Sikkerhedspolitik

Informationssikkerhedspolitik for DIFO og Punktum dk

Gruppe	Sikkerhedspolitik
Godkender	Jakob Bring Truelsen
Ansvarlig	Erwin Lansing
Version / ID	21.1.0 / 00002
Ændret af	Julius Lehn Weile
Ændret	15.08.2023
Review dato	26.06.2024
Dokument	Endelig
Sikkerhedsklassifikation	Offentlige informationer
Informationstype	Information – hvis intet indhold

Informationssikkerhedspolitik for DIFO og Punktum dk

Om politikken

Denne politik gælder for både DIFO og Punktum dk.

Da Punktum dk er det operationelle selskab angives Punktum dk i det efterfølgende som den centrale enhed, uagtet at politikken gælder både for DIFO og Punktum dk.

Politikken er løbende blevet udbygget og revideret. Senest i juni måned 2023.

Informationssikkerhedspolitik for Punktum dk

Punktum dk ønsker med denne informationssikkerhedspolitik, der er den overordnede ramme for informationssikkerheden i Punktum dk at tilkendegive, at vi prioriterer informationssikkerhed højt.

Informationssikkerhedspolitikken skaber sammen med en løbende risikovurdering grundlaget for, at der træffes foranstaltninger, der effektivt og tilpasset vores forhold tilgodeser, at kritiske og følsomme informationer og informationssystemer bevarer deres fortrolighed, integritet og tilgængelighed.

- *Fortrolighed*, der skal sikre, at informationer beskyttes mod afsløring og uautoriseret anvendelse samt eventuelle øvrige krav, der stilles af myndigheder, kunder, DIFO og Punktum dks ledelse.
- *Integritet*, der skal sikre, at informationer er fuldstændige, nøjagtige og reproducerbare, og at anvendte IT-programmer fungerer korrekt.
- *Autenticitet*, der skal sikre, at informationer er ægte og at der kan være tillid til gyldigheden af en transmission, en meddelelse eller afsender.
- *Tilgængelighed*, der skal sikre, at informationer med tilhørende programmer og faciliteter er tilgængelige på de aftalte tidspunkter.

Informationssikkerhedspolitikken skal understøtte omgivelsernes forventninger og opfattelse af DIFO og Punktum dk som en troværdig og respekteret virksomhed og administrator af domænenavne og medvirke til, at der skabes en sikkerhedskultur.

Målsætning

Punktum dk ønsker at opretholde og løbende udbygge et informationssikkerhedsniveau, der opfylder kravene i ISO 27001, Ledelsessystemer for Informationssikkerhed (ISMS). Kravene skærpes på veldefinerede områder, hvor der er specielle lovkrav, aftaleretslige forhold eller særlige risici afdækket ved den årlige risikovurdering.

Punktum dk er omfattet af NIS og vil også blive det af NIS2, fordi vi er en del af kritisk dansk infrastruktur. NIS har kunne håndteres inden for rammerne af ISO 27001. NIS 2 forventes at give anledning til justeringer.

Punktum dk bruger hændelsesrapportering og håndtering til at forbedre processor. Dertil vil NIS2 styrke og strømline hændelsesforløbet.

Det er Punktum dks mål at sikre:

At Punktum dk i kraft af en effektiv, nutidig og sikker databehandling har de bedste forudsætninger for løbende at optimere administrationen af domænenavne uden at gå på kompromis med datasikkerhed og driftsstabilitet og samtidig fremstå som en troværdig og respekteret virksomhed, samarbejdspartner og arbejdsgiver.

Det skal blandt andet gøres ved at efterleve ISO 27001, Ledelsessystemer for Informationssikkerhed (ISMS), herunder

- sikre, at data og informationer er korrekte, tilgængelige og anvendes korrekt af personer, der retmæssigt skal kunne anvende disse,
- forebygge uheld og skader, som kan opstå og begrænse konsekvenserne af eventuelle uheld og skader til en for Punktum dk (og omverdenen) acceptabel størrelse,
- sikre, at videreførelse af Punktum dks informationssystemer efter nedbrud og/eller skader vil kunne ske inden for en acceptabel tidshorisont,
- sikre adgangsstyring, så at uvedkommende ikke umiddelbart kan opnå adgang til data og systemer, der kan misbruges til skade for Punktum dk, vores kunder, medarbejdere og samarbejdspartnere,
- etablere en passende sikring af, at forsøg på overtrædelse eller tilsidesættelse af sikkerhedsforanstaltningerne i videst muligt omfang vil blive opdaget, og at aktiviteten kan føres tilbage til den eller de personer, som måtte være involveret,
- sikre, at medarbejdere opnår og opretholder en nødvendig sikkerhedsbevidsthed,
- sikre, at medarbejdere sikres tryghed, så der ikke er incitament til at skjule en eventuelt begået fejl,
- sikre, at Punktum dk overholder lovgivning, bestemmelser og indgåede aftaler,
- sikre, at en tværorganisatorisk beredskabsstyring, der er nødvendige for Punktum dks fortsatte drift.
- sikre, at informationssikkerheden løbende tilpasses og forbedres til ændrede omgivelser og nye trusler.

Ovenstående mål konkretiseres i en række målepunkter, som løbende ajourføres og danner baggrund til beslutning om tilpasninger eller nye initiativer for at fremme informationssikkerheden.

Gyldighedsområde

Informationssikkerhedspolitikken gælder for alle vores medarbejdere og andre, der er godkendt til at

anvende Punktum dks IT-aktiver. Disse omfatter alle informationssystemer (maskiner, programmer, kommunikationssystemer), som benyttes af Punktum dk, uanset om de er stationære, bærbare, anvendes på samarbejdspartneres adresser, i private hjem via netværk eller som stand-alone.

Relevante krav til overholdelse af informationssikkerhedspolitikken indarbejdes i samarbejdsaftaler med eksterne leverandører, samarbejdspartnere, serviceorganisationer, udlejere m.fl.

Ledelsen påser, at informationssikkerhedspolitikken revurderes og ajourføres, når særlige forhold begrunder det, dog altid mindst én gang om året.

Organisation og ansvar

Det overordnede ansvar for informationssikkerheden i Punktum dk påhviler bestyrelsen.

Direktionen har ansvaret for at fastlægge det nødvendige sikkerhedsniveau og indstille større nødvendige aktiviteter til godkendelse. Desuden skal ledelsen sikre, at alle medarbejdere, leverandører, samarbejdspartnere og konsulenter, der arbejder på vegne af Punktum dk, efterlever kravene fra ISO 27001 eller ækvivalent informationssikkerhedsstandard og overholder denne informationssikkerhedspolitik.

Sikkerhedsforummet består af direktøren, den informationssikkerhedsansvarlige (Sikkerhedschefen) og IT-chefen og har ansvaret for at eskalere beredskab og afklare særlige hændelser af informationssikkerhedsmæssig karakter.

IT-chefen og sikkerhedschefen har ansvar for løbende at orientere direktionen om særlige informationssikkerhedsmæssige forhold.

Sikkerhedschefen har ansvaret for koordinering af alt sikkerhedsarbejde, herunder at etablere, fastholde og koordinere arbejdet i organisationen.

Til at sikre organisationens efterlevelse af lovgivning og egne regler er der etableret en compliance enhed, der efterser dette. I compliance enheden indgår Sikkerhedschefen, personale fra Drift og fra juridisk afdeling.

Alle Punktum dks medarbejdere er personligt ansvarlige for at overholde og agere i henhold til informationssikkerhedspolitikken og følge de retningslinjer og procedurer, der er fastlagt.

Sikkerhedsbevidsthed

Punktum dk ønsker med denne informationssikkerhedspolitik at tilkendegive, at informationssikkerhed prioriteres højt. Det gøres ved en bevågenhed fra ledelsens side og ved en klar placering af sikkerhedsmæssige ansvarsområder.

Alle medarbejdere vil løbende blive informeret og uddannet om informationssikkerhed i relevant omfang, så at de er opmærksomme på sikkerhedsrisici og i stand til at følge ord og ånd i de givne politikker og retningslinjer.

Der arbejdes løbende med at skabe viden om hvad der er god adfærd inden for informationssikkerhed, ligesom dette løbende testes ved brug af eksterne aktører.

Dispensationer

Kun direktionen kan i konkrete situationer dispensere fra informationssikkerhedspolitikken. Sikkerhedschefen skal konsulteres forud for en dispensation. Sikkerhedschefen afdækker konsekvenserne af en dispensation med organisationen. Bestyrelsen skal informeres om væsentlige dispensationer.

Brud på informationssikkerheden

Punktum dk kan ikke acceptere brud på informationssikkerheden, der skyldes forsætlig eller grov uagtsomhed. Direktionen behandler eventuelle sanktioner i forbindelse med tilsigtede overtrædelser af informationssikkerhedspolitikken efter gældende regler og procedurer i Punktum dk.

Et brud på informationssikkerheden der skyldes uforsætlighed vil blive rettet straks, analyseret og påtalt efter gældende regler og procedurer i Punktum dk.

Referencer

Denne informationssikkerhedspolitik er uddybet med detaljerede implementeringsretningslinjer, herunder ikke mindst retningslinjer vedrørende almene passwords og root passwords, i overensstemmelse med ISO 27001 og er yderligere beskrevet i Punktum dks medarbejderhåndbog.

Godkendelse

Informationssikkerhedspolitikken godkendes af DIFO og Punktum dks bestyrelse og revurderes mindst en gang om året.

Denne informationssikkerhedspolitik er senest godkendt af bestyrelsen den 22. juni 2023 og indstilles til bestyrelsen til fornyet godkendelse den 21. juni 2024.