KIBERNETINIO
SAUGUMO REIKALAVIMAI IŠORĖS ŠALIMS
2022 m. gegužės mėn. 26 d.

CYBER SECURITY REQUIREMENTS FOR EXTERNAL PARTIES
26 May, 2022

1. DOKUMENTO PASKIRTIS, APIMTIS IR TAIKYMAS

1.1. Paskirtis

LKAB “Klaipėdos Smeltė” (toliau – Bendrovė) siekia užtikrinti savo IT sistemų (apima – IT taikomąsias, verslo ir gamybines programas, IT infrastruktūrą, palaikymo sistemas) saugumą. Išorės šalių pasitelkimas kelia neišvengiamą riziką Bendrovės IT aplinkai, kuri gali sukelti neigiamas pasekmes Bendrovės IT sistemoms ar pačiai verslo aplinkai. Išorės šalys teikdamos paslaugas ir prisijungdamos prie Bendrovė IT sistemų privalo vadovautis šia tvarka ir geriausiomis kibernetinio saugumo užtikrinimo rekomendacijomis.

1.2. Apimtis

Ši tvarka galioja tiekėjams, rangovams, konsultantams ir kitiems darbuotojams, įskaitant visą su trečiosiomis šalimis susijusį personalą (toliau - Tiekėjas), kurie turi prieigą ar naudoja Bendrovės IT sistemas.

1.3. Taikymas

Bendrovės nustatyti informacijos ir kibernetinio saugumo reikalavimai taikomi visiems fiziniams ir juridiniams asmenims, jų subrangovams, su kuriais Bendrovė sudaro sutartis ir užsako IT sistemų priežiūros bei vystymo paslaugas. Bendrovės darbuotojams.

1.4. Tikslas

Pagrindinis Bendrovės kibernetinio saugumo tvarkos tikslas dėl išorės šalių - sumažinti galimą riziką, susijusią su Tiekėjų prieiga prie Bendrovės informacinių sistemų ar išteklių, neatsižvelgiant į jų teikiamų paslaugų tipą ir jų santykius su Bendrove (teisinius, sutartinius ar kitokio pobūdžio, nesusijusius su darbo santykiais), siekiant užtikrinti Bendrovės veiklos nepertraukiamumą, apsaugoti Bendrovei ir jos

1. PURPOSE, SCOPE AND APPLICATION OF THE DOCUMENT

1.1. Purpose

LKAB "Klaipėdos Smeltė" (hereinafter - the Company) aims to ensure the security of its IT systems (includes - IT applications, business and production programs, IT infrastructure, support systems). The use of external parties poses an unavoidable risk to the Company's IT environment, which may cause negative consequences for the Company's IT systems or the business environment itself. When providing services and connecting to the Company's IT systems, external parties must follow this procedure and the best recommendations for ensuring cyber security.

1.2. Scope

This procedure applies to suppliers, contractors, consultants and other employees, including all personnel related to third parties (hereinafter referred to as the Supplier), who have access to or use the Company's IT systems.

1.3. Application

The information and cyber security requirements established by the Company apply to all natural and legal persons, their subcontractors, with whom the Company enters into contracts and orders IT system maintenance and development services. Company employees.

1.4. Objective

The main objective of the Company's cyber security procedure regarding external parties is to reduce the potential risks associated with the Suppliers' access to the Company's information systems or resources, regardless of the type of services they provide and their relationship with the Company (legal, contractual or other, not related to employment relations), in order to ensure the continuity of the Company's activities,

klientams priklausančios informacijos konfidencialumą, vientisumą ir prieinamumą.

to protect the confidentiality, integrity and availability of information belonging to the Company and its customers.

2.BENDROSIOS NUOSTATOS

Tiekėjas teikdamas paslaugas ar kurdamas programinę įrangą privalo vadovautis kibernetinio saugumo gerosiomis praktikomis ir standartais (pvz. ISO27001, NIST: National Institute of Standards and Technology, CIS Center for Internet Security, Agile ir pan.).

Bendrovė pasilieka teisę prireikus keisti šią tvarką. Visi jos pakeitimai išplatinami el. priemonėmis.

Jei kuris nors iš šių įsipareigojimų nebus įvykdytas, Bendrovė pasilieka teisę taikyti prevencines ir teisines priemones, kurias ji laiko tinkamomis, Tiekėjo, su kuriuo sudaryta sutartis, atžvilgiu.

Tiekėjai, kai to reikalaujama, privalo pateikti Bendrovei informaciją apie su teikiama paslauga susijusių asmenų funkcijas ir pareigas, kontaktų informaciją, ir pranešti apie bet kokius pokyčius (naujų darbuotojų priėmimą, atleidimą, pakeitimą ar funkcijų ar pareigų pasikeitimą), susijusius su šiais santykiais.

Tiekėjai privalo užtikrinti, kad visi jų darbuotojai būtų apmokyti tinkamai teikti paslaugas Bendrovei, tiek konkrečiais paslaugos teikimo klausimais, tiek apskritai informacijos saugumo klausimais.

Tiekėjai privalo užtikrinti, kad visi jo darbuotojai, taip jo samdomos išorės šalys būtų susipažinę su šios tvarkos nuostatomis, suprastų Bendrovės kibernetinio saugumo politikos reikalavimus ir įsipareigotų jų laikytis. Bendrovė bet kuriuo metu gali pareikalauti informacijos ar įrodymų, kaip laikomasi sutartinių reikalavimų.

Bendrovė pasilieka teisę atlikti patikrinimus, susijusius su Tiekėjo teikiamomis paslaugomis ar prižiūrimomis sistemomis, siekiant užtikrinti kibernetinį saugumą Bendrovės IT sistemose ir infrastruktūroje.

2. GENERAL PROVISIONS

When providing services or developing software, the supplier must follow cyber security good practices and standards (e.g. ISO27001, NIST: National Institute of Standards and Technology, CIS Center for Internet Security, Agile, etc.).

The company reserves the right to change this procedure if necessary. All its changes are distributed by e-mail, web page or etc.

If any of these obligations are not fulfilled, the Company reserves the right to apply preventive and legal measures, which it considers appropriate, against the Supplier with whom the contract has been concluded.

Suppliers, when required, must provide the Company with information about the functions and responsibilities of the persons providing the services, contact information, and notifications of any changes (admission of new employees, dismissal, replacement of functions or change of duties) related to this relationship.

Suppliers must ensure that all their employees are trained to properly provide services to the Company, both in specific issues of service provision and in general information security issues.

Suppliers must ensure that all their employees, as well as external parties hired by them, are familiar with the provisions of this procedure, understand the requirements of the Company's cyber security policy and undertake to comply with them. The Company may at any time request information or evidence of compliance with contractual requirements.

The Company reserves the right to perform inspections related to the services provided or systems maintained by the Supplier in order to ensure cyber security in the Company's IT systems and infrastructure.

2.1. Informacijos konfidencialumas

Visa informacija, dokumentacija, programos, programiniai kodai, verslo procesai, susiję su Bendrove ar jos verslu, su kuria Tiekėjai gali susipažinti teikdami paslaugas, laikoma konfidencialia informacija. Atitinkamai ši informacija turi būti prieinama, ja turi būti keičiamasi ir ji turi būti tvarkoma laikantis tikslų, kurie aprašyti paslaugų teikimo sutartyse. Atitinkamai abi šalys įsipareigoja laikytis konfidencialumo sutarties įsipareigojimų visą paslaugos teikimo laikotarpį, taip pat ir suderintą laikotarpį po santykių nutraukimo. Prieš pradedant teikti paslaugas ar dalintis informacija, Tiekėjas su Bendrove pasirašo konfidencialumo sutartį.

Baigus teikti paslaugas, visi ištekliai ir informacija, kuria galėjo naudotis Tiekėjas siekiant tinkamai atlikti paslaugą, turi būti grąžinti Bendrovei. Tiekėjas, pasibaigus sutarties galiojimo terminui, įsipareigoja saugiai sunaikinti sutartinių įsipareigojimų įvykdymui surinktą Bendrovei priklausančią informaciją, Bendrovei pareikalavus – pateikti informacijos sunaikinimo įrodymus.

2.2. Intelektinė nuosavybė

Būtina užtikrinti, kad būtų laikomasi teisinių apribojimų naudojant visą medžiagą, saugomą intelektinės nuosavybės teisės aktais. IT programų naudojimas be atitinkamų licencijų, Bendrovės informacinėse sistemose yra griežtai draudžiamas. Draudžiama naudoti, perduoti, transformuoti ar viešai skelbti bet kokio tipo kūrinius ar išradimus, kurie priklauso Bendrovei intelektinės nuosavybės teisėmis, be atitinkamo raštiško jos leidimo.

2.3.Keitimasis informacija

Visi informacijos mainai tarp Bendrovės ir Tiekėjų vykdomi pagal atitinkamą prekių/paslaugų teikimo ir/arba konfidencialumo sutartį taip, kad ši informacija negalėtų būti naudojama už šios sutarties ribų arba kitais tikslais.

Kalbant apie keitimąsi informacija, toliau nurodyta veikla laikoma neleistina:

2.1. Confidentiality of information

All information, documentation, programs, software codes, business processes related to the Company or its business, with which the Suppliers can get acquainted while providing services, are considered as confidential information. Accordingly, this information must be accessible, exchanged and managed in accordance with the purposes described in the service contracts. Accordingly, both parties undertake to comply with the obligations of the confidentiality agreement for the entire period of service provision, as well as for an agreed period after the termination of the relationship. Before starting to provide services or share information, the Supplier signs a confidentiality agreement with the Company.

Upon completion of the services, all resources and information that the Supplier may have used to properly perform the service must be returned to the Company. After the expiration of the contract, the supplier undertakes to securely destroy the information belonging to the Company collected for the fulfillment of contractual obligations, and upon the request of the Company - to provide evidence of the destruction of the information.

2.2. Intellectual property

It is necessary to ensure that legal restrictions are observed when using all material protected by intellectual property laws. The use of IT programs without appropriate licenses in the Company's information systems is strictly prohibited.

The use, transfer, transformation or public announcement of any type of works or inventions owned by the Company by intellectual property rights is prohibited without the appropriate written permission of the Company.

2.3. Exchange of information

All information exchanges between the Company and Suppliers are carried out in accordance with the relevant goods/services provision and/or confidentiality agreement in such a way that this information cannot be used outside of this agreement or for other purposes.

In relation to the exchange of information, the following activities are considered impermissible:

- autorių teisių saugoma informaciją, pažeidžiančios intelektinės apsaugos teisės aktus, perdavimas ar priėmimas;

- bet kokios pornografinės ar seksualinio pobūdžio medžiagos, rasistinės, diskriminacinės medžiagos perdavimas ar priėmimas;

- bet kokių kitų rūšių pareiškimų ar pranešimų, kurie gali būti laikomi įžeidžiančiais ar neteisėtais, perdavimas ir priėmimas;

- neskelbtinos informacijos perdavimas ar priėmimas, išskyrus atvejus, kai tai leidžiama raštu ir elektroniniu būdu perduodama užšifruota informacija;

- saugomos informacijos perdavimas neįgaliotoms trečiosioms šalims;

- su sutartimi nesusijusios informacijos perdavimas ar priėmimas;

- dalyvavimas internetinėje veikloje, pavyzdžiui, lošimai, naujienų grupės, žaidimai ar kitoje veikloje, tiesiogiai nesusijusioje su paslaugos teikimu;

- internete ir kitose aplinkose draudžiama bet kokia veikla, galinti pakenkti Bendrovės įvaizdžiui ir reputacijai.

2.4. Tinkamas Bendrovės išteklių naudojimas

Bendrovės ištekliai, kuriais naudojasi Tiekėjai, turi būti naudojami tik paslaugų teikimo įsipareigojimams ir tikslams vykdyti. Jokiomis aplinkybėmis jų negalima naudoti veiklai, nesusijusiai su paslaugos teikimo tikslu, arba veiklai, kuri gali būti laikoma neteisėta, pavyzdžiui, trečiųjų šalių intelektinei nuosavybei padaryta žala, duomenų apsaugos taisyklių pažeidimai ir pan.

- transmission or reception of copyrighted information that violates intellectual property legislation;

- transmitting or receiving any pornographic or sexual material, racist, discriminatory material;

- transmitting and receiving any other type of statements or messages that may be considered offensive or illegal;

- transmission or reception of confidential information, except for cases where it is permitted in writing and electronically transmitted encrypted information;

- transfer of protected information to unauthorized third parties;

- transmission or receipt of information not related to the contract;

- participation in online activities such as gambling, newsgroups, games or other activities not directly related to the provision of the service;

- on the Internet and in other environments, any activity that may harm the image and reputation of the Company is prohibited.

2.4. Appropriate use of the Company's resources

The Company's resources used by the Suppliers must be used only to fulfill the obligations and objectives of service provision. Under no circumstances they cannot be used for activities unrelated to the purpose of providing the service, or for activities that may be considered illegal, such as damage to third-party intellectual property, violations of data protection regulations, etc.

Tiekėjai įsipareigoja naudoti Bendrovės išteklius, laikydamiesi Bendrovės kibernetinio saugumo politikos.

Siekdama užtikrinti tinkamą Bendrovės išteklių naudojimą, Bendrovė gali įdiegti kontrolės, stebėjimo ar audito priemones, kurios, jos nuomone, yra būtinos, kai to reikia kibernetiniam saugumui užtikrinti.

Jei nustatoma, kad Tiekėjas arba bet kuris jo darbuotojas netinkamai naudojo Bendrovės išteklius arba informaciją, apie šią aplinkybę turi būti pranešta Tiekėjui, kad būtų galima imtis atitinkamų veiksmų. Bendrovė pasilieka teisę imtis bet kokių teisinių veiksmų savo teisėms apsaugoti. Bet kokia informacija, bylos, dokumentai, patekę į Bendrovės tinklą arba į bet kokią kitą prie jo prijungtą įrangą internetu, el. paštu ar bet kokiu kitu būdu, turi atitikti šioje tvarkoje nustatytus reikalavimus, ypač tuos, kurie susiję su intelektine nuosavybe, asmens duomenų apsauga, virusų ir kenkėjiškų programų kontrole.

2.5. Tiekėjo įsipareigojimai

Tiekėjai privalo užtikrinti, kad visi jų darbuotojai, kurie, vykdydami savo funkcijas, turi prieigą prie Bendrovės informacinių sistemų, duomenų ar kitų išteklių privalo laikytis šių pagrindinių principų:

• Tiekėjas, turintis prieigą prie Bendrovės informacinių sistemų, yra atsakingas už savo darbuotojų atliekamą veiklą, todėl labai svarbu, kad prisijungimo duomenys būtų žinomi tik tam asmeniui, kuriam jie skirti ir jokiomis aplinkybėmis nebūtų atskleisti kitiems asmenims;

• Tiekėjo darbuotojams draudžiama naudoti kito vartotojo ar kolegos prisijungimo duomenis;

• Tiekėjai turi būti susipažinę su visais IT kibernetinio saugumo reikalavimais, tvarkomis, kurios taikomos Bendrovėje, ir jų laikytis;

• Tiekėjo darbuotojai, turintys prieigą prie Bendrovės informacinių sistemų, privalo pasirinkti kokybiškus slaptažodžius (turinčius ne mažiau kaip

Suppliers undertake to use the Company's resources in compliance with the Company's cyber security policy.

In order to ensure the proper use of the Company's resources, the Company may implement control, monitoring or audit measures that it deems necessary when it is necessary to ensure cyber security.

If it is determined that the Supplier or any of its employees have misused the Company's resources or information, this circumstance must be reported to the Supplier so that appropriate action can be taken. The Company reserves the right to take any legal action to protect its rights.
Any information, files, documents that have entered the Company's network or any other equipment connected to it via the Internet, e-mail by mail or in any other way, must meet the requirements set forth in this procedure, especially those related to intellectual property, personal data protection, virus and malware control.

2.5. Obligations of the supplier

Suppliers must ensure that all their employees who, in the performance of their functions, have access to the Company's information systems, data or other resources must comply with the following basic principles:

• The supplier who has access to the Company's information systems is responsible for the activities performed by his employees, therefore it is very important that the login data is known only to the person for whom it is intended and should not be disclosed to other persons under any circumstances;

• Employees of the supplier are prohibited from using login data of another user or colleague;

• Suppliers must be familiar with all IT cyber security requirements, procedures that are applied in the Company and comply with them;

• The Supplier's employees who have access to the Company's information systems must choose high-quality passwords (with at least 14 characters

14 simbolius, sudarytus iš didžiųjų ir mažųjų raidžių, skaitmenų ir specialiųjų ženklų, kuriuose nėra jokios lengvai atspėjamos informacijos);

consisting of capital and lowercase letters, numbers and special characters that do not contain any easily guessed information);

• Tiekėjo darbuotojai, turintys prieigą prie Bendrovės informacinių sistemų, privalo pakeisti savo laikinuosius slaptažodžius arba kai yra požymių, kad kiti naudotojai galėjo juos žinoti;

• Employees of the Supplier who have access to the Company's information systems must change their temporary passwords or when there are indications that other users may have known them;

• Atlikus darbus prieiga prie sistemų turi būti deaktyvuota ir/arba išjungta;

• Access to systems must be deactivated and/or turned off after work is completed;

upplier employees who have access to the

• Tiekėjo darbuotojai, turintys prieigą prie Bendrovės informacinių sistemų, turi užtikrinti, kad jų įranga yra apsaugota, kai ji lieka be priežiūros;

• Company's information systems must ensure that their equipment is protected when it is left unattended;

• Slaptažodžiai negali būti saugomi ar perduodami atviru tekstu. Tik laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo naudotojo vardo, jeigu IT sistemų naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio ar nėra techninių galimybių IT sistemų naudotojui perduoti slaptažodį šifruotu kanalu ar saugiu elektroniniu ryšių tinklu;

• Passwords cannot be stored or transmitted in “open text” format. Only a temporary password can be transmitted in “open text” format, but separately from the user's name, if the user of the IT systems does not have the ability to decrypt the received encrypted password or there is no technical possibility to transmit the password to the user of the IT systems via an encrypted channel or a secure electronic communication network;

• Visose IT sistemose, prieš pradedant jas eksploatuoti, privaloma pakeisti standartinius (gamintojų) slaptažodžius į Bendrovėje nustatytus slaptažodžių tvarkos reikalavimus atitinkančius slaptažodžius, pakeisti slaptažodžiai perduodami IT skyriui;

• In all IT systems, before putting them into operation, it is mandatory to change the standard (manufacturer) passwords to passwords that meet the password procedure requirements set by the Company, the changed passwords are transferred to the IT department;

• IT sistemose turi būti išjungiamos visos nereikalingos gamyklinės naudotojų paskyros (tame tarpe svečio „Guest“ paskyra);

• All unnecessary factory user accounts must be disabled in IT systems (including the Guest account);

• Bet kokia nesankcionuota prieiga prie Bendrovės IT sistemų ir duomenų ar įrangos - draudžiama;

• Any unauthorized access to the Company's IT systems and data or equipment is prohibited;

• Prieiga prie Bendrovės IT sistemų turi būti suteikiama vadovaujantis principu „Būtina darbui“;

• Access to the Company's IT systems must be granted in accordance with the principle "Necessary for work";

• Paprastiems vartotojams draudžiama suteikti administratoriaus teises;

• Ordinary users are prohibited from granting administrator rights;

• Tiekėjo darbuotojai, turintys prieigą prie Bendrovės informacinių sistemų, turi laikytis "švaraus stalo" taisyklių, kad apsaugotų popierinius dokumentus, IT laikmenas ir nešiojamąsias laikmenas ir sumažintų neteisėtos prieigos prie informacijos, jos praradimo ar sugadinimo riziką tiek įprastomis darbo valandomis, tiek ne darbo valandomis (popierinius dokumentus ir IT laikmenas laikyti užrakintus, užrakinti naudotojų sesijas, kai jie paliekami be priežiūros, apsaugoti informacijos priėmimo ir perdavimo taškus, pašalinti apsaugą ir t. t.)

• Tiekėjo darbuotojai, turintys prieigą prie Bendrovės informacinių sistemų, be raštiško leidimo negali laužtis, apeiti ar kaip kitaip pažeisti Bendrovės IT saugumo sistemas. Tiekėjo darbuotojams draudžiama rinkti ir analizuoti tinklo duomenų srautą, išskyrus atvejus, kai tai daroma su Bendrovės sutikimu;

• Prieš atliekant bet kokius pakeitimus Bendrovės Informacinėse sistemose ar infrastruktūroje, Tiekėjas privalo šios pakeitimus suderinti su Bendrove ir gauti jos leidimą. Pakeitimų derinimas vykdomas rašytine forma.

• Supplier employees who have access to the Company's information systems must follow "clean table" rules to protect paper documents, IT media and portable media and reduce the risk of unauthorized access to, loss or corruption of information, both during normal working hours and outside of working hours (keep paper documents and IT media locked, lock user sessions when left unattended, protect information reception and transmission points, remove security, etc.)

• The supplier's employees, who have access to the Company's information systems, may not hack, circumvent or otherwise violate the Company's IT security systems without written permission. Employees of the Supplier are prohibited from collecting and analyzing network data traffic, except in cases where this is done with the consent of the Company;

• Before making any changes to the Company's Information Systems or infrastructure, the Supplier must coordinate these changes with the Company and obtain its permission. Coordination of changes is carried out in written form.

2.6. Įrangai keliami saugumo reikalavimai

Visi įrenginiai, turintys prieigą prie Bendrovės informacinių sistemų, nepriklausomai nuo to, kam jie priklauso, turi atitikti Bendrovės nustatytą IT kibernetinio saugumo politiką, ypatingą dėmesį skiriant toliau nurodytoms aplinkybėms:

• prieiga prie sistemų visada suteikiama naudojant vartotojo vardą ir slaptažodį, papildomai rekomenduojamos kelių faktorių (MFA) autentifikavimo priemonės;

• visa įrenginiuose esanti programinė įranga turi būti licencijuota, neviršyti gamintojo numatytą gyvavimo ciklą, įdiegtos naujausios saugumo pataisos ir atnaujinimai;

• įrenginiuose turi būti įdiegtos, veikiančios ir atnaujintos apsaugos nuo kenkėjiškos programinės įrangos priemonės;

2.6 Safety requirements for equipment

All devices that have access to the Company's information systems, regardless of who owns them, must comply with the IT cyber security policy established by the Company, paying special attention to the following circumstances:

• access to systems is always provided using a username and password, multi-factor authentication (MFA) is additionally recommended;

• all software in the devices must be licensed, not exceed the manufacturer's expected life cycle, the latest security fixes and updates installed;

• devices must have anti-malware protection installed, working and updated;

• nustatyta ekrano apsauga, kuri įsijungtų po 15 minučių neveikimo. Įrenginiui atrakinti reikalauti slaptažodžio arba alternatyvios priemonės, užtikrinančios, kad įrenginiu negalėtų naudotis neįgaliotas asmuo;

• įrenginiuose draudžiama visa programinė įrangą, bylos ar kita informacija, prieštaraujanti Bendrovės saugumo tvarkai arba galinti pažeisti Bendrovės IT informacines sistemas. Šis punktas apima visas priemones, kuriomis siekiama surinkti informaciją apie vartotojus arba gauti neteisėtą prieigą, pavyzdžiui, šnipinėjimo, tinklo skenavimo priemones, slaptažodžių nustatymo priemones ir pan.

Tiekėjai turi užtikrinti, kad sistemų pajėgumai būtų tinkamai valdomi, vengiant galimų šių sistemų išsijungimų ar veikimo sutrikimų dėl resursų perpildymo. Projektuojant sistemas turi būti numatytas minimalus 30% resursų rezervas.

Projektuojant kritines Bendrovės IT sistemas, numatyti sistemų dubliavimo (angl. – „High availability“), atstatymo nelaimės atveju (ang. – „Disaster recovery“) sprendimus.

2.7. Nuotolinio darbo saugumo reikalavimai

Įvertinus galimas rizikas ir suteikiant Tiekėjui galimybę dirbti nuotolinėje kompiuterizuotoje darbo vietoje priklausančioje Tiekėjui bei suteikiant nuotolinę prieigą prie Bendrovės IT sistemų Bendrajame duomenų tinkle būtina:

• prieiga, kurią Tiekėjas naudoja jungtis prie Bendrovės sistemų per nuotolinę prieigą, turi būti įjungta tik tuo laikotarpiu, kai ji tam būtina, ir išjungiama, kai ji nenaudojama;

• nuotolinio ryšio sujungimas ir nuotolinės prieigos suteikimas vyksta vadovaujantis principu „Būtina darbui“;

• prieiga prie Bendrovės IT sistemų leidžiamos tik per VPN tinklą, privaloma naudoti kelių faktorių autentifikavimą (MFA);

• a screen saver set to activate after 15 minutes of inactivity. Require a password to unlock the device or an alternative means to ensure that the device cannot be used by an unauthorized person;

• all software, files or other information that contradicts the Company's security procedures or may damage the Company's IT information systems are prohibited in the devices. This clause includes all means to collect information about users or gain unauthorized access, such as spying, network scanning tools, password cracking tools, etc.

Suppliers must ensure that the capacity of the systems is properly managed, avoiding possible shutdowns or malfunctions of these systems due to resource overflow. When designing the systems, a minimum resource reserve of 30% must be provided.

When designing the Company's critical IT systems, solutions for system duplication (English - "High availability") and restoration in the event of a disaster (English - "Disaster recovery") are provided.

2.7. Remote work security requirements

After assessing the possible risks and giving the Supplier the opportunity to work at a remote computerized workplace owned by the Supplier and providing remote access to the Company's IT systems in the Common Data Network, it is necessary:

• the access used by the Supplier to connect to the Company's systems via remote access must be enabled only during the period when it is necessary for this, and disabled when it is not used;

• connection of a remote connection and provision of remote access takes place in accordance with the principle "Necessary for work";

• access to the Company's IT systems is allowed only through the VPN network, multi-factor authentication (MFA) must be used;

• leidžiama jungtis prie Bendrovės IT sistemų ir programų, tik per išorės šaliai paruoštą aplinką - PAM sistemą ar „JumpBox“ serverį, tam skirtą tinklo potinklį (VLAN). Visi išorės šalių veiksmai gali būti įrašomi ar kaip kitaip fiksuojami;

• draudžiama nuotolinė prieiga, jeigu nenaudojamas saugus VPN ryšys. Jungtis apeinant VPN tinklą, PAM ar „JumpBox“ serverį, galima tik išimtinais atvejais, gavus Bendrovės leidimą;

• Privaloma įsitikinti, kad IT sistemos, kompiuterinė įranga ir duomenų tinklai, iš kurių jungiamasi per nuotolį, yra saugūs ir patikimi (atnaujinta operacinė sistema ir kita programinė įranga, įdiegta antivirusinė programinės įranga, įjungta ir sukonfigūruota ugniasienė ir t.t.).

2.8. Saugumo incidentų pranešimai

Tiekėjai privalo nedelsdami pranešti Bendrovės IT skyriui (elektroniniu paštu it@smelte.lt arba tiesiogiai IT skyriaus darbuotojui) apie visus pastebėtus ar įtariamus kibernetinio saugumo incidentus, pažeidžiamumus ar grėsmes, aptiktas Bendrovės informacinėse sistemose.

3. SAUGUMO PRINCIPAI

3.1. Programinės įrangos saugumas

Tiekėjai, kurie atlieka programinės įrangos kūrimo, modifikavimo, konfigūravimo darbus ir (arba) taikomųjų programų testavimus Bendrovės informacinėse sistemose, turi laikytis šių reikalavimų:

• programinės aplinkos, kuriose vykdomas kūrimo, diegimo, konfigūravimo ar testavimo veikla, turi būti atskirta nuo gamybinių aplinkų;

• visos prieigos prie informacinių sistemų, kuriose saugoma ar apdorojama informacija, turi būti apsaugotos ugniasiene;

• visą užsakomosios programinės įrangos kūrimo procesą kontroliuoja ir prižiūri Bendrovė. Tiekėjas sukurtą programinės įrangos išeities kodą, konfigūracijas, vartotojus ir jų slaptažodžius ir pan. perduoda IT skyriui. Programų išeities kodas ir jo pakeitimai talpinami Bendrovei priklausančioje

• it is allowed to connect to the Company's IT systems and programs, only through an environment prepared for an external party - PAM system or "JumpBox" server, dedicated network subnet (VLAN). All actions of external parties may be recorded or otherwise recorded;

• remote access is prohibited unless a secure VPN connection is used. Connecting by bypassing the VPN network, PAM or JumpBox server is possible only in exceptional cases, with the permission of the Company;

• It is necessary to make sure that the IT systems, computer equipment and data networks from which remote connections are made are secure and reliable (updated operating system and other software, installed anti-virus software, enabled and configured firewall, etc.).

2.8. Security incident reports

Suppliers must immediately notify the Company's IT department (by e-mail it@smelte.lt or directly to an employee of the IT department) of all observed or suspected cyber security incidents, vulnerabilities or threats detected in the Company's information systems.

3. SECURITY PRINCIPLES

3.1. Software security

Suppliers who perform software development, modification, configuration work and/or application testing in the Company's information systems must comply with the following requirements:

• software environments in which development, installation, configuration or testing activities are performed must be separated from production environments;

• all accesses to information systems where information is stored or processed must be protected by a firewall;

• the entire process of custom software development is controlled and supervised by the Company. Software source code, configurations, users and their passwords, etc. created by the supplier is forwarded to the IT department. The source code of the programs and its changes are

programaminio kodo valdymo paskyroje (GIT ar pan.);

stored in the program code management account belonging to the Company (GIT or similar);

• programinės įrangos specifikacijose turi būti aiškiai nurodyti saugumo reikalavimai, kurių turi būti laikomasi kuriant Bendrovei skirtą programinę įrangą;

• the software specifications must clearly indicate the security requirements that must be met when developing the software for the Company;

• vartotojų identifikavimas, autentifikavimas, prieigos kontrolė ir t.t. įtraukiama į programinės įrangos projektavimo, kūrimo, įgyvendinimo ir naudojimo ciklą;

• user identification, authentication, access control, etc. is included in the software design, development, implementation and use cycle;

• draudžiama prisijungimo prie IT sistemų informaciją į programuoti į išeities kodą;

• it is forbidden to program the information of connection to IT systems into the source code;

• kuriant programinę įrangą būtina atsižvelgti į kuriamo programinio kodo higieną (nenaudoti pasenusių bibliotekų, neištaisytų pažeidžiamumo klaidų);

• when developing software, it is necessary to take into account the hygiene of the developed software code (do not use outdated libraries, uncorrected vulnerability errors);

• kuriant programinę įrangą būtina atsižvelgti į vidinius Bendrovės verslo procesus, užtikrinti, kad nauja programinė įranga nesugadintų ar kaip kitaip neigiamai paveiktų Bendrovės informacines sistemas ar informaciją;

• when developing software, it is necessary to take into account the Company's internal business processes, to ensure that the new software does not damage or otherwise negatively affect the Company's information systems or information;

• testavimo aplinkoje pagrindinių duomenų bazių duomenys turi būti naudojami tik tada, kai yra įmanoma užtikrinti, kad taikomos saugumo priemonės yra lygiavertės gamybinėje aplinkoje taikomoms priemonėms;

• in the testing environment, the data of the main databases must be used only when it is possible to ensure that the applied security measures are equivalent to the measures applied in the production environment;

• programinio kodo klaidos turi būti rodomos tik sistemas prižiūrintiems administratoriams;

• program code errors must be displayed only to system administrators;

• Tiekėjas atliekant informacinių sistemų bandymus užtikrina, kad nėra palikta informacijos nutekėjimo spragų ir visi galimi pažeidimai yra užblokuoti, tik tada programinę įranga gali būti perkelta į gamybinę aplinką;

• During information system tests, the supplier ensures that there are no information leakage gaps and all possible violations are blocked, only then the software can be transferred to the production environment;

• Bendrovė atlieka periodinius informacinių sistemų pažeidžiamumo skanavimus, kurių metu siekiama įsitikinti ar naujai įdiegtoje, ar Tiekėjo prižiūrimoje sistemoje nėra palikta kibernetinio saugumo pažeidžiamumo spragų. Nustačius

• The company performs periodic vulnerability scans of information systems, during which the aim is to make sure that there are no cyber security vulnerability gaps left in the newly installed system or the system maintained by the

tokius pažeidžiamumas, Tiekėjas juos nedelsiant pašalina.

3.2.Tęstinumo valdymas

Tiekėjai prižiūrintis Bendrovės IT kritines sistemas turi turėti, Bendrovei pareikalavus pateikti, veiklos tęstinumo ir nelaimės atveju veiklos atkūrimo (angl. – „Disaster recovery“) planą. Šie planai turi būti parengti remiantis rizikos vertinimu, siekiant nustatyti visus rizikos veiksnius, kurie gali pakenkti Bendrovės veiklai.

Tiekėjai turi užtikrinti, kad jų veiklos tęstinumo ir atkūrimo planai, yra veikiantys, nelaimės atveju Bendrovės veikla būtų atkurta į pradinę padėtį.

Tiekėjai prižiūrintis Bendrovės IT kritines sistemas turi turėti, Bendrovei pareikalavus pateikti, rizikos valdymo priemonių planą, veiklos draudimus.

3.3. Tinklo saugumas

Bendrovės tinklai turi būti tinkamai valdomi ir kontroliuojami, užtikrinant, kad juose nebūtų nekontroliuojamų prieigų ar jungčių, kurių rizika nėra identifikuota ir suvaldyta.

Tinklai, kuriais galima naudotis Bendrovės infrastruktūra, turi būti tinkamai apsaugoti ir atitikti saugos prisijungimo (angl. – „VPN“) tvarkos reikalavimus.

3.4. Pakeitimų valdymas

Tiekėjai turi užtikrinti, kad visi paslaugai teikti naudojamos infrastruktūros pakeitimai būtų kontroliuojami ir autorizuojami, garantuojant, kad joks nekontroliuojamas komponentas nebūtų Bendrovės infrastruktūros dalis.

Tiekėjas patikrinta, ar visa nauja įranga ir/ar sprendimai, kuriuos jis diegia Bendrovės infrastruktūroje, tinkamai veikia ir atitinka tikslus, dėl kurių jie buvo diegiami.

Visi pakeitimai turi būti įgyvendinami pagal gamintojų ar kibernetinės saugos nustatytus reikalavimus ir rekomendacijas, kad nebūtų neigiamo ar nenumatyto šalutinio poveikio jų veikimui ar saugumui.

Supplier. Upon detection of such vulnerabilities, the Supplier shall remove them immediately.

3.2. Continuity management

Suppliers maintaining the Company's critical IT systems must have a business continuity and disaster recovery plan, upon request by the Company. These plans must be prepared based on a risk assessment to identify all risk factors that may harm the Company's operations.

Suppliers must ensure that their business continuity and recovery plans are in place to restore the Company's operations to their original state in the event of a disaster.

Suppliers who oversee the Company's IT critical systems must have, upon request by the Company, a plan of risk management measures, operational insurances

3.3. Network security

The company's networks must be properly managed and controlled, ensuring that there are no uncontrolled accesses or connections for which risks have not been identified and managed.

The networks through which the Company's infrastructure can be used must be properly protected and comply with the requirements of the security connection ("VPN") procedure.

3.4. Change management

Suppliers must ensure that all changes to the infrastructure used to provide the service are controlled and authorized, guaranteeing that no uncontrolled component is part of the Company's infrastructure.

The Supplier has checked whether all new equipment and/or solutions that he installs in the Company's infrastructure work properly and meet the goals for which they were installed.

All changes must be implemented in accordance with the requirements and recommendations established by manufacturers or cyber security, so that there are no negative or unforeseen side effects on their performance or security.

Pakeitimų valdymo procedūros turi garantuoti, kad kritinių komponentų pakeitimai būtų sumažinti iki minimumo ir būtų atliekami tik tie, kurie yra būtini ar gali padaryti žalos Bendrovės veiklai.

Change management procedures must guarantee that changes to critical components are reduced to a minimum and that only those that are necessary or may cause damage to the Company's operations are carried out.

Tiekėjai užtikrina, kad visos naujai diegiamos ar keičiamos Bendrovės informacinės sistemos, turi būti tinkamai dokumentuojamos, pateikiamos schemos, planai, aprašymai, instrukcijos ir t.t.

Tiekėjas perspėja Bendrovę apie visus techninius pažeidžiamumus, susijusius su Bendrovės infrastruktūra ir sistemomis, siekiant sukontroliuoti galimas rizikas.

Suppliers ensure that all newly installed or changed information systems of the Company must be properly documented, diagrams, plans, descriptions, instructions, etc. must be provided.

The Supplier warns the Company about all technical vulnerabilities related to the Company's infrastructure and systems in order to control possible risks.