Dubex A/S

Overordnet ISMS- og informationssikkerhedspolitik

Version 3.4

Klassifikation: Offentlig

Dubex A/S, den 25. april 2023

Overordnet ISMS- og informationssikkerhedspolitik for Dubex A/S

Versionshistorik

Version	Dato	Status	Rettelse
1.0	25-mar-2008	Final	TBR/LAB oprettet
2.0	25-maj-2010	Final	Opdateret med ISO 27001 politik.
3.0	7-april-2014	Final	Opdateret med ISO 27001:2013 politik
3.1	30-maj-2016	Final	Reviewet og godkendt af nuværende bestyrelse
3.2	26-marts-2020	Final	Reviewet og godkendt af bestyrelsen. Dato opdateret
	23-april-2020	Final	Dato opdateret ifm. opdateret dato på SoA
3.3	29-april-2021	Final	Reviewet og godkendt af bestyrelsen.
3.4	18-maj-2022	Final	Reviewet og godkendt af bestyrelsen.
3.5	24-april-2023	Final	Reviewet og godkendt af bestyrelsen.

Dokumentinformation

Dokument nummer:	
Dokument version:	3.5
Status:	Final
Ansvarlig forfatter:	Sofie Freja Christensen
Klassifikation	Offentlig
Sidste opdatering:	25. april 2023

Indholdsfortegnelse

1 Politik

Dette er Dubex' overordnede politik for dets ledelsessystem for informationssikkerhed (ISMS), omfattende en beskrivelse af den overordnede informationssikkerhedspolitik og det valgte anvendelsesområde.

1.1 Indledning

Dubex' ISMS skaber rammerne for en operationel informationssikkerhedspolitik, der udmøntes i etableringen af fastsatte procedurer og instruktioner for Dubex' informationssikkerhedshåndtering. Dermed etableres et grundlag for det daglige arbejde med informationssikkerhed inden for Dubex' virke. Ansvarsplacering, retningslinjer, procedurer, risikovurdering og beredskabsplaner er således emner, der reguleres under dette ledelsessystem.

Dubex' ISMS-system er baseret på:

- Efterlevelse af den internationale standard ISO/IEC 27001 og de udvalgte styringsmål og foranstaltninger fra ISO/IEC 27002 standarden.

- Alle relevante regler, lovkrav, retningslinjer, vejledninger og kontrakter inden for Dubex' forretningsområde, persondatalovgivningen, markedsføringsloven, statens krav og arbejdsmarkedsaftaler.

- Almindeligt accepterede metoder og procedurer for informationssikkerhed.

1.2 Anvendelsesområde (Scope)

Informationssikkerhed i forbindelse med udvikling, levering og servicering af løsninger og ydelser inden for it-sikkerhed i henhold til Redegørelse for Anvendelighed, dateret den 25. april 2023.

1.3 Mål

Dubex' gennemfører alle nødvendige aktiviteter for at sikre:

- **Tilgængelighed:** At Dubex' forretningssystemer normalt er tilgængelige 24/7, og at der vedligeholdes et beredskabsniveau som sikrer, at normal drift af de kritiske forretningssystemer kan reetableres indenfor 2 timer inden for normal arbejdstid, og indenfor 4 timer uden for normal arbejdstid.

- **Integritet:** At opnå en pålidelig og korrekt funktion af informationssystemerne med minimeret risiko for ukorrekt datagrundlag, f.eks. som følge af menneskelige og systemmæssige fejl eller udefrakommende hændelser, som fx udtrykt i de årlige rapporteringer, målinger og review af kritiske sikkerhedshændelser.

- **Fortrolighed:** At Dubex' data, og kundernes data i Dubex' varetægt ved brug af klassifikation, kryptering og adgangskontrol, kun er tilgængelige for de personer og på den måde, som klassifikationen tilskriver, som fx udtrykt i de årlige målinger og review af klassifikationsgraden.

Det er Dubex' mål at opretholde et informationssikkerhedsniveau, der fører til certificering efter standarden ISO/IEC 27001:2022, samt udarbejdelse af ISAE3000-erklæring.

Sikkerhedsniveauet fastlægges i det enkelte tilfælde under hensyntagen til arbejdets gennemførelse og økonomiske ressourcer. Målsætningen om et højt sikkerhedsniveau afvejes med ønsket om en hensigtsmæssig og brugervenlig anvendelse af IT, herunder det forhold, at de ansatte sikkerhedskonsulenter har andre behov i deres daglige arbejde, end de mere administrative eller salgsorienterede medarbejdere. Dubex risikohåndteringsplan opdateres og reviewes af ledelsen årligt, samt ved større ændringer.

Dubex gennemfører de aktiviteter der er nødvendige for at holde medarbejdere, orienterede om ISMS'et, dets politik, procedurer og instruktioner, samt medarbejdernes ansvar over for virksomhedens informationer og systemer. Dette indbefatter introduktionsforløb for nye medarbejdere, årlige awareness-tests mv.

1.4 Vores holdninger og principper

Informationssikkerhed i Dubex implementeres efter følgende overordnede holdninger:

- Dubex' virke afhænger af håndteringen af ofte følsomme informationer i elektronisk form. Af denne grund behandles informationssikkerhed som sidestillet med forretningssikkerhed.
- Dubex arbejder med informationssikkerhed som en integreret del af forretningen, hvilket har betydning for Dubex' troværdighed over for samarbejdspartnere og kunder.
- Som forhandler af nye løsninger er Dubex indstillet på forsøgsvis at anvende nyeste teknologier, på en styret og struktureret måde, hvor en sikker implementering har højeste prioritet.
- Som en sikkerhedsvirksomhed vedligeholder, understøtter og fastholder Dubex et højt vidensniveau hos alle medarbejdere, som en del af forretningssikkerheden.
- Dubex er en sikkerhedsvirksomhed med en lav risikovillighed, hvilket lægges til grund for hvilke risici der kan accepteres, og hvilke der skal nedbringes eller overføres.
- Såfremt eksterne parter berøres af sikkerhedshændelser hos Dubex, vil Dubex kommunikere ærligt og troværdigt over for berørte parter.

1.5 Ansvar

Ansvaret for den daglige styring af Dubex' informationssikkerhed er placeret hos sikkerhedschef Jacob Herbst.

Hvis en medarbejder opdager trusler mod eller brud på informationssikkerheden, eller får mistanke om det, skal vedkommende straks underrette rette sikkerhedschefen om det. I sidste ende er det den ansvarlige for den daglige styring af informationssikkerheden.

Medarbejdere der bryder Dubex' informationssikkerhedspolitik, eller de heraf fastsatte procedurer og instruktioner, vil blive mødt med de forholdsregler, som Dubex' procedurer og personalepolitik foreskriver.

1.6 Opfølgning

Dubex måler, vurderer og følger op på informationssikkerhedsområdet på følgende måde:

- Løbende entydig registrering og opfølgning på hændelser inden for informationssikkerhedsområdet.
- Løbende registrering af alle tiltag inden for informationssikkerhedsområdet
.
- Opfølgning på vidensniveau inden for informationssikkerhedsområdet i Dubex.
- Risikovurderinger, der gennemføres ved større ændringer, og mindst én gang om året.
- Gennemførelse af uafhængige tredjepartsrevisioner og evalueringer af informationssikkerheden.

På baggrund af dette reviewer og revurderer ledelsen ISMS- og informationssikkerhedspolitikken én gang om året, samt ved større ændringer.

1.7 Godkendelse

Denne politik er vedtaget af Dubex' bestyrelse april 2023

_____	_____	_____
Jørgen Bardenfleth	Jacob Herbst	Gorm Mandsberg

_____
Klaus Kongsted

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registereret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Gorm Mandsberg
Underskriver
Serienummer: e2911059-167b-4527-9bac-4c71e063bf86
IP: 212.237.xxx.xxx
2023-04-25 12:38:22 UTC
MitID

Jacob Herbst
Underskriver
Serienummer: 4ee4ddb4-1d6e-4fe8-b54a-8c82c3370402
IP: 148.64.xxx.xxx
2023-04-25 12:51:42 UTC
MitID

Navnet er skjult
Underskriver
Serienummer: 846550b8-62cb-48d1-be08-171907c49b97
IP: 135.180.xxx.xxx
2023-04-26 03:30:20 UTC
MitID

Jørgen Vilhelm Løvenørn Bardenfleth
Underskriver
Serienummer: PID:9208-2002-2-816014968039
IP: 188.183.xxx.xxx
2023-04-27 20:06:03 UTC
NEM ID