
Sikkerhedsinstruks for services leveret af TDC Group selskaber

Dokument Information

Forfatter	Christian Rozet
Med forfatter	Andreas Chr. Bisgaard-Petersen
Dokumentnavn	SI0003 Sikkerhedsinstruks for services leveret af TDC Group selskaber
Review dato	March 2020

For reference mellem ISO27001, TDC Politikker and TDC Standarder se TDC Group Statement of Applicability (SOA)

Versions Historie

Dato for frigivelse	Versions No.	Ændrings årsag
Maj 2018	v0.1	Draft
Maj 2018	v1.0	Godkendt af SVP/Group Chief Security Officer
September 2019	v1.1	Group Security Review og klar til forretnings review / pre-godkendelse (DPO kontor)

Distributions og Sign-Off Liste

Dette dokument version er udleveret til følgende personer for review og sign off.

Navn	Område	Påkrævet aktion
Michael Kayser Vestergaard	Head of Risk Management	Pre-godkendelse
Tone Thingbø	Deputy CSO / CISO	Godkendelse

Dokument ejer

Når dokumentet er godkendt, skal alle henvendelser vedrørende indhold rettes til:

Navn:	TDC Group Security
-------	--------------------

Indhold

1. Formål	4
2. Dækning	4
3. Sikkerhedsinstruks	4
3.1 Instruks.....	4
6. Dokument kontrol.....	5

1. Formål

Formålet med dette dokument er der er angive hvilke sikkerhedsinstrukser der er gældende for services leveret af TDC Group.

Ydermere er formålet med dette dokument eksplicit at sikre, at risiko og compliance sikkerhedsprincipperne i TDC er højt prioriteret og lever op til bedst practice.

2. Dækning

Sikkerhedsinstruksen gælder for services leveret af TDC Group selskaber.

3. Sikkerhedsinstruks

3.1 Instruks

For at garantere, at den leverede service er sikker, er de sikkerhedsforanstaltninger relateret til drift, egenkontrol, sikkerhed, beredskab, kompetencer, processer og økonomi, blevet implementeret på interne og eksterne systemer i brug i forbindelse med levering af ydelsen.

Nedenstående findes en opsummering på disse sikkerhedsforanstaltninger:

Informationssikkerhedspolitik, inklusiv: principper og retningslinjer, governance-model med roller og ansvar

- Operationelle procedurer og ansvarsområder, inklusiv: dokumenterede driftsprocedurer, sikkerhedskopiering (back-up), virus og malware beskyttelse, overvågning av systemanvendelse og auditlogging, administrator- og operatør logging, hændelses håndtering (sikkerhedsmæssige konsekvenser)
- Organisering af informationssikkerhed, inklusiv: dokumenteret og implementeret ansvar for informationssikkerhed, fortrolighedsaftaler, rapportering om informationssikkerhedshændelser
- Styring af adgang, inklusiv: administration af brugeradgang og brugeradgangskoder (password), evaluering af brugeradgangsrettigheder, inddragelser af adgangsrettigheder, styring av netværksadgang, politik for anvendelse af netværkstjenester herunder autentifikation af brugere med ekstern forbindelse, kommunikation med og mellem IT-systemer herunder kryptering
- Anskaffelse, udvikling og vedligeholdelse af informationssystemer, inklusiv: sikring af systemfiler, udvikling of test miljøer skilt fra produktionsmiljøer, styring af leverandører af driftssystemer således at krav til sikkerhed og regulatoriske krav efterleveres, asset management og data klassifikation er implementeret.

6. Dokument kontrol

Dokumentet skal revideres årligt eller i tilfælde af væsentlige ændringer i forudsætningerne for dokumentet.

Dokument Reference: SI0003