

BALTIC DATA CENTER

SAUGOS POLITIKA

Versija: 2.2

Pakeitimų istorija:

<i>Versija</i>	<i>Data</i>	<i>Autorius</i>	<i>Kas keista</i>	<i>Peržiūrėta ir patvirtinta, (tvirtintojas, data)</i>
1.0	2006.07.05	Gediminas Pilipavičius	Pirma dokumento versija	Generalinio Direktoriaus Įsakymas Nr. IS-1678 2006.08.03
2.0	2007.06.15	Jevgenij Kaplanas	Papildyti saugos principai	Generalinio Direktoriaus Įsakymas Nr. 2007
2.2	2008.09.15	Jevgenij Kaplanas	Papildyta ir atnaujinta	Generalinio Direktoriaus Įsakymas Nr. 2008

TURINYS

1. APIMTIS	3
2. INFORMACIJOS SAUGOS APIBRĖŽIMAS	3
3. INFORMACIJOS SAUGOS TIKSLAS	3
4. INFORMACIJOS SAUGUMO POLITIKOS IŠIMTYS	4
5. TEISINIAI REIKALAVIMAI, KURIE RODO KRYPTĮ INFORMACIJOS SAUGOS VEIKLAI.....	4
6. GRĖSMĖS SAUGAI	4
7. KLIENTO IR PASLAUGŲ TEIKĖJO ATSAKOMYBĖS	4
8. ĮMONĖS SAUGOS VALDYMAS	5
8.1 Rizikų valdymo komitetas	5
8.2 Skyrių lygio saugos valdymas	6
8.3 Su Sauga susijusių incidentų valdymas	6
8.4 Pranešimų apie su sauga susijusius incidentus valdymas	6
8.5 Saugos priemonių prioritetizavimas	6
9. SAUGOS PRINCIPAI	7
9.1 Pagrindiniai informacijos saugos įgyvendinimo principai	7
9.2 Su darbuotojais susijusi sauga	7
9.3 Saugos apmokymai	8
9.4 Fizinė sauga	8
9.5 Veiklos tęstinumo valdymas.....	9
9.6 Licenzijų, techninės ir programinės įrangos valdymas	9
9.7 Sistemų priežiūra	9
9.8 Informacijos laikmenų valdymas ir sauga.....	9
9.9 Patekimo į sistemą kontrolė	10
9.10 Vartotojų identifikavimas ir slaptažodžių valdymas.....	10
9.11 Informacinių vertybių klasifikacija ir kontrolė	10
9.12 Apsauga nuo piktavališkos programinės įrangos	10
9.13 Atitikimas	10
9.14 Kova prieš kibernetinius nusikaltimus	11
9.15 Įstatymų ir taisyklių reikalavimų laikymasis	11
10. POLITIKOS ĮSIGALIOJIMO DATA.....	11

1. APIMTIS

Įmonės sauga – neatsiejama įmonės veiklos dalis, siekiant įmonės verslo tikslų. Įmonės saugos tikslas yra sukurti ir išsaugoti pačias palankiausias įmonės verslo sąlygas, apsaugoti jos veiklą, visapusiškai valdyti grėsmes. Įmonės saugos mes siekiame nuosekliai tobulindami ir įgyvendindami įmonės saugos politiką.

Informacijos saugumas pasiekiamas įgyvendinant tinkamą priežiūros metodų, kurių tarpe yra politikos, procedūros, tvarkos, rinkinį. Šie priežiūros metodai yra įdiegti, siekiant užtikrinti, kad ypatingi organizacijos saugumo tikslai būtų vykdomi.

UAB „BALTIC DATA CENTER“ (toliau vadinama – BDC) Saugos politika (toliau šiame dokumente nurodoma kaip Saugos Politika) apibrėžia privalomus saugos reikalavimus, kurių turi būti laikomasi įmonėje. Politika detaliau yra aprašoma įmonės patvirtintomis saugos tvarkomis, instrukcijomis, procedūromis, kurios yra privalomos, bei rekomendacijomis, kurių patariama laikytis.

Visa įmonės saugos dokumentacija yra tvarkoma lietuvių kalba. Saugos Politika yra klasifikuojama kaip viešas dokumentas ir todėl yra prieinama visam įmonės personalui, subrangovams bei partneriams.

Saugos tvarkos, instrukcijos, procedūros bei rekomendacijos yra klasifikuojamos kaip vidiniai dokumentai ir todėl yra prieinamos tik įmonės darbuotojams, jei atskirais atvejais nėra nustatyta kitaip.

2. INFORMACIJOS SAUGOS APIBRĖŽIMAS

Informacijos sauga – veikla, skirta duomenų perdavimo ir naudojimo konfidencialumui, vientisumui ir patikimumui garantuoti.

Konfidencialumas reiškia, kad informacija gali naudotis tik tie, kurie yra įgalioti ja naudotis.

Vientisumas reiškia, kad visuose darbo su informacija etapuose ji išlieka tos pačios originalios formos, kurią nustato jos savininkas.

Patikimumas reiškia galimybę naudotis duomenimis ir informacinėmis sistemomis visada, kai to reikia, ir tiek laiko, kiek reikia.

Informacijos saugos įgyvendinimo principai išdėstyti 11 dalyje.

3. INFORMACIJOS SAUGOS TIKSLAS

Informacijos saugos tikslas yra užtikrinti veiklos tęstinumą bet kuriomis sąlygomis. Mūsų teikiamos paslaugos, produktai ir vidinės operacijos turi atitikti įstatymų bei kitų teisės aktų reikalavimus. Mes turime patenkinti kliento ir kitų suinteresuotų šalių poreikius ir lūkesčius saugos srityje. Todėl kiekvienas įmonės darbuotojas yra asmeniškai atsakingas už saugą įmonėje.

Pagrindinė BDC veiklos sąlyga yra sugebėjimas būti vertinamiems esant patikimu ir garbingu partneriu. Šio patikimumo ir geros reputacijos užtikrinimas reikalauja, kad įmonė laikytųsi įstatymų, Vyriausybės nutarimų ir kad galėtų įvykdyti visus įsipareigojimus, kurie yra numatyti sutartyse bei verslo praktikoje.

Ryšium su tuo, pakankamo informacijos saugumo užtikrinimas yra vertinamas kaip bendrai priimtas įsipareigojimas. Norint pasiekti mūsų saugos tikslą vienu iš pagrindinių principų yra **nuolatinis saugos gerinimas**. Saugos gerinimo darbas vykdomas remiantis paslaugų teikimui naudojamo turto rizikų analizės rezultatais bei naujovėmis saugos srityje.

INFORMACIJOS SAUGUMO POLITIKOS IŠIMTYS

Informacijos saugumo politikos išimtis taikomos, kuomet griežtas saugumo tvarkų ar procedūrų laikymasis:

- ženkliai sumažintų išteklių našumą ar neigiamai įtakotų paslaugos kokybę;
- pareikalautų žymių finansinių išlaidų;
- būtų per daug sudėtinga techniškai;
- užimtų nepriimtinais daug laiko.

Išimtyms yra taikomos pagal Informacijos saugumo politikos ir procedūrų išimčių taikymo tvarką.

4. TEISINIAI REIKALAVIMAI, KURIE RODO KRYPTĮ INFORMACIJOS SAUGOS VEIKLAI

Daug įstatymų reglamentuoja informacijos saugą įmonės veikloje. Saugos politika remiasi tiek Lietuvos Respublikos įstatymais, Vyriausybės nutarimais bei kitais teisės aktais, tiek tarptautiniu mastu pripažintais dokumentų, iš kurių pagrindiniai yra Europos Sąjungos informacijos saugos direktyva 2002m. liepos 12d. (2002/58/EU) bei ISO 27001:2005 standartas, reikalavimais. Be įstatymų ir kitų teisės aktų dar yra sutartys bei susitarimai tarp BDC ir klientų, tiekėjų/subrangovų bei partnerių, kurių įmonė turi sugebėti laikytis, ir jie yra labai svarbūs. Papildomai prie to, įmonė dar turi laikytis nerašytų kliento bei interesų grupių taisyklių ir lūkesčių, kad būtų laikoma saugia informacinių sistemų paslaugų teikėja.

5. GRĖSMĖS SAUGAI

Saugai kyla daug skirtingų grėsmių. Tik kai kurios iš jų yra tiesiogiai susijusios su informacinėmis technologijomis. Grėsmės apibendrintai gali būti skirstomos į šias 4 kategorijas:

1. Išorės žmonių sąlygotas informacijos konfidencialumo, vientisumo ar pasiekiamumo praradimas (vagystės, tyčinis sugadinimas, pramoninis šnipinėjimas, krizės visuomenėje)
2. Su įmonės darbuotojais susijusios grėsmės
3. Techninės grėsmės, tiesiogiai susijusios su fizine aplinka; pvz., ugnis, vanduo, sutrikimai elektros tiekime ir t.t.
4. Gamtinės grėsmės (ypatingos gamtinės sąlygos ir natūralūs neįprasti reiškiniai)

Įmonės saugos vadovybė seka naujienas šiose srityse. Saugos Politika, tvarkos, procedūros, instrukcijos bei rekomendacijos yra atnaujinamos, kad atitiktų vykstančius pasikeitimus.

6. KLIENTO IR PASLAUGŲ TEIKĖJO ATSAKOMYBĖS

BDC yra IT paslaugų teikėjas vidiniams ir išoriniams klientams. Informacinės sistemos savininkas yra tiesiogiai atsakingas už informacijos ar informacinės sistemos apsaugos poreikių nustatymą. Įmonė turi įsitikinti, kad informacinės sistemos savininkas supranta savo atsakomybę. Kaip IT paslaugų teikėjas, BDC yra atsakingas už pakankamą saugumą užtikrinančias priemones, kurios atitiktų esančius kliento ir vidinius poreikius. Įstatymai

ir Vyriausybės potvarkiai gali numatyti panašią informacijos apsaugos atsakomybę paslaugos teikėjui kaip ir savininkui.

7. ĮMONĖS SAUGOS VALDYMAS

Įmonės vadovybė nustato visus saugos principus įmonės mastu. Įmonės vadovybė skiria atsakingą už Saugą darbuotoją, kuris atsako už saugos klausimus įmonės mastu, bei jį pavaduojantį darbuotoją. Atsakingas už saugą darbuotojas atsiskaito įmonės vadovybei. Atsakingas už saugą darbuotojas yra Saugos Politikos savininku. Politika yra peržiūrima bent kartą per metus.

Atsakingas už saugą darbuotojas yra atsakingas už:

- su sauga įmonėje susijusių darbų bendrą koordinavimą;
- su sauga susijusių incidentų tyrimą ir raportavimą Įmonės vadovybei.

Atsakingas už saugą darbuotojas turi teisę:

- sušaukti Rizikų valdymo komiteto posėdį;
- apriboti vartotojo teises į informaciją, jei tai gresia informacijos saugumui;
- pateikti savo išvadas apie įvykusius ir/arba galimus saugumo incidentus vadovybei;
- koordinuoti sudarytų saugumo užtikrinimo komandų darbą;
- gauti iš darbuotojų informaciją, susijusią su informacijos saugumu ir jo pažeidimais;
- rekomenduoti padalinių vadovams skirti užduotis informacijos saugumo būklei gerinti.

Kiekvienas darbuotojas yra atsakingas už įmonės saugą savo aplinkoje bei atsako už tai, kad informacija, duomenimis, sistemomis naudotųsi tik tam įgalioti asmenys. Kiekvienas privalo laikytis įsakymų, instrukcijų ir taisyklių, susijusių su sauga. Apie kiekvieną saugos pažeidimą būtina nedelsiant pranešti tiesioginiam vadovui.

Kiekvienas vidaus kompiuterinio tinklo vartotojas gali naudotis asmeniniu kompiuteriu, kompiuterizuota savo darbo vieta ar informacinėmis sistemomis tik savo asmens slaptažodžiu įrodęs savo tapatybę.

Įmonės struktūrinių padalinių vadovai atsako už tai, kad darbuotojai naudotųsi informacija, duomenimis ir informacinėmis sistemomis tik pagal nustatytas taisykles ir tik tiek, kiek reikia pareigoms atlikti bei už pakankamą įmonės saugos funkcijų vykdymą, tobulinimą ir priežiūrą savo padaliniuose. Jų užduotis yra sukurti tokią įmonės verslo aplinką, kurioje grėsmės įmonės darbuotojams, verslui, turtui ir klientams būtų pačios mažiausios.

Kiekvienas informacijos, duomenų, informacinių sistemų savininkas, saugotojas ir administratorius atsako už tai, kad vartotojas galėtų naudotis informacija, duomenimis, duomenų perdavimo sistemomis tik pagal nustatytas taisykles ir kad jis galėtų prieiti tik prie tos informacijos, prie kurios prieiti jis yra įgaliotas.

Įmonės direktorius atsako už Saugos Politikos įdiegimą įmonėje.

Susijusių rizikos faktorių įvertinimas ir valdymas vykdomas naudojant PJKG proceso modelį: **planavimas** (Plan), **įdiegimas** (Do), **kontrolė** (Check), **gerinimas** (Act).

7.1 Rizikų valdymo komitetas

Atsakingas už saugą darbuotojas, finansų direktorius, įmonės generalinis direktorius ir skyrių direktoriai sudaro Rizikų valdymo komitetą. Atsakingas už saugą darbuotojas yra Rizikų valdymo komiteto pirmininkas. Rizikų valdymo komitetas yra organas, kuris bendrai atsako už saugos klausimų iškelimą ir jų sprendimą.

Rizikų valdymo komitetas renkasi bent du kartus per metus.

Paprastai šiame komitete svarstomi šie dalykai:

- peržiūrima ir patvirtinama saugos politika ir visos atsakomybės;
- tikrinami reikšmingi informacinių vertybių pasikeitimai, susiję su pagrindinėmis grėsmėmis;
- peržiūrimi ir tikrinami informacijos saugos incidentai;
- tvirtinami pagrindiniai informacijos saugos stiprinimo pasiūlymai.

Kai prireikia, įmonės vadovybė arba Rizikų valdymo komitetas gali sudaryti specialias darbuotojų grupes, atsakingas už tam tikros saugos srities nuolatinio pasiruošimo palaikymą.

7.2 Skyrių lygio saugos valdymas

Skyrių direktoriai yra atsakingi už saugos priežiūrą savo skyriuje. Kiekvienas skyrius yra atsakingas už informacijos saugą sistemose, kurias jis naudoja savo darbe. Skyriaus direktorius atsako už saugos incidentų raportavimą atsakingam už saugą darbuotojui pagal Saugos incidentų valdymo procedūrą.

7.3 Su Sauga susijusių incidentų valdymas

Su Sauga susiję incidentai reikalauja skubaus organizacijos reagavimo tam, kad incidentas būtų suvaldytas. Atsakingas už saugą darbuotojas yra atsakingas už įmonės vidinį incidento tyrimą. Įmonės ryšių su žiniasklaida darbuotojas yra atsakingas už incidento/krizės komunikavimą.

BDC turi keleto lygių incidento/krizės valdymo organizaciją. Pagrindinis principas yra toks, kad incidentai turi būti sprendžiami vietoje, jei įmanoma. Skyrių direktoriai yra atsakingi už incidentų/krizių, kurios įvyko jų skyriuje, sprendimą. Vadovų atsakomybėje yra eskalacija į aukštesnį lygį priklausomai nuo įvykio pobūdžio. Incidentų valdymo organizacijos dalis yra įmonės Rizikų valdymo komitetas, kuris imasi atsakomybės tik ypatingais atvejais. Saugos incidentų valdymo procesas yra aprašytas įmonės saugos incidentų valdymo procedūroje. Procedūra taip pat padengia ir krizės komunikavimo klausimus.

7.4 Pranešimų apie su sauga susijusius incidentus valdymas

Atsakingas už saugą darbuotojas sudaro praneštų incidentų suvestinę kartą per 6 mėn. Ši suvestinė yra vienu iš šaltinių nuolatiniam saugos gerinimo procesui.

7.5 Saugos priemonių prioritetizavimas

Kai reikia priimti sprendimus, koku eiliškumu ką daryti, tokia tvarka turi būti taikoma:

1. apsaugoti žmonių gyvybę ir sveikatą;
2. apsaugoti konfidencialią ir kitą labai svarbią informaciją;
3. apsaugoti likusią informaciją;
4. išvengti sistemos sugadinimo;
5. apsaugoti sistemos veikimą.

8. SAUGOS PRINCIPAI

8.1 Pagrindiniai informacijos saugos įgyvendinimo principai

- Visa įmonės informacija ir duomenys turi paskirtą savininką. Jie prieinami, naudojami ir platinami tik reglamentuotu būdu ir turi būti saugomi pagal nustatyto minimalaus saugos lygio reikalavimus, jei nenurodyta kitaip.
- Informacijos, duomenų savininkas arba įgaliotas asmuo klasifikuoja duomenis, informaciją pagal svarbą ir nustato tikslius saugos lygius. Informacija, duomenys, informacijos perdavimo sistemos yra saugomi ir naudojami pagal jo nustatyto lygio reikalavimus.
- Informacijos savininkas arba įgaliotas asmuo suteikia teises į informaciją, už kurią atsako, tik tiems asmenims, kuriems tai yra būtina darbui atlikti.
- Struktūriniai padaliniai sukuria nenumatytų situacijų valdymo planus ir juos reguliariai atnaujinama, kad užtikrintų nenutrūkstamą sistemų veikimą, esant neįprastoms sąlygoms ar kritinei situacijai.
- Įmonėje turi būti sistemingai saugomasi kompiuterių virusų. Efektyvios antivirusinės sistemos turi būti kuriamos, diegiamos, prižiūrimos, atnaujinamos ir tobulinamos.
- Kiekvienas įmonės darbuotojas pagal savo pareigas dalyvauja kuriant, įgyvendinant ir tobulinant įmonės saugos procesus.
- Įmonėje laikomasi Saugos Politikos, tvarkų ir procedūrų. Dokumentų, susijusių su įmonės sauga, patobulinimai ar papildymai yra skelbiami skyrių susirinkimuose, saugos mokymuose arba visos įmonės susirinkimuose. Skubūs pakeitimai pranešami elektroniniu paštu.
- Pastebėjęs įmonės saugos pažeidimus, kiekvienas darbuotojas pagal savo įgaliojimus privalo juos šalinti.
- Kiekvienas atvejis, susijęs su įmonės saugos pažeidimais, turi būti užregistruotas ir apie jį informuotas struktūrinio padalinio vadovas.
- Įmonės vadovybė turi būti periodiškai informuojama apie pašalintus pažeidimus.
- Kiekvienas įmonės struktūrinis padalinys tiria ir analizuoja grėsmes, susijusias su įmonės sauga savo veiklos srityje ir tobulina savo veiklą atsižvelgdamas į analizės rezultatus.
- Kiekvienas vadovas seka su jo veikla susijusių saugos sričių naujoves ir plėtrą šalyje bei užsienyje.
- Kiekvienas struktūrinis padalinys bendradarbiauja ir plėtoja bendradarbiavimą su svarbiausiomis saugos sričių interesų grupėmis.

8.2 Su darbuotojais susijusi sauga

Kiekvienas BDC darbuotojas privalo laikytis politikos ir saugos instrukcijų ir pranešti savo vadovui apie aptiktas problemas, grėsmes arba veiksmus, kurie yra priešingi nurodytiems instrukcijose.

Kiekvienas darbuotojas privalo pasirašyti konfidencialumo sutartį (įtraukta į Darbo tvarkos taisykles kaip jų sudedamoji dalis), kuri galioja ir pasibaigus darbo santykiams su įmone. Konfidencialumo sutartys taip pat turi būti pasirašomos su subrangovo ar partnerio darbuotojais, konsultantais ir kitais, kurie dirba įmonei. Įmonės konfidencialumo sutartyje nurodoma, kas sudaro profesinę paslaptį. Neviešinamų punktų susitarimai turi būti naudojami visais atvejais, kai konfidencialumo, slaptumo ar informacijos atskleidimas yra priskiriamas savininkui (ar aukštesnes pareigas turintiems asmenims).

Kiekvieno darbuotojo biografijos faktai, išsilavinimas, kvalifikacija gali būti tikrinama. Tikrinimo metodai priklauso nuo darbuotojo einamų pareigų, priėjimo prie informacijos ir teisinių dalykų. Subrangovų ar partnerių darbuotojai bei konsultantai taip pat gali būti tikrinami priklausomai nuo jų vykdomų darbų.

Organizacijos firminių blankų laiškinių popierių, atspausdintos formos ir kiti dokumentai turi būti tinkamai prižiūrimi, kad būtų išvengta netinkamo jų panaudojimo.

Tiek fizinių, tiek elektroninių raktų skolinimas yra draudžiamas. Šis įsipareigojimas turi būti įtrauktas ir į darbo sutartį.

Visi darbuotojai privalo laikytis organizacijos informacijos saugumo taisyklių. Bet kokie informacijos saugumo incidentai, kylantys jų nesilaikant, turi nedelsiant sulaukti drausminančių veiksmų.

8.3 Saugos apmokymai

Pradinis saugos apmokymas privalo būti dalimi darbuotojui pravedamo pirminio instruktažo. Saugos politika, tvarkos ir instrukcijos privalo būti žinomos ir komunikuojamos visiems darbuotojams. Žinojimo lygis priklauso nuo atliekamo darbo. Tai taip pat taikoma subrangovams ir partneriams. Kai personalo nariai keičia darbą, jų informacijos saugumo poreikiai turi būti pakartotinai įvertinti ir suteikiami reikalingi mokymai.

Nuolatiniai darbuotojai turi būti informuoti apie informacijos saugumo užtikrinimo priemones, kurios didintų žinias ir mokytų juos atpažinti galimas grėsmes bei tinkamai nuo jų apsisaugoti.

Vartotojai ir techninis personalas turi būti tinkamai apmokyti ir paruošti darbui su naujomis sistemomis, jiems turi būti suteikta pakankamai žinių apie visų naujų sistemų funkcionavimą ir jų panaudojimą praktikoje.

Skyrių direktoriai yra atsakingi už tai, kad jų darbuotojai būtų tinkamai apmokyti darbuotojų saugos ir sveikatos, priešgaisrinės saugos klausimais.

8.4 Fizinė sauga

Fizinė apsauga pasiekama sudarant aplink komercinės veiklos patalpas ir informacijos apdorojimo įrangą keletą saugos barjerų. Kiekvieno barjero sukuriama saugumo aptvara padidina bendrąjį saugumą. Įmonė naudoja saugumo barjerus siekdama apsaugoti sritis, kuriose įrengta informacijos apdorojimo įranga, bei dirba įmonės darbuotojai. Kiekvieno barjero išdėstymas ir tvirtumas priklauso nuo rizikos įvertinimo rezultatų. Detaliau reikalavimai įmonės patalpoms aprašyti BDC Patalpų apsaugos taisyklėse.

Asmenis, darbuotojus taip pat kaip ir lankytojus, kurie lankosi įmonės patalpose, privalo būti įmanoma identifikuoti. Visi darbuotojai privalo segėti darbuotojo pažymėjimą su nuotrauka ir visi lankytojai turi segėti lankytojo pažymėjimą. Autentiškumo patvirtinimui, nuotrauka ant pažymėjimo turi būti identiška nuotraukai, kuri saugoma įmonės vidinėje sistemoje.

BDC darbuotojas, pas kurį atvyko lankytojas(-ai), yra atsakingas už lankytojų pasitikimą šioms atvykus ir už jų palydėjimą iš patalpų jiems išvykstant.

Fotografavimas ir/arba vaizdo/garso įrašymas BDC patalpose be leidimo yra draudžiamas. Ši taisyklė galioja ir kitai įrangai, turinčiai tokias galimybes (mobiliems telefonams ir pan.). Leidimą gali suteikti bet kuris RVK narys.

Taikoma apsauga turi būti proporcinga identifikuotoms rizikoms. Siekiant sumažinti nesankcionuotos kreipties riziką arba daromą žalą dokumentams, duomenų laikmenoms ir informacijos apdorojimo įrangai, yra taikoma "švaraus stalo" tvarka.

Visi darbuotojai turi žinoti, kad jie turi palydėti pašalinius asmenis, pastebėtus organizacijos patalpose, iki įmonės atsakingo asmens arba iki apsaugos posto,.

8.5 Veiklos tęstinumo valdymas

Įmonė iš anksto yra pasiruošusi tyčiniam ar netyčiniam informacijos saugos pažeidimui. Tvarkos, aprašytos įmonės Saugos Incidentų Valdymo Procedūroje, privalo būti laikomasi, kai informacija yra pateikiama nepaprastomis sąlygomis arba krizių metu.

Grėsmės pagrindinei įmonei IT infrastruktūrai yra valdomos remiantis įmonės Saugos incidentų valdymo procedūroje aprašytais nurodymais. Skyriai privalo nustatyti ir dokumentuoti priemones, kurių imamasi, jei verslui svarbi informacinė sistema tampa grėsmių ar saugos atakų objektu. Skyriai užtikrina, kad reikiamas darbuotojų skaičius būtų prieinamas krizinėje situacijoje, kad patenkintų kliento poreikius.

Komercinės veiklos nepertraukiamumo planas turi būti periodiškai tikrinamas, kad būtų garantuota, jog administracija ir personalas žino, kaip jį reikia vykdyti.

8.6 Licenzijų, techninės ir programinės įrangos valdymas

Įmonė privalo vykdyti techninės/programinės įrangos licenzijų sutartis. Visa techninė ir programinė įranga, naudojama įmonės informacijos architektūroje, privalo būti įsigyta iš patikimų šaltinių bei atitikti įmonės saugumo reikalavimams.

8.7 Sistemų priežiūra

Kai planuojamos informacijos saugos priemonės, reikiamas informacijos saugos, sistemos naudojamumo bei kaštų, atsirandančių dėl informacijos saugos, lygis turi būti subalansuotas. Priemonės, kurios yra per daug griežtos, neturi būti taikomos, jei tai veda prie nepagrįstai didelių sąnaudų arba jei jos padaro sistemą per daug sudėtingą naudojimui. Iš visų darbuotojų, subrangovų ir trečių šalių vartotojų turi būti reikalaujama atkreipti dėmesį ir pranešti apie bet kokias pastebėtas ar įtariamas saugos spragas sistemose ar paslaugose.

Kvalifikuoti inžinieriai turi aprūpinti visą įmonės licencijuotą, nupirktą arba išnuomotą kompiuterinę įrangą reikiamomis eksploatacijos priemonėmis.

8.8 Informacijos laikmenų valdymas ir sauga

Informacijos apsaugos lygis turi būti įvertintas visuose informacijos apdorojimo etapuose. Informacija privalo būti saugoma duomenų laikmenose, kurios užtikrina atitinkamą informacijos saugumo lygį, bei turi būti laikoma tinkamai. Detaliai tai aprašyta Informacijos laikmenų valdymo tvarkoje.

8.9 Patekimo į sistemą kontrolė

Informacinių sistemų vartotojai turi teisę pasiekti tik tas bylas, duomenų laikmenas, sistemas ir kitus resursus, kurie jiems reikalingi darbo užduočių atlikimui. Šios patekimo į sistemą teisės ir jų priežiūra turėtų būti valdoma techninėmis priemonėmis, kai tik yra prasminga tai daryti. Faktas, kad resursas dėl vienokių ar kitokių priežasčių nėra techniškai apsaugotas, nesuteikia teisės neįgalotiems vartotojams juo naudotis. Visa kompiuterinė įranga ar terminalai privalo saugoti laikomus duomenis įėjimo slaptažodžiais. Pavyzdžiai kaip tai gali būti realizuota yra:

- automatiškai aktyvuojama, slaptažodžiu apsaugota ekrano užsklanda;
- automatinis vartotojo išregistravimas iš sistemos po tam tikro laikotarpio, kurio metu vartotojas nedirba su sistema;
- arba kitos priemonės, kurios užrakina sistemą, su kuria nedirbama.

8.10 Vartotojų identifikavimas ir slaptažodžių valdymas

Vartotojų kodai, slaptažodžiai, identifikavimo įrenginiai, pažymėjimai su nuotrauka ir kiti susiję daiktai yra skirti vartotojui asmeniškai, jei nėra vienareikšmiškai nurodyta kitaip. Neleidžiama niekam kitam perduoti šių asmeninių daiktų net ir laikinam naudojimui. Nurodymų, susijusių su informacijos saugos instrukcijomis, pavyzdžiui, reguliarius slaptažodžių keitimas, privalo būti laikomasi net jei naudojamos technologijos neverčia to daryti.

8.11 Informacinių vertybių klasifikacija ir kontrolė

Įmonės informacinės vertybės privalo būti klasifikuojamos ir saugomos remiantis informacinių vertybių klasifikavimo ir valdymo taisyklėmis. Bazinis klasifikavimo lygis kliento informacinėms vertybėms yra konfidencialu.

Skyriai yra atsakingi už vidinės informacijos apsaugą, prekybos paslapčių ar kitos konfidencialios informacijos apsaugą nuo neįgalotų vartotojų. Ši pareiga saugoti informaciją apima tiek fizinę duomenų apsaugą (išorės žmonės, lankantys įmonės patalpas ar dirbantys jose), tiek loginę duomenų apsaugą (pasiekimas duomenų per tinklą).

8.12 Apsauga nuo piktavališkos programinės įrangos

Visa įranga, jungiama prie įmonės naudojamo tinklo, privalo būti aprūpinta antivirusinėmis priemonėmis. Skyriai yra įpareigoti apsaugoti sistemas, už kurias jie yra atsakingi, nuo virusų ir kitų sugadinimo rizikų. Naudojami tinklai privalo būti apsaugoti techninėmis priemonėmis (ugniasienės, ID Sistemos, VPN infrastruktūra ir t.t.) tam, kad būtų kontroliuojamas patekimas iš nepatikimų tinklų. Apsikeitimas informacija naudojant tinklą

Įmonės naudojama elektroninio pašto sistema ir prieiga prie interneto yra skirti įmonės verslui. E-paštas yra laikomas asmeniniu ir konfidencialiu, ir jam taikomi pagrindiniai susirašinėjimo privatumo principai. Neleidžiama e-paštu siųsti neapsaugotos konfidencialios informacijos.

E-pašto, betarpiško keitimosi pranešimais sistemų ir Interneto naudojimas yra aprašytas Elektroninio pašto, betarpiško keitimosi pranešimais sistemų (instant messaging) ir interneto naudojimo tvarkoje.

8.13 Atitikimas

Įmonės ar kliento darbuotojas yra įpareigotas laikytis tiek BDC Saugos Politikos, tiek ir išorinės organizacijos saugos bei eksploatacijos politikų, kai jis naudoja duomenų perdavimo tinklą pasiekti resursus, valdomus tos išorinės organizacijos.

Kiekvienas skyrius yra atsakingas už tai, kad skyriuje būtų laikomasi informacijos saugos.

Gedimai ir trūkumai, surasti saugos audito ar testų metu, turėtų būti ištaisomi kaip įmanoma greičiau. Laikini sprendimai tam tikrais atvejais gali būti reikalingi nedelsiant. Atsakingas už saugą darbuotojas kartu su pavaduojančiu darbuotoju peržiūrės saugos priemones, kurių imasi skyriai.

Šios politikos pažeidimai bus nagrinėjami ir interpretuojami kaip darbo sutarties pažeidimai.

8.14 Kova prieš kibernetinius nusikaltimus

Tinkle privaloma aukščiausio lygio apsauga. Įmonės, atsakingi už tinklo ir išorines komunikacijas, turi būti paruošti taip, kad galėtų įvertinti riziką ir sukurti apsaugos sistemas, kurios kuo labiau mažintų kibernetinių nusikaltimų grėsmę.

Turi būti paruošti, prižiūrimi ir reguliariai tikrinami veiklos atstatymo planai, kurie užtikrintų, kad galimų išorinių kibernetinių nusikaltimų padaryta žala būtų kuo mažesnė, o atstatymas atliekamas kiek galima greičiau.

Kibernetinių nusikaltimų vykdytojai turi būti patraukti baudžiamojon atsakomybėn pagal įstatymą. Tūri būtų užtikrintas tinkamas įkalčių rinkimas ir jų apsauga.

8.15 Įstatymų ir taisyklių reikalavimų laikymasis

Organizacija privalo pilnai laikytis duomenų apsaugos įstatymų tiek, kiek jie tiesiogiai susiję su organizacijos veikla.

Darbuotojams draudžiama rašyti užgaulias pastabas apie kitus asmenis ir organizacijas.

Informacija iš Interneto ar kitų elektroninių šaltinių gali būti draudžiama naudoti arba persiųsti be autorinių teisių savininko leidimo.

Tekstas iš ataskaitų, knygų ar dokumentų gali būti draudžiamas dauginti ar naudoti be autorinių teisių savininko leidimo.

9. POLITIKOS ĮSIGALIOJIMO DATA

Ši Įmonės Saugos Politika įsigalioja nuo 2008-09-15. Ji pakeičia iki šiol naudotą Politikos versiją.