|  |
| --- |
|  **Vejledning til anvendelse af Wired Relations’ rammeværktøj** |

Wired Relations’ rammeværktøj\* kan anvendes direkte i jeres arbejde med databeskyttelse og informationssikkerhed– men kan selvfølgelig også anvendes som inspiration til jeres eget materiale. I kan ændre efter behov, så det bliver præcis, som I ønsker det.

**OBS!** Der kan være afsnit, som ikke er relevante for alle organisationer. Hvis dette er tilfældet, vil det tydeligt fremgå af teksten.

Der vil være steder i teksten, hvor der er lagt op til, at I indsætter organisationen navn eller andet. Dette vil i så fald være markeret jf. følgende: [*indsæt organisationens navn*].

I bunden af hvert dokument vil der fremgå en tabel, som giver et overblik over dokumentets version, seneste opdatering, samt hvem der har ansvaret for dokumentet.

**Retningslinjer for medarbejdere i forhold til informationssikkerhed og databeskyttelse**

**1. Formål**

Disse retningslinjer beskriver, hvad du som medarbejder skal vide og gøre for at sikre, at [*indsæt organisationens navn*] opretholder et passende sikkerhedsniveau og overholder den databeskyttelsesretlige lovgivning.

**2. Sikkerhedsforanstaltninger**

Følgende afsnit beskriver hvilke sikkerhedsforanstaltninger, du skal træffe.

**2.1. Brug af systemer og enheder**

Systemer

Du må kun behandle personoplysninger i systemer, som er godkendt hertil af virksomheden, og behandlingen må kun ske på en måde, der er godkendt af virksomheden.

Såfremt du er i tvivl om, hvorvidt et system, eller en speciel anvendelse af et system, er godkendt af virksomheden, skal du afklare dette med compliance-teamet.

Såfremt du ønsker at anvende et system, som ikke er godkendt af virksomheden, skal du anmode om godkendelse.

Du anmoder om godkendelse af et nyt system ved at sende følgende oplysninger til compliance-teamet:

* Hvilket system er der tale om?
* Hvem er leverandør af systemet?
* Har du afklaret det forretningsmæssige behov og samspil med andre systemer, samt budget i forbindelse med anvendelsen systemet med din leder?
* Hvordan skal systemet anvendes?
* Hvorfor er der behov for at anvende systemet?
* Hvilke personoplysninger behandles i systemet?
* Hvilke integrationer ønsker du at anvende til systemet?

Disse retningslinjer skal også følges, hvis du vil anvende en ny integration til et system, der allerede er godkendt.

Tildeling af brugerrettigheder

Du er kun blevet tildelt de brugerrettigheder, som du har behov for forbindelse med udførelsen af dit arbejde. Hvis du bliver opmærksom på, at du er blevet tildelt flere brugerrettigheder, end du har behov for, er du forpligtet til at informere din nærmeste leder herom, således at dine brugerrettigheder kan blive ændret.

Du må kun benytte dine tildelte brugerrettigheder, når du har et arbejdsmæssigt behov.

Brug af enheder

Du skal anvende den computer, du har fået udleveret af virksomheden til at udføre dit arbejde. Din arbejdscomputer er personlig, hvilket betyder, at den kun må anvendes af dig. Når du forlader din arbejdscomputer, skal den være låst. Passwordet til din arbejdscomputer må kun kendes af dig.

Følgende systemer må tilgås fra dine private enheder, fx din smartphone:

* [*Indsæt systemer*]
* [*indsæt systemer*]
* [*indsæt systemer*]
* [*indsæt systemer*] \*

Du skal vurdere, om du har et arbejdsmæssigt behov for at anvende ovenstående systemer på dine private enheder, inden du tager systemerne i brug på en privat enhed.

Når du anvender dine private enheder i arbejdsmæssig sammenhæng, skal du sikre, at den pågældende enhed er omfattet af de sikkerhedsforanstaltninger, der fremgår af disse retningslinjer.

* Ved anvendelsen af [*indsæt systemer*] på dine private enheder, skal du være ekstra opmærksom på, at du har implementeret passende sikkerhedsforanstaltninger; herunder at din enhed skal være låst med et password, der er mindst 6-cifre langt og passwordet må kun kendes af dig.

Såfremt du har behov for at anvende et system, der ikke fremgår af ovenstående liste på en privat enhed, skal du anmode om specifik godkendelse til anvendelsen af det pågældende system. Anmodningen skal fremsættes til compliance-teamet, således at det sikres, at virksomheden har et overblik over, hvilke enheder der anvendes til behandlingen af oplysninger.

Såfremt du anvender et system på en privat enhed, der ikke fremgår af ovenstående liste, skal du implementere følgende yderligere sikkerhedsforanstaltninger:

* Enheden skal være låst med et password, der er mindst 6-cifre langt. Passwordet må kun kendes af dig.
* Du skal modtage awareness-træning, der er specifikt målrettet brugen af private enheder i arbejdsmæssig sammenhæng.

Du må ikke tilgå systemer fra offentlige enheder.

De seneste opdateringer til systemer og enheder skal altid være installeret.

**2.2 Passwords**

Adgang til systemer og enheder mv. skal være begrænset af en adgangskontrol bestående af et unik ID med et personligt password. Følgende retningslinjer skal anvendes ved brugen af passwords:

1. [*indsæt system*] skal anvendes til alle passwords.
2. Midlertidige adgangskoder skal ændres straks.
3. Passwords er fortrolige og må ikke deles med andre.
4. Passwords må ikke kunne ses på skærmen i forbindelse med en login-session.
5. Passwords må ikke efterlades synlige og/eller kunne tilgås af andre.
6. Den systemansvarlige skal sikre, at systemet er underlagt adgangsbegrænsning i overensstemmelse med disse retningslinjer.
7. Der skal anvendes et unikt password for hvert system.
8. Ved mistanke om at et password er blevet kompromitteret, skal passwordet ændres straks og der skal ske underretning til [*indsæt organisationens navn*] compliance-team samt [*indsæt organisationens navn*] ledelse hurtigst muligt.

**2.3. Remote-arbejde**

Når du arbejder remote, er det vigtigt, at du sikrer, at der ikke er udefrakommende, der kan se din skærm eller høre dine opkald.

Du skal være tilsluttet en VPN, når du arbejder remote. Du må aldrig tilslutte din arbejdscomputer til offentlige netværk.

**Online** møder

Når du laver en skærmdeling i et online møde, skal du sikre, at det ikke er muligt at se oplysninger, der ikke er relevante for det pågældende møde. Du skal i den forbindelse huske at slå notifikationer mv. fra.

**2.4. Clean desk policy**

Fysisk

[*indsæt organisationens navn*] har clean desk policy (fysisk og digital). Det betyder, at når du forlader din arbejdsstation, skal denne, så vidt det er muligt, være ryddet for fortrolige oplysninger; herunder personoplysninger og kundedata mv.

Du må ikke have fysiske dokumenter liggende på dit bord, når du forlader kontoret. Når du forlader kontoret skal fysiske dokumenter være opbevaret i et aflåst skab. Du skal ligeledes sikre, at du ikke efterlader fysiske dokumenter andre steder fx i printeren.

Når du bortskaffer fysiske dokumenter, skal dette gøres op en måde, hvor du sikrer dig, at disse ikke kan tilgås af andre.

Digital

Dit arbejde skal som udgangspunkt gemmes i [*indsæt system*]. Hvis de dokumenter, du ønsker at gemme, ikke bør kunne tilgås af alle medarbejdere i virksomheden, skal du aftale med din nærmeste leder, hvordan du gemmerne dokumenterne. Det kan fx være i en mappe, hvor kun du og din afdelingsleder har adgang.

Du skal, så vidt det er muligt, holde dit digitale skrivebord (og lokale drev) ryddet for dokumenter.  Du bør tjekke ugentligt, at der ikke ligger dokumenter på dit lokale drev.

**3. Kommunikation og informationsdeling**

Alle oplysninger; herunder personoplysninger og kundedata mv. skal som udgangspunkt behandles fortroligt.

Tavshedspligt

Alle medarbejdere er omfattet af tavshedspligt vedrørende kundeoplysninger mv. under og efter ophør af ansættelsesforholdet. Brud på tavshedspligten betragtes som grov misligholdelse af ansættelsesforholdet og kan medføre øjeblikkelig bortvisning. Du pådrager dig endvidere erstatningsansvar efter dansk rets almindelige erstatningsregler over for eventuelle direkte eller indirekte tab, der påføres som følge af brud på tavshedspligten.

Det fremgår af din ansættelseskontrakt, at du er underlagt tavshedspligt både under ansættelsen og efter fratrædelse.

Videregivelse

*Ekstern videregivelse*

Du må som udgangspunkt ikke dele oplysninger med nogen uden for virksomheden, hvis dette ikke sker som et normalt led i dit arbejde.

*Intern deling*

Såfremt du har et arbejdsmæssigt behov for at dele oplysninger med en kollega, skal du kunne redegøre for, at du har et arbejdsmæssigt formål.

Kommunikationskanaler

Kommunikation med kunder må udelukkende ske gennem de kommunikationskanaler, der er godkendt af virksomheden. Du må ikke kommunikere med kunder gennem andre kanaler fx gennem sociale medier.

Du må som udgangspunkt ikke anvende dit private telefonnummer til at kommunikere med kunder. Hvis du mener, at du har et arbejdsmæssigt behov for at anvende dit private telefonnummer i arbejdsmæssig sammenhæng, skal du anmode om tilladelse til dette. Anmodningen skal fremsættes til compliance-teamet, således at det sikres, at virksomheden har et overblik over, hvilke kanaler der anvendes til kommunikation.

**4. Awareness**

Det er vigtigt, at du holder dig opdateret om virksomhedens retningslinjer for informationssikkerhed.  Virksomheden har en awareness-indsats, der har til formål løbende at skærpe din opmærksomhed på informationssikkerhedsmæssige problemstillinger.

Som medarbejder er du forpligtet til at følge virksomhedens awareness-træning. Hvis du ikke har mulighed for at deltage i en awareness-session, skal du læse de referater, der efterfølgende udsendes.

**5. Databeskyttelsesretlige hændelser**

Dette afsnit omhandler særlige situationer, som du skal være opmærksom på, fordi virksomheden har en forpligtelse til at reagere.

**5.1. Brud på persondatasikkerheden**

Et brud på persondatasikkerheden er defineret ved:

“*et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet”.*

Det kan fx være hvis du kommer til at sende en mail til en forkert person eller hvis du mister en enhed, der indeholder personoplysninger.

Hvis du bliver opmærksom på, at der er sket et brud på persondatasikkerheden skal du handle i overensstemmelse med [*indsæt organisationens navn*] *politik for håndtering af brud på persondatasikkerheden, afsnit 4.*

**5.2. Anmodninger vedrørende de registreredes rettigheder**

Hvis du bliver opmærksom på, at virksomheden har modtaget en anmodning, der omhandler de registreredes rettigheder, skal du handle i overensstemmelse med [*indsæt organisationens navn*] *politik for sikring af de registreredes rettigheder, afsnit 3.*

###

###

### **Dokumentinformation**

|  |  |
| --- | --- |
| Dokumentversion |  |
| Dato for udgivelse af denne version |  |
| Ansvarlig |  |
| Status |  |