DANSK VERSION:

Information Sikkerhed i TDC Group

For at sikre tilgængeligheden, sikkerheden og beskyttelsen af data for TDC Groups drift og services, har TDC Group implementeret et Information Security Management System (ISMS) baseret på den internationale sikkerheds standard ISO27001:2013.
[https://www.iso.org/isoiec-27001-information-security.html].

Et ISMS system håndterer systematisk en organisations politikker og procedure på en sikker måde og har fokus på at beskytte fortroligheden, integriteten og tilgængeligheden af information som TDC Group håndterer både til intern brug og på vegne af kunder.

TDC Group's ISMS er bygget for at sikre kontinuerligt forbedringer og implementerer sikkerheden i organisationen baseret på en risiko- og sikkerheds vurdering. Dette betyder at sikkerhedsforanstaltningerne er blevet implementeret baseret på en vurdering af identificeret trusler, risici og svagheder i IT-miljøet og organisationen.

Målsætningen af TDC Group's ISMS er:

- At undgå uautoriseret adgang til information, som betyder at information kun er tilgængelig for individer der har et arbejd-relateret behov
- At sikre fortrolighed af informationer, som betyder at ingen data skal kunne tilgås af uautoriserede
- At sikre integritet, som betyder at data skal være beskyttet mod forvrængning eller korruption
- At implementere Continuity Management for at sikre tilgængelighed til systemer og information, som betyder at Business Continuity er sikret så data er tilgængelig når de behøves
- At håndtere platforme og løsninger ifølge ITIL, sikre kontinuerlige forbedringer af platformen og løsningen gennem en 'livs-cyklus' management
- Opfyldelse af regulatoriske og juridiske krav, som betyder at gældende lov og regulativer er identificeret og kravene er opfyldte
- Opmærksomhed skabelse samt træning i sikkerhed af medarbejderne, som betyder at alle medarbejdere er trænet i håndtering af information på en sikker facon
- Håndtering af sikkerheds hændelser, som betyder at der er procedure etableret for afrapportering, besvarelse og oprydning efter enhver sikkerheds hændelse
- At håndtere sikkerhedsrisici, som betyder at der er procedurer etableret for at beskytte platformen og services mod sikkerheds svagheder, trusler og risici
- At sikre compliance af ISO27001:2013, som betyder at bedste praksis i beskyttelse af information er implementeret

Målsætningen af TDC Group's ISMS er opnået ved at TDC Group har gennemført:

- Sikkerheds Governance gennem veldefinerede organisatoriske strukturer, roller og ansvarlighed
- Juridisk og regulatorisk compliance identifikations mekanismer
- Risiko og sikkerheds håndtering
- Erklæring om anvendelighed og gennemførelse af præstationsmålinger
- Sikkerheds opmærksomhedsskabende trænings program
- Sikkerheds hændelses håndtering gennem TDC Group's 'Security Operations Center' monitorering af TDC Group's infrastruktur og håndtering af hændelser indenfor TDC Group og monitorering af trusler på et globale niveau. Monitorering og gennemgang af implementering af ISMS gennem internt og eksternt revision, risici vurdering og afrapportering på manglende overensstemmelser

- Proaktivt og korrigerende sikkerhedskontroller for at opretholde sikkerhedsmålsætningen eller afhjælpe faktiske eller potentielle risici identificeret gennem revision, gennemgange, observationer, monitorering, sikkerheds hændelser eller begivenheder
- Compliance Review og revision udføres både af interne og eksterne ressourcer

TDC Group samarbejder med andre Europæiske telekommunikations organisationer i forhold til udviklingen af trusler og risici.

På det fysiske sikkerheds områder har TDC Group implementeret Forsikring & Pension standardarder, som bliver kontinuerligt auditeret.
[http://www.forsikringogpension.dk/virksomheder/fpsikring/Sider/fpsikring.aspx]

Hvis du ønsker at læse den fulde TDC Group ISMS Framework, så vær god at kontakte din Account Manager eller gennem Kunde Support.

ENGLISH VERSION:

Information Security in TDC Group

In order to ensure the security, privacy and availability of the TDC company operations and services, and to safeguard critical data and information, TDC has implemented a so-called Information Security Management System based on the international security standard ISO27001:2013. [https://www.iso.org/isoiec-27001-information-security.html]

An information Security Management System (ISMS) is a set of policies and procedures for systematically managing an organizations information in a secure way, and has focus on protecting the confidentiality, integrity and availability of the information that TDC is handling both for internal use and on behalf of its customers.
The TDC ISMS is modeled to ensure continuous improvement and is basing the implementation of security in the organization on risk- and security assessments. This means that the security measures have been implemented based on assessments of identified threats, risks and weaknesses to the IT-environment and organization.

The goals and objectives of the TDC ISMS are:
- To prevent unauthorized access to information –meaning that information only is accessible to individuals that have a work-related need.
- To assure confidentiality of information assets – meaning that no data shall be disclosed to unauthorized.
- To ensure integrity – meaning that the data shall be protected against distortion or corruption
- To implement continuity management to ensure availability of systems and information - meaning that business continuity is ensured so that data is available when needed
- To manage platforms and solutions according to ITIL – ensuring continuous improvements of the platforms and solutions through lifecycle management
- Fulfillment of regulatory and legislative requirement – meaning that applicable laws and regulations are identified and the requirements are fulfilled
- Awareness and security training of staff – meaning that all staff are trained in handling information in a secure way
- To manage security incidents – meaning that there are procedures established for reporting, responding and remediating any security incidents

- To manage security risks – meaning that there are procedures in place for protecting the platforms and services against security weaknesses, threats and risks
- To ensure compliance with ISO27001:2013 – meaning that Best Practice for the protection of information (information security) is implemented

The goals and objectives of the TDC ISMS are accomplished through TDC Group having established:

- Security governance with defined organizational structures, roles and responsibilities
- Legal and regulatory compliance identification mechanisms
- Risk and security management
- Statement of applicability and implementation of performance metrics
- Security Awareness training program
- Security incident management through a TDC" Security Operations Center" monitoring TDC's infrastructure and handling incidents within TDC and monitoring the global treat level. Monitoring and review of the implementation of the ISMS through measures such as internal and external audits, risk assessments and non-conformance reporting.
- Proactive and corrective security controls to sustain security objectives or remediate actual or potential risks identified through audits, reviews, observation, monitoring, security incidents and events.
- Compliance reviews and audits performed both by internal and external auditors

TDC is cooperating with other European telecommunications organizations regarding the development of threats and risk.

In the physical security area TDC has implemented the Forsikring & Pension standards (Insurance and Pension) which is continuously audited.
[http://www.forsikringogpension.dk/virksomheder/fpsikring/Sider/fpsikring.aspx]

If you wish to read the full TDC Group ISMS Framework, please contact your account manager or customer support