Brugeroprettelsesblanket for ekstern adgang: Z-bruger (eksl. adgang til Sharepoint)

Denne blanket udfyldes ved oprettelse/genoprettelse af Z-brugere. Nedennævnte oplysninger skal angives for at brugerkonto oprettes.

En Z-bruger kan max have en løbetid på 1 år, herefter skal den forlænges. Følg processen for forlængelse. Det er z-brugerens chef i Banedanmarks opgave at journalisere blanketten korrekt jf. Banedanmarks procedure.

Oplysninger for system og dataadgang *Udfyldes af z-brugers chef i Banedanmark.*		
Navn (Fulde navn - for-, mellem- og efternavn)	**Mobiltelefon (personlig[1])**	**Fødselsdato (*dd.mm.åååå)***
Firma	**Firmaadresse**	
Personlig mailadresse i firmaet (ikke BDK mailadresse)	**Journalnr. (F2)**	
Systemer der ønskes adgang til (plus evt. roller)		
Aftalen starter (dd.mm.åååå)	**Aftalen ophører (dd.mm.åååå)**	
Godkendelse *Blanketten SKAL være godkendt af z-brugerens chef i Banedanmark og skal fremsendes fra chefens e-mail-postkasse. Mailen gælder som dokumentation for, at z-brugerens chef har godkendt oprettelsen samt accepteret at der tildeles dataadgang som anført ovenfor.*		
Navn på chef i Banedanmark, der accepterer brugeroprettelsen	**Initialer**	**Dato**

[1] Med personlig mobiltelefonnummer menes en mobiltelefon som brugeren anvender i det daglige, og altid er i besiddelse af når adgang til BDK's systemer skal etableres.

BANEDANMARK

Procesbeskrivelse for oprettelse, forlængelse og nedlæggelse af Z-brugere

Her beskrives processen for oprettelse, forlængelse og nedlæggelse af brugertypen "Z-brugere".
En Z-bruger tildeles til eksterne konsulenter, der typisk ikke arbejder på en Banedanmark lokation. En Z-bruger kan ikke få udleveret en Banedanmark PC.

En Z-bruger får adgang til en specifik applikation, server eller service igennem Z-brugerportalen (zportal2.bane.dk). De typisk bestilte adgange er til ProArc og ENK.

Oprettelse af Z-bruger
Ved oprettelse af Z-bruger følges nedenstående proces:

1. Z-brugerens chef i Banedanmark indhenter nødvendig information og udfylder blanketten (se link til Z-bruger oprettelsesblanket ovenfor).
2. Z-brugeren læser Bilag 1 (Informationssikkerhed for medarbejdere hos leverandører) og Bilag 2 (Oplysning om behandling af dine personoplysninger) og udfylder Bilag 3 (Tro- og loveerklæringen).
3. Z-brugerens chef i Banedanmark sender den udfyldte blanket til ServiceDesk: 14700@bane.dk. Der skal medsendes en godkendelse fra z-brugerens chef i Banedanmark.
4. ServiceDesk indhenter godkendelse fra pågældende systemejer (systemejer kan fremsøges i POINT), for de systemer, som z-brugeren ansøges om at tilgå. Systemejer kan/må gerne være sammenfaldende med godkendende chef jf. punkt 1 og 3.

   Ved indhentelse af godkendelse skal ServiceDesk skrive følgende informationer til systemejeren: z-brugerens navn, z-bruger firmanavn, systemer, der ønskes adgang til samt navn på chef i Banedanmark, der accepterer brugeroprettelsen.

   ServiceDesk skal inden indhentelse af godkendelse hos systemejer sikre, at blanketten er godkendt og indsendt af z-brugerens chef i Banedanmark. Skulle den ikke være dette, afvises denne.
5. Systemejer er ansvarlig for at sikre, at det kontrolleres, om der er arbejdsmæssigt behov for den ønskede adgang. Systemejer kan uddelegere godkendelsen til rette person i forretningen, som har kendskab til det arbejdsbetingede behov i systemet. Systemejer kan godkende eller afvise via mail eller direkte i sagen i ServiceNow.
6. ServiceDesk kontrollerer, at alle krævede informationer fremgår, at Tro og Love-erklæring er udfyldt og underskrevet og foretager derefter brugeroprettelsen på det eksterne domæne. Hvis krævede informationer ikke er udfyldt, stoppes oprettelsen og blanketten sendes retur til afsender.
7. Hvis alle krævede informationer fremgår, sender ServiceDesk mail til den nye z-bruger med oplysning om brugernavn og password. Z-brugeren chef i Banedanmark samt systemejer orienteres af ServiceDesk om, at z-brugeren er oprettet.

Nedlæggelse af Z-bruger

Ved nedlæggelse af Z-bruger følges nedenstående proces:

1. Z-brugeren chef i Banedanmark eller en af denne udpeget bemyndiget retter henvendelse til ServiceDesk med angivelse af brugers informationer og beder om, at z-brugeren bliver lukket.
2. ServiceDesk informerer systemejeren om, at z-brugeren nedlægges og fjerner tildelte adgange/rettigheder på z-brugeren, hvorefter z-brugeren deaktiveres.

Forlængelse af Z-bruger

1. Z-brugerens chef i Banedanmark retter henvendelse til ServiceDesk på 14700@bane.dk / 8234 4700 og beder ServiceDesk om forlængelse af Z-brugeren. Chefen skal sikre, at der foreligger en gyldig tro- og loveerklæring for forlængelsesperioden. Z-brugeren kan maksimalt forlænges 1 år.

Tro- og loveerklæring er gyldig i 10 år.

Genoprettelse af nedlagt Z-bruger

1. Følger oprettelsesproceduren. ServiceDesk opdaterer relevant information og fjerner evt. gamle rettigheder/adgange.

Definition af roller og rollers ansvar

Ansvar: Z-brugerens chef i Banedanmark

Z-brugerens chef i Banedanmark, er den chef i Banedanmark (sektions-, områdechef eller direktør), der laver aftalen om, at z- brugeren skal arbejde for Banedanmark

- Chefen er ansvarlig for oprettelsen og nedlæggelsen af z-brugere.
- Chefen er ansvarlig for, at blanketten for z-brugeroprettelse sendes fra chefens e-mail postkasse.
- Chefen er ansvarlig for at journalisere blanketten og tro og love-erklæringen i F2
- Chefen er ansvarlig for at have et overblik over, hvilke Z-brugere, der oprettes på dennes vegne (listen kan trækkes fra F2)
- Chefen er ansvarlig for at give besked til ServiceDesk i tilfælde af ændringer omkring z-brugeren.

Ansvar: Servicedesk

- Servicedesk registrerer henvendelsen fra z-brugerens chef i Banedanmark og sikrer, at den er sendt og godkendt af z-brugerens chef i Banedanmark
- Servicedesk indhenter godkendelse fra systemejer
- ServiceDesk kontrollerer, at alle krævede informationer fremgår, at Tro og Love-erklæring er udfyldt og underskrevet
- Servicedesk opretter eller nedlægger Z-brugeren
- Servicedesk skal sikre at systemejers godkendelse eller afvisning fremvisning fremstår synlig i sagen.

Ansvar: Systemejer
Systemejeren har ejerskab jf. SL08 og Banedanmarks fælles POINT.

- Systemejer er ansvarlig for at sikre, at det kontrolleres, om der er arbejdsmæssigt behov for den ønskede adgang. Systemejer kan uddelegere godkendelsen til rette person i forretningen, som har kendskab til det arbejdsbetingede behov i systemet.
- Systemejeren er ansvarlig for at oprettelsen godkendes eller afvises og at dette er synlig enten via mail eller direkte i sagen i ServiceNow

Bilag 1
Informationssikkerhed for medarbejdere hos leverandører

Informationssikkerhed

- **For dig, som arbejder for en leverandør hos Banedanmark**

Dette materiale er til dig, som er ekstern medarbejder hos en leverandør til Banedanmark, og som i forbindelse med din opgavevaretagelse har adgang til Banedanmark informationer og data, enten via eget udstyr eller via udstyr udleveret/ejet af Banedanmark. Dette kan for eksempel være X- og Z-brugere.
Du skal som medarbejder hos en leverandør til Banedanmark overholde de overordnede krav, der er fastsat i Banedanmarks informationssikkerhedspolitik. Nærværende dokument og *10 råd for god informationssikkerhed – en pjece* samler de regler og anvisninger, som du skal følge, når du arbejder med informationer og data i Banedanmark.
En overtrædelse af regler og anvisninger på informationssikkerhedsområdet kan efter en individuel og konkret vurdering få konsekvenser for dit ansættelsesforhold i Banedanmark.
Når du starter som ekstern medarbejder i Banedanmark, skal du skrive under på, at du vil følge reglerne for informationssikkerhed. Det gør du ved at underskrive den tilsendte "Tro og love-erklæring", som er vedhæftet brugeroprettelsesblanketten.

Informationssikkerhed er alles ansvar- også dit!

1 ID/ADGANGSKORT I BANEDANMARK

Når du opholder dig på Banedanmarks områder og lokationer, skal du bære dit id/adgangskort eller gæstekort synligt, og det skal fremvises på forlangende, hvis nogen spørger om det.
Du må ikke låne dit kort ud eller lukke ukendte personer ind i Banedanmarks bygninger. Ser du personer uden synligt legitimationskort, så spørg om deres ærinde og følg dem evt. til deres vært eller receptionen. Mister du dit adgangskort/id-kort, skal du straks informere din nærmeste leder herom.

2 PASSWORD/ ADGANGSKODE

Dine adgangskoder er personlige og må ikke deles med andre – heller ikke IT-afdelingen/support.
Det er vigtigt, at dine koder er unikke, og at du ikke bruger de samme koder både privat og til arbejdsbrug.
Dit password skal som minimum være på 12 karakterer - gerne flere - bestående af en kombination af små/store bogstaver og tal/tegn.
Undgå passwords, der indeholder initialer, navne, mærkedage og ord, der kan slås op i ordbøger samt produkt- eller projektnavne.
Vær opmærksom på, at brugen af æ, ø og å i passwords, kan give udfordringer i nogle programmer som f.eks. SAP, og særligt i den operationelle IT.
Ved mistanke om læk eller misbrug skal du straks skifte dine adgangskoder. Hvis du har glemt dit password, kan du få hjælp hos Servicedesk på tlf.: 82344700 eller e-mail: 14700@bane.dk.

3 ADGANGSSTYRING

Det er en medarbejders leder (eller en lederbemyndiget), der anmoder om de autorisationer, som ServiceDesk skal udstede til brugeren.
Systemejer er ansvarlig for at medarbejdere, der får adgang til informationsaktivet, kun har rettigheder, til det, de har behov for og at der regelmæssigt foretages review af brugere og adgangsrettigheder.
Du skal dog også selv være opmærksom, og gøre systemejer opmærksom på det, hvis du har fået adgang til noget, du ikke burde have adgang til.
Privilegerede adgangsrettigheder (f.eks. administratorkonti) til informationsaktiver tildeles kun i begrænset omfang og er begrænset til personer med arbejdsbetinget behov.
Når ansættelsen eller den midlertidige kontrakt ophæves, trækkes dine rettigheder tilbage, og du skal aflevere ID/adgangskort, IT-udstyr, mm., inden sidste arbejdsdag. Ved orlov eller andet længerevarende fravær deaktiveres brugerens adgangsrettigheder.

4 SIKKERHED I UDVIKLINGS-, TEST- OG HJÆLPEPROCESSER

I Banedanmark er informationssikkerhed en integreret del af kravene til udvikling. Hvis du er involveret i anskaffelse, udvikling og/eller vedligeholdelse af systemer, er du som medarbejder hos en leverandør til Banedanmark ansvarlig for korrekt håndtering af data involveret i disse processer.
Banedanmarks informationssikkerhedspolitik fastsætter, at udviklings-, test- og driftsmiljøer skal adskilles for at nedsætte risikoen for uautoriseret adgang til eller ændringer af driftsmiljøet. Der må ikke foretages test på driftssystemer, bortset fra helt ekstraordinære omstændigheder, hvor andet ikke er muligt og, hvor der på forhånd er anmodet om, og opnået godkendelse af, enten af accept af den

øgede risiko, som forholdet medfører, eller af dispensation for reglerne med henblik på, at kunne efterleve dem inden for en bestemt periode. Se desuden TL11 Regelsæt ISO.A12 Driftssikkerhed

5 KLASSIFICERING AF BANEDANMARKS INFORMATIONER OG DATA

Du er ansvarlig for, at de informationer og data, du arbejder med, bliver håndteret og opbevaret korrekt. Du skal vide, hvilke *typer* af information og data du arbejder med, således, at du kan sørge for, at de bliver korrekt behandlet og lagret (gemt)[2].
Information og data i både digital og fysisk form i Banedanmark inddeles i fem niveauer, som fastsætter, hvordan de skal behandles: Offentlige informationer, interne informationer, Banedanmark fortrolig information, personoplysninger, og Nationale sikkerhedsbestemmelser (her træffes separate foranstaltninger efter behov).

Skemaet nedenfor kan anvendes til at udlede, hvordan forskellige informationstyper bør behandles/lagres. Hvis materialet indeholder flere typer information (f.eks. offentlig information og fortrolige eller følsomme personoplysninger), skal materialet klassificeres og behandles efter den mest restriktive klassificering. For mere information om klassificering se desuden politik for klassificering af information og informationsoverførsel.
Vær generelt opmærksom på hvilke personer der har adgang til de mapper, hvor du gemmer informationer – og husk journaliseringspligten.

* F.eks. SharePoint, OneDrive, HR Manager eller F2

** Outlook må ikke anvendes som arkiv eller til at gemme materialer og informationer der indeholder ikke allerede offentlige personoplysninger. Dette skal i stedet opbevares i relevant godkendt Banedanmark system, f.eks. SharePoint eller F2

[2] Banedanmark er underlagt forvaltningslov, offentlighedslov og arkivlov, hvilket betyder der til enhver tid kan søges aktindsigt i Banedanmarks sager, samt at overdragelse af arkivalier mellem Banedanmark og myndigheder/virksomheder kun må ske efter aftale. Beslutning om udlevering af oplysninger træffes ud fra lovenes kriterium.

		Informationstype			
		Offentlig information	Intern information *inkl. almindelige personoplysninger*	BDK fortrolig information	Fortrolige /følsomme personoplysninger
	Eksempler på informationstype	*Stillingsopslag, offentligt kendte baneprojekter*	*Adresse, arbejdstelefon nr., CV*	*Referater fra styregruppemøder, ledelsesbeslutninger*	*Helbredsoplysninger, fagforeningsoplysninger*
Behandlingstype	Ved print	Ingen krav	FollowMe	FollowMe	FollowMe
	Lagring på bærbar	Ingen krav	Relevant Banedanmark godkendt system*	Relevant Banedanmark godkendt system*	Sagsbehandlings-system (F2)
	Lagring på fællesdrev	Ingen krav	Relevant Banedanmark godkendt system*	Relevant Banedanmark godkendt system*	Sagsbehandlings-system (F2)
	Lagring i OneDrive	Ingen krav	Relevant Banedanmark godkendt system*	Banedanmark godkendt system*	Sagsbehandlings-system (F2)
	Lagring i Teams	Gem i SharePoint og tilgå via Teams	Relevant Banedanmark godkendt system*	Relevant Banedanmark godkendt system*	Sagsbehandlings-system (F2)
	Lagring i SharePoint	Ingen krav	Relevant Banedanmark godkendt system*	SharePoint	Sagsbehandlings-system (F2)
	Lagring i Outlook	Ingen krav	SharePoint eller F2**	SharePoint eller F2**	Sagsbehandlings-system (F2)**
	Lagring på USB/ekstern harddisk el. lig.	Anvend Banedanmark godkendte enheder	Anvend Banedanmark godkendte enheder	Relevant Banedanmark system*	Sagsbehandlings-system (F2)**
	Opbevaring af papir på Banedanmarks lokationer	Ingen krav	Aflåst i skab	Aflåst i skab	Aflåst i skab
	Papir: transport og fjernarbejdsplads	Ingen krav	Under opsyn	Under opsyn	Under opsyn
	Papir: hjemmearbejdsplads	Ingen krav	Under opsyn/ i aflåst skab	Under opsyn/ i aflåst skab	Under opsyn/ i aflåst skab

6 Opbevaring, behandling og lagring af Banedanmarks informationer og data

Du skal sikre, at fysiske materialer, der indeholder alt information undtagen det offentligt tilgængelige, opbevares på forsvarlig vis (låses ind i et skab) og makuleres, når de ikke længere bruges. Der er skraldespande til makulering på Banedanmarks lokationer. Dokumenter, der indeholder alt information undtagen det offentligt tilgængelige, skal udskrives via "Follow-me print" eller via fortrolig print, hvis "Follow-me print" ikke er tilgængelig på lokationen.
Dette betyder også, at hvis du kortvarigt forlader din arbejdsplads, mens du arbejder med fysiske informationer, der indeholder alt andet end det offentligt tilgængelige, skal du sikre dig, at en kollega med adgang til samme information holder øje med arbejdspladsen, indtil du er tilbage. Ellers skal materialerne låses inde.

Efter brug af møde- eller uddannelsesfaciliteter skal møde- eller uddannelsesleder sikre sig, at der ikke efterlades klassificerede informationer på borde, vægge, whiteboards, flip boards eller i affaldsspande/papirkurve mv.
Har du undtagelsesvis behov for at bruge en USB-nøgle, så anvend udelukkende USB-nøgler, som du har fået udleveret af Banedanmark.

Opbevaring af digitale data og informationer

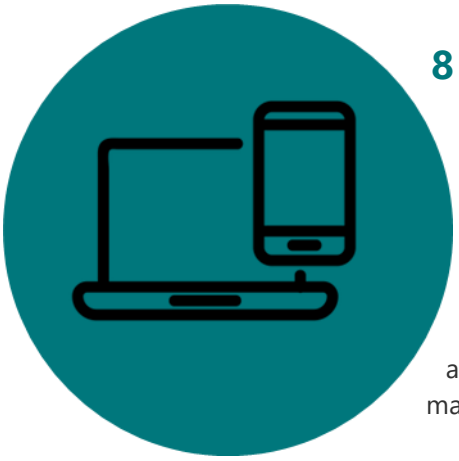
Digitale informationer og data, undtagen det offentligt tilgængelige, lagres i SharePoint, OneDrive eller på andre systemer, som Banedanmark har kontrol over. Journaliseringspligtigt materiale skal lagres i F2 eller SharePoint Online). Find yderligere information om journaliseringspligt samt god forvaltningsskik samt Sletning og journalisering i Banedanmark.
Dette sikrer, at data ikke går tabt eller at det kan gendannes i tilfælde af systemfejl. Vær opmærksom på, hvem (både interne og eksterne) har adgang til det sted, hvor du lægger dine dokumenter. Vær ligeledes opmærksom på hvilke beskyttelseskrav, der er til stede og ret dokumenterne til, så de passer til de tilgængelige informationer såvel som til de tilknyttede brugere.
Arbejdsrelateret information og data må ikke permanent lagres lokalt på computeren, da indholdet ikke kan sikkerhedskopieres. Dette giver risiko for, at information og data kan gå tabt, og at mange timers arbejde er spildt.
Hvis du har adgang til Banedanmark information via din egen arbejdsgivers PC'er skal du også her være opmærksom på at slette informationer du eventuelt har gemt lokalt på computeren.

OneDrive

I Banedanmark anvendes OneDrive Business, hvor du kan oprette, redigere, overføre, slette og tilgå dine dokumenter fra alle computere, tablets og smartphones. Du kan anvende OneDrive til at dele filer med andre, dog ikke med nogen udenfor Banedanmarks domæne.
Indhold, der indeholder alt information undtagen det offentligt tilgængelige, må ikke gemmes i eller deles fra OneDrive. OneDrive giver derfor heller ikke mulighed for at journalisere. Du må dog midlertidigt gemme de ting, som du vurderer, *ikke* indgår i Banedanmarks forvaltning, dvs. som *ikke* har journaliseringspligt, på OneDrive. Det kan fx være en kladde til et dokument, der senere skal indgå i et projekt eller lignende.

7 Tilladt behandling af Banedanmark udstyr (hardware og software)

Det er ikke tilladt at skille udstyr ad eller ændre i udstyrets standardopsætninger.
Det er kun tilladt at downloade, kopiere, anvende og videresende ophavsretsbeskyttet materiale, fx licenskrævende programmer, bøger, fotos, musik, osv., hvis Banedanmark har købt rettigheder til det.
Du må kun installere og anvende software, der er godkendt af Banedanmark. Har du særlige arbejdsbetingede behov, der ikke udbydes, kan du ansøge om godkendelse af software på IT's serviceportal under IT> IT Bestillinger> Bestilling af software.



8 BRUG AF E-MAIL OG MØDEINDKALDELSER

E-mails kan indeholde forsøg på informationstyveri gennem phishing og ransomware. Derfor er det vigtigt, at du altid er *yderst* opmærksom på mulige trusler, når du modtager e-mails fra interne kolleger såvel som fra eksterne afsendere. Dette særligt, hvis e-mailen indeholder links og vedhæftede filer, eller hvis du bliver bedt om fx at indtaste bruger-id eller adgangskode. Hvis du er i tvivl så om troværdigheden af en e-mail, skal du

1. Tjekke afsender: Se efter fejl i mailadressen. Er du i tvivl, så kontakt den person, der angives som afsender
2. Tjekke det link, afsenderen vil have dig til at klikke på: Hold musen hen over linket og tjek, hvilken adresse, den peger på. Find eventuelt adressen på anden vis.
3. Tjekke indhold: Du kan blive bedt om at aflevere personlige eller følsomme oplysninger - det skal du ikke. Se desuden på ordlyden og tænk over, om afsenderen normalt ville formulere sig sådan.
4. Indrapporter: indrapporter mailen via Microsoft indrapporteringsknap.

Ret henvendelse til ServiceDesk, hvis du er i tvivl på e-mail 14700@bane.dk eller tlf.: 8234 4700.
Din arbejdsmail skal bruges i forbindelse med arbejde. Du må ikke tilgå din private mail på Banedanmarks udstyr med undtagelse af kombinerede tjenestetelefoner, frie telefoner eller tablets, hvor der er indgået aftale om privat brug. Det er ikke tilladt at videresende mails til/fra Banedanmark til private mailadresser eller andre arbejdsmailadresser, da dette potentielt kan forringe informationssikkerheden.

I særlige tilfælde kan Banedanmark åbne e-mails og dokumenter for at se, om der skulle være Banedanmark oplysninger i det (fx information om projekter, som er nødvendigt for videre arbejde), men hvis indholdet ved åbning ser ud til at være privat, så skal Banedanmark straks lukke ned igen.
Outlook må ikke anvendes som arkiv eller til at gemme/opbevare materiale. Mails, vedhæftninger og andet materiale, som har betydning for sagsbehandlingen, skal i stedet journaliseres i overensstemmelse med Banedanmarks retningslinjer herom. Metode for journalisering som ekstern aftales med den kontraktansvarlige.

Alle mails, dokumenter og andet materiale skal derudover slettes fra Outlook, når det ikke længere er relevant for det konkrete formål. Hvis der er tale om journaliseringspligtigt materiale, vil der som hovedregel ikke være grund til opbevaring i Outlook efter journalisering.
Husk i den forbindelse at slette indholdet af både din indbakke (herunder evt. undermapper) og sendt post.

Når mails markeres som slettet, flyttes de til slettet post. Indholdet af denne mappe skal slettes manuelt hver 30. dag. Først når dette er sket, er mailen slettet.
Det er vigtigt, at der så vidt muligt IKKE sendes personoplysninger rundt i Banedanmark per e-mail. Se retningslinjer for håndtering af personoplysninger her.

Mødeindkaldelser

Benyt funktionen "privat" i Outlook, når indholdet i mødeindkaldelser eller mødets karakter er fortroligt/følsomt eller send alternativt vedhæftede filer i en separat mail eller direkte link i stedet for at indsætte dem i invitationen. Dette gælder, hvis indholdet indeholder informationer eller data, der er Banedanmark Fortrolig, fortrolig/følsomme personoplysning eller nationale sikkerhedsinformationer, men kan også efter vurdering give mening ved andre forhold.

Send Digitalt

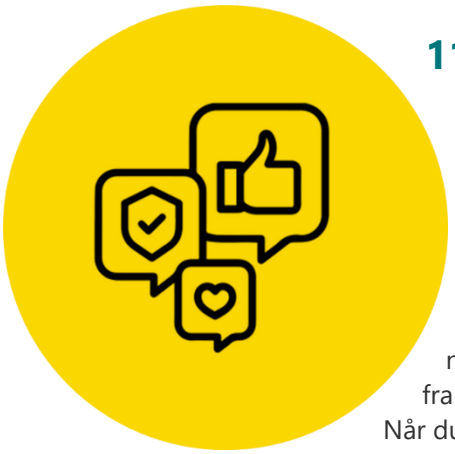
Hvis du har behov for at sende informationer og data, der indeholder alt andet end offentligt tilgængelige informationer, til eksterne modtagere, skal du bruge "Send Digitalt" funktionen i Outlook. Funktionen bestilles via serviceportalen under IT> IT Bestillinger> Bestilling af software. Her vælger man "andet software", hvor man selv skal skrive navnet på softwaren (Send Digitalt).
Vær opmærksom på, at denne funktion kræver, at brugeren har en Banedanmark PC.

9 Brug af internet

Internetforbindelsen fra din arbejdscomputer/tablet skal primært anvendes arbejdsrelateret.
Arbejder du udenfor Banedanmarks lokationer, fx hoteller eller lufthavne, anbefales det kun at bruge trådløse netværk, der kræver specifikt log-in. Anvend altid Banedanmarks VPN-opkobling, da du derved beskytter transaktioner over nettet.
Banedanmark kan stilles til ansvar for alle transaktioner til og fra internettet, vær derfor altid opmærksom på at undgå internetsider, som kan udgøre en sikkerhedsrisiko eller har ulovligt indhold.
Vær også opmærksom på, at din brug af internettet logges af Banedanmark med henblik på at undgå eller opklare sikkerhedsrelaterede hændelser eller brud.

10 Brug af sociale medier

Du kan bruge sociale medier såvel som andre digitale tjenester til arbejdsrelaterede formål, når du gør det med omtanke. Banedanmark har en lang række officielle profiler på flere sociale medier som Facebook, Instagram, Twitter, LinkedIn og YouTube.
Det er tilladt for alle medarbejdere at dele indhold fra disse kanaler. Du må dog ikke omtale eller dele Banedanmark Fortrolig information eller fortrolige/følsomme personoplysninger, herunder billeder eller videoer.
Vær derfor generelt ekstra påpasselig, når du deler informationer på de sociale medier. Når du fx deler billeder af andre på sociale medier, deler du faktisk personoplysninger, og her gælder reglerne om databeskyttelse. Spørg derfor altid om lov, inden du lægger billeder af en anden person på sociale medier.



11 IT-Udstyr: På arbejdet, rejsen og hjemmearbejdspladsen

Det IT-udstyr, der stilles til din rådighed, er Banedanmarks ejendom, og det er dit ansvar at passe godt på det. Hvis IT-udstyret opbevares og behandles groft uforsvarligt eller udlånes til tredjeperson, vil der ved eventuelle tab eller skader kunne blive tale om erstatningspligt.

Efterlad aldrig din computer/tablet ulåst. Hold windows-tasten nede og tryk på "L", så computeren bliver låst. *Også* hvis du blot går fra skærmen efter en kop kaffe.

Når du forlader arbejdspladsen, skal skrivebordet ryddes for alle informationer undtaget informationer, der er offentlige tilgængelige. Anbring dokumenterne i et aflåst skab eller skuffe. Nøgler må ikke efterlades frit tilgængeligt fx siddende i låsen, på borde eller i uaflåste skuffer. Skriveborde skal være ryddet for alt andet end faste installationer og ikke databærende IT-udstyr[3]. personlige effekter, billeder mv. er tilladt i begrænset omfang.

Bemærk; for at sikre god hygiejne skal skriveborde og mødeborde så vidt muligt være fri for genstande, således at rengøring kan gennemføres på effektiv og betryggende måde.
Arbejdsstationer (stationære computere, bærbare computere, tablets, smartphones mv.) skal være konfigureret med en godkendt passwordbeskyttet screensaver, der aktiveres efter maksimalt 15 minutters inaktivitet (3 minutter for tablets og smartphones).
Computerskærme, der anvendes til behandling af alle informationer undtagen offentligt tilgængelige og interne, skal være placeret, så risikoen for uautoriseret aflæsning af informationer reduceres mest muligt.[4]

IT-udstyr må ikke efterlades i det offentlige rum uden opsyn og skal låses inde eller medtages ved arbejdsophør. Alt mobilt udstyr skal opbevares forsvarligt, fx i et aflåst skab. Har du brug for at efterlade udstyr i en bil, skal det låses inde i bilen bagagerum. Bærbart udstyr må ikke udlånes til tredjeperson.
Overvej, om det er nødvendigt at læse, skrive eller tale om interne arbejdsmæssige forhold under transporten. Alle informationer, der ikke er offentlige tilgængelige må ikke kunne læses, overhøres eller på anden vis tilgås af uvedkommende.

Distancearbejde/ hjemmearbejdsplads

Ved hjælp af VPN, MFA (MultiFactorAuthentification-app) samt internetportal kan du få adgang til relevante informationssystemer hos Banedanmark fra fx din bopæl.

[3] Af hensyn til trafikafviklingen finder bestemmelserne vedr. indelåsning af dokumenter og nøgler mv. ikke anvendelse i operative trafikafviklingsområder, hvor det er en del af faste driftsprocedurer, at disse kontinuerligt er tilgængelige for de det tjenstgørende personale.
[4] Af hensyn til trafikafviklingen finder bestemmelserne vedr. automatisk screensaver og låsning af skærm ved inaktivitet ikke sted for arbejdsstationer, der operationelt og aktivt anvendes i trafikafviklingen.

Når du arbejder med Banedanmarks informationer fra en distancearbejdsplads eller hjemmearbejdsplads, er du omfattet af de samme sikkerhedsmæssige regler, som når du fysisk befinder dig på en arbejdsplads i Banedanmark.
Du er ansvarlig for, at uvedkommende ikke får adgang til Banedanmarks systemer og informationer. Dette gælder også ægtefæller, samlevende, børn mv. Du skal ligesom på Banedanmarks lokationer sørge for at låse alt information, der ikke er offentligt tilgængeligt inde, afskaffe det på forsvarlig vis samt undgå at holde møder/samtaler i rum, hvor andre kan lytte med.

12 Returnering af udstyr

Alle medarbejdere er ansvarlige for at aflevere defekt eller tidligere anvendt IT-udstyr til IT-Onsite, fx i forbindelse med ansættelsens ophør. Udstyr, hvorpå der har været lagret Banedanmark Fortrolig information, fortrolige eller følsomme personoplysninger eller nationale sikkerhedsinformation, skal mærkes tydeligt, således at sikker sletning/destruktion sker.
Husk også, at ID/adgangskort og lignende skal afleveres ved sidste arbejdsdag.

13 Brud på Informationssikkerhed

Du har pligt til at indberette informationssikkerhedsbrud, sårbarheder eller sikkerhedshændelser, fx brud på persondatasikkerheden. Viden forpligter.

En informationssikkerhedshændelse er en samlet betegnelse for alle de forskellige typer af tekniske og menneskeskabte uheld/brud, der kan udgøre en risiko for de informationer og data, der behandles af Banedanmark. Dette gælder både for digitale og fysiske informationer og data. Det kan fx være informationer og data, der fejlagtigt slettes, ændres eller videregives til de forkerte. Det kan være utilsigtet (en fejl) eller tilsigtet (fx hacking). Hvis hændelsen drejer sig om personoplysninger, er der tale om brud på persondatasikkerheden, og det er ved sådanne brud vigtigt, at disse skal indberettes *hurtigst* muligt og uden unødig forsinkelse.

Det er også vigtigt at vide, at informationssikkerhedshændelse både dækker over, når der *er sket* et informationssikkerhedsbrud, men også hvis du opdager noget, der *ville kunne lede* til et informationssikkerhedsbrud (fx en dør med kode/adgangskontrol, der ikke lukker fx ind til et datacenter eller en leverandør til Banedanmark, der ved en fejl sender et brugernavn og password).

Bliver du opmærksom på noget, der kan have betydning for informations-sikkerheden, skal du øjeblikkeligt kontakte Servicedesk på e-mail 14700@bane.dk eller tlf.: 8234 4700. Har du brug for hjælp til rapportering af informationssikkerhedshændelser, kan du kontakte din nærmeste leder. Yderligere rådgivning kan du finde ved at kontakte sektionen for Cyber- og informationssikkerhed (CIS) på informationssikkerhed@bane.dk

BANEDANMARK

14 KONTAKTOPLYSNINGER

IT-Support via Servicedesk
For indmeldelse af fejl, bestilling, services og generel support, kontakt Servicedesk på
E-mail: 14700@bane.dk/ Tlf: 8234 4700 / via Serviceportalen

IT-Onsite
Adresser og åbningstider er:
- Carsten Niebuhrs gade 43: mandag kl.08:00-11:00, samt den første arbejdsdag i måneden kl.08:00-11:00
- Ringsted: onsdag kl.08:00-11:00 (lokale 01.02)

Husk sagsnummer! Inden du henvender dig til IT-Onsite, skal du have oprettet en sag hos Servicedesk.

Cyber- og Informationssikkerhed (CIS)
Har du brug for rådgivning vedrørende informationssikkerhed, kan du skrive til sektionen for Cyber- og Informationssikkerhed (CIS) på informationssikkerhed@bane.dk

Persondatabeskyttelse
Har du spørgsmål vedrørende GDPR (databeskyttelsesforordningen) og hvordan vi arbejder med emnet i Banedanmark, kan du skrive til GDPR@bane.dk .
Banedanmark har også en databeskyttelsesrådgiver (også kaldet DPO, kort for Data Protection Officer). DPO'en kan hjælpe med at besvare spørgsmål om dine rettigheder, og hvordan Banedanmark behandler dine oplysninger. Du kan kontakte DPO'en via mail: DPO@bane.dk

Bilag 2
Oplysning om behandling af dine personoplysninger

Banedanmark er overordnet dataansvarlig for behandlingen af de personoplysninger, som vi har modtaget om dig. Banedanmark har følgende kontaktoplysninger: Banedanmark, Carsten Niebuhrs Gade 43, 1577 København V., banedanmark@bane.dk , +45 8234 0000, CVR-nr: 18632276.

Kontaktoplysninger for Banedanmarks databeskyttelsesrådgiver:
Carsten Niebuhrs Gade 43, 1577 København V., dpo@bane.dk

Banedanmark behandler følgende kategorier af personoplysninger om dig:

- Kontaktoplysninger
- Fødselsdato
- Navn på din arbejdsgiver og din chef
- Systemer der ønskes adgang til
- Oplysninger om du har underskrevet tro- og loveerklæringen

Det retslige grundlag, behandlingen bygger på, er den indgåede kontrakt med din arbejdsgiver om at løse arbejdsopgaver hos Banedanmark. Retsgrundlaget er derfor Banedanmarks legitime interesser, jf. databeskyttelsesforordningens art. 6, stk. 1, litra f.
Formålet med behandlingen af dine personoplysninger, som også udgører Banedanmarks legitime interesser, er:

- At håndtere dig som bruger af Banedanmarks IT- og adgangssystemer
- At sikre en entydig identifikation af dig i Banedanmark på tværs af Banedanmarks processer og systemer

Banedanmark videregiver efter omstændighederne dine personoplysninger til offentlige myndigheder, når der krav herom, og vores leverandører. Dine data vil eventuelt blive videregivet til lande udenfor EU/EØS, da Banedanmark benytter NNIT som IT- leverandør.

Meddelelse af personoplysninger er ikke lovpligtigt, men et krav i henhold til en kontrakt mellem Banedanmark og din arbejdsgiver. Oplysningerne hidrører på den baggrund fra dig selv eller din arbejdsgiver.

Dine personoplysninger slettes 5 år efter endt tilknytning til Banedanmark med mindre anden lovgivning og/eller andre administrative behov forlænger sletningsfristen.

Dine rettigheder

- Dine rettigheder er efter omstændighederne:
- Ret til at se oplysninger (indsigtsret)
- Ret til berigtigelse (rettelse)
- Ret til sletning

- Ret til begrænsning af behandling
- Ret til at transmittere oplysninger (dataportabilitet)
- Ret til indsigelse

Hvis du vil gøre brug af dine rettigheder, skal du kontakte os.

Datatilsynet varetager klagemyndigheden i forbindelse med Databeskyttelsesforordningen i Danmark. Eventuelle klager i den forbindelse skal fremsendes til dem. Du finder Datatilsynets kontaktoplysninger på www.datatilsynet.dk.

Bilag 3
Tro- og loveerklæring: Aftale med eksterne samarbejdspartnere

Denne erklæring udfyldes og underskrives af medarbejderen i det firma, som Banedanmark har indgået kontrakt med.

Undertegnede erklærer hermed, at jeg iagttager fuldstændig tavshedspligt med de forhold og oplysninger, jeg måtte komme i besiddelse af i forbindelse med dataadgang til Banedanmark.

Jeg bekræfter desuden, at jeg har gennemlæst og overholder Bilag 1 "Informationssikkerhed for medarbejdere hos leverandører" og i øvrigt følger de instruktioner, jeg får i forbindelse med dataadgangen.

I det tilfælde, at der konstateres misbrug, forbeholder Banedanmark sig til enhver tid ret til at lukke for adgangen til systemet.

Navn (med blokbogstaver)

Firma

Dato og underskrift