrages til anden medarbejder uden om IT-afdelingen.
- IT-afdelingen kan på ethvert tidspunkt kræve bestemte programmer installeret og afinstalleret på en udstyr, for at sikre performance, stabilitet og sikkerhed.
- Det er ikke tilladt at modificere IT-aktiver og ændre deres fysiske fremtoning.
- Problemløsning på IT-udstyr kan medføre sletning af indholdet. Foretages der ikke systematisk backup af udstyret, skal alle data kopieres til Instituttets systemer ved først givne lejlighed.
- Kun systemansvarlige må foretage indgreb i systemopsætninger og maskineri, eller forsøge omgåelse af sikringssystemer i en afprøvningsfase.
- PC'ere, mobiltelefoner og øvrige databærende medier skal indleveres til rensning i IT-afdelingen, der beslutter eventuel overdragelse til anden medarbejder. Udstyr der ikke skal benyttes mere skal indleveres til IT afdelingen til rensning og skrotning.
- Bliver IT-udstyr stjålet, skal det øjeblikkeligt meldes til IT-afdelingen.

4.3. Programmer

Medarbejdere må kun downloade og installere programmer på Instituttets arbejdsstationer, hvis disse programmer er nødvendige for at se en given oplysning eller for udførelse af de daglige opgaver.

IT afdelingen forbeholder sig retten til på ethvert tidspunkt at lukke brugerens adgang til netværket, hvis installeret software udgør en sikkerhedsrisiko eller er i strid med licensregler.

Eventuelle ønsker om særligt licenserede programmer eller adgang til Cloud tjenester skal forelægges IT-chefen. Vurdering af anskaffelsen sker i samarbejde med den forretningsansvarlige og IT-chefen.

4.4. Lagring af data

Alle data skal gemmes på systemer med aktiv backup. Overførsel af data til computerens harddisk er kun tilladt som kopi, og må ikke foretages for fortroligt og personfølsomt materiale, medmindre harddisk benytter aktivt krypteringssoftware godkendt af IT-afdelingen.

Der foretages fuld backup af alle centralt placerede løsninger. Decentralt placerede løsninger som fx laboratorieudstyr foretages der tilsvarende backup af, hvis de er registret til backup i IT-afdelingen.

Overførsel af data til løse databærende medier, ud over sikkerhedskopiering, må ikke foretages af fortroligt og personfølsomt materiale.

Fortroligt og personfølsomt materiale må ikke kopieres til tjenester på Internettet som fx Dropbox. Det er ikke tilladt at anvende nogen former for automatiserede fil synkroniseringstjenester udover løsninger leveret af IT-afdelingen.

Databærende medier, som skal kasseres, skal afleveres til IT-afdelingen, som skal sørge for sletning eller overvåget fysisk destruktion. Der må ikke lagres data af fortroligt og personfølsomt materiale på databærende medier, medmindre medie benytter aktivt krypteringssoftware godkendt af IT-afdelingen.

Følgende prioriterede rækkefølge skal følges for datalagring:

1. **Grundsystemer**
   Som udgangspunkt skal data være lagret på vores grundsystemer som Økonomisystem, Opgavesystem, HR-web, QA mv., og der bør ikke håndteres data i kopi andre steder.
2. **GDPR mapper**
   Persondata som ikke opsamles i forbindelse med konkret opgaveløsning (med reference til opgaven), skal placeres i mapper mærket med GDPR. Der findes GDPR mapper på Organization, Personal, GDPRspace og i din Outlook til mails.
3. **Laboratoriedata/Måledata**
   Data der er opsamlet fra laboratorieudstyr eller tilsvarende skal lagres på TI Folders Labspace.
4. **Projektdata**
   Data som hidrører opgaver oprettet efter produktionskriteriet skal gemme på TI Folders Projects.
5. **Data fra kundeopgaver og administration**
   Øvrige data i forbindelse med opgaveløsning og administration skal gemmes i center- eller divisionsmapper på TI Folders Organization.
6. **Data med krav om særlige rettigheder**
   Data som har særlige dokumenterbare krav til adgangsforhold og arkivering kan gemmes på Workspace.

7. Ledelsesdata/Personlige data
Data som er streng personlige eller som benyttes i forbindelse med ledelse gemmes under TI Folders Personal.

4.5. Fillagring (TI-Folders)
Alle filer skal lagres på TI Folders, som er Instituttet centrale fil-arkiv. Sikring af databaser, systemer og tilsvarende skal ske separat gennem aftaler med IT-afdelingen, og må som udgangspunkt ikke lagres på TI Folders.

Udarbejdes materiale uden mulighed for opkobling til Instituttets netværk, skal materialet kopieres til Instituttets systemer og netværk ved først givne lejlighed.

TI-Folders er opbygget med syv primære adgange og en række arkiver, hvor medarbejderne kan lagre og dele filer.

- **Organization** – Hierarkisk opdeling af mappestruktur efter organisationsplan. Adgang gives alene efter organisatorisk ansættelsesforhold. I enkelte tilfælde har medarbejdere dobbelt ansættelse, men alle rettigheder til mapper sættes automatisk efter HR-system dagligt.
- **Organization Archive**
  Filer under Organization arkiveres automatisk årligt og flyttes til skrivebeskyttet arkiv. Filerne placeres i en spejlet mappestruktur fra Organization. Arkiverede data slettes efter 5 år. GDPR mapper er undtaget for arkivering.
- **Projects** – Rettigheder til mappestruktur følger oprettede projekter i Økonomisystemet. Medarbejdere med rettighed til at registrere timer på et projekt, vil automatisk have skriveret til projektmappen. Herudover har ledere og chefer i divisionen adgang og udvalgte medarbejdere i Økonomi.
- **Projects Archive**
  Projekter som er slutfaktureret (elimineret) i økonomisystem overføres til skrivebeskyttet arkiv. Arkiverede data gemmes løbende år plus 5 år.
- **Workspace** – Medarbejdere definerer selv læse og skriverettigheder på tværs af organisationen. Den medarbejder der opretter et Workspace vil med initialer stå som ejer, og vedkommende er den eneste, der kan administrere rettigheder til mappen. Workspace må kun anvendes hvis særlige adgangsrettigheder er påkrævet, særlige arkiveringsregler er påkrævet, ved samarbejde på tværs af divisioner eller ved håndtering af systemintegration hvor mappestruktur ikke må ændres
- **Workspace Archive** - Workspace mapper kan kun arkiveres af Workspace-ejer. Arkiverede mapper slettes efter 5 år. Skrivebeskyttet adgang gives automatisk til de medarbejdere, der tidligere har haft adgang. Tilhører en mappe en fratrådt medarbejder arkiveres mappen automatisk. Overførsel af ejerskab kan kun foretages af mappeejer. Er mappeejer fratrådt kan medarbejder med eksisterende adgang få tildelt ejerskab. I alle andre forhold skal der foreligge en godkendelse fra Personale og Udvikling.
- **GDPRspace**
  Variant af Workspace til GDPR data. Der foretages ikke automatisk sletning og arkivering.
- **Labspace** – Rettigheder til mapper oprettes ud fra laboratoriekonto som tilknyttes en eller flere laboratoriesystemer. En laboratoriekonto tilhører altid en ansvarlig medarbejder. Herudover kan en række personlige login tilknyttes, for at kunne udveksle data.
- **Labspace Archive** - Labspace mapper kan arkiveres af Labspace-ejer. Skrivebeskyttet adgang gives automatisk til de medarbejdere, der tidligere har haft adgang. Overførsel af ejerskab kan kun foretages af den ansvarlige for den tilknyttede laboratoriekonto.

- **Group** – Medarbejdere har kun læseadgang, og Group benyttes til at formidle centrale dokumenter fra Fællesfunktioner og bestemte ledelsesfunktioner.
- **Personal** – Personlig mappe hvor kun medarbejderen har adgang. Mappen må ikke bruges til filer i forbindelse med kundeopgaver. Ledere og chefer tildeles en GDPR mappe under Personal til medarbejderforhold.
  Personal Archive
  Filer under Organization arkiveres automatisk årligt og flyttes til skrivebeskyttet arkiv. Filerne placeres i en spejlet mappestruktur fra Organization. Arkiverede data slettes efter 5 år. GDPR mapper er undtaget for arkivering.

Alle rettigheder kontrolleres automatisk og dagligt mod ansættelsesoplysninger i Personale og Udvikling og system og projektrettigheder i Økonomisystem.

Backup af TI i Folders sker efter følgende specifikke regler:

- Der tages løbende backup af TI Folders og mindst hvert 24-72 time. Gemmes og slettes filen inden backupsystemet tager en kopi, kan indholdet ikke genskabes
- Åbne filer, systemfiler, databaser og mapper med mere end 100.000 filer kan der ikke garanteres backup af (*best effort*)
- Filer kan genskabes 30 dage tilbage fra dags dato - derefter er det i 30 dages intervaller, som gemmes fem år
- Filer på TI Folders fjernes ikke af IT-afdelingen, men bemærk, at genskabelse af filer fra backup kun kan garanteres fem år bagud.
- IT-afdelingen foretager ingen validering af om indholdet af filer i filmapper er korrekt. Det påhviler alene dataejerne at sikre, at de relevante filer er tilstede, og at denne validering sker under hensyn til de aftaler der indgås med eksterne og i forhold til denne politik.

4.6. Mails, Skype og anden digital kommunikation

E-mails og anvendelse af internettet i øvrigt betragtes som en del af Teknologisk Instituts forretningsmæssige korrespondance, som tilhører Instituttet. Teknologisk Institut har derfor til enhver tid ret til at gøre sig bekendt med og disponere over e-mailkorrespondance som enhver anden korrespondance til og fra Teknologisk Institut.

Mails opfattes som et arbejdsredskab, og det forventes derfor, at mails kun i begrænset omfang anvendes i privat sammenhæng. Såfremt Instituttets e-mails anvendes privat, skal dette anføres i emnefeltet med ordet ”Privat”.

Alle mails opsamles og vil kunne blive åbnet og læst i forbindelse med teknisk problemløsning. Instituttet forbeholder sig endvidere ret til at åbne alle e-mails eller spærre for trafik ved akut virusangreb, overvågning af driftsstatus samt ved mistanke om urigtig anvendelse eller misligholdelse af ansættelsesforholdet.

Medarbejderes postkasser betragtes som personlige. Medarbejdere kan selv give andre adgang og øvrige tildeles kun adgang af IT-afdelingen med skriftlig godkendelse fra personalechefen eller den administrerende direktør.

Medarbejdere har ansvar for at mails besvares hurtigst muligt, og medarbejdere kan ved fravær give andre medarbejdere adgang til deres oplysninger i Outlook gennem rettighedsstyring.

Stedfortræderrettigheder for personlige Outlook profiler må ikke benyttes (send på vegne af), medmindre godkendelse foreligger fra Personale og Udvikling.

Automatisk videresendelse af mail må kun ske til anden Institut-adresse, og aldrig eksternt for Instituttet.

Instituttets systemer må ikke anvendes til indhold af anstødelig, religiøs eller politisk art, og det er ikke tilladt for medarbejderne at sende SPAM mail som vittigheder, kædebreve og lignende. Brud på disse regler kan få konsekvenser for ansættelsesforholdet.

Der må ikke udsendes uopfordrede salgsfremmende budskaber, tilbud, nyhedsbreve eller tilsvarende i form af mail til kunder og partnere uden deres forudgående bestilling, accept eller godkendelse.

Alle udsendte mails skal indeholde Instituttets autosignatur med henvisning til Instituttets Privatlivspolitik.

Alle mails følger en slette politik på 5 år fra modtagelse eller afsendelse. Undtaget er filer flyttet til GDPR mappe som automatisk slettes efter 180 dage.

4.7 Midlertidige filer
Midlertidige filer, downloadede filer mappe og filer lagret i Papirkurv på PC slettes ugentligt.

4.8. Databeskyttelse i forbindelse med udveksling af data og digital signatur
Fysisk og elektronisk forsendelse af institutinformation til partnere, leverandører eller andre skal ske efter aftale med dataejer, og der skal foreligge en databehandleraftale. Såfremt der er tale om forretningsfølsom eller personfølsom information, skal indholdet krypteres. Kun krypteringssoftware godkendt af IT-afdelingen må benyttes.

Der skal udvises særlig opmærksomhed i forbindelse med printindhold, og hvem der har mulighed for at læse indholdet under udskrivning.

Anvendelse af digitale signaturløsninger kan ske som en integreret del af værktøjerne både til kommunikation og til identifikation. Det gælder ved login (identifikation) såvel som ved udveksling af signerede/krypterede elektroniske meddelelser med virksomheder, borgere og andre offentlige myndigheder. I en række funktioner vil det endvidere være nødvendigt, at medarbejdere har mulighed for at anvende offentligt NemID som adgangsnøgle til offentlige tjenester/internetportaler.

Elektroniske rapporter og certifikater kan endvidere signeres digitalt.

4.9. Labkonti (flerbrugerkonti)
Ud over det personlige login kan der til laboratorieudstyr tilknyttes en labkonto, som er en flerbrugerkonto, der kan benyttes af flere medarbejdere til at få adgang til laboratorieudstyr. En labkonto kan efter afdelingens ønske knyttes til en eller flere enheder, men der er altid en ansvarlig for kontoen. Stopper den ansvarlige medarbejder skal ansvaret overføres til ny ansvarlig medarbejder, der udpeges af nærmeste chef. Krav til skift og opbygning af password følger kravene til det personlige login.

Adgangsrettigheder for en labkonto giver kun adgang til den valgte labkonto og til en fildelingsfolder kaldet Labspace på TI Folders. Afdelingen kan til et Labspace (fildelingsfolderen) også udpege personlige

login som også skal have adgang, så data let kan deles og behandles. En labkonto giver ikke adgang til personlige ressourcer herunder mail.

4.10. Uddannelse af medarbejdere
Det er den enkelte leders ansvar, at medarbejderne gennem formel uddannelse og daglig træning, opnår en tilstrækkelig forståelse for Instituttets IT-systemer, så disse håndteres og betjenes korrekt, til sikring af at data altid er korrekte og valide, alternativt at fejl kan opdages.

Det er den enkelte leders ansvar at alle medarbejdere er bekendte med Instituttets IT-sikkerhedspolitikker, relevante IT-sikkerhedsregler, rapporteringsregler og konsekvenser ved brud på disse.

Enhver leder skal sikre IT-videndeling inden for sit ansvarsområde. Afdelingen skal gennem opgavefordeling, uddannelse og projektarbejde organiseres på en måde, der begrænser risikoen for, at der opstår ´nøglemedarbejdere´ på IT-funktioner.

4.11. Medarbejdernes opmærksomhed omkring IT-sikkerhed
Medarbejdere skal være opmærksomme på afvigelser fra det normale i brug af Instituttets IT-systemer: Ukendte mails, mails fra ukendte kilder, mails med ejendommelige overskrifter, dobbelt sign-on, hjemmesider, mails eller telefonopkald, som forsøger at lokke identiteter, koder og lignende fra brugeren, eller andre hændelser på computeren, som afviger fra hvordan systemet plejer at reagere.

Afvigelser skal omgående rapporteres til IT-afdelingen.

4.12. Anvendelse af Internetbaserede services (Cloudtjenester, sociale netværk mv.)
Dette punkt dækker enhver anvendelse af Internetbaserede services som for eksempel communities, sociale netværk, eksterne hjemmesider, fildeling og andre gruppebaserede tjenester.

Al anvendelse af Internet baserede services kræver forudgående godkendelse fra IT & Kommunikation, samt at der foreligger en databehandleraftale. Godkendte services kan findes kan findes i Positivlisten. I det omfang det er muligt skal adgang ske krypteret og ved anvendelse af 2-faktor identifikation.

Arbejdsrelateret ikke-fortroligt materiale af enhver art må kun publiceres efter forudgående godkendelse af centerchefen. Indeholder materialet personoplysninger, herunder billed- og videomateriale, om medarbejdere, kunder, leverandører og andre samarbejdspartnere, må publicering udelukkende ske med deres accept.

Instituttet har rettigheden til alt arbejdsrelateret materiale, der som led i Teknologisk Instituts aktiviteter produceres med henblik på publicering.

Enhver gruppe der etableres på de sociale medier, som repræsenterer Teknologisk Institut, og som benytter Instituttets navn og/eller logo skal godkendes af centerchefen og IT-chefen. Ejerskab af en sådan gruppe skal overdrages til nærmeste leder ved fratrædelse. Links til eksterne websteder er tilladt så længe webstederne ikke indeholder eller har direkte links til materiale, der kan virke stødende, er ulovlige eller udgør en sikkerhedsmæssig risiko.

4.13. Anvendelse af IT-services på foranledning af kunde/partner
Cloudtjenester der ikke er på positivlisten kan anvendes, hvis det sker på foranledning af en kunde eller samarbejdspartner i forbindelse med en kundeopgave, et projekt eller et tilsvarende samarbejde.

I den forbindelse er det afgørende at

- der foreligger skriftlig dokumentation for samarbejdet med en aftalt slutdato
- Cloudtjenesten ikke er oprettet/initieret af medarbejder på teknologisk Institut
- vi har dokumentation for, at der foreligger en databehandleraftale mellem kunde/samarbejdspartner og udbyderen af Cloudtjenesten. Er tjenesten placeret udenfor EU skal der ligeledes foreligge et overførselsgrundlag.
- tjenesten kun indeholder personoplysninger godkendt af vedkommende selv
- konto nedlægges, når samarbejde ophører

I det omfang det er muligt skal adgang ske krypteret og ved anvendelse af 2-faktor identifikation.

4.14. Privat anvendelse af IT-services
Privat anvendelse af Internettet fra Instituttets computere må ikke ske i arbejdstiden. Dette inkluderer privat anvendelse af services som communities, sociale netværk, fildeling og andre gruppebaserede tjenester. Enhver sammenblanding af private og arbejdsmæssige forhold skal undgås. Insttituttets mailadresser må ikke anvendes til login/identifikation.

Der må kun i begrænset omfang sendes private mails på Instituttets mail systemer. Mails med tilknyttede dokumenter kan afvises. Private mails bør mærkes PRIVAT. Al mail trafik registreres og sikkerhedskopieres og vil kunne blive åbnet og læst i forbindelse med teknisk problemløsning. Det er ikke tilladt at videresende e-mail til medarbejdernes private mailadresser og lignende uden for Instituttet.

Instituttets computere må ikke anvendes til download og kopiering af spil, ulicenseret musik og software eller af materialer af anstødelig, religiøs eller politisk art. Konstateret piratkopiering vil kunne medføre konsekvenser for ansættelsesforholdet, og i særlige tilfælde til politianmeldelse.

Der må kun foretages privat e-handel fra Instituttets IT-systemer, hvis handelen ikke på nogen måde kan kompromittere Instituttet, eller forpligte dette. Privat e-handel må kun ske uden for arbejdstiden. Af regnskabsmæssige årsager er det ikke tilladt at benytte mobiltelefonen som betalingsmiddel, hvor afregningen sker over mobilabonnementet. Betalinger skal ske med betalingskort.

4.15. Sikring af arbejde foretaget udefra
Som udgangspunkt er alt arbejde med Instituttets IT-systemer og data underlagt Instituttets sikkerhedspolitiker, uanset hvor arbejdet foretages fra.

Opkobling til Instituttets netværk fra fjernarbejdspladser med PC (hjemme, hoteller, andre virksomheder, hot-spots m.fl.) må kun ske ved brug af VPN.

Benyttes privat udstyr til opkobling mod Teknologisk Institut, må data ikke overføres til den private computer, hverken ved filoverførsel, som tilknyttet mail fil eller på anden måde.

Medarbejderes brug af offentlig tilgængeligt PC udstyr (for eksempel i lufthavne, på internetcafeer, på hoteller mv.) til skrivning, internetsøgning og lignende i forbindelse med arbejde skal begrænses. Mail må kun håndteres fraudstyr udleveret af IT-afdelingen.

Eventuel brug må ikke omfatte fortrolig eller personfølsom information. Personnavne og lignende klart identificerbart i teksten skal sløres. Det skal sikres, at eventuelle data på det fremmede udstyr er slettet inden udstyret forlades.

Adgang til services som mail og app's kan kun ske fra mobile devices med brug af Instituttets officielle styringssoftware (MDM).

4.16. Brug af kameraer, lydoptagelser og TV-overvågning på Teknologisk Institut
Det er ikke tilladt for eksterne som kunder og gæster, at optage nogen form for billeder på Instituttets laboratorier uden skriftelig tilladelse fra ledelsen. Gives tilladelsen er afdelingens chef ansvarlig for hvilke emner der fotograferes.

Tv-overvågning kan benyttes i forbindelse med overvågning af de normale adgangsveje, samt af særligt følsomme områder og afdelinger til løbende kontrol af personers uretmæssige adgang og uhensigtsmæssige opførsel. Medarbejderne skal være orienteret og overvågningen skal være skiltet.

Optagelserne lagres og gemmes i en længere fastlagt periode, til brug for eventuel politimæssig efterforskning, hvorefter de overspilles eller slettes. Opbevaring, sletning og kassation skal følge Instituttets regler for sletning af databærende medier.

Telefonsamtaler fra Instituttets telefonsystemer optages ikke uden forudgående aftale med berørte medarbejdere.

4.17. Fjernadgang og remote-værktøjer
VPN må kun benyttes af medarbejdere på Teknologisk Institut med tildelte initialer. Installation af VPN-software må kun foretages af IT-afdelingen og ske på udstyr godkendt af IT-afdelingen (med øvrige sikkerhedskrav opfyldt).

Benyttelse af remote-værktøjer må kun ske efter accept fra bruger. Remote-værktøjer skal være godkendt af IT afdelingen. Alle tilslutninger med remote-værktøjer - samt forsøg på tilslutning - logges med angivelse af bruger/pc som har taget adgang, samt tilslut- og frakoblingstidspunkt.

4.18. Inaktivitet
Ved fratrædelse spærres netværksadgange, men herudover medfører inaktivitet spærring af netværkskonti og PC-adgang.

- Netværkskonti (logon) spærres ved inaktivitet i 90 dage. Kan genåbnes af IT-afdelingen ud fra kontrol af ansættelsesforhold.
- Netværksstik kan være blokeret ved inaktivitet i 90 dage. Genåbnes ved at kontakte IT afdelingen.
- PC's adgang til netværk spærres ved inaktivitet i 45 dage. Genåbnes ved at kontakte IT afdelingen og kun efter sikkerhedsopdatering af udstyr.

4.19. Fratrædelse
Ved en medarbejders fratrædelse skal nærmeste chef vurdere risikoen ved, at medarbejderen fortsat har sine IT-rettigheder frem til fratrædelsesdagen og sikre, at rettigheder og data overføres til andre medarbejdere. Alle adgange til Instituttets IT-systemer lukkes automatisk for den pågældende senest ved sidste arbejdsdags ophør.

Telefon henvises til Instituttets hovednummer eller andet nummer på fratrædelsesdag og seks måneder frem. Fratrådte medarbejdere fjernes fra Instituttets adresselister senest næste arbejdsdag.

Mail der modtages til fratrådt medarbejder kan efter fratrædelse leveres til anden medarbejderes interne postkasse. Fuld adgang til fratrådt medarbejders postkasse kan kun tildeles efter skriftlig godkendelse fra Personalechef eller Direktion.

Ønske om forlængelse af netværksadgang ud over fratrædelsesdato (afviklingsforretning) skal godkendes af Personale og Udvikling med ny slutdato. Bemærk at alle postkasser er aktive og modtager post efter medarbejders fratræden. Alle postkasser som har tilhørt medarbejdere svarer med standardbesked (autosvar) om, at medarbejder ikke længere er ansat og henviser til vores reception. Postkasser slettes efter et år.

Ved en medarbejders fratrædelse skal lånte IT-aktiver (id-kort, tokens, mobiltelefon, computere, routere mv.) returneres senest den sidste arbejdsdag.

Befinder væsentlige effekter sig på en bortvists hjemadresse, skal nærmeste chef vurdere behovet for at effekterne kræves udleveret omgående eller afhentes på bopælen. Instituttet kvitterer for overdragelsen. Medarbejderens computere og datafiler gennemgås snarest muligt og relevant indhold overdrages til andre medarbejdere. Nærmeste chef er ansvarlig for aktiviteterne.

PC'ere, mobiltelefoner og øvrige databærende medier skal indleveres til rensning i IT-afdelingen, før udstyret må overdrages til anden medarbejder. Databærende medier der ikke er krypteret skal destrueres af IT-afdelingen.

TI Folders Workspace mapper overføres til andre gruppemedlemmer eller slettes. TI Folders Personal slettes ved fratrædelse.

4.20. Løst ansatte (vikarer, praktikanter og medhjælpere)

Adgang til brug af systemerne skal begrænses til de systemer, som er nødvendige for funktionernes udførelse. Adgangen skal, hvis teknisk muligt, begrænses med dato- og tidsinterval.

Nærmeste leder er ansvarlig for, at vikaren eller praktikanten er bekendt med Instituttets sikkerhedspolitik og regler på området. I særlige tilfælde kan en clearing af vikaren være nødvendig. De tildelte adgange skal periodisk undergå revision.

Kun medarbejdere med tildelte initialer og underskreven aftale kan få adgang til Instituttets netværk. Tildeling af adgange til alle centrale systemer skal godkendes af Personale og Udvikling.

4.21. Netværksadgang for gæster

Gæster må ikke benytte Instituttets kablede netværk, men kan benytte gæstekonti (tildelt for 8 timer) på det trådløse net.

5. REFERENCER

Henvisning fra:
SOP 6.8
SOP 7.1
SOP 7.2
SOP 7.3
SOP 7.4