Sikkerhetsinstruks

Denne sikkerhetsinstruks skal leses og signeres av alle ansatte før oppstart av ansettelsesforholdet.

bouvet

Gjelder fra:	Versjon:
01.11.2024	3.1

Versjonshistorikk

Versjon	Dato	Beskrivelse	Ansvarlig
2.0	01.08.2023	Baseline	Knut Dischington
3.0	20.01.2024	Små justeringer i kap 7 og 9, oppdatert signeringsfelter	Knut Dischington
3.01	01.02.2024	Oppdatert kap 16 med «Store bokstaver»	Knut Dischington
3.1	01.11.2024	Nytt kapittel 4	Knut Dischington

1. Generelt om personlig ansvar og IT-sikkerhet

Det skal ikke gis opplysninger til noen utenfor selskapet om påloggingsrutiner, brukernavn og/eller felles passord til de forskjellige systemene som inngår i Bouvets eller Bouvets kunders infrastruktur.

Dette gjelder også etter en eventuell fratredelse fra selskapet.

Alle personlige passord skal holdes strengt personlig og man er selv ansvarlig for at passordet ikke er lett å gjette. Du kan ikke dele passordet med kolleger, familiemedlemmer, samboere eller noen annen tredjeperson.

Passord skal ikke noteres ned slik at andre kan få fatt i dette, og man skal ikke skru på automatisk lagring av passord i nettlesere.

Alle steder hvor det kan brukes to-faktor innlogging, skal dette gjøres.

Dersom du har mistanke om at noen kjenner ditt passord, skal passordet endres umiddelbart og det skal rapporteres som en sikkerhetshendelse.

Den ansatte forplikter seg til å holde seg oppdatert på og følge reglene for informasjonssikkerhet og basis sikkerhetskompetanse for sine roller, slik de er beskrevet på Bouvets Intranett.

2. E-post og kalender

E-postsystemet er ment som et arbeidsverktøy. Personlig bruk av e-post er tillatt, men må ikke komme i konflikt med arbeidet. Utvis forsiktighet med hva du bruker Bouvetmailen til.

Kalenderen i e-postsystemet er åpen og kan leses av alle kolleger. Unngå derfor å legge inn sensitiv informasjon eller merk med «privat».

3. Selskapets rett til innsyn

Det er ikke praksis i selskapet å overvåke de ansattes innhold i e-post og andre kommunikasjons- eller lagringsmedia, men selskapet forbeholder seg retten til innsyn dersom;

- det er nødvendig for å ivareta den daglige driften (f.eks. i forbindelse med sykdom eller annet fravær)
- det er nødvendig for å ivareta selskapets berettigede interesser
- det er begrunnet mistanke om grovt pliktbrudd eller andre forhold som kan gi grunnlag for oppsigelse eller avskjed.

Beslutning om innsyn tas av personalansvarlig, sammen med Sikkerhetssjef (CISO). Den ansatte vil så langt det er mulig bli varslet på forhånd ved behov for innsyn og få anledning til å uttale seg før innsyn gjennomføres. Den ansatte skal så langt det er mulig gis anledning til å være til stede under innsynet og har rett til å la seg bistå av tillitsvalgt eller annen representant. Hvordan innsyn har foregått, hva innsynet har bestått i og hvem som deltok skal dokumenteres skriftlig.

4. Bruk av Bouvet ID-kort

Alle ansatte skal, så lenge de oppholder seg i våre lokaler, til enhver tid bære Bouvet ID-kort med bilde og navn (adgangskort) godt synlig rundt halsen. Dette for at vi effektivt skal kunne identifisere evt. ikke-ansatte som oppholder seg i lokalene, og gjøre nødvendige tiltak overfor disse.

Du skal ikke bære adgangskortet synlig utenfor våre lokaler.

Du skal ikke publisere bilder som viser adgangskortet ditt på internett, inkludert alle former for nettsamfunn, sosiale media og andre typer kanaler, uten å på forhånd ha fått godkjenning fra CISO.

Husk dessuten at tilsvarende regler kan gjelde hos kunden, så få tillatelse først.

5. Logging og beskyttelse mot uønskede hendelser

Bouvet benytter flere forskjellige verktøy for å beskytte maskiner, identiteter og annen infrastruktur mot dataangrep og uønskede hendelser. Disse verktøyene analyserer både trafikk og innhold på Bouvets maskiner og andre Bouvet-kontrollerte enheter. Ved varsling fra disse verktøyene vil Intern IT & Sikkerhet analysere det konkrete tilfellet og varsle brukeren hvis det finns behov for korreksjon. Det vil alltid opprettes en sikkerhetshendelse («Security Incident Report») i Bouvets hendelsessystem, med kopi til personalansvarlig.

6. Lagring

Alt materiale, som f.eks. dokumenter, kildekode, design, data osv. som produseres av den ansatte for Bouvet eller Bouvets kunder, skal lagres på Bouvet-administrerte eller kunde-administrerte IT-løsninger. Det skal ikke lagres slikt materiale på tredjepartsløsninger der Bouvet eller kunden ikke har administrativ kontroll på tilganger og innhold. Eksempler på dette kan være privat Dropbox, Apple iCloud og Google Drive.

7. Arbeidsverktøy

Alle ansatte får utdelt nødvendig arbeidsverktøy ved oppstart, vanligvis en Bouvet-kontrollert PC/Mac og mobiltelefon.

Du skal aldri låne ut eller dele dette utstyret til andre, det være seg Bouvet-ansatte, familiemedlemmer eller andre.

I forbindelse med oppdrag kan den ansatte også få en kunde-kontrollert PC/Mac for bruk mot kundens løsninger og infrastruktur.

Det er kun disse Bouvet- eller kunde-kontrollerte enhetene som skal benyttes i arbeidssammenheng. Man skal aldri logge inn på Bouvets eller kundens løsninger og infrastruktur fra andre enheter enn disse. Man skal følge Bouvets til enhver tid gjeldende fjernaksess-policy.

8. Ansattes blogging og bruk av sosiale medier

Det er positivt at ansatte skriver på nettet om aktiviteter i Bouvet som er interessante for eksterne, f.eks. frokostseminarer, gode blogginnlegg, foredrag som holdes av ansatte eller lignende.

Man må utøve god dømmekraft med hensyn til hva man sier på nettet om Bouvet, kunder, partnere, konkurrenter og kolleger. Vær bevisst på at det i praksis er vanskelig å skille på hva du sier som representant for Bouvet og som privatperson. Opptre i samsvar med allmenne regler for god folkeskikk.

Dersom det har blitt publisert ulovlig materiale på vegne av Bouvet eller materiale som kan skade selskapets omdømme, ta kontakt med kommunikasjonsansvarlig for hjelp til å håndtere det.

Signering på politiske opprop

Bouvet skal selvsagt ikke mene noe om du skal signere politiske opprop, men vi ønsker at du gjør det som privatperson. Det innebærer at vi ikke ønsker at du signerer med Bouvet.

9. Policy i forhold til bruk av opphavsrettslig beskyttet materiale

Bouvet erverver lisenser for bruk av programvare for datamaskiner fra en rekke selskaper/ programvareprodusenter. Bouvet eier ikke denne programvaren eller dokumentasjonen knyttet til den, og har, med mindre det er godkjent av programvareprodusenten, ikke rett til å kopiere den, med unntak av sikkerhetskopier. Bouvets ansatte skal bruke programvare i samsvar med de lisensbetingelsene som gjelder for den forskjellige programvaren.

Bouvets ansatte skal ikke laste ned eller laste opp uautorisert programvare eller annet opphavsrettslig beskyttet materiale som filmer, musikk, bilder etc. over internett.

I henhold til gjeldende lover om opphavsrett, kan ulovlig kopiering av programvare medføre sivilt erstatningssøksmål og straffeansvar, som bøter og fengsel. Bouvet tillater ikke kopiering av programvare eller annet opphavsrettslig beskyttet materiale. Bouvets ansatte som lagrer, får tak i, eller bruker uautoriserte kopier av opphavsrettslig beskyttet materiale for datamaskiner må påregne å bli stilt til ansvar for dette, og forholdet kan også medføre avskjedigelse.

Enhver tvil om hvorvidt en ansatt kan installere, kopiere eller bruke en gitt kopi av programvare eller bruke et program eller annet opphavsrettslig beskyttet materiale, skal tas opp med nærmeste leder før man går i gang.

Nedlasting, lagring eller videresending av straffbart materiale som f.eks. barneporno, rasistisk materiale m.m. er under enhver omstendighet forbudt og vil kunne være oppsigelsesgrunn.

Eiendom og opphavsrett og andre immaterielle rettigheter til det som leveres gjennom oppdrag, herunder rett til endring, bearbeidelse og videreoverdragelse, tilligger kunden eller Bouvet, avhengig av den aktuelle kontrakt. Bouvets ansatte kan ikke hevde opphavsrett på noen deler av det som

leveres i oppdraget eller materiale som tas med inn i oppdraget, uten skriftlig avtale på forhånd. Dette gjelder uavhengig av når og i hvilken sammenheng slikt materiale er utarbeidet

10. Håndtering av presse-/media

Den generelle taushetsplikten gjelder også ved henvendelser fra presse og media. Alle slike henvendelser skal henvises til leder for kommunikasjon.

Da Bouvet generelt anser mediedekning som profilskapende egenmarkedsføring, kan ledere med ansvar for et forretningsområde, et fagområde eller et produktområde på generell basis uttale seg uten forhåndsgodkjenning dersom henvendelsen og det etterfølgende oppslaget antas å være et faglig orientert oppslag.

Den som uttaler seg til presse/media må be om å få lese gjennom oppslaget før det trykkes/sendes. Vedkommende bør også be journalisten sende kopi av oppslaget til Bouvet. Medarbeideren skal sørge for at kommunikasjonsansvarlig i selskapet gjøres kjent med oppslaget.

11. Børsens innsideregler

Bouvet ASA er børsnotert, og alle ansatte i samtlige av Bouvet ASAs datterselskaper er av den grunn omfattet av børsens innsideregler knyttet til sensitiv informasjon. Innsideinstruksen finnes på Min side og skal leses av alle.

I tillegg gjøres det oppmerksom på at enhver medarbeider som under oppdrag hos kunde får tilgang til sensitiv informasjon eller utfører oppdrag som antas å kunne påvirke kursen merkbart, er i en situasjon hvor børsens innsideregler kan komme i betraktning. Det vil si informasjon som en fornuftig investor sannsynligvis vil benytte som en del av grunnlaget for sin investering,

12. Ansattes uavhengighet

Dersom en medarbeider eller dennes nærstående har betydelige eierinteresser i selskaper som er i, eller er i ferd med å komme i, et kunde- eller leverandørforhold til Bouvet, skal adm. direktør informeres for å vurdere mulige habilitetskonflikter. Betydelige eierinteresser defineres i denne sammenheng som en eierandel på over 20 %. Med nærstående menes ektefelle/partner/samboer, barn, foreldre og søsken.

13. Håndtering av arbeid for konkurrerende kunder

Som en hovedregel anser vi å arbeide for flere bedrifter innen samme virksomhetsområde eller bransje, som en fordel for både Bouvet og kunden, all den tid Bouvet's og konsulentens bransjekunnskap har nær sammenheng med et oppdrags kvalitet.

I enkelte tilfeller kan et oppdrags natur stille krav til tiltak utover den alminnelige taushetsplikten. Dette gjelder eksempelvis ved formulering av strategier, utarbeiding av langsiktige handlingsplaner og ved utvikling av løsninger som ikke skal offentliggjøres før lanseringstidspunktet.

Avtale om sikkerhetstiltak utover alminnelig taushetsplikt skal alltid være nedtegnet skriftlig og gjelde for en definert tidsperiode og slike sikkerhetstiltak skal godkjennes av adm. direktør før de tilbys ovenfor en kunde.

14. Taushetsplikt

Alle ansatte har plikt til å bevare taushet om alle forhold man får kjennskap til gjennom sitt ansettelsesforhold så vel innenfor selskapet som hos selskapets kunder eller hos våre partnere. Dette gjelder både kundeinformasjon og interne bedriftsanliggender i Bouvet.

Taushetsplikten gjelder også etter at ansettelsesforholdet opphører. Når ansettelsesforholdet opphører skal all informasjon som anses å være taushetsbelagt returneres.

Taushetsplikten er absolutt med de unntak som følger av lov.

15. Brudd på sikkerhetsrutiner

Enhver ansatt i Bouvet har plikt til å snarest melde fra dersom man får kjennskap til brudd på rutiner for informasjonssikkerhet. Det er etablert en egen kanal for å rapportere om slike brudd, som nås via intranettet.

Alle meldinger om brudd på sikkerhetsrutiner vil bli undersøkt og tiltak iverksettes om nødvendig. Tilsiktede brudd på sikkerhetsrutiner kan medføre oppsigelse eller avskjed.

16. Bouvet’s kunders retningslinjer og regler

Den ansatte skal alltid følge Bouvets, og der dette er relevant, kundens sikkerhetsrutiner. I de tilfeller kunden har en strengere policy, skal denne følges.

17. Erklæring

Undertegnede bekrefter å ha lest og forstått innholdet i denne instruks og forplikter seg til å følge denne. Signeres fysisk eller digitalt.

Navn (STORE BOKSTAVER)

Sted/dato

Signatur

Ett eksemplar beholdes av arbeidstaker og ett returneres elektronisk til Personalavdelingen for arkivering.