

Når du arbejder for staten

En sikkerhedsinstruks til statens bygninger
og digital sikkerhed



Indhold

INDLEDNING

SIKKERHED

- KLASSIFISERINGSNIVEAU

- ID-KORT OG NØGLER

ARBEJDSMILJØ

SÆRLIGE OMRÅDER

VED AKUTTE HÆNDELSER

- NØDUDGANGE OG FLUYGVEJE

ALARMER

DIGITAL SIKKERHED

- FORTROLIGE OPLYSNINGER SKAL BEHANDLES FORTROLIGT

- VÆR MEGET FORSIGTIG MED "DATALOKKERE"

- BRUG INTERNETTET OG MAILBOKS PÅ EN SIKKER MÅDE

- PAS PÅ SIKKERHEDEN PÅ DINE BÆRBARE MEDIER

PARKERING

KONTAKTPERSONER

RYGNING OG RUSMIDLER

KRAV TIL LEGITIMATION

Indledning

Denne sikkerhedsinstruks er udarbejdet af Bygningsstyrelsens Center for Facility Management. Retningslinjerne skal efterleves af leverandørens medarbejdere, ligesom instruksens skal udleveres i forbindelse med instruering af leverandørens medarbejdere.

Kontaktpersonen er den lokale BYGST FM-medarbejder fra Bygningsstyrelsen.

Husk, at der er lokale krav og retningslinjer hos den enkelte kunde, som ligeledes skal overholdes.

Kontakt den lokale BYGST FM-medarbejder for yderligere information.

Sikkerhed

Det er vigtigt, at du sikrer, at ingen uvedkommende får/kan få adgang til statens bygninger. Ingen udgangsdøre må efterlades åbne/fastkilet.

Klassificeringsniveau

Der gælder forskellige klassificeringsniveauer i forhold til sikkerhedskravene hos leverandørens medarbejdere. Klassificeringsniveauet afhænger af, hvilke opgaver du skal løse.

Som udgangspunkt kræver det en registermæssig undersøgelse (sikkerhedstjek) at arbejde i statens bygninger. Der kan dog være opgaver, der udføres på lokaliteter, som kræver et udvidet sikkerhedstjek kaldet en sikkerhedsgodkendelse. Kunden beslutter, hvilket niveau der gælder på den pågældende lokalitet, eller hvilket sikkerhedsniveau der gælder i forhold til opgaven, som skal udføres.

En registermæssig undersøgelse eller sikkerhedsgodkendelse **skal** være gennemført, inden arbejdet kan gå i gang.

ID-kort og nøgler

Alle leverandørens ansatte der færdes på statens område, skal bære synligt ID-kort. I modsat fald kan det medføre bortvisning.

ID-kort og nøgler er strengt personligt og må ikke overdrages til andre.

Mister du dit ID-kort eller nøgle, skal dette omgående meldes til nærmeste chef, kontaktperson og i receptionen, hvis der er reception på lokaliteten.



ID-kort

Arbejdsmiljø

Alt arbejde der udføres i staten skal udføres i henhold til gældende arbejdsmiljøregler. Hvis du er i tvivl, skal du kontakte den lokale kontaktperson.

Særlige områder

Der kan være områder i statens bygninger, der ikke er tilgængelige uden følgeskab af en medarbejder fra kunden. Al skiltning eller anden instruks vedr. færden **skal** til hver en tid følges. Hvis du er i tvivl, så spørg den lokale kontaktperson.

Ved akutte hændelser

Personskade, brand mv.

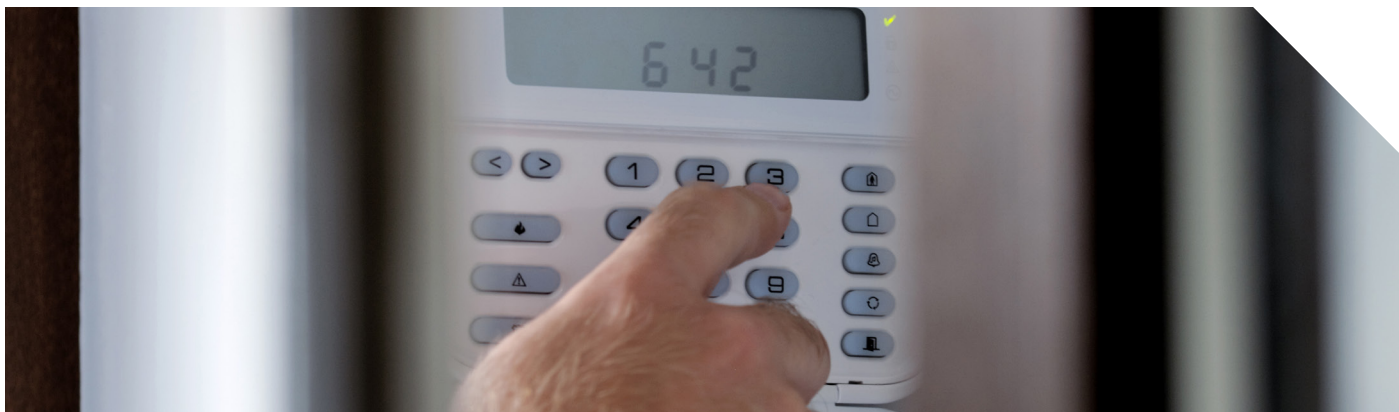
Udøv altid livredende førstehjælp og alarmering:

- Ring 112 og afgiv melding
- Hvem er du, og hvor ringer du fra
- Hvad der er sket (skadens omfang)
- Hvor det er sket (nøjagtig adresse)
- Hvor mange tilskadekomne
- Aftal altid mødested, tilkørselsvej og dit telefonnummer
- Ring herefter til den lokale kontaktperson eller receptionen

Nødudgange og flugtveje

Du skal altid gøre sig bekendt med de ophængte flugtvejsplaner i statens bygninger.

Arbejde ved nødudgange skal altid koordineres med den lokale kontaktperson. Når en nødudgang spærres af, skal en alternativ udgang anvises ved skiltning. Længerevarende afspærringer af nødudgange kræver myndighedsgodkendelse. Afspærring af nødudgange skal varsles rettidigt til din kontaktperson, så denne kan varsle brugerne.



Alarmer

Før man går i gang med arbejde, som kunne have en indvirkning på brandalarmer m.v., skal du gøre sig bekendt med de alarmer, som findes i bygningen. Kontaktpersonen kan oplyse, om der findes brandalarmer i bygningen.

Hvis der er behov for frakobling af tyverialarm, brandalarmer eller andre alarmer i særlige områder, skal dette godkendes af din kontaktperson.

Fejlalarmer

- Tyverialarm – Politiet kontaktes automatisk ved alarm. Du skal øjeblikkeligt informere din kontaktperson.
- Brandalarm – Brandvæsenet kontaktes automatisk ved alarm. Du skal øjeblikkeligt informere din kontaktperson.
- Kun brandvæsenet må fra-og tilkoble brandalarmen igen.

Der henvises derudover til instruks på ophængte lokale brandplaner.

Digital sikkerhed

Hvis du skal arbejde i statens IT-systemer hos den enkelte kunde, skal du have tjek på IT-sikkerheden. I følgende afsnit beskrives, hvilke IT-sikkerhedsmæssige regler du som minimum **skal** overholde.

Husk, at der er lokale krav og retningslinjer hos den enkelte kunde, som ligeledes skal overholdes. Kontakt den lokale BYGST FM-medarbejder (din kontaktperson) for yderligere information.

Fortrolige oplysninger

Fortrolige oplysninger skal behandles forsvarligt og sikkert.

- Pas på print med fortrolige oplysninger
- Eksterne mails med fortrolige oplysninger skal sendes krypteret
- Lås PC'en, når du forlader den





Vær meget forsigtig med "Datalokkere"

Vær opmærksom og på vagt over for forsøg på at lokke data eller andre oplysninger ud af dig, der kan bruges til at skade dig eller kunden:

- Pas på forsøg, hvor nogen forsøger at franarre informationer.
- Udlever aldrig dit password. Statens IT beder aldrig om password.
- Det er altid i orden at spørge fremmede, hvem de er, og hvad de laver her.
- Er du blevet udsat for et angreb, kontakt straks IT-afdelingen hos kunden.

Brug internettet og mailboks på en sikker måde

Vær opmærksom på filer og programmer, du kommer i besiddelse af, så disse ikke kan skade dig eller kunden.

- Download kun filer eller programmer fra kilder, du kender. Gør man det alligevel fra upålidelig kilde ved en fejl, kontakt straks IT-afdelingen hos kunden.
- Åbn aldrig mistænkelige mails. Kommer du alligevel til det, kontakt IT-afdelingen hos kunden.

Pas på sikkerheden på dine bærbare medier

Beskyt dine bærbare medier, så fremmede ikke kan bruge disse til at skade dig eller kunden:

- Bærbare medier skal være beskyttet af password og lås på skærm, der aktiveres umiddelbart ved inaktivitet.
- Tab og tyveri af bærbare medier meldes straks til Statens IT, kundens IT-afdeling og den lokale kontaktperson.
- Reglerne gælder også egne bærbare medier, der synkroniserer med webmail/webkontor.
- Har du en smartphone fra kunden, skal den have mobilkontrol installeret (Mobile Device Management). Spørg din kontaktperson, hvis du er i tvivl, om mobiltelefonen har det.



Parkering

Leverandøren er selv ansvarlig for at overholde lokale parkeringsbestemmelser. Kontakt din kontaktperson, hvis du er i tvivl om, hvor du kan parkere.

Rygning og rusmidler

Rygning er ikke tilladt indendørs i statens bygninger.

Udendørs kan der lokalt være indrettet rygerum. På alle øvrige adresser er det tilladt at ryge på de udendørs fællesarealer, dog minimum 5 m fra bygningerne.

Det er strengt forbudt at medbringe eller indtage alle former for rusmidler på statens arealer. Dette gælder også alkohol.

Overtrædelse medfører bortvisning og eventuelt politianmeldelse.



Krav til legitimation

Alle ISS' ansatte og dennes underleverandører skal til enhver tid bære leverandørens ID-kort. Det skal indeholde:

1. Firmanavn
2. Fulde navn
3. Fødselsdato
4. Medarbejdersnummer
5. Sikkerhedsklassifikationsgrad: TTJ/FTR/HEM/YHEM.
6. Firmanavn, såfremt medarbejderen er ansat hos en underleverandør.

Kan kunden afvise en leverandør-ansat?

Kunden kan afvise en ISS-ansat eller dennes underleverandør såfremt nedenstående krav til legitimation ikke er opfyldt.

Legitimation skal være en eller flere af følgende:

1. Pågældende bærer uniform – enten ISS-uniform eller uniform fra underleverandør (udvalgte receptionister undtaget).
2. Pågældende kan fremvise ISS' ID-kort, som også udstedes til underleverandører.
3. Pågældende kan fremvise gyldigt billedlegitimation.
4. Pågældende kan fremvise gyldigt Arbejds- og opholdskort udstedt af de danske udlændingemyndigheder, hvis relevant.

Inden for normal arbejdstid kan kunden ringe til ISS på **38 17 17 75** eller på mail iss-servicecenter-bygst@iss.dk, som herefter på baggrund af unikt medarbejdersnummer på ID-kortet kan oplyse om pågældendes ansættelsesforhold.