Säkerhetsinstruktioner

Dessa säkerhetsinstruktioner ska läsas och undertecknas av alla anställda innan anställningen påbörjas.

bouvet

Gäller från:	Version:
01.11.2024	3.1

Versionshistorik

Version	Datum	Beskrivning	Ansvarig
2.0	01.08.2023	Baseline	Knut Dischington
3.0	20.01.2024	Små justeringar i kap. 7 och 9, uppdaterade signeringsfält	Knut Dischington
3.01	01.02.2024	Uppdaterat kap. 16 med "Stora bokstäver"	Knut Dischington
3.1	01.11.2024	Nytt kapitel 4	Knut Dischington

1. Allmänt om personligt ansvar och IT-säkerhet

Ingen utomstående får ges information om inloggningsrutiner, användarnamn och/eller gemensamma lösenord till de olika system som ingår i Bouvets eller Bouvets kunders IT-miljö.

Detta gäller även efter att du eventuellt lämnat din tjänst på företaget.

Alla personliga lösenord är strängt personliga och det är ditt ansvar att se till att dina lösenord är svåra att gissa sig till. Personliga lösenord får inte delas med kollegor, familjemedlemmar, sammanboende eller andra utomstående.

Skriv inte ner lösenord så att andra kan få tillgång till dem, och aktivera inte automatisk lagring av lösenord i webbläsare.

Tvåfaktorsautentisering för inloggning ska användas där det är möjligt.

Om du misstänker att någon känner till ditt lösenord ska du omedelbart ändra det och rapportera det som en säkerhetshändelse.

Alla anställda är skyldiga att hålla sig uppdaterade och följa reglerna om informationssäkerhet och säkerhetskompetens för sina respektive roller. Information om detta finns på Bouvets intranät.

2. E-post och kalender

E-postsystemet är i första hand ett arbetsverktyg. Det är tillåtet att använda e-postsystemet för privata ändamål, så länge detta inte påverkar arbetet. Var varsam med vad du använder Bouvetmejlen till.

Kalendern i e-postsystemet är öppen och kan läsas av alla kollegor. Undvik därför att lämna känslig information i kalendern, eller märk sådan information med "privat".

3. Företagets rätt till insyn

Det är inte praxis för företaget att övervaka de anställdas innehåll i e-post och andra kommunikations- eller lagringsmedier, men företaget förbehåller sig rätten till insyn i det fall:

- det är nödvändigt för verksamhetens dagliga drift (t.ex. i samband med sjukdom eller annan frånvaro)
- det är nödvändigt för att tillvarata företagets legitima intressen
- det finns välgrundad misstanke om ett grovt brott mot gällande förpliktelser eller annan omständighet som kan vara skäl för uppsägning eller avsked.

Beslut om insyn fattas av personalansvarig, tillsammans med säkerhetschef (CISO). Den berörda medarbetaren kommer i möjligaste mån att meddelas i förväg om insyn i dennes e-postkonton anses nödvändigt. Han/hon kommer också ges möjlighet att lämna synpunkter innan så sker. Medarbetaren ska i möjligaste mån ges möjlighet att närvara under insynsprocessen och har rätt att ha med sig ett fackligt ombud eller annan representant. Hur insynsprocessen har gått till, vad den bestått i och vem som deltog ska dokumenteras skriftligen.

4. Användning av Bouvet ID-kort

Alla anställda ska, så länge de vistas i våra lokaler, alltid ha på sig sitt Bouvet ID-kort (passerkort) väl synligt runt halsen. Detta för att vi enkelt ska kunna identifiera eventuella icke-anställda som vistas i lokalerna och vidta nödvändiga åtgärder. Du får inte bära passerkortet synligt utanför våra lokaler. Du får inte publicera bilder som visar ditt passerkort på internet, inklusive någon form av online-communities, sociala medier och andra typer av kanaler, utan föregående godkännande från CISO. Kom också ihåg att liknande regler kan gälla hos kunden, så skaffa tillstånd först.

5. Loggning och skydd mot oönskade händelser

Bouvet använder sig av flera olika verktyg för skydda datorer, identiteter och annan infrastruktur mot dataintrång och oönskade händelser. Dessa verktyg analyserar både trafik och innehåll på Bouvets datorer och andra Bouvet-kontrollerade enheter. Vid rapportering från dessa verktyg kommer Intern IT & Säkerhet att analysera den aktuella händelsen och meddela användaren om det finns behov av att genomföra korrigeringar. Det upprättas alltid en säkerhetshändelse ("Security Incident Report") i Bouvets händelsesystem, med kopia till personalansvarig.

6. Lagring

Allt material, som exempelvis dokument, källkod, design, data osv. som produceras av den anställda för Bouvet eller Bouvets kunder, ska lagras i IT-lösningar som administreras av Bouvet eller Bouvets kunder. Sådant material får inte lagras i tredjepartslösningar där Bouvet eller kunden inte har administrativ kontroll över åtkomst och innehåll. Exempel på sådana tredjepartslösningar är Dropbox, Apple iCloud och Google Drive.

7. Arbetsverktyg

Alla anställda får sig tilldelade nödvändiga arbetsverktyg när de börjar, vanligtvis en Bouvet-kontrollerad PC/Mac och mobiltelefon.

Du får aldrig låna ut denna utrustning till andra, vare sig Bouvet-anställda, familjemedlemmar eller någon annan.

I samband med uppdrag kan den anställda även få en kundkontrollerad PC/Mac för användning mot kundens lösningar och infrastruktur.

Endast dessa Bouvet- eller kundkontrollerade enheter får användas i arbetssammanhang. Man får aldrig logga in på Bouvets eller kundens lösningar och infrastruktur från andra enheter än dessa. Följ alltid Bouvets, för tidpunkten gällande, policy angående fjärranslutning.

8. Användning av bloggar och sociala medier

Det är positivt att medarbetare skriver på webben om Bouvet-aktiviteter som är intressanta för externa läsare, till exempel frukostseminarier, bra blogginlägg, föredrag som hålls av medarbetare och liknande.

Medarbetare som uttalar sig i olika medier om Bouvet, kunder, partner, konkurrenter och kollegor ska agera med gott omdöme. Var medveten om att det i praktiken är svårt att avgöra om en person

uttalar sig som representant för Bouvet eller som privatperson. Uppträd i enlighet med vedertagna uppfattningar om vad som är ett gott folkvett.

Om du upptäcker att det publicerats otillåtet material i Bouvets namn, eller material som kan skada företagets rykte, ska kommunikationsavdelningen kontaktas så att de kan hjälpa till att hantera ärendet.

Undertecknande av politiska upprop

Bouvet ska naturligtvis inte lägga sig i om du undertecknar politiska upprop, men vi vill att du gör det som privatperson. Det innebär att vi inte vill att du undertecknar med Bouvet.

9. Policy gällande upphovsrättsskyddat material

Bouvet använder programvara på licens från en mängd olika företag och programvarutillverkare. Bouvet äger inte sådana programvaror eller tillhörande dokumentation och har inte rätt att kopiera dem utan godkännande från programvarutillverkaren, med undantag för säkerhetskopior. Bouvets medarbetare ska använda programvaror i enlighet med de licensvillkor som gäller för den aktuella programvaran.

Bouvets medarbetare får inte ladda ner eller ladda upp oauktoriserad programvara eller annat upphovsrättsskyddat material, såsom filmer, musik, bilder etc. via internet.

Enligt gällande lagar om upphovsrätt kan olovlig kopiering av programvara leda till juridiska påföljder såsom skadestånd, böter och i värsta fall fängelsestraff. Bouvet tillåter ingen kopiering av programvara eller annat upphovsrättsskyddat material. Medarbetare som lagrar, erhåller eller tillskansar sig, eller använder oauktoriserade kopior av upphovsrättsskyddade data kan ställas till ansvar. Detta kan även leda till avsked.

Kontakta närmaste chef om du är det minsta osäker på om en medarbetare får eller inte får installera, kopiera eller använda en kopia av en programvara eller annat upphovsrättsskyddat material.

Att ladda ner, lagra eller vidarebefordra olagligt material, som t.ex. barnpornografi, rasistiskt material etc. är under alla omständigheter förbjudet och kan leda till uppsägning.

Ägande- och upphovsrätten och andra immateriella rättigheter till sådant som levereras genom uppdrag, däribland rätten till ändring, bearbetning och vidarebefordran, innehas av kunden eller Bouvet, beroende på det aktuella avtalet. Bouvets medarbetare får inte göra anspråk på upphovsrätten för någon del av det som levereras i ett uppdrag, eller för material som ingår i ett uppdrag, utan föregående skriftligt avtal.
Detta gäller oavsett när och i vilket sammanhang sådant material har utarbetats.

10. Hantering av press/media

Den generella tystnadsplikten gäller även vid förfrågningar från press och media. Alla sådana förfrågningar ska hänvisas till chef för kommunikation.

Generellt sett anser Bouvet att publicitet i media är en form av profilskapande marknadsföring. Därför kan chefer med ansvar för ett affärsområde, ämnesområde eller produktområde i allmänhet uttala sig utan föregående godkännande, om förfrågan och den efterföljande artikeln/inslaget antas vara relevant och intressant.

Den som talar med pressen/media ska begära att få läsa igenom artikeln/inslaget före publicering. Vederbörande bör även be journalisten skicka en kopia av artikeln/inslaget till Bouvet. Medarbetaren ska också informera kommunikationschefen om publiceringen.

11. Börsens insiderregler

Bouvet ASA är börsnoterat, och alla anställda i samtliga av Bouvet ASA:s dotterbolag omfattas därför av börsens insiderregler gällande känslig information. Insiderreglerna finns på Min sida och ska läsas av alla.

Observera också att en medarbetare som under uppdrag hos en kund får tillgång till känslig information, eller utför uppdrag som antas kunna påverka kursen märkbart, befinner sig i en situation där börsens insiderregler kan vara tillämpliga. Det vill säga information som en normal investerare sannolikt skulle ta hänsyn till vid en investering.

12. Anställdas oberoende

Om en medarbetare eller hans/hennes närstående har betydande ägarintressen i bolag som har eller håller på att ingå en kund- eller leverantörsrelation med Bouvet ska vd informeras så att han/hon kan avgöra om en intressekonflikt föreligger. I detta sammanhang definieras betydande ägarintressen som en ägarandel på mer än 20 %. Med närstående avses maka/make/partner/sambo/barn, föräldrar och syskon.

13. Arbete för konkurrerande verksamhet

Att en inhyrd medarbetare har uppdrag för flera företag inom samma verksamhetsområde eller bransch betraktar vi som huvudregel som en fördel för både Bouvet och kunden, så länge Bouvets och konsultens branschkunskaper har nära koppling till ett uppdrags kvalitet.

Beroende på uppdragets karaktär kan det ställas särskilda krav utöver tystnadsplikten. Detta gäller till exempel vid utformning av strategier och långsiktiga handlingsplaner eller vid utveckling av lösningar som inte får offentliggöras före lansering.

Avtal om säkerhetsåtgärder utöver den allmänna tystnadsplikten ska alltid vara skriftliga och gälla för en definierad tidsperiod. Sådana säkerhetsåtgärder ska också godkännas av vd innan de erbjuds till kund.

14. Tystnadsplikt

Alla anställda omfattas av tystnadsplikt när det gäller sådant man får kännedom om genom sin anställning, såväl inom företaget som hos kunder eller våra partner. Detta gäller både kundinformation och Bouvets interna affärsangelägenheter.

Tystnadsplikten gäller även efter att anställningsförhållandet upphört. När anställningsförhållandet upphör ska medarbetaren återlämna all information som anses vara konfidentiell.

Tystnadsplikten är absolut med undantag för vad som är lagstadgat.

15. Brott mot säkerhetsrutiner

Alla anställda på Bouvet är skyldiga att snarast rapportera om man får kännedom om brott mot rutiner gällande informationssäkerhet. En särskild kanal för att rapportera sådana överträdelser har upprättats och nås via intranätet.

Alla rapporter om överträdelser av säkerhetsrutinerna kommer att undersökas och vid behov ska åtgärder vidtas. Uppsåtliga överträdelser av säkerhetsrutinerna kan leda till uppsägning eller avsked.

16. Riktlinjer och regler för Bouvets kunder

Den anställda ska alltid följa Bouvets, och när så är relevant, kundens säkerhetsrutiner. I de fall kunden har en striktare policy ska den följas.

17. Intygande

Jag bekräftar härmed att jag har läst och förstått dessa säkerhetsinstruktioner och förbinder mig att följa dem.

Namn (STORA BOKSTÄVER)

Ort/datum

Namnteckning

Ett exemplar behålls av medarbetaren och ett returneras elektroniskt till personalavdelningen för arkivering.