Please scroll down for ENGLISH version of this document "Instructions for external partners on secure use of Bane NOR's information systems".

1. NORSK: Instruks for eksterne partnere om sikker bruk av Bane NORs informasjonssystemer

1.1. Hensikt og omfang

Denne instruksen gjelder for alle brukere fra eksterne selskaper og organisasjoner («partnere») som får tilgang til Bane NORs IT-utstyr, systemer, dokumenter eller informasjon. Instruksen inneholder regler og retningslinjer for sikker bruk av Bane NORs informasjonssystemer. Øvrige bestemmelser i avtaler, herunder taushetsplikt, opphavsrett og lignende gjelder også. Instruksen gjelder i og utenfor arbeidstid.

Sikkerhet avhenger av den enkelte medarbeiders holdning og at hver enkelt tar ansvar for sikkerheten. Informasjonssikkerhet handler om å sikre rett tilgang til IT-systemer, at informasjon ikke kommer på avveie, ikke blir utilgjengelig og ikke blir endret av uvedkommende.

1.2. Retningslinjer for IKT-utstyr og programvare

1.2.1. IKT-utstyr for Bane NOR-tilgang

Bane NOR tillater at du benytter egnet IKT-utstyr (PC, mobiltelefon og nettverk) for tilgang til Bane NORs informasjonssystemer gitt at du følger denne instruksen og de konkrete retningslinjene beskrevet i dette dokumentet.

1.2.2. Godkjent programvare og utstyr

Du skal følge din organisasjons retningslinjer for godkjent programvare og utstyr, samt følge organisasjonens oppdateringer. I hovedsak skal datamaskin/PC være underlagt selskapets system for forvaltning av datamaskiner og mobiltelefon/nettbrett skal i hovedsak registreres i selskapets system for styring av mobile enheter (MDM).

1.2.3. Skille mellom privat og jobb

Det er god praksis at IKT-utstyr som benyttes i jobbsammenheng ikke benyttes til private formål. Privat innhold skal ikke lagres i Bane NOR sine systemer. Det er god praksis å ha en egen, dedikert epost-adresse for arbeid.

1.2.4. Virus og skadevare

Ved mistanke om virus eller annen skadevare, slå umiddelbart av enheten og kontakt din organisasjons brukerstøtte.

1.2.5. Tapt eller mistet utstyr

Ved tapt eller mistet utstyr, ta umiddelbart kontakt din organisasjons brukerstøtte.

1.3. Tilganger og publisering

1.3.1. Tilganger hos Bane NOR

Som ekstern Bane NOR-partner skal du kun ha tilgang til de systemer og den informasjon som er nødvendig for å utføre arbeidsoppgavene dine og som du er godkjent for å behandle. Du skal ikke på noen måte tilegne deg annen tilgang. Dersom du oppdager at du har tilgang til mer, feil eller annen informasjon eller funksjoner, ta kontakt med din nærmeste leder eller tilgangsansvarlig.

Tilgang gis med en begrenset varighet. Du vil få varsel på epost når det er på tide med forlengelse.

Hvis arbeidsforholdet endres eller avsluttes skal tilganger oppdateres slik at du til ethvert tidspunkt har riktige tilganger.

1.3.2. Publisering av Bane NOR-innhold

Innhold og data fra Bane NOR-systemene du har fått tilgang til skal ikke publiseres videre uten samtykke fra informasjonseier i Bane NOR.

1.4. Din digitale brukeridentitet

1.4.1. Brukernavn

Ditt brukernavn er din egen individuelle identitet for digital tilgang og skal kun benyttes av deg. Du er ansvarlig for all systemtilgang som skjer med ditt brukernavn.

1.4.2. Epost-adresse

For tilgang til Bane NOR skal du benytte jobb-mail. Individuelle e-postkontoer skal benyttes for registrering av brukere. Det er ikke tillatt med felles epost-konto hvor brukernavn og passord deles.

1.4.3. Passord

Passord og andre tilgangskoder er strengt personlig og skal holdes hemmelig. Passord skal umiddelbart byttes ved mistanke om at det er blitt kjent for andre. Passord skal være lette å huske, men avanserte nok til at andre ikke kan gjette dem og skal derfor ikke inneholde informasjon som fødselsdato, telefonnummer eller navn på familiemedlemmer. Du må bytte passord regelmessig, og varsel om dette gis normalt fra systemet god tid i forveien.

1.4.4. Sterk pålogging (Multifaktorautentisering - MFA)

Der hvor multifaktorautentisering (MFA) kreves må man aktivere og benytte dette, fortrinnsvis via en autentiseringsapp som Microsoft Authenticator.

1.5. Klassifisering av informasjon

All informasjon som lages, lagres og publiseres via Bane NORs systemer klassifiseres som enten ÅPEN, INTERN eller SENSITIV. Du vil etter søknad kunne få tilgang til informasjon og funksjoner i ulike informasjonssystemer med ulike informasjonsklasser ut ifra tjenstlig behov.

Tips: For de aller fleste som arbeider i eller med informasjon fra Bane NORs IT-systemer, så er det INTERN informasjon det dreier seg om. Så sørg for å følge reglene for INTERN når du jobber til vanlig og ta ekstra forhåndsregler de gangene du skal arbeide med noe SENSITIVT.

Nivå (farge)	Retningslinjer
ÅPEN (GRØNN)	Det oppfordres til å følge tilsvarende retningslinjer som for INTERN.
INTERN (GUL)	Merking og behandling: INTERN informasjon skal merkes med ordet «INTERN» i store bokstaver. Dersom du får eller behandler informasjon som ikke er merket med INTERN, men som burde vært klassifiseres slik, så skal du allikevel følge instruksene for INTERN. Hvilke enheter du kan benytte: For tilgang til INTERN informasjon og funksjoner **SKAL** du enten bruke en **partnerkontrollert enhet** eller en **tilstrekkelig sikret enhet**. Lagring og sletting: • Informasjonen **kan** lagres på brukerens enhet og enhetens lagringstjeneste og/eller organisasjonens lagringstjeneste (slik som filserver, selskapets OneDrive, Teams, Sharepoint, arkivsystem eller lignende fagsystem). • Det er **ikke** tillatt å lagre informasjonen på andre steder slik som din *private* OneDrive / Google Drive, iCloud, DropBox / Facebook og lignende. • Informasjon **skal** slettes når behandling er fullført og tjenstlig behov ikke tilsier fortsatt lagring.
SENSITIV (RØD)	Merking og behandling: SENSITIV informasjon skal merkes med ordet «SENSITIV» i store bokstaver. Dersom du får eller behandler informasjon som ikke er merket med SENSITIV, men som burde vært klassifiseres slik, så skal du allikevel følge instruksene for SENSITIV. Hvilke enheter du kan benytte: For tilgang til SENSITIV informasjon og funksjoner **MÅ** du benytte en **partnerkontrollert enhet.** Lagring og sletting: • SENSITIV informasjon kan **KUN** lagres på en partnerkontrollert enhet eller en lagringstjeneste som er under kontroll av partnerselskapet, slik som filserver, selskapets OneDrive, Teams, Sharepoint, arkivsystem eller lignende fagsystem. • Det er **ikke** tillatt å lagre informasjonen på andre steder slik som din private OneDrive / Google Drive, iCloud, DropBox / Facebook og lignende. • SENSITIV informasjon **MÅ** slettes når behandling er fullført og tjenstlig behov ikke tilsier fortsatt lagring.

1.6. Tillatte enheter

1.6.1. Partnerkontrollert enhet

Det er anbefalt å benytte partnerkontrollert enhet for tilgang til INTERN. Det er påkrevet å benytte partnerkontrollert enhet for tilgang til SENSITIV.

Aksepterte partnerkontrollerte enheter er:

A. **Jobb-PC** fra arbeidsgiver som er meldt inn i selskapets Active Directory, som har oppdatert programvare og som har virusprogram og lignende sikkerhetssystemer kjørende. Se også retningslinjer for personlig datamaskin/PC nedenfor.

B. **Mobil/smarttelefon/nettbrett** eller lignende med aktivt sikkerhetsprogram fra arbeidsgiver (ofte kalt MDM – Mobile Device Management feks Intune). Se også retningslinjer for personlig / delt mobil/smarttelefon/nettbrett nedenfor.

C. **Enheter utlånt fra Bane NOR** med tilsvarende sikkerhetsmekanismer.

1.6.2. Tilstrekkelig sikret enhet

Retningslinjer for akseptable tilstrekkelig sikrede enheter er:

A. Personlig enhet - datamaskin/PC eller mobil/smarttelefon/nettbrett:

1) Som bare brukes av deg, fortrinnsvis til arbeid.
2) Som er låst med passord/kode/fingeravtrykk/ansiktsgjenkjenning eller tilsvarende låsemekanisme som bare du kan låse opp og som automatisk låser seg ved inaktivitet.
3) Som du hele tiden sørger for å oppdatere programvare på (OS, applikasjoner, plugins osv)
4) Som er fri for skadelig programvare og potensielt tvilsomme apper. Du må selv passe på.
5) Som har installert sikkerhetsprogrammer dersom det er anbefalt av leverandør, arbeidsgiver, myndigheter e.l. Du må selv holde deg orientert om dette.
6) Som oppbevares under tilsyn, eller at enheten låses inn herunder låst hus, låst rom, kjøretøy, skap osv eller låses fast når den ikke er under tilsyn.
7) Som du selv sørger for å slette informasjon fra.
8) Som du har slått på eventuelle funksjoner for automatisk sletting ved tyveri, tap eller uautorisert bruk av enheten.

B. Delt enhet - datamaskin/PC eller mobil/smarttelefon/nettbrett (bør unngås!):

1) Som brukes av et fåtall personer med avgrensede arbeidsoppgaver og til arbeid relatert til Bane NOR slik som drift, vedlikehold, utbygging og forvaltning av jernbane, tog, eiendom og tilsvarende.
2) Som har en fast hovedansvarlig for enheten som sørger for IT-sikkerheten.
3) Som er låst med passord/kode/fingeravtrykk/ ansiktsgjenkjenning eller tilsvarende låsemekanisme som bare de aktuelle brukerne kan låse opp og som automatisk låser seg ved inaktivitet.
4) Som ellers følger samme retningslinjer for personlig enhet.

1.7. Kontakt

Kontakt din leder, brukerstøtte i din organisasjon eller IT-avdeling ved spørsmål.

1.8. Unntak

Eventuelle unntak fra dette dokumentet krever skriftlig tillatelse fra Bane NOR.

1.9. Revisjonsoversikt

Rev nr	Dato	Hovedendring
0.1	27.09.2021	Første versjon.
0.2	26.11.2021	Resktrukturert og tydeliggjort innhold.

2. ENGLISH: Instructions for external partners on secure use of Bane NOR’s information systems

2.1. Purpose and scope

These instructions apply to all users from external companies and organizations ("partners") that are granted access to Bane NOR's IT equipment, systems, documents, or information. The instructions contain rules and guidelines for safe use of Bane NOR's information systems. Other rules and regulations in agreements, including the duty of confidentiality, intellectual property and the like also apply. The instructions must be followed during and outside working hours.

Security depends on the individual employee's attitude and that each and everyone takes responsibility for safety. Information security is about ensuring right access to IT systems, avoiding unauthorized access, ensuring that information does not get lost, become inaccessible and is not changed by unauthorized persons.

2.2. Guidelines for ICT equipment and software

2.2.1. ICT equipment for Bane NOR access

Bane NOR allows you to use suitable ICT equipment (PC, mobile phone, and network) for accessing Bane NOR's information systems, if you follow the instructions and the specific guidelines described in this document.

2.2.2. Approved software and equipment

You must follow your organization's guidelines for approved software and equipment, and you must follow your organization's software update policies. The computer / PC should be enrolled in the company's system for managing computers, and the mobile phone / tablet should be registered in the company's system for managing mobile devices (MDM).

2.2.3. Distinguish between private and work

It is good practice that ICT equipment used in a work context is not used for private purposes. Private content shall not be stored in Bane NOR's systems. It is good practice to have a separate, dedicated email address for work.

2.2.4. Virus and malware

If you suspect virus or other malware, turn off your device immediately and contact your organization's support.

2.2.5. Lost equipment

If your equipment is lost, contact your organization's support team immediately.

2.3. Access and publishing

2.3.1. Access to Bane NOR

As an external Bane NOR partner, you shall only have access to the systems and information you need to do the work and perform the tasks that you are approved and authorized to. You shall not in any way acquire other access. If you discover that you have access to more than you have been granted access to, contact your nearest manager or access manager.

Access is granted for a limited duration. You will be notified by email when it is time for an extension.

If the employment relationship is changed or terminated, access must be updated so that you always have the correct access.

2.3.2. Publishing of Bane NOR content

Content and data from the Bane NOR systems you have been granted access to shall not be republished without approval from the information owner in Bane NOR.

2.4. Your Digital Identity

2.4.1. Username

Your username is your own private identity for digital access and should be used by you only. You are responsible for all system access with your username.

2.4.2. E-mail address

For access to Bane NOR's systems, you must use your job/company e-mail address. Individual e-mail accounts must be used for registration of users. It is not allowed with a common email account where usernames and passwords are shared.

2.4.3. Password

Passwords and other access codes are strictly personal and must be kept secret. Password should be changed immediately if it is suspected that it has become known to others. Passwords should be easy to remember, but advanced enough so that others cannot guess them and should therefore not contain information such as date of birth, telephone number or names of family members. You must change your password regularly. Notification about password change is often sent from the system in advance.

2.4.4. Strong authentication (Multifactor Authentication - MFA)

Multifactor Authentication (MFA) must be enabled and used where it is required. Preferably by an authentication app such as Microsoft Authenticator.

2.5. Information Classification

All content that is created, stored, and published via Bane NOR's systems are classified as either OPEN, INTERNAL or SENSITIVE. By request and after approvals you will be able to access information and functions in multiple systems with different level of Information Classification based on service needs.

Tip: Most people working with information in Bane NOR's IT systems will handle INTERNAL information. So make sure you follow the rules of INTERNAL when you work as usual, and take extra precautions when you will be working on something SENSITIVE.

Classification (color)	Guidelines
OPEN (GREEN)	It is recommended to follow the same guidelines as for INTERNAL.
INTERNAL (YELLOW)	Marking and processing: INTERNAL information must be marked with the word "INTERN" in capital letters. If you receive or process information that is not marked with “INTERN”, but that should have been classified as such, then you should still follow the instructions for INTERNAL. Which devices you can use: For access to INTERNAL information and functions, you **MUST** either use a **partner-controlled device** or a **sufficiently secured device**. Storage and deletion: • The information **can** be stored on the user's device and the device's storage service and / or the organization's storage service (such as file server, company OneDrive, Teams, SharePoint, archive system or similar company provided system). • It is **not** allowed to store the information in other places such as your *private* OneDrive / Google Drive, iCloud, Drobox / Facebook and similar. • Information **must** be deleted when processing is completed, and service needs do not indicate continued storage.
SENSITIVE (RED)	Marking and processing: SENSITIVE information must be marked with the word «SENSITIV» in capital letters. If you receive or process information that is not marked with «SENSITIV», but that should have been classified as such, then you should still follow the instructions for SENSITIVE. Which devices you can use: To access SENSITIVE information and functions, you **MUST** use a **partner-controlled device**. Storage and deletion: • SENSITIVE information can **ONLY** be stored on a partner-controlled device or a storage service that is under the control of the partner company, like file server, company OneDrive, Teams, SharePoint, archive system or similar. • It is **not** allowed to store the information in other locations such as your private OneDrive / Google Drive, iCloud, DropBox / Facebook and the like. • SENSITIVE information **MUST** be deleted when processing is complete and service needs do not indicate continued storage.

2.6. Allowed Devices

2.6.1. Partner-controlled devices

It is recommended to use a partner-controlled device for access to INTERNAL. It is required to use a partner-controlled device for access to SENSITIV.

Accepted partner-controlled devices are:

A. **Work PC** from employing company that is registered in the company's Active Directory, and has updated software, virus programs and similar security systems running. See also personal computer / PC guidelines below.

B. **Mobile / smartphone / tablet** or similar with active security program from the employing company (often called MDM - Mobile Device Management eg Intune). See also guidelines for personal / shared mobile / smartphone / tablet below.

C. **Device on loan from Bane NOR** with corresponding security mechanisms.

2.6.2. Sufficiently secured device

Guidelines for sufficiently secured devices are:

A. Personal device - computer / PC or mobile / smartphone / tablet rules:

1) Device is used by you only, preferably for work.
2) Device is locked with a password / code / fingerprint / face recognition or equivalent locking mechanism that only you can unlock, and which automatically locks in case of inactivity.
3) You always make sure to update software on the device (OS, applications, plugins, etc.)
4) Device is free from malicious software and potentially risky apps. It is your responsibility to ensure proper use and device management.
5) Device has security programs installed if recommended by the supplier, employer, authorities, or the like. You need to keep yourself informed about this.
6) Device is stored under supervision, or that the device is stored in a locked location, like locked houses, locked rooms, locked vehicles, locked locker etc. or physically locked to desk or similar when it is not under supervision.
7) You yourself make sure to delete information from the device.
8) You have turned on any functions for automatic deletion in case of theft, loss, or unauthorized use of the device.

B. Shared device - computer / PC or mobile / smartphone / tablet (should be avoided!):

1) Device is used by a few people with limited Bane NOR related work task, within areas like operation, maintenance, development and management of railways, trains, real estate, and the like.
2) The device has a permanent main responsible that ensures IT security.
3) Device is locked with a password / code / fingerprint / face recognition or equivalent locking mechanism which only the relevant users can unlock and which automatically locks in case of inactivity.
4) You follow the same guidelines for personal device.

2.7. Contact

Contact your leader, user support or IT department in your organization if you have any questions.

2.8. Exceptions

Any exceptions from this document require written permission from Bane NOR.

2.9. Revision overview

Rev nr	Date	Main change
0.1	27.09.2021	First version.
0.2	26.11.2021	Restructured and clarified content.