Informationssikkerhedspolitik for VUC Lyngby

Version	Dato	Ændret af	Godkendt af
1.0	01.11.2020	KMA	

Indhold

Formål

Informationssikkerhedspolitikken indeholder de overordnede sikkerhedsmålsætninger og danner grundlag for udformning af virksomhedens informationssikkerhedshåndbog, der forstås som fællesbetegnelsen af informationssikkerhedspolitikken med de underliggende retningslinjer og forretningsgange.

Informationssikkerhedspolitikken er en vigtig del af virksomhedens sikkerhedsforanstaltninger og beskriver det ledelsesgodkendte niveau for sikkerhed. Dermed skal politikken ligeledes understøtte bevidstheden om informationssikkerhed i virksomhedens organisation og virke. De retningslinjer, der udformes for at understøtte informationssikkerhedspolitikkens hovedmålssætninger, skal sikre, at alle medarbejdere arbejder med og forholder sig til informationssikkerhed i det daglige arbejde.

Vi ser ikke kun et højt sikkerhedsniveau som et krav for at kunne overholde lov- og myndighedskrav, men også som et kvalitetselement for at kunne tilbyde en sikker service for vores samarbejdspartnere.

Omfang

Informationssikkerhedspolitikken dækker alle tekniske og organisatoriske forhold, der har direkte eller indirekte indflydelse på drift og brug af vores informationsaktiver.

Informationssikkerhedspolitikken er gældende for alle vores medarbejdere, dog vil den have den største betydning for de medarbejdere, som til dagligt bruger vores informationsaktiver i forbindelse med behandling og opbevaring af personoplysninger.

Alle leverandører og samarbejdspartnere, som har fysisk eller logisk adgang til vores systemer, data og informationer skal gøres bekendt med politikken og følge den.

Hovedmålsætninger og sikkerhedsniveau

Sikkerhedsmålsætning:
"Vi vil have et tilstrækkeligt informationssikkerhedsniveau for alle ansatte og samarbejdspartnere som gør brug af virksomhedens informationsaktiver. Dette gælder både fysiske dokumenter, arkiver, it-systemer, hardware samt elektroniske datamedier i virksomheden."

Et tilstrækkeligt informationssikkerhedsniveau opnås igennem implementerede sikkerhedsforanstaltninger, der sikrer:

1) Fortrolighed, integritet og tilgængelighed af systemer og data i forhold til den risikovurdering, der er fastsat for hver af de konkrete systemer og data.
2) Beskyttelse af informationsaktiver, medarbejdernes kompetencer, virksomhedens image og informationer/oplysninger i vores varetægt.

For at fastholde det tilstrækkelige sikkerhedsniveau skal følgende overholdes:

- Der skal forefindes retningslinjer og forretningsgange, som tilsikrer, at informationssikkerhed er en integreret del af vores drift og daglige arbejde.
- Vi skal igennem kontrakt- og leverandørstyring sikre, at brugen af eksterne konsulenter, samarbejdspartnere og leverandører ikke har en negativ effekt på informationssikkerheden.
- Vi skal følge op på informationssikkerheden ved løbende vedligehold og optimering af informationssikkerhedspolitikken og de dertilhørende retningslinjer og forretningsgange. Målet er at sikre en struktureret og kontinuerlig forbedringsproces.

Organisation og ansvar

Sikkerhedsmålsætning:
"Alle medarbejdere har ansvar for informationssikkerheden. De er bekendte med og efterlever vores informationssikkerhedspolitik og dens retningslinjer."

Planlægning, implementering og kontrol af informationssikkerhed er defineret af ledelsen.
Informationssikkerhedskoordinatoren er ansvarlig for implementering og vedligeholdelse af informationssikkerheden og er ansvarlig for opfølgning på sikkerhedshændelser.

Informationssikkerhedspolitikken revurderes og godkendes i forbindelse med eventuelle situationer, der tilsiger det. Ledelsen er ansvarlig for at arbejde med informationssikkerhed på et strategisk niveau, således

at informationssikkerhedsmæssige overvejelser inddrages i alle væsentlige beslutninger. Medarbejdere er ansvarlige for at efterleve retningslinjer og procedurer for sikkerhed i det daglige arbejde.

Den nødvendige viden om og kompetence indenfor informationssikkerhed formidles til alle medarbejdere, og der bliver løbende arbejdet med holdninger og viden om informationssikkerhed. Ledelsen er ansvarlig for, at Informationssikkerhedspolitikken overholdes.

Overtrædelse af Informationssikkerhedspolitikken

Alle medarbejdere er forpligtet til at efterleve den til enhver tid gældende Informationssikkerhedspolitik med tilhørende retningslinjer og forretningsgange. En overtrædelse kan, efter omstændighederne, medfører sanktioner.
Hvis en medarbejder er vidende om, at Informationssikkerhedspolitikken overtrædes, skal det meddeles til ledelsen hurtigst muligt.

Hvis der opstår situationer, hvor kravene i Informationssikkerhedspolitikken ikke kan efterleves, skal der skriftligt anmodes om dispensation af ledelsen. Eventuelle afvigelser fra kravene skal dokumenteres, og der skal indføres alternative sikringsforanstaltninger.

1. Informationssikkerhedsstrategi

VUC Lyngby har formuleret og vedtaget denne politik vedr. informationssikkerhed, som formidles til alle medarbejdere og relevante eksterne parter.
Informationssikkerhedspolitikken gennemgås en gang årligt, samt opdateres efter evalueringsrunden. Alle medarbejdere og relevante eksterne parter bliver orienteret om alle relevante ændringer.

2. Risikovurdering og -håndtering

Der foretages årligt en risikovurdering på virksomhedens informationsaktiver med hensyntagen til trusler, sårbarheder, sandsynlighed og konsekvens.

Baseret på risikovurderingen implementeres der tiltag til at reducere højrisikoområder og diverse beredskabsplaner, backupstrategier og sikkerhedsforanstaltninger justeres iht. risikovurderingen.

3. Organisering af informationssikkerhed

3.1. Interne organisatoriske forhold

3.1.1. Funktionsadskillelse

Det er så vidt muligt sikret, at ingen enkeltperson kan få adgang til, ændre på eller bruge aktiver uden autorisation eller uden at det opdages.

3.1.2. Kontakt med myndigheder

I tilfælde af at der er behov for at kontakte myndigheder i forbindelse med brud på sikkerheden er rektor Inge Voller eller GDPR-ansvarlig ansvarlig herfor.

4. Medarbejdersikkerhed

4.1. Før ansættelsen

Alle medarbejdere underskriver en fortrolighedserklæring/tavshedserklæring.

4.2. Under ansættelsen

Ledelsen kræver, at alle medarbejdere fastholder informationssikkerhed

Medarbejderne bliver løbende holdt ajour med Informationssikkerhedspolitikken og procedurer i det omfang, det er relevant for deres jobfunktion.

Der er en fastsat procedure der sikrer at brugerrettigheder justeres ved ændringer i ansættelsesforholdet.

4.3. Ansættelsens ophør

Brugeres rettigheder i it-systemer og andre informationsaktiver lukkes ved ansættelsesophør.

5. Leverandørforhold og styring af informationsaktiver

5.1. Informationssikkerhed i leverandørforhold

Der er indgået aftaler om informationssikkerhedskrav med relevante leverandører gennem de respektive aftaler eks. Databehandleraftaler.

Der er udarbejdet detaljerede leverandøraftaler for at undgå misforståelser mellem organisationen og leverandøren.

Hvis det vurderes at være nødvendigt, indgås der fortroligheds- og hemmeligholdelsesaftaler med relevante eksterne parter.

5.2. Anskaffelse og udvikling af informationsaktiver

Krav til informationssikkerhed er omfattet af kravene, som stilles til nye informationssystemer eller forbedringer af eksisterende informationssystemer.

5.3. Portable Devices/mobile enheder

For denne politik er Portable Devices defineret som enhver enhed med adgang til firmaets netværk, data og/eller informationsaktiver og som er mobil/flytbar i sit design, dvs. den omfatter bl.a. laptops, tablets og smartphones. Flytbare medier inkluderer, men er ikke nødvendigvis begrænset til USB-nøgler, eksterne harddiske og andre datalagringsenheder. Det anbefales at anvendelse af flytbare medier som USB-nøgler begrænses så meget som muligt.

5.3.1. Tekniske krav

Alle mobile enheder skal leve op til følgende:

- Alle enheder skal efterleve virksomhedens generelle krav til IT-sikkerhed.
- Alle enheder skal være beskyttet af passwords, der efterlever virksomhedens generelle krav til passwordsikkerhed. Disse må ikke være identiske med passwords brugt andre steder.
- Til alle funktioner, hvor virksomheden anvender kryptering, skal dette også anvendes på mobile enheder.
- Kun enheder, der administreres af virksomhedens IT-afdeling, må forbindes til virksomhedens interne netværk.

5.3.2. Brugskrav

Al brug af mobile enheder skal efterleve følgende krav:

- Brugerne må kun behandle data på mobile enheder i den udstrækning det er nødvendigt for udførelsen af deres arbejde.
- Brugerne skal uden unødigt ophold melde alle tabte eller stjålne enheder til den Lokal IT-support ITCN og/eller GDPR-ansvarlig, når de bliver bekendt med tabet/tyveriet.
- Hvis en medarbejder mistænker, at der er sket uretmæssig adgang til virksomhedens data/systemer via en mobil enhed, skal dette uden unødigt ophold rapporteres til Lokal IT-support ITCN og/eller GDPR-ansvarlig.
- Mobile enheder må ikke være ”jailbroken” eller ”rooted” eller have software/firmware installeret, som kan give adgang til funktionalitet, der ikke er tiltænkt at være tilgængelig for brugeren.
- Brugeren må ikke synkronisere noget af enhedens indhold til egne cloud-services.
- Brugere må ikke have piratversioner af software eller andet ulovligt materiale på enhederne.
- Applikationer må kun installeres fra officielle kilder, som er godkendt af platform-ejeren, f.eks. Appstore eller Google Play Butik. Kode eller applikationer fra ukendt eller usikker kilde må ikke installeres uden forudgående godkendelse fra Lokal IT-support ITCN.
- Enheder skal holdes ajourført med opdateringer fra producenten.
- Enhederne må ikke tilsluttes en pc, som ikke har opdateret malware-beskyttelse eller efterlever virksomhedens sikkerhedspolitik.
- Enhederne skal være krypteret i henhold til virksomhedens standarder.
- Brugerne skal være varsomme med at kombinere personlig og arbejdsrelateret e-mail på deres enheder. De skal især være opmærksomme på, at virksomhedens data kun sendes via virksomhedens mailsystem. Hvis en bruger mistænker at virksomhedens data er blevet sendt fra en personlig e-mailkonto, enten som brødtekst eller som vedhæftet fil, skal de gøre Lokal IT-support ITCN og/eller GDPR-ansvarlig opmærksom på dette uden unødigt ophold.

5.3.3. Sikkerhedsprocedure for Portable Devices

Hvis det konstateres, at en enhed eller en bruger ikke efterlever kravene, kan det resultere i, at brugeren bliver frataget adgangsrettigheder til virksomhedens e-mail/systemer/applikationer fra den pågældende mobile enhed eller at enheden låses, indtil yderligere undersøgelser kan foretages.

Hvis undersøgelserne viser, at regelbruddet også har medført et databrud, håndteres dette efter proceduren i pkt. 10.

Hvis undersøgelser ydermere viser, at regelbruddet har medført en vedvarende kompromittering af enhedens sikkerhed, kan Lokal IT-support ITCN og GDPR-ansvarlig beslutte at hele enhedens hukommelse slettes ("device wipe").

Hvis brugeren har egne private data liggende på enheden, er det brugerens eget ansvar at have sikret en backup af disse. Virksomheden påtager sig intet ansvar for et eventuelt tab af brugerens private data som følge af et "device wipe" i forbindelse med et brud på ovenstående regler.

5.4. Bortskaffelse af informationsaktiver

Når der ikke længere er behov for et medie/en mobil enhed, skal det bortskaffes på forsvarligvis.

Alle medarbejdere og eksterne brugere skal aflevere alle virksomhedens aktiver i deres besiddelse tilbage, når deres ansættelse, kontrakt eller aftale ophører.

6. Adgangsstyring

6.1. De forretningsmæssige krav til adgangsstyring

Medarbejdere og eksterne partnere får kun adgang til informationer i et omfang som er proportionelt med deres stilling og beføjelser dvs. at der kun bliver tildelt de adgange til information, som pågældende har behov for, for at kunne udføre sine arbejdsopgaver.

Netværket kan tilgås via WiFi og beskyttes af password.

6.2. Administration af brugeradgang

6.2.1. Tildeling af brugeradgang og afmelding

Alle brugere har deres eget unikke bruger-ID. Fællesbrugere anvendes kun, hvis det er nødvendigt af forretnings- eller driftsmæssige årsager.

Privilegerede adgangsrettigheder til informationsaktiver, operativsystemer, databaser og applikationer er begrænset til de brugere, som har et arbejdsrelateret behov herfor.

Nedlagte bruger-ID bliver regelmæssigt slettet og en gang årligt gennemføres et ekstra tjek af at nedlagte brugere er slettet.

6.2.2. Styring af brugeres adgangskoder

Brugeres identitet bliver verificeret før der tildeles nye, ændrede eller midlertidige adgangskoder. Forudbestemte adgangskoder fra leverandører ændres efter installation af systemer eller software. Brugeren skal ændre deres adgangskode første gang de logger ind.

6.3. Brugernes ansvar

Brugere må ikke udlevere deres ID eller password til andre. Brugere må ikke registrere deres ID eller password på papir, i software-filer eller på mobile enheder, medmindre der er tale om en sikker password vault. Brugere skal ændre deres password ved mistanke om kompromittering.

6.4. Styring af system- og applikationsadgang

6.4.1. Begrænset adgang til informationer

Virksomhedens tilstræber at indrette systemer og applikationer således, at det er muligt at give forskellige brugere/brugergrupper adgang til forskellige funktioner, forskellige data samt forskellige rettigheder, f.eks. læse, skrive-, slette- og execute-rettigheder alt efter behov, for på den måde at minimere unødige adgange.

6.4.2. Procedure for sikker log-on

Bruger-ID/brugerkonti bliver låst efter 5 fejlslagne log-on-forsøg for at beskytte mod brute force-angreb.

Fejlslagne og gennemførte log-on-forsøg bliver logget.

Brugeren skal ændre deres adgangskode første gang de logger ind.

Passwordet som indtastes vises som * og ikke i klar tekst og transmitteres ikke som klar tekst for at undgå, at de opsnappes af sniffer-programmer.

Inaktive sessioner afsluttes efter 3 minutter med inaktivitet.

6.4.3 System for administration af adgangskoder
Systemet for administration af adgangskoder sikrer

- brugen af unikke bruger-ID'er og adgangskoder
- at adgangskoderne af høj kvalitet
- at brugeren skifter adgangskode ved første log-on
- at tidligere anvendte adgangskoder ikke kan genbruges
- at adgangskoder ikke vises på skærmen under indtastning
- at adgangskoder transmitteres i krypteret form

7. Fysisk sikring og miljøsikring
Alle yderdøre er sikret med alarmer og låst uden for åbningstid. Alle vinduer er lukkede når de ikke er under opsyn.

Det er installeret branddøre og indbrudsalarmer.

Der udføres eftersyn på udstyr efter leverandørens anbefalinger. Det er kun godkendte personer, som udfører reparationer og vedligeholdelse på udstyr.

Brugere skal holde deres skriveborde og arbejdsstationer ryddet for papir og flytbare lagringsmedier, når arbejdsstationen forlades.

Papir og elektroniske lagringsmedier skal låses inde, når de ikke benyttes.

Computere og terminaler skal være logget af eller beskyttet med skærmlås.

Dokumenter, som indeholder følsom eller klassificeret information, skal straks fjernes fra printere.

7.1. Videoovervågning:
Som led i sikkerhedsforanstaltningerne omkring VUC Lyngbys fysiske rammer, er der videoovervågning på området. VUC Lyngby vil til enhver tid sikre, at al brug af videoovervågning, vil ske i overensstemmelse med tv-overvågningsloven.

Virksomheden sikrer, at kun medarbejdere med arbejds-/sikkerhedsbetinget behov kan få adgang til tv-overvågningssystemet og lokalet, hvor optagelserne fra tv-overvågningen kan tilgås.

Medarbejdere som giver uvedkommende adgang til lokalet eller systemet vil få en advarsel baseret på en individuel vurdering.

Alle optagelser gemmes i maks 30 dage, hvorefter de slettes.

8. Driftssikkerhed
8.1. Malwarebeskyttelse
Brugerne er oplyst om, at de ikke må installere uautoriseret software, dvs. programmer der ikke er godkendt af operativsystemets udbyder, på virksomhedens computere. Hvis anvendelsen af uautoriseret software er nødvendig for virksomhedens drift, skal det undersøges og godkendes af virksomhedens IT-ansvarlige før installation må finde sted.

Der er installeret malwaresporings- og reparationssoftware til at scanne computere. Antimalware-systemer opdateres løbende.

8.2. Backup
Der tages løbende backup af organisationens informationsaktiver, og disse testes regelmæssigt.

Der tages daglig backup af ændringer fra dagen før og en gang om ugen tages fuld backup og inkrementel backup hvert 10 minut.

Backupkopierne opbevares adskilt fra organisationens hovedkontor ekstern hos ITCN.

9. Kommunikationssikkerhed

9.1. Styring af netværkssikkerhed

Gæstenetværk er separeret fra organisationens interne netværk.

Adgangen mellem netværksdomæner er styret ved hjælp af en firewall gateway.

Trådløse netværk er adskilt fra organisationens interne netværk.

9.2. Informationsoverførsel

Følsomme og fortrolige oplysninger skal overføres krypteret via mail eller sikker post.

Det er ikke tilladt at efterlade telefonsvarerbeskeder med følsomme og fortrolige oplysninger.

Det er ikke tilladt at have fortrolige samtaler på offentlige steder eller over usikre kommunikationskanaler i åbne kontorer eller mødesteder.

Brugerne skal være meget opmærksomme på at elektroniske meddelelser adresseres korrekt.

10. Styring af informationssikkerhedsbrud

10.1. Ansvar og procedure

Procedurer er fastlagt, så det er kompetente medarbejdere, som håndterer brud. Der er etableret et fast kontaktpunkt for opdagelse og rapportering af brud.

Der er udarbejdet rapporteringsskemaer ved informationssikkerhedshændelser til at understøtte rapportering.

10.2. Rapportering af informationssikkerhedshændelser

Alle brugere har ansvar for hurtigst muligt at rapportere informationssikkerhedshændelser til den GDPR-ansvarlige.

Situationer, der skal rapporteres, er ved mistanke om:

- Fysiske papirer med personfølsomme oplysninger som ligger fremme efter endt arbejdsdag.
- Sende mail med personfølsomme oplysninger til en forkert person
- Forlagt en print med personfølsomme oplysninger i fx printerrum eller personalekøkken
- Stjålne enheder
- Menneskelige fejl
- Ukontrollerede systemændringer
- Overtrædelse af politikker eller retningslinjer
- Fejl i software eller hardware
- Brud på adgangskontrollerne.

10.3. Rapportering af informationssikkerhedssvagheder

Alle brugere har pligt til at rapportere observererede svagheder i informationssystemer og tjenester til den GDPR-ansvarlige. Det er ikke tilladt for almindelige brugere at forsøge at be- eller afkræfte en eventuel svaghed, da dette kan opfattes som et forsøg på at lave et sikkerhedsbrud.

10.4. Håndtering af informationssikkerhedsbrud

Ved brud bliver der:

- indsamlet beviser hurtigst muligt efter hændelsen
- hvis relevant, udarbejdet en analyse af informationssikkerheden
- foretaget fejlafhjælpning efter behov
- foretaget logning af alle involverede beredskabsaktiviteter for senere analyse
- kommunikeret om bruddet til andre interne og eksterne parter, der har behov for denne viden

- foretaget håndtering af den eller de informationssikkerhedssvagheder, som har forårsaget eller været medvirkende til bruddet
- foretaget formel lukning og registrering af bruddet efter en vellykket håndtering
- fortages en evaluering på baggrund af bruddets karakter om hændelsen skal anmeldes til Datatilsynet og/eller skal informere de registrerede, som er påvirket af bruddet.

Efter brud bliver der foretaget en analyse af identificerede kilder til bruddet. Den viden, der opnås ved at analysere og håndtere informationssikkerhedsbrud, bliver anvendt til at nedsætte sandsynligheden for eller virkningen af fremtidige brud.

11. Overensstemmelse

Virksomheden er opmærksom på, at vi er underlagt diverse lovgivning og kontraktkrav, herunder GDPR.