POLITIK FOR INFORMATIONS-SIKKERHED OG DATABESKYTTELSE

Information er et af Bravidas vigtigste aktiver, og informations-håndtering udgør en væsentlig del af arbejdet. Vi håndterer hver dag følsomme oplysninger om vores egne aktiviteter, om vores kunder og om andre interessenter. Adgang til pålidelig information er en forudsætning for, at Bravida fortsat kan have succes og effektivt udvikle sig og levere vores kundetilbud på en bæredygtig og innovativ måde.

Formål:

Det overordnede formål med Bravidas arbejde med informationssikker-hed og databeskyttelse er at sikre afbalanceret beskyttelse af Bravidas informationsaktiver. De rigtige informationer skal være tilgængelige for den rigtige person på det rigtige tidspunkt. De personoplysninger, Bravida håndterer, behandles i overensstemmelse med gældende databeskyttelseslovgivning.

Det systematiske arbejde med informationssikkerhed og databeskyt-telse sikrer en robust, sikker og pålidelig informationsforsyning via tilstrækkelig beskyttelse og minimering af risici. Formålet med arbejdet er også at forebygge hændelser, der negativt påvirker mulighederne for at drive en hensigtsmæssig virksomhed.

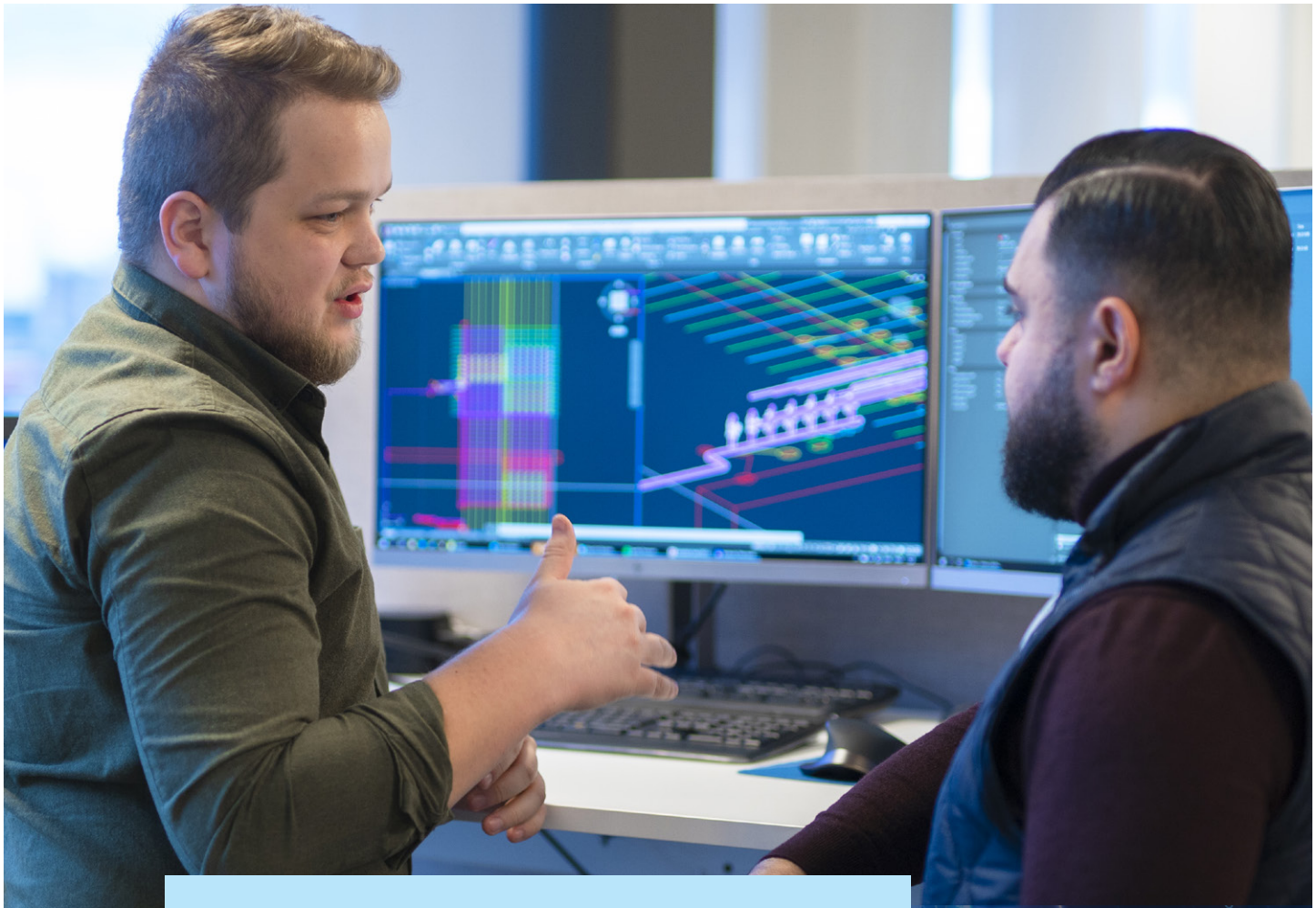
Omfang:

Politikken gælder hele Bravida-koncernen og al information uden undtagelse, uanset om den behandles manuelt eller automatisk, og uanset dens form og det miljø, den forekommer i. Al beskyttelsesværdig information skal klassificeres efter følsomhedsgrad.

Politikken henvender sig til alle, der håndterer Bravidas informationer, og den beskriver ledelsens syn på og Bravidas vejledende principper for informationssikkerhedsarbejdet og for databeskyttelse.

Beskyttelsen af informationsaktiver skal være udformet, så den opfylder organisationens sikkerhedskrav. Det gælder også, når Bravidas informationer eller informationssystemer håndteres af en ekstern part, og når Bravida håndterer andres information.

bravida



Principper

Bravida overholder myndighedskrav og god praksis inden for informationssikkerhed og databeskyttelse.

Informationssikkerhed

Bravidas arbejde med informationssikkerhed og databeskyttelse skal være systematisk, langsigtet og baseret på et helhedssyn, der tager udgangspunkt i information, men også omfatter processer, mennesker og teknologi. Arbejdet er baseret på den etablerede standardserie SS-ISO/IEC 27000 og tager udgangspunkt i regelmæssige risikoanalyser, der har til formål at afbalancere det rigtige beskyttelsesniveau i alle dele af virksomheden.

Informationssikkerhedsarbejdet skal sikre:

FORTROLIGHED

Informationen stilles ikke til rådighed for og videregives ikke til uautoriserede personer, enheder eller processer, og videregives heller ikke på anden måde bevidst eller ubevidst til andre end autoriserede personer.

INTEGRITET

Informationen kan ikke ændres af uautoriserede personer ved en fejl eller på grund af uregelmæssigheder i IT-systemer eller drift. Informationen skal være pålidelig, nøjagtig og fuldstændig.

TILGÆNGELIGHED

Informationen skal være tilgængelig, når der er brug for det, i det forventede omfang, på det rigtige tidspunkt og på det rigtige sted.

bravida

Databeskyttelse

Ansvarligt og systematisk databeskyttelsesarbejde. Bravida påtager sig det fulde ansvar for vores behandling af personoplysninger og arbejder systematisk og struktureret på at sikre overholdelse af regler og etablerede principper.

LOVLIGHED

Al vores behandling af personoplysninger sker i overensstemmelse med gældende love og regler og er præget af Bravidas værdier og disse vejledende principper.

RIGTIGHED

Alle de personoplysninger, Bravida indsamler og behandler, skal være korrekte og om nødvendigt ajourførte.

GENNEMSIGTIGHED

Bravida skal altid handle åbent og gennemsigtigt og give klare og tilgængelige oplysninger om, hvordan vi behandler persondata, og hvilke rettigheder den enkelte har.

FORMÅLSBEGRÆNSNING

Al vores behandling af personoplysninger sker med et udtrykkeligt og legitimt formål, og vi er bevidste om, at det fastsatte formål udgør rammerne for vores behandling af personoplysninger.

DATAMINIMERING

Vi behandler kun den mængde personoplysninger, der er tilstrækkelig, relevant og nødvendig for at opfylde formålet.

OPBEVARINGSBEGRÆNSNING

Vi opbevarer ikke personoplysninger længere, end det er nødvendigt for at opfylde det angivne formål.

SIKKERHEDSBEVIDSTHED OG DATABESKYTTELSE GENNEM DESIGN

Vi beskytter de personoplysninger, vi behandler, og træffer passende sikkerhedsforanstaltninger, både tekniske og organisatoriske, for at beskytte personoplysningerne.

For hvert af områderne informationssikkerhed og databeskyttelse skal der gennemføres og dokumenteres organisatoriske, administrative og tekniske sikkerhedsforanstaltninger på en sådan måde, at det kan kontrolleres, at der er opnået et tilstrækkeligt beskyttelsesniveau. Afvigelser skal opdages, håndteres og danne grundlag for forbedringer.

Ansvar

Bestyrelsen træffer beslutninger om politikken, den administrerende direktør har det endelige ansvar, og ansvaret for at drive området fremad er uddelegeret til CISO. Det operationelle ansvar for informationssikkerhed følger på alle niveauer det normale uddelegerede forretningsansvar, og lederne har ansvaret for at implementere indholdet af denne politik i deres egne virksomheder.

Bravidas administrerende direktør har det endelige ansvar for informationssikkerheden og for overordnede sikkerhedsforhold af styrende karakter. Ansvaret omfatter sikring af, at der er økonomiske og menneskelige ressourcer med de rigtige kompetencer til informationssikkerhedsarbejdet.

ALLE, DER HÅNDTERER BRAVIDAS INFORMATION

- Alle, der håndterer Bravidas information, skal vide, hvad deres eget ansvar omfatter, og have et godt kendskab til de sikkerhedsregler, der gælder.
- Personer, der håndterer Bravidas information, skal regelmæssigt gennemføre den nødvendige uddannelse for at kunne opretholde informationssikkerhed og databeskyttelse.

SERVICE MANAGER OG INFORMATIONSEJER

- Alle IT-tjenester og det udstyr, tjenesterne benytter, håndteres inden for rammerne af Bravidas styringsmodel. Ansvaret under styringsmodellen indbefatter, at sikkerhedskravene til IT-tjenesterne opfyldes.
- Al beskyttelsesværdig information skal have en ejer. Informationsejeren har ansvaret for at klassificere informationen og fastsætte de sikkerhedskrav, der er nødvendige for at opnå tilstrækkelig beskyttelse af informationen.
- Service Manager og informationsejeren skal på baggrund af regelmæssige risiko- og sårbarhedsanalyser og indtrufne hændelser træffe de nødvendige foranstaltninger for at sikre, at Bravidas informationsaktiver er passende beskyttet.

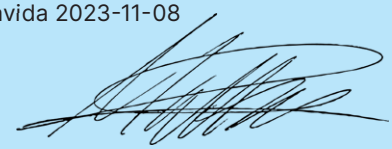
Gennemgang og opfølgning

Overholdelse af politikken for informationssikkerhed og databeskyttelse med tilhørende retningslinjer samt de implementerede sikkerhedsforanstaltninger skal regelmæssigt overvåges. Resultaterne af sikkerhedsarbejdet rapporteres årligt i forbindelse med ledelsens gennemgang.

Politikken for informationssikkerhed og databeskyttelse med tilhørende regler skal gennemgås og opdateres årligt, eller hvis der sker væsentlige ændringer i organisationen eller omverdenen, for at sikre, at politikken fortsat er hensigtsmæssig, korrekt og effektiv.

Gennemgangen skal omfatte en vurdering af Bravidas muligheder for at forbedre vores regler og organisationens tilgang til informationssikkerhed og databeskyttelse på grundlag af ændringer i Bravidas omverden, virksomhedens forudsætninger, lovkrav og det tekniske miljø.

Bravida 2023-11-08



Mattias Johansson, administrerende direktør og koncernchef

Alle politikker gennemgås hvert år.

bravida