Telia Company

SUPPLIER SECURITY DIRECTIVE

Table of contents

TIEKĖJO SAUGUMO DIREKTYVOS

Turinys

1 Description This document "Supplier Security Directive" describes the security requirements applicable to suppliers and other identified business partners to Telia Company. Additional security requirements may apply if agreed by involved parties.	**1. Aprašymas** Šis dokumentas „Tiekėjo saugumo direktyvos" (toliau – Saugumo direktyvos) apibrėžia saugumo reikalavimus, taikomus tiekėjams ir kitiems Telia Company verslo partneriams. Šalių susitarimu gali būti taikomi papildomi saugumo reikalavimai.
2 Definitions	**2. Sąvokos**
1. "**Agreement**" shall mean the agreement between Telia Company and Supplier or other identified business partner to the Telia Company group under which the Supplier Security Directive apply, and to which the Supplier Security Directive is part thereof.	1. **Susitarimas** – reiškia tarp Telia Company ir Tiekėjo arba kito Telia Company grupės verslo partnerio sudarytą sutartį, kurios neatsiejama dalimi yra Saugumo direktyvos.
2. **"Buyer**" shall mean Telia Company AB or the relevant Telia Company Affiliate.	2. **Pirkėjas** – tai Telia Company AB ar atitinkamas Telia Company filialas.
3. "**Buyer's Data**" shall mean data or other information that the Buyer, or a person acting on behalf of the Buyer, makes available to the Supplier, including but not limited to Personal Data, and the result of Supplier's processing of such data.	3. **Pirkėjo duomenys** – tai duomenys ar kita informacija, kurią Pirkėjas arba asmuo, veikiantis Pirkėjo vardu, suteikia Tiekėjui, įskaitant, bet neapsiribojant, Asmens duomenimis, ir Tiekėjo tokių duomenų tvarkymo rezultatas.
4. "**Information Processing Facilities**" shall mean any information processing system, services or infrastructure, or the physical locations housing them.	4. **Informacijos tvarkymo infrastruktūra** – bet kokia informacijos apdorojimo sistema, paslaugos ar infrastruktūra arba fizinės jų įrengimo vietos.
5. **"Log"** shall mean to record details of information or events in an organized record-keeping system, usually sequenced in the order in which the information or events occurred.	5. **Registruoti (angl. *log*)** – registruoti informacijos arba įvykių detales organizuotoje registro įrašų tvarkymo sistemoje, paprastai tokia eilės tvarka, kokia buvo gauta informacija arba įvyko įvykiai.
6. "**Personal Data**" shall mean any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be directly or indirectly identified by reference to an identifier such as a name, address, social security number, subscription number, IP address, location data, an online identifier, traffic data or message content or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person.	6. **Asmens duomenys** – bet kokia informacija susijusi su fiziniu asmeniu, kurio tapatybė nustatyta arba kurio tapatybę galima tiesiogiai arba netiesiogiai nustatyti pagal identifikatorių, kaip antai vardą ir pavardę, adresą, asmens kodą, telefono numerį, IP adresą, buvimo vietos duomenis ir interneto identifikatorių, srauto duomenis ar žinutės turinį arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius.
7. **"Applicable Data Protection Laws"** shall mean all information subject to applicable data protection laws, including without limitation to "Directive on privacy in electronic communications" (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector) and "General Data Protection Regulation" (Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 94/46/RC) and any amendments, replacements or renewals thereof (collectively the "EU Legislation"), all binding national laws implementing the EU Legislation and other binding data protection or data security directives, laws, regulations and rulings valid at the given time.	7. **Asmens duomenų apsaugos teisės aktai** - visi galiojantys teisės aktai, kurie reglamentuoja asmens duomenų apsaugą ir saugumą, įskaitant, tačiau tuo neapsiribojant, Direktyva dėl privatumo ir elektroninių ryšių (Direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje) ir Bendrasis duomenų apsaugos reglamentas (2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinama Direktyva 95/46/EB) ir bet kokie pakeitimai, papildymai ar atnaujinimai (kartu vadinami ES teisės aktais), visi taikytini nacionaliniai įstatymai, įgyvendinantys ES teisės aktus ir kitos privalomos duomenų apsaugos arba duomenų saugumo direktyvos, reglamentai, įstatymai ir sprendimai, galiojantys tuo metu.
8. **"Regulatory Requirements"** shall mean all applicable laws, rules, regulations and treaties, in	8. **Taikytini reikalavimai** – tai visi bet kokios tarptautinės politinės ir ekonominės organizacijos

force from time to time, of any international political and economic organization (e. g. European Union), country, state, administrative agency or governed body (e. g. the relevant Financial Services Authority, Data Protection Authority, Consumer Protection Agency or Chemicals Agency), as well as any applicable case law, orders, decisions, licences, recommendations, policies, standards and guidelines issued by the said bodies, courts and/or by self-regulatory or advisory organisations and industry sector groups.	(pvz. Europos Sąjungos), šalies, valstybės, administracinės įstaigos ar valdžios institucijos (pvz., atitinkamos Finansinių paslaugų priežiūros institucijos, Duomenų apsaugos inspekcijos, Vartotojų teisių apsaugos tarnybos ar Cheminių medžiagų kontrolės tarnybos) įvesti tam tikru metu galiojantys taikytini įstatymai, taisyklės, iki teisės aktai ir sutartys bei bet kokia galiojanti teismų praktika, įstatymai, sprendimai, licencijos, rekomendacijos, politikos, standartai ir gairės, kurias išleido minėtos įstaigos, teismai ir (arba) savireguliavimo ar konsultacinės organizacijos per ūkio sektorių grupes.
9. "**Services**" shall mean the services to be provided by the Supplier to the Buyer, or a person acting on behalf of the Supplier as further defined in the Agreement between the parties.	9. **Paslaugos** – tai paslaugos, kurias Tiekėjas arba jo vardu veikiantis asmuo teikia Pirkėjui, kaip apibrėžta tarp šalių sudarytame Susitarime.
10. "**Supplier**" shall refer to the counter-party who supplies any kind of deliverables to Buyer identified as "Supplier", "Vendor, "Partner" or the equivalent in the relevant Agreement.	10. **Tiekėjas** – sandorio šalis, kuri tiekia bet kokios rūšies objektus Pirkėjui, kuris įvardijamas kaip „Tiekėjas", „Vendorius", „Partneris" arba lygiavertė šalis, nurodyta atitinkamame Susitarime.
11. "**Supplier Personnel**" shall mean any person working on behalf of the Supplier such as employees, consultants, contractors and sub-suppliers.	11. **Tiekėjo darbuotojai** – bet kurie Tiekėjo vardu ar pavedimu veikiantys asmenys, įskaitant darbuotojus, konsultantus, rangovus ir subtiekėjus.
12. "**Security Control**" shall mean any technical countermeasure, organizational setup or a process, that helps to maintain IT systems security-quality properties.	12. **Saugumo kontrolė** – tinkamos techninės ir organizacinės priemonės, kurios užtikrina IT sistemų saugumą.
13. "**Security Incident**" shall mean a single or a series of unwanted or unexpected security events that have a significant probability of compromising business operations and threatening security.	13. **Saugumo incidentas** – pavienis įvykis ar įvykių serija, kuris sukelia ar gali sukelti neteisėtą prisijungimą ar sudaryti sąlygas neteisėtai prisijungti prie informacinės sistemos, sutrikdyti ar pakeisti informacinės sistemos veikimą.
14. "**Sensitive Products**" and "**Sensitive Services**" shall mean any product or Services defined as sensitive by the Buyer. Sensitive Products or Sensitive Services shall be clearly documented in the applicable Agreement.	14. **„Jautrūs produktai"** ir **„Jautrios paslaugos"** reiškia bet kokį produktą ar paslaugas, kurias Telia apibrėžia kaip jautrias. Jautrūs produktai ir Jautrios paslaugos turi būti aiškiai apibrėžti galiojančiame Susitarime
15. **"Industry Standard"** shall mean a practice, method, process or criteria, such as well as known security best practices supporting high standards of resilience, and use of unbroken protocols etc, that is formally approved by industry members.	15. **Industrijos standartas** – tai praktika, metodas, procesas ar kriterijai, taip pat žinoma geriausia saugumo praktika, palaikanti aukštus atsparumo standartus, nenutrūkstamų protokolų naudojimą ir kt. kas formaliai patvirtinta pramonės narių.
16. "**Pseudonymisation**" shall mean the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person	16. **Pseudonimų suteikimas** – asmens duomenų tvarkymas taip, kad asmens duomenys negalėtų būti priskirti konkrečiam duomenų subjektui nesinaudojant papildoma informacija, jeigu tokia papildoma informacija yra saugoma atskirai ir jos atžvilgiu taikomos tinkamos techninės ir organizacinės priemonės, kurios užtikrina asmens duomenų nepriskyrimą konkrečiam fiziniam asmeniui.
3 Scope The Supplier Security Directive applies when:	**3. Apimtis** Saugumo direktyvos taikomos, kai:

1. The Supplier will process Buyer's Data, excluding the contact information required to establish or maintain a business relationship.
2. The Supplier will have unescorted access to Buyer's premises, excluding external areas.
3. The Supplier will access Buyer's network or IT systems, including remote access.
4. The Supplier will handle Buyer's information processing equipment.
5. The Buyer has deemed the Supplier as a provider of Sensitive Products and/or Sensitive Services and identified Supplier as such under the relevant Agreement.

4 The Supplier's overall responsibility

1. The Supplier is fully responsible for the Supplier Personnel's compliance with the Supplier Security Directive.
2. The Supplier shall implement the measures required to ensure compliance to the Supplier Security Directive prior to commencing any assignment for the Buyer.
3. The Supplier shall, at the request of the Buyer, inform the Buyer how the Supplier complies with the Supplier Security Directive and what measures the Supplier has taken to comply with the Supplier Security Directive.
4. The Supplier shall inform the Buyer at **cert@teliacompany.com** and **csirt@telia.lt** about any Security Incident (including but not limited to incidents in relation to the processing of Personal Data) as soon as possible but no later than 24 hours after the Security Incident has been identified. See Section 5.14 "Security incident management" below.
5. The Supplier shall assure that any processing of Buyer's Data will be compliant with the Supplier Security Directive.
6. The Supplier shall not allow any access to Buyer's Data (it may also concern new, extended, updated, prolonged or in any other way changed real-time network access) in breach of the Agreement to any party without prior written approval by the Buyer.

5 Security requirements

5.1 Risk Management

5.1.1 Security risk management

1. The Supplier shall identify and evaluate security risks related to confidentiality, integrity and availability; and based on such evaluation to implement appropriate technical and organizational measures to ensure a level of security which is appropriate to the risk.
2. The Supplier shall have documented processes and routines for handling risks within its operations.

1. Tiekėjas tvarkys Pirkėjo duomenis, išskyrus kontaktinę informaciją, reikalingą verslo santykiams užmegzti ar palaikyti.
2. Tiekėjas turės nelydimą prieigą prie Pirkėjo patalpų, išskyrus išorines zonas.
3. Tiekėjas turės prieigą prie prie Pirkėjo tinklo ar IT sistemos, įskaitant nuotolinę prieigą.
4. Tiekėjas prižiūrės Pirkėjo informacijos tvarkymo įrangą.
5. Pirkėjas laiko Tiekėją Jautrių produktų ir (arba) Jautrių paslaugų tiekėju pagal atitinkamą Susitarimą.

4. Tiekėjo bendra atsakomybė

1. Tiekėjas yra visiškai atsakingas už tai, kad Tiekėjo darbuotojai laikytųsi Saugumo direktyvų.
2. Tiekėjas prieš pradėdamas vykdyti bet kokias Pirkėjo pavestas užduotis privalo įgyvendinti šiuose Saugumo direktyvose nurodytas priemones.
3. Gavęs Pirkėjo prašymą, Tiekėjas privalo informuoti Telia apie tai, kaip Telia laikosi Saugumo direktyvų ir kokių priemonių Tiekėjas ėmėsi siekiant užtikrinti šių Saugumo direktyvų laikymąsi.
4. El. pašto adresu cert@teliacompany.com ir **csirt@telia.lt**Tiekėjas privalo informuoti Pirkėją apie bet kokį Saugumo incidentą (įskaitant, tačiau tuo neapsiribojant, incidentus, susijusius su Asmens duomenų tvarkymu) nedelsiant, bet ne vėliau kaip per 24 valandas nuo Saugumo incidento nustatymo. Žiūrėti 5.14 skyrių „Saugumo incidentų valdymas".
5. Tiekėjas privalo užtikrinti, kad bet koks vykdomas Pirkėjo duomenų tvarkymas atitiktų Saugumo direktyvas.
6. Tiekėjas neturi teisės suteikti prieigos prie Pirkėjo Asmens duomenų (šis draudimas taip pat taikomas ir naujos prieigos suteikimui, prieigos išplėtimui, prieigos atnaujinimui, prieigos pratęsimui arba kokiu nors kitu būdu prieigos prie tinklo suteikimui, pakeitimui ir pan.) pažeidžiant Sutartį jokiam kitam asmeniui be išankstinio raštiško Pirkėjo sutikimo.

5. Saugumo reikalavimai

5.1. Rizikos valdymas

5.1.1. Saugumo rizikos valdymas

1. Tiekėjas privalo nustatyti ir vertinti saugumo rizikas, susijusias su konfidencialumu, informacijos vientisumu ir prieinamumu ir, remdamasis tokiu įvertinimu, įgyvendinti tinkamas technines ir organizacines priemones, kurios užtikrintų atitinkamą saugumo lygį
2. Tiekėjas privalo dokumentais įtvirtinti savo veiklos rizikos valdymo procesus ir procedūras.

3. The Supplier shall periodically assess the risks related to information systems and processing, storing and transmitting information. The Supplier shall ensure that residual risks identified during assessment of information systems are periodically reviewed, updated and actively mitigated.

5.1.2 Security risk management for Personal Data

1. The Supplier shall identify and evaluate security risks related to confidentiality, integrity and availability and based on such evaluation to implement appropriate technical and organizational measures to ensure a level of security which is appropriate to the risk of the specific Personal data types and purposes being processed by the Supplier, including inter alia as appropriate:

   a) The pseudonymization and encryption of personal data
   b) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
   c) The ability to restore the availability and access to Buyer's Data in a timely manner in the event of a physical or technical incident

   d) A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

2. The Supplier shall have documented processes and routines for handling risks when processing Personal Data on behalf of Buyer.

3. The Supplier shall periodically assess the risks related to information systems and processing, storing and transmitting Personal Data.

5.2 Information security policies

1. The Supplier shall have a defined and documented information security management system (ISMS) including an information security policy and procedures in place, which shall be approved by the Supplier's management, published within Supplier's organization and communicated to relevant Supplier Personnel.

2. The Supplier shall periodically review the Supplier's security policies and procedures and update them if required to ensure their compliance with the Supplier Security Directive.

3. Tiekėjas privalo periodiškai vertinti rizikas, susijusias su informacinėmis sistemomis, ir duomenų tvarkymu, saugojimu ir perdavimu. Tiekėjas užtikrina, kad vertinant informacines sistemas nustatyta likusi rizika būtų periodiškai peržiūrima, atnaujinama ir aktyviai mažinama.

5.1.2. Asmens duomenų saugumo rizikos valdymas

1. Tiekėjas privalo nustatyti ir vertinti saugumo rizikas, susijusias su konfidencialumu, informacijos vientisumu ir prieinamumu ir, remdamasis tokiu įvertinimu, įgyvendinti tinkamas technines ir organizacines priemones, kurios užtikrintų tokį saugumo lygį, kuris atitiktų Asmens duomenų kategorijų, Asmens duomenų tvarkymo tikslų riziką, įskaitant, *inter alia*:
   a) Pseudonimų Asmens duomenims suteikimą ir asmens duomenų šifravimą

   b) Priemones, kurios užtikrintų nuolatinį Asmens duomenis tvarkančių sistemų ir paslaugų konfidencialumą, vientisumą, pateikiamumą ir atsparumą

   c) Priemones, kurios nedelsiant užtikrintų Asmens duomenų pateikiamumą ir prieigą prie duomenų fizinio ar techninio incidento atveju;

   d) Reguliarų techninių ir organizacinių priemonių, kuriomis užtikrinamas Asmens duomenų tvarkymo saugumas, tikrinimo ir veiksmingumo vertinimo procesą.

2. Tiekėjas privalo dokumentais įtvirtinti savo veiklos rizikos valdymo procesus ir procedūras, kiek tai susiję su Asmens duomenų tvarkymu Pirkėjo pavedimu.
3. Tiekėjas privalo periodiškai vertinti rizikas, susijusias su informacinėmis sistemomis ir Asmens duomenų tvarkymu, saugojimu ir perdavimu.

5.2. Informacijos saugumo politika

1. Tiekėjas privalo turėti apibrėžtą ir dokumentais įtvirtintą informacijos saugumo valdymo sistemą (ISVS), įskaitant informacijos saugumo politiką ir procedūras, kurios turi būti patvirtintos Tiekėjo vadovybės, paskelbtos Tiekėjo organizacijoje, ir atitinkami Tiekėjo darbuotojai turi būti tinkamai su jomis supažindinti.

2. Tiekėjas privalo periodiškai peržiūrėti Tiekėjo saugumo politiką ir procedūras bei, esant poreikiui, jas atnaujinti, kad jos atitiktų Saugumo direktyvas.

Telia Company

5.3 Organization of information security

1. The Supplier shall have defined and documented security roles and responsibilities within its organization.

2. The Supplier shall appoint at least one person having appropriate security competence, bearing ultimate responsibility for implementing the security measures under the Supplier Security Directive and who shall be the single point of contact for Buyer's security staff.

5.4 Human resources security

1. The Supplier shall ensure that the Supplier Personnel handles information in accordance with the level of confidentiality required under the Agreement.
2. The Supplier shall ensure that relevant Supplier Personnel is aware of the approved use (including use restrictions as the case may be) of information, facilities and systems under the Agreement. Buyer has the right to request a signed receipt from each and every Supplier Personnel stating that he or she has understood and will comply with the Supplier Security Directive and the approved use of information, systems and facilities.

3. The Supplier shall ensure that any Supplier Personnel performing assignments under the Agreement is trustworthy, meets established security criteria and has been, and during the term of the assignment will continue to be, subject to appropriate screening and background verification.
4. Supplier shall not, without informing and getting the Buyer's prior written approval, assign any Supplier Personnel to Buyer's assignment that:
   i. have any conflict of interest in relation to Buyer or the relevant assignment, or
   ii. has been convicted to imprisonment for any criminal offense during the three (3) year period prior to the engagement or the assignment (if applicable),

   if that Supplier Personnel will in any manner:
   a) process Personal Data relating to Buyer customers or staff, or to Buyer's customer's, or
   b) assist with tasks classified as sensitive by Buyer.

   The Buyer shall provide information about what tasks are classified as sensitive at the time of entering into the Agreement or the latest two weeks prior to a Supplier's Personnel engagement or assignment commences.
5. The Supplier shall ensure that Supplier Personnel with security responsibilities is adequately trained to carry out security related duties.

5.3. Informacijos saugumo organizavimas

1. Tiekėjas privalo apibrėžti ir dokumentais įtvirtinti saugumo roles ir atsakomybes savo organizacijoje.

2. Tiekėjas privalo paskirti bent vieną asmenį, turintį tinkamos kompetencijos saugumo srityje, prisiimantį galutinę atsakomybę už Saugumo direktyvose numatytų saugumo priemonių įgyvendinimą ir kuris būtų kontaktinis asmuo ryšiams su Pirkėjo darbuotojais, atsakingais už saugumą.

5.4. Žmogiškųjų išteklių saugumas

1. Tiekėjas užtikrina, kad jo darbuotojai tvarkytų informaciją laikydamiesi tokio konfidencialumo lygio, kuris nustatytas konfidencialios informacijos tvarkymui pagal Susitarimą.
2. Tiekėjas užtikrina, kad atitinkami Tiekėjo darbuotojai būtų susipažinę su informacijos, įrenginių ir sistemų naudojimo reikalavimais (įskaitant nustatytus naudojimo apribojimus) pagal Susitarimą. Pirkėjas turi teisę reikalauti iš Tiekėjo pateikti kiekvieno ir visų Tiekėjo darbuotojų pasirašytus dokumentus, įrodančius, kad jie suprato Saugumo direktyvas ir sutinka jų laikytis, įskaitant patvirtintus sistemų ir įrenginių naudojimo reikalavimus.

3. Tiekėjas užtikrina, kad visi Tiekėjo darbuotojai, atliekantys atitinkamas užduotis pagal Sutartį, yra patikimi, atitinka nustatytus saugumo kriterijus ir jų atžvilgiu buvo ir, užduočių atlikimo laikotarpiu, bus atliktas patikimumo vertinimas.

4. Tiekėjas negali, neinformavęs ir negavęs išankstinio rašytinio Pirkėjo sutikimo, paskirti savo darbuotojų atlikti užduočių, jeigu yra nustatyta, kad:
   i. yra interesų konfliktas, susijęs su Pirkėju ar jos pavedimu atliekama užduotimi ar
   ii. Tiekėjo darbuotojas buvo nuteistas už bet kokią nusikalstamą veiką per paskutinius trejus metus iki užduoties paskyrimo (jeigu taikoma),

   jeigu Tiekėjo darbuotojai:
   a) tvarkys Pirkėjo darbuotojų ar klientų Asmens duomenis arba
   b) padės atlikti užduotis, kurias Pirkėjas laiko jautriomis.

   Pirkėjas pateikia informaciją apie tai, kokios užduotys yra apibrėžiamos kaip jautrios tuo metu, kai sudaromas Susitarimas arba ne mažiau kaip likus 2 (dviem) savaitėms iki įsipareigojimų ar užduoties vykdymo.
5. Tiekėjas užtikrina, kad Tiekėjo darbuotojai, atsakingi už saugumą, yra tinkamai apmokyti vykdyti su saugumu susijusias užduotis.

Telia Company

6. The Supplier shall provide or ensure periodical security awareness training to relevant Supplier Personnel. Such Supplier training shall include, without limitation:
   a) How to handle customer information security (i.e. the protection of the confidentiality, integrity and availability of information);
   b) Why information security is needed to protect customers information and systems;
   c) The common types of security threats (such as identity theft, malware, hacking, information leakage and insider threat);
   d) The importance of complying with information security policies and applying associated standards/procedures;
   e) Personal responsibility for information security (such as protecting customer's privacy-related information and reporting actual and suspected Security Incidents).

5.5 Asset management

1. The Supplier shall have a defined and documented asset management system in place, and maintain up-to-date records of all relevant assets and their owners. Information assets include but are not limited to IT systems, backup and/or removable media containing confidential or secret information, access rights, software and configuration.
2. The Supplier shall label, treat and protect information according to a pre-defined information classification following Industry Standard (including, but not limited to, removable media storage, disposal and physical transfer).
3. The Supplier shall implement measures to ensure protection against accidental, unauthorized or unlawful loss, destruction, alteration or damage to Buyer data transmitted, stored or otherwise processed.
4. The Supplier shall keep an updated list of Buyer's data processed. The list shall contain the following information:
   a) The processed data
   b) Storage details, such as asset name, location etc.
5. The Supplier shall return or destroy (as determined by the Buyer) any of the Buyer's Data and copies thereof. The Supplier shall issue a signed acknowledgement or a deletion certificate upon termination of the Agreement.

6. Tiekėjas privalo užtikrinti periodinius saugumo mokymus atitinkamiems Tiekėjo darbuotojams. Tokie Tiekėjo mokymai privalo apimti šiuos aspektus:
   a) Kaip užtikrinti kliento informacijos saugumą (t. y. konfidencialumo apsauga, informacijos vientisumas ir prieinamumas);
   b) Kodėl informacijos saugumas būtinas siekiant tinkamai apsaugoti kliento informaciją bei sistemas;
   c) Kokios yra bendrosios saugumo grėsmės (pavyzdžiui, tokios kaip tapatybės vagystė, kenkėjiškos programos, įsilaužimas, informacijos nutekėjimas ir vidaus grėsmės);
   d) Kodėl svarbu laikytis informacijos saugumo politikos ir susijusių standartų/procedūrų;
   e) Kokia yra darbuotojų asmeninė atsakomybė už informacijos saugumą (pavyzdžiui, Asmens duomenų apsauga, pranešimų apie faktinius ir įtariamus saugumo incidentus pateikimas).

5.5. Informacinio turto valdymas

1. Tiekėjas turi turėti apibrėžtą ir dokumentais įtvirtintą informacinio turto valdymo sistemą ir palaikyti atnaujintus įrašus apie visą informacinį turtą bei jo valdytojus. Informacinis turtas apima, įskaitant, tačiau tuo neapsiribojant, IT sistemas, atsarginės kopijas (angl. *backup*) ir (arba) išimamas kompiuterinių duomenų saugojimo laikmenas, kuriose yra konfidencialios ar slaptos informacijos, prieigos teises, programinę įrangą ir konfigūraciją.
2. Tiekėjas privalo klasifikuoti, tvarkyti ir saugoti informaciją pagal iš anksto apibrėžtą informacijos klasifikavimo sistemą, vadovaujantis tuo metu galiojančiais Industrijos standartais (įskaitant, bet neapsiribojant, išimamų kompiuterinių duomenų laikmenų saugojimą, naikinimą bei jų fizinį perdavimą).
3. Tiekėjas privalo įgyvendinti tinkamas priemones, skirtas apsaugoti Pirkėjo duomenis nuo atsitiktinio, neleistino ar neteisėto praradimo, sunaikinimo, pakeitimo, sugadinimo ar kitokio tvarkymo.
4. Tiekėjas privalo saugoti atnaujinamus įrašus apie Pirkėjo pavedimu tvarkomus duomenis. Įrašuose turi būti nurodoma ši informacija:
   a) Tvarkomi duomenys
   b) Informacija susijusi su duomenų saugojimu, pvz. informacinės sistemos pavadinimas, vieta ir t. t.
5. Tiekėjas grąžina arba sunaikina (Pirkėjo pasirinkimu) visus Pirkėjo duomenis ir jų kopijas nutrūkus sutartiniams santykiams. Nutrūkus Susitarimui Tiekėjas išduoda

6. The Supplier shall not extract information from the Buyers Data or the Buyer's customer Data, it should be described by the Supplier and explicitly approved by the Buyer before executing in operation; including but not limited to;
   a) Information directly or indirectly related to customers of the Buyer, including statistics.
   b) Information relating to the configuration of systems or equipment describing topology or in bulk.
   c) All machine-to-machine communication, such as extracting data for analytics that is not directly connected to the service delivered.

5.6 Access control

1. The Supplier shall have a defined and documented access control policy for facilities, sites, network, system, application and information/data access (including physical, logical and remote access controls), an authorization process for user access and privileges, procedures for revoking access rights and an acceptable use of access privileges for the Supplier Personnel in place.
2. The Supplier shall have a formal and documented user registration and de-registration process implemented to enable assignment of access rights.
3. The Supplier shall assign all access privileges based on "need-to-know" and "least privilege" principles.
4. The Supplier shall use strong authentication (multi-factor) for remote connection access, elevated access and/or any other type of privileged access.
5. The Supplier shall ensure all relevant Supplier Personnel has a personal, unique and non-transferable identifier (user ID), and use an appropriate authentication technique, keeping accountability of user's actions.

5.7 Encryption

1. The Supplier shall ensure proper and effective use of cryptography on information classified as confidential and secret (such as Personal Data) according with Buyer's confidentiality classification scheme, per Section 6.
2. The Supplier shall protect cryptographic keys.

pasirašytą patvirtinimą, jog duomenys buvo ištrinti arba pateikia ištrynimo sertifikatą.

6. Tiekėjas neišgauna informacijos iš Pirkėjo duomenų ar Pirkėjo klientų duomenų. Tokie veiksmai, turi būti aprašyti ir aiškiai patvirtinti Pirkėjo prieš vykdant operacijas, įskaitant, bet neapsiribojant:
   a) Informacija, tiesiogiai ar netiesiogiai susijusi su Pirkėjo klientais, įskaitant statistiką.
   b) Informacija, apie sistemų ar įrangos konfigūraciją, arba informacija apibūdinanti topologiją arba viską bendrai.
   c) Visa *machine-to-machine* komunikacija tokia, kaip duomenų rinkimas analizei, kurie nėra tiesiogiai susijusi su teikiama paslauga.

5.6. Prieigos kontrolė

1. Tiekėjas privalo turėti apibrėžtą ir dokumentais įtvirtintą įrenginių, objektų, tinklo/ų, sistemų, prašymų pateikimo ir prieigos prie informacijos/duomenų (įskaitant fizinės, loginės ir nuotolinės prieigos kontrolės priemones) prieigos kontrolės politiką; leidimų, susijusių su vartotojų prieiga ir atitinkamomis privilegijomis, suteikimo procesą, prieigos teisių panaikinimo ir tinkamo prieigos naudojimo procedūras Tiekėjo darbuotojams.
2. Tiekėjas turi turėti apibrėžtą ir dokumentais įtvirtintą vartotojų registravimo ir išregistravimo procedūrą, pagal kurią suteikiamos prieigos teisės.
3. Visas prieigos teises Tiekėjas skiria vadovaudamasis „būtina žinoti" ir „mažiausių privilegijų" principais (angl. *the principle of need-to-know and principle of least privilege*).
4. Tiekėjas privalo naudoti saugų (angl. *multi-factor*) autentifikavimą nuotolinio ryšio prieigai, aukštesnių privilegijų prieigai ir (arba) bet kokiai kitai privilegijuotai prieigai.
5. Tiekėjas privalo užtikrinti, kad Tiekėjo darbuotojai turėtų asmeninį, unikalų ir neperduodamą identifikatorių (vartotojo ID), ir privalo naudoti tinkamą autentifikavimo būdą, išlaikant vartotojų veiksmų atskaitomybę.

5.7. Šifravimas

1. Tiekėjas privalo užtikrinti tinkamą ir efektyvų kriptografijos naudojimą informacijai, kuri laikoma konfidencialia ir slapta (pavyzdžiui, Asmens duomenys), vadovaujantis šiose Saugumo direktyvose pateikiama Pirkėjo konfidencialumo klasifikavimo schema 6 skyriuje.
2. Tiekėjas privalo apsaugoti kriptografinius raktus.

Telia Company

5.8 Physical and environmental security

1. The Supplier shall protect Information Processing Facilities against external and environmental threats and hazards, including power/cabling failures and other disruptions caused by failures in supporting utilities. This includes physical perimeter and access protection.
2. The Supplier shall protect goods received or sent on behalf of the Buyer from theft, manipulation and destruction.

5.8.1 Admission to Buyer's premises and Buyer's leased premises

The Supplier's admission to Buyer's premises and property (such as datacenter buildings, office buildings, technical sites) is subject to the following:

1. The Supplier shall follow local regulations (such as regulations for "restricted areas") for Buyer's premises when performing the assignments under the Agreement.
2. Supplier Personnel shall carry ID card or a visitor's badge visible at all time when working within Buyer's the premises.
3. After completing the assignment, or when Supplier Personnel is transferred to other tasks, the Supplier shall without delay inform the Buyer of the change and return any keys, key cards, certificates, visitor's badges and similar items.
4. Keys or key cards shall be personally signed for by Supplier Personnel and shall be handled according to the written rules given upon receipt;
5. Loss of the Buyer's key or key card shall be reported without delay to Buyer.
6. Photograph or video recording within Buyer's premises without permission is strictly prohibited.
7. Buyer's goods shall not be removed from Buyer's premises without permission
8. Supplier Personnel shall not allow unauthorized persons access to the premises.

5.9 Operations security

1. The Supplier shall have an established change management system in place for making changes to business processes, Information Processing Facilities and systems. The change management system shall include tests and reviews before changes are implemented, such as procedures to handle urgent changes, roll back procedures to recover from failed changes, logs that show, what has been changed, when and by whom.

5.8. Fizinis ir aplinkos saugumas

1. Tiekėjas privalo tinkamai apsaugoti informacijos tvarkymo įrenginius nuo išorės ir aplinkos grėsmių ir pavojų, įskaitant elektros energijos/kabelių gedimus ir kitus sutrikimus, kylančius dėl pagalbinių įrenginių gedimų. Tai apima fizinę perimetro ir prieigos apsaugą.
2. Tiekėjas saugo Pirkėjo gautas ar atsiųstas prekes nuo vagystės, manipuliavimo ir sunaikinimo.

5.8.1. Leidimas įeiti į Pirkėjo patalpas

Tiekėjui leidžiama įeiti į Pirkėjo patalpas (pvz., duomenų centrų pastatus, biurų pastatus, techninius objektus) tik jei laikomasi šių sąlygų:

1. Tiekėjas laikosi teisės aktų (pavyzdžiui, teisės aktų, reglamentuojančių patekimą į „saugomas zonas") ir Pirkėjo nustatytų vidinių tvarkų būdamas Pirkėjo patalpose ir atlikdamas atitinkamas užduotis/veiksmus pagal Sutartį ir Duomenų tvarkymo sutartį;
2. Būdami Pirkėjo patalpose, Tiekėjo darbuotojai privalo visuomet matomoje vietoje nešioti asmens tapatybę įrodantį lankytojo pažymėjimo.
3. Tiekėjo darbuotojams atlikus atitinkamus veiksmus/užduotis arba tais atvejais, kai Tiekėjo darbuotojai perkeliami vykdyti kitas užduotis, Tiekėjas nedelsdamas praneša Pirkėjui apie pasikeitimą ir grąžina išduotus raktus, raktų korteles, pažymėjimus, lankytojo pažymėjimus ir pan.
4. Raktai arba el. įėjimo kortelės turi būti asmeninės ir skirtos naudoti tik Tiekėjo atitinkamiems darbuotojams, o raktų arba el. įėjimo kortelių administravimas vykdomas pagal nustatytas taisykles, su kuriomis supažindinama jų išdavimo metu.
5. Pametus Pirkėjo raktą arba el. įėjimo raktų kortelę turi būti nedelsiant pranešta Pirkėjui;
6. Draudžiama be leidimo fotografuoti ir filmuoti Pirkėjo patalpos.
7. Draudžiama be leidimo išnešti Pirkėjo turtą iš jo patalpų.
8. Tiekėjo darbuotojams draudžiama įleisti pašalinius asmenis į patalpas.

5.9. Operacijų saugumas

1. Tiekėjas privalo turėti įdiegtą pakeitimų valdymo sistemą, skirtą verslo procesų, Informacijos tvarkymo įrenginių ir sistemų pakeitimams. Pakeitimų valdymo sistema turi apimti bandymus ir peržiūras, atliekamas prieš įgyvendinant pakeitimus, pavyzdžiui, skubių pakeitimų tvarkymo procedūras, atstatymo po nepavykusių pakeitimų procedūras, įrašus, kurie rodo, kas buvo pakeista, kada ir kas tai atliko.

2. The Supplier shall implement malware protection to ensure that any software used for Supplier's provision of the deliverables to the Buyer is protected from malware. 3. The Supplier shall make backup copies of critical information and test back-up copies to ensure that the information can be restored as agreed with the Buyer. 4. The Supplier shall Log and monitor activities, such as create, reading, copying, amendment and deletion of processed data, as well as exceptions, faults and information security events and regularly review these. Furthermore, the Supplier shall protect and store (for at least 6 months) Log information, and on request, deliver monitoring data to the Buyer. Anomalies, incidents and/or indicators of compromise shall be reported according to the incident management requirements, Section 5.14. 5. The Supplier shall have defined, documented and monitored procedures for administrative operations of computing environments where the Buyer's Data and the Buyer's customer Data is processed. 6. The Supplier shall manage vulnerabilities of all relevant technologies such as operating systems, databases, applications proactively and in a timely manner. 7. The Supplier shall establish security baselines (hardening) for all relevant technologies such as operating systems, databases, applications. 8. The Supplier shall ensure development is segregated from test and production environment. 9. The Supplier shall implement network Security Controls such as service level, firewalling and segregation to protect information systems and, upon request, be able to provide related logs and evidence to the Buyer. 10. In case Buyer's data is processed on a multi-tenant environment operated by the Supplier, the Supplier shall implement security controls to isolate Buyers Data from tenants and unauthorized users, following Industry Standard.	2. Tiekėjas įdiegia apsaugą nuo kenkėjiškų programų, tam kad bet kokia programinė įranga, kuri naudojama teikiant paslaugas Pirkėjui, būtų apsaugota nuo kenkėjiškų programų. 3. Tiekėjas daro atsargines ypatingai svarbios informacijos kopijas ir išbando atsargines kopijas, siekdamas užtikrinti, kad informacija būtų atkurta, kaip buvo susitarta su Pirkėju. 4. Tiekėjas registruoja ir stebi vartotojų veiklą, naudojamas išimtis, gedimus ir informacijos saugumo įvykius bei reguliariai juos peržiūri. Be to, Tiekėjas saugo ir laiko (ne mažiau kaip 6 mėnesius arba teisės aktuose numatytą ilgesnį terminą) registro įrašų informaciją ir, paprašius, pateikia duomenis Pirkėjui. Apie pažeidimus, incidentus ir (arba) galimus pažeidimus turi būti pranešama pagal 5.14 skyrių „Saugumo incidentų valdymas“. 5. Tiekėjas turi turėti dokumentuotas, patvirtintas ir prižiūrimas kompiuterinių aplinkų, kuriose tvarkomi Pirkėjo ir Pirkėjo klientų duomenys, administravimo procedūras. 6. Tiekėjas privalo aktyviai ir laiku valdyti visų atitinkamų technologijų, įskaitant (bet neapsiribojant) operacinės sistemos, duomenų bazės, taikomosios programos, pažeidžiamumus. 7. Tiekėjas nustato saugumo stiprinimo (en. *hardening*) reikalavimus visoms atitinkamoms technologijoms, tokioms kaip operacinės sistemos, duomenų bazės, taikomosios programos. 8. Tiekėjas privalo užtikrinti, kad vystymas būtų atskirtas nuo testavimo ir gamybinės aplinkos. 9. Tiekėjas privalo įgyvendinti tinklo saugumo kontrolės priemones, tokias kaip paslaugų prieinamumas, ugniasienės ir (tinklų) atskyrimas, siekiant apsaugoti informacines sistemas ir esant prašymui pateikti įrodymus ir žurnalų įrašus Pirkėjui. 10. Tuo atveju, kai Pirkėjo duomenys yra tvarkomi Tiekėjo valdomoje daugialypėje aplinkoje, Tiekėjas įgyvendina saugumo priemones , kad Pirkėjo duomenys būtų izoliuoti nuo kitų klientų ir neįgaliotų vartotojų pagal Industrijos standartus.
5.10 Communications security 1. The Supplier shall ensure that at least all communication of information classified as internal, confidential or secret is secured according to the Buyer's information classification description in section 6 (Information	**5.10. Komunikacijos saugumas** 1. Tiekėjas užtikrina tinkamą komunikacijos, kuri klasifikuojama kaip vidinė, konfidenciali arba slapta, saugumą pagal Pirkėjo pateiktą informacijos klasifikavimo aprašymą 6 skyriuje (Informacijos konfidencialumo aprašymas ir informacijos tvarkymui taikomi reikalavimai).

Telia Company

security confidentiality classification description and handling requirements).

5.11 System acquisition, development and maintenance (when software development or system development is provided to the Buyer by Supplier)

1. The Supplier shall implement rules for development lifecycle of software and systems including change and review procedures.
2. The Supplier shall establish, document and maintain principles for secure system architecture and those principles shall be applied to the Supplier's information system development and implementation efforts.
3. The Supplier shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.
4. The Supplier shall test security functionality during development in a controlled environment.
5. The Supplier shall not use the Buyers data for testing purposes unless it is required by the Buyer.
6. The Supplier shall ensure that information involved in application services, passing over public networks shall be protected from fraudulent activity, unauthorized disclosure and modification.
7. The Supplier shall ensure the protection of confidentiality and integrity of information involved in application service transactions.

5.12 Personal Data processing

This section (5.12) shall apply whenever the Supplier is considered as Data Processor of Personal Data where the Buyer is the Data Controller. The following terms constitutes the controller´s instructions on the security requirements of personal data. The terms specify the minimum-security requirements regarding Personal Data. The general legal terms of the DPA is attached to the Master Agreement. Sections (4.2.3 – 4.2.5.) regarding Access Control and Operational Security are applicable for Data at rest and Data in use.

1. The Supplier shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk related to the processing. In assessing the appropriate level of security account shall be taken of the risks from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data processed. Based on the results of the privacy risk assessment the Supplier shall plan, implement and control the processes

5.11. Sistemų įsigijimas, kūrimas ir priežiūra (kai Tiekėjas atlieka programinės įrangos arba sistemos kūrimą Pirkėjui)

1. Tiekėjas privalo įgyvendinti programinės įrangos ir sistemų kūrimo gyvavimo ciklo taisykles, įskaitant pakeitimų ir peržiūros procedūras.
2. Tiekėjas nustato, dokumentuoja ir prižiūri saugios sistemos architektūros principus ir šie principai turi būti taikomi Tiekėjo informacinių sistemų kūrimui ir diegimui.
3. Tiekėjas įdiegia saugias aplinkas, sistemų kūrimui ir integravimui, kurios apima visą sistemos kūrimo gyvavimo ciklą.
4. Kūrimo proceso metu Tiekėjas atlieka saugumo funkcionalumo bandymus kontroliuojamoje aplinkoje.
5. Tiekėjas įsipareigoja nenaudoti Pirkėjo duomenų testavimo tikslais, nebent to reikalauja pats Pirkėjas.
6. Tiekėjas užtikrina, kad bet kokia taikomųjų paslaugų informacija, perduodama viešaisiais tinklais būtų apsaugota nuo apgaulingos veiklos, neteisėto atskleidimo ir keitimo.
7. Tiekėjas užtikrina informacijos, susijusios su programų paslaugų sandoriais, konfidencialumą ir vientisumą.

5.12. Asmens duomenų tvarkymas

Šis (5.12) skyrius taikomas, kai Tiekėjas yra laikomas asmens duomenų tvarkytoju, o Pirkėjas duomenų valdytoju. Šios sąlygos yra duomenų valdytojo nurodymai dėl asmens duomenų tvarkymui keliamų saugumo reikalavimų. Sąlygose nurodomi minimalūs Asmens duomenų saugumo reikalavimai. Duomenų tvarkymo sutarties bendrosios teisinės sąlygos pridedamos prie Pagrindinės sutarties. Nenaudojamiems (*en. Data in rest*) ir naudojamiems duomenims (*en*. *Data in use)* yra taikomi Prieigos kontrolės ir Operacijų saugumo skyriai.

1. Tiekėjas užtikrina ir įgyvendina tinkamas technines ir organizacines priemones tvarkomų duomenų saugumo lygiui užtikrinti. Vertinant tinkamą saugumo lygį, reikia atsižvelgti į riziką, kurią gali sukelti atsitiktinis ar neteisėtas tvarkomų asmens duomenų sunaikinimas, praradimas, pakeitimas, neteisėtas atskleidimas ar prieiga prie tvarkomų asmens duomenų. Tiekėjas remdamasis privatumo rizikos vertinimo rezultatais planuoja,

Telia Company

needed to meet data protection and privacy requirements.
2. The Supplier shall promote Privacy by Design and put into place accountability and governance measures.
3. The Supplier shall inform the Buyer at **controlcenterem-security@teliacompany.com** and **csirt@telia.lt** about any incidents in relation to Personal Data without undue delay after the Personal Data Incident has been identified.
4. **Data at rest:** The Supplier shall ensure the confidentiality, integrity, availability and resilience of processing systems and services. The Supplier shall ensure that Personal Data storage is logically and physically protected and controlled, has restricted access control and is protected according to section 6 (**Error! Reference source not found.**). Personal Data shall be classified and handled at least as Confidential.
5. **Data in transit:** The Supplier shall implement robust security controls to ensure that Personal Data is transferred through protected communication channels in a controlled and trusted network, or in a secure portable storage to ensure the confidentiality and integrity of Personal Data. Security controls such as TLS, SFTP etc. according to current Industry Standards.
6. **Data in use:** The Supplier shall ensure that Personal Data is only processed by authorized person(s) in a controlled workspace and protected from harmful use. Furthermore, the Supplier shall ensure that privacy policy is in place that privacy processes are implemented, that awareness programs are deployed, that change management control is in place and that dual-control principles are implemented.

5.13 The Supplier relationship with sub-contractors

1. The Supplier shall reflect the content of the Supplier Security Directive in its agreements with sub-contractors that perform tasks assigned under the Agreement.
2. The Supplier shall regularly monitor, review and audit sub-contractors compliance with the Supplier Security Directive.
3. The Supplier shall, at the request of the Buyer, provide to Buyer with evidence regarding sub-contractors compliance with the Supplier Security Directive.

5.14 Security incident management

1. The Supplier shall have established procedures for Security Incident management.

įgyvendina ir kontroliuoja procesus tam, kad atitiktų duomenų apsaugos ir privatumo reikalavimus.
2. Tiekėjas skatina Pritaikytąją duomenų apsaugą ir įdiegia atskaitomybės ir valdymo priemones.
3. Tiekėjas elektroniniu paštu **controlcenterem-security@teliacompany.com** ir **csirt@telia.lt** informuoja apie bet kokį incidentą, susijusį su tvarkomais Asmens duomenimis nedelsiant nuo Asmens duomenų incidento nustatymo.
4. **Nenaudojami duomenys:** Tiekėjas užtikrina duomenų konfidencialumą, vientisumą, prieinamumą ir atsparumą. Tiekėjas užtikrina, kad Asmens duomenys būtų logiškai ir fiziškai apsaugoti ir kontroliuojami, būtų ribojama prieiga ir saugomi pagal 6 skyrių (Informacijos konfidencialumo aprašymas ir informacijos tvarkymui taikomi reikalavimai). Asmens duomenys turi būti klasifikuojami ir tvarkomi kaip konfidencialūs.
5. **Siunčiami duomenys:** Tiekėjas įgyvendina patikimas saugumo priemones (tokias kaip TLS. SFTP ir kt. pagal aktualius Industrijos standartus), kad užtikrintų Asmens duomenų perdavimą saugiais ryšių kanalais kontroliuojamame ir patikimame tinkle arba saugioje nešiojamojoje saugykloje, kad būtų užtikrintas Asmens duomenų konfidencialumas ir vientisumas.
6. **Naudojami duomenys:** Tiekėjas užtikrina, kad Asmens duomenis tvarkytų tik įgaliotas asmuo (-ys) kontroliuojamoje ir apsaugotoje nuo žalingo naudojimo darbo vietoje. Be to, Tiekėjas užtikrina, kad yra įdiegta Privatumo politika, įgyvendinti privatumo procesai, vykdomos privatumo mokymų programos, veikia pakeitimų valdymo kontrolė ir įgyvendinti dvigubos kontrolės principai.

5.13. Tiekėjo santykiai su subtiekėjais

1. Tiekėjas į savo sudaromas sutartis su subtiekėjais, atliekančiais jiems pavestas užduotis, numatytas Susitarime, įtraukia Saugumo direktyvose apibrėžtus reikalavimus,.
2. Tiekėjas reguliariai stebi, peržiūri ir audituoja subtiekėjų atitiktį Saugumo direktyvoms.
3. Pirkėjui paprašius, Tiekėjas pateikia Pirkėjui subtiekėjų atitikties Saugumo direktyvoms įrodymus.

5.14. Saugumo incidentų valdymas

1. Tiekėjas privalo turėti nustatytas saugumo incidentų valdymo procedūras.

2. The Supplier shall inform the Buyer at **controlcenterem-security@teliacompany.com** and **csirt@telia.lt** about any Security Incident without undue delay after the Security Incident has been identified.
3. All reporting of security related incidents shall be treated as confidential information and be encrypted, using Industry Standard encryption methods such as PGP or equal Industry Standard encryption.
4. The security incident report shall contain at least the following information:
   a) Notwithstanding the requirement for immediate notification, the Supplier shall, comprise a written preliminary report to the Buyer of any security incident that could possibly affect the Buyer or the Buyer's assets in any imaginable way
   b) Sequence of events, including actions taken during the incident handling
   c) Affected portions of the infrastructure, systems and information
   d) Estimated (or, upon a high level of uncertainty, worst-case) consequences/impact;
   e) Consequence reducing measures already implemented
   f) Risk-reducing measures already implemented
   g) Consequence reducing measures to be implemented, including implementation plan (date; responsible; dependencies);
   h) Risk reducing measures to be implemented, including implementation plan (date; responsible; dependencies);
   i) Experiences summary including root cause analysis.
5. The Supplier shall provide the Buyer with support in case of forensic investigation.

5.15 Business continuity management

The Supplier shall:

1. Have documented processes and routines for handling business continuity including disaster recovery.
2. Ensure that information security is embedded into the business continuity plans.
3. Periodically identify, analyze and evaluate business continuity risks and take necessary actions to control and mitigate such risks.
4. Periodically, at least annually (unless otherwise agreed), assess the efficiency of its business continuity management including disaster

2. Tiekėjas privalo neatidėliodamas informuoti Pirkėją apie bet kokį Saugumo incidentą el. pašto adresu **controlcenterem-security@teliacompany.com ir csirt@telia.lt.**
3. Visi pranešimai apie saugumo incidentus laikomi konfidencialia informacija ir yra šifruojami naudojant Standartinius šifravimo metodus, tokius kaip (angl.) PGP ar pagal atitinkamą Industrijoje priimtą standartą.
4. Saugumo incidento ataskaitoje Tiekėjas (įskaitant, tačiau tuo neapsiribojant) privalo pateikti šią informaciją:
   a) Nepaisant reikalavimo nedelsiant pranešti Pirkėjui apie saugumo pažeidimą, Tiekėjas privalo parengti Pirkėjui pirminę rašytinę ataskaitą apie bet kokį saugumo incidentą, bet kokiu įmanomu būdu galintį turėti įtakos Pirkėjui, jo turtui;
   b) Pateikti įvykių sekos aprašymą, įskaitant veiksmus, kurių buvo imtasi siekiant valdyti incidentą;
   c) Nurodyti incidento paveiktos infrastruktūros dalis, sistemas ir informaciją;
   d) Nurodyti numatomą (esant dideliam neapibrėžtumui, apibūdinti blogiausią scenarijų) incidento poveikį ir pasekmes;
   e) Nurodyti įgyvendintas pasekmių mažinimo priemones
   f) Nurodyti įgyvendintas rizikos mažinimo priemones
   g) Nurodyti ketinamas įgyvendinti incidento padarinių (pasekmių) mažinimo priemones, įgyvendinimo planą (nurodant terminą, atsakingus asmenis ir priklausomybes)
   h) Nurodyti ketinamas įgyvendinti rizikos mažinimo priemones, įgyvendinimo planą (nurodant terminą, atsakingus asmenis ir priklausomybes)
   i) Pateikti incidento valdymo patirties santrauką, įskaitant pagrindinių priežasčių analizę.
5. Tiekėjas teikia Pirkėjui reikiamą pagalbą tyrimų atvejais.

5.15. Veiklos tęstinumo valdymas

Tiekėjas privalo:

1. Turėti dokumentais įtvirtintus savo veiklos tęstinumo valdymo procesus ir procedūras įskaitant atkūrimą nelaimės atveju.
2. Užtikrinti, kad informacijos saugumas būtų įtrauktas į verslo tęstinumo planus.
3. Periodiškai nustatyti, analizuoti ir vertinti verslo tęstinumo riziką ir imtis būtinų veiksmų tokiai rizikai kontroliuoti ir sušvelninti.
4. Periodiškai, bent kasmet (nebent susitarta kitaip) vertinti savo veiklos tęstinumo valdymo efektyvumą, įskaitant atkūrimą nelaimės atveju,

recovery, and compliance with availability requirements (if any).

5.16 Compliance

1. The Supplier shall comply with all Regulatory Requirements and contractual requirements including but not limited to Personal Data protection
2. The Supplier shall, on request, provide the Buyer with a compliance status report with regards to the security requirements without any unjustified delay.
3. The Supplier shall at the request of the Buyer, inform the Buyer how the Supplier complies with the security requirements and what measures the Supplier has taken to comply with the security requirements.
4. The Supplier shall regularly monitor, review and audit sub-contractor´s compliance with the security requirements.
5. The Supplier shall, at the request of the Buyer, provide the Buyer with evidence regarding sub-contractor's compliance with the security requirements.
6. The Buyer has the right to audit how the Supplier and its sub- contractors fulfil the security requirements or corresponding requirements.
7. If an incident falls under legal requirements to be reported to the authorities, the Buyer shall be entitled to perform incident audit within three (3) hours' notice.
8. If an incident does not fall under legal requirements to be reported to the authorities, the Buyer shall be entitled to perform incident audit with five (5) days' notice.
9. As to surveillance requests about Buyer's customers and users received outside of Buyer's normal routines (e.g. if received directly by the Supplier), such must be referred to Buyer.

ir atitiktį nustatytiems reikalavimams (jeigu tokie nustatyti).

5.16. Atitiktis

1. Tiekėjas įsipareigoja laikytis Taikytinų reikalavimų ir sutartinių įsipareigojimų, įskaitant, bet neapsiribojant, susijusių su Asmens duomenų apsauga
2. Pirkėjo prašymu Tiekėjas nedelsiant pateikia Pirkėjui atitikties saugumo reikalavimams ataskaitą.
3. Tiekėjas Pirkėjo prašymu informuoja Pirkėją, kaip Tiekėjas laikosi saugumo reikalavimų ir kokių priemonių Tiekėjas ėmėsi, kad atitiktų saugumo reikalavimus.
4. Tiekėjas reguliariai stebi, tikrina kaip subtiekėjai laikosi saugumo reikalavimų.
5. Tiekėjas Pirkėjo prašymu pateikia Pirkėjui įrodymus, kaip subtiekėjas laikosi saugumo reikalavimų.
6. Pirkėjas turi teisę patikrinti kaip Tiekėjas ir jo subtiekėjai laikosi saugumo reikalavimų ar su jais susijusių reikalavimų.
7. Jei pagal teisės aktus apie incidentą turi būti pranešta institucijoms, Pirkėjas turi teisę incidento auditą atlikti pranešus prieš 3 valandas.
8. Jei apie incidentą pagal teisės aktus neturi būti pranešta valdžios institucijoms, Pirkėjas turi teisę incidento auditą atlikti pranešus prieš 5 dienas.
9. Užklausos apie Pirkėjo klientus ir vartotojus, kurios gautos ne pagal įprastą Pirkėjo tvarką (pvz. jei Tiekėjas jas gavo tiesiogiai), turi būti perduotos Pirkėjui.

Telia Company

6 Information security confidentiality classification description and handling requirements

6.1 Information classification description

Class	Description	Examples of information types
Secret	The unauthorized access or disclosure of information could **seriously damage Buyer**, its organization, critical functions, workforce, business partners and/or its customers.	- annual report and result before they have been released - certain information based on legal requirements or specific customer agreements or non-disclosure agreements
Confidential	The unauthorized access or disclosure of information could **damage** Buyer, its organization, critical functions, workforce, business partners and/or its customers.	- certain information based on legal requirements e.g. personal data of customers or employees - sensitive business plans, strategies and decisions (e.g. marketing plans)
Internal	The unauthorized access or disclosure of information could cause **minor damage** Buyer, its organization, critical functions, workforce, business partners and/or its customers.	- information that is meant for Buyer internal use - communication materials targeted to all Buyer employees e.g. related to Buyer organization, strategy, products, employee services
Public	The unauthorized access or disclosure of information causes **no damage** Buyer, its organization, critical functions, workforce, business partners and/or its customers.	- annual report and result after they have been released - marketing materials and press releases that are published - information that needs to be published based on legal requirements

6. Informacijos konfidencialumo aprašymas ir informacijos tvarkymui taikomi reikalavimai

6.1. Informacijos klasifikavimo aprašymas

Klasė	Aprašymas	Informacijos r pavyzdžiai
Slapta	Neteisėta prieiga prie tokios informacijos arba jos atskleidimas gali padaryti didelę žalą Pirkėjui, jos organizacijai, esminėms funkcijoms, darbuotojams, verslo partneriams ir (arba) jos klientams.	- metinė ataska finansiniai rezu juos paskelbiar - tam tikra infor priskiriama šiai pagal teisės ak reikalavimus ar konkrečius susitarimus su klientais arba informacijos neatskleidimo susitarimus
Konfidencialu	Neteisėta prieiga prie tokios informacijos arba jos atskleidimas **gali padaryti žalą** Pirkėjui, jos organizacijai, esminėms funkcijoms, darbuotojams, verslo partneriams ir (arba) jos klientams.	- tam tikra teisė aktais numatyt informacija, **pv klientų arba darbuotojų as duomenys** - jautrūs verslo strategijos ir sprendimai (pv rinkodaros plar
Vidaus naudojimui	Neteisėta prieiga prie tokios informacijos arba jos atskleidimas gali **nežymiai pakenkti** Pirkėjui, jos organizacijai, esminėms funkcijoms, darbuotojams, verslo partneriams ir (arba) jos klientams.	- informacija, k skirta naudojim Pirkėjui viduje - komunikacinė medžiaga, skirt visiems Pirkėjo darbuotojams, informacija, sus Pirkėjo organiz strategija, prod darbuotojų paslaugomis
Viešam naudojimui	Neteisėta prieiga prie tokios informacijos arba jos atskleidimas **nepakenktų** Pirkėjui, jos organizacijai, esminėms funkcijoms, darbuotojams, verslo partneriams ir (arba) jos klientams.	- metinė ataska finansiniai rezu po jų paskelbin viešai - rinkodaros me ir pranešimai sp kurie yra paske viešai - informaciją, k būti paskelbta remiantis teisė reikalavimais

Telia Company

6.2 Information security confidentiality classification handling requirements

Class	Who may access the information	How to store	How to transfer	How to use	How to assess need for protection (risk based approach)
Secret	Appointed persons only	Logically and physically secure storage i.e. encrypted or locked	Through secure communication channels or in a secure portable storage (locked)	To be used within secure areas that are protected from insight and eavesdropping (by unauthorized persons)	It shall be very hard to break the protection. Only highly motivated and/or resourceful attackers could dismantle the protection.
Confidential	A limited *and controlled* group of persons only	Logically and physically controlled and trusted storage with strict access control	Through secure communication channels or within a controlled and trusted network, or in a secure portable storage	To be used by authorized persons for business purposes only within a controlled workspace or place protected from insight and eavesdropping (by unauthorized persons)	It shall be hard for unauthorized persons to get access to the information. Only well motivated attackers could dismantle the protection.
Internal	Those who perform work for Buyer	Under logical and physical access control	Through protected communication channels or within a trusted network	To be used by authorized persons for business purposes only within a controlled workspace or place protected from insight and eavesdropping (by unauthorized persons)	It shall be unlikely for unauthorized persons to get access to the information. Only motivated attackers could dismantle the protection.
Public	No restrictions	No restrictions	No restrictions	No restrictions	No restrictions

6.2. Informacijos tvarkymo reikalavimai

Klasė	Kas gali gauti prieigą prie informacijos	Kaip informacija turi būti saugoma	Kaip informacija turi būti perduodama	Kaip informacija turi būti naudojama	Kaip įve informa saugojin būtinybė (rizika pagrįsta metodas
Slapta	Tik paskirtieji asmenys	Logiškai ir fiziškai saugioje, tx. šifruotoje arba užrakinamoje, saugykloje	Naudojantis saugiais ryšio kanalais arba saugiomis (rakinamomis) nešiojamomis duomenų saugojimo laikmenomis	Tokia informacija turi būti naudojama saugiose vietose, kurios yra apsaugotos nuo pamatymo ir slapto pasiklausymo (kurį vykdo pašaliniai asmenys)	Turi būti sunku pa apsaugą profesion įsilaužėli galėtų pa apsaugą
Konfidencialu	Tik nibota ir *kontroliuojama* asmenų grupė	Logiškai ir fiziškai kontroliuojamoje ir patikimoje saugykloje, kur užtikrinama griežta patekimo kontrolė	Naudojantis saugiais ryšio kanalais arba kontroliuojamu ir patikimu tinklu arba naudojantis saugiomis nešiojamomis duomenų saugojimo laikmenomis	Tokią informaciją gali naudoti įgalioti asmenys išimtinai verslo tikslais kontroliuojamoje darbo vietoje arba vietoje, kuri yra apsaugota nuo pamatymo ir slapto pasiklausymo (kurį vykdo pašaliniai asmenys)	Turi būti sunku pašalinia asmenim gauti prie prie tokio informac Tik labai profesion įsilaužėli galėtų pa apsaugą
Vidaus naudojimui	Tie, kurie dirba Pirkėjui	Logiškai ir fiziškai kontroliuojant prieigą	Naudojantis apsaugotais ryšio kanalais arba patikimo tinklo ribose	Tokią informaciją gali naudoti įgalioti asmenys išimtinai verslo tikslais kontroliuojamoje darbo vietoje arba vietoje, kuri yra apsaugota nuo pamatymo ir slapto pasiklausymo (kurį vykdo pašaliniai asmenys)	Turi būti mažai tik pašalinia asmenim gauti prie prie tokio informac Tik profesion įsilaužėli galėtų pa apsaugą
Viešam naudojimui	Apribojimų nėra	Apribojimų nėra	Apribojimų nėra	Apribojimų nėra	Apribojim nėra