

PATVIRTINTA
Valstybės įmonės Turto banko
generalinio direktoriaus
2023 m. liepos d.
įsakymu Nr. P1-

VALSTYBĖS ĮMONĖS TURTO BANKO MINIMALŲS INFORMACIJOS SAUGOS REIKALAVIMAI PASLAUGŲ TEIKIMUI

I SKYRIUS BENDROSIOS NUOSTATOS

1. Šiuo dokumentu yra nustatomi minimalūs informacijos saugos reikalavimai ir darbo principai (toliau – Reikalavimai), taikomi valstybės įmonės Turto bankas (toliau – Turto bankas) paslaugas teikiantiems tiekėjams, taip pat jų pasitelktoms trečiosioms šalims, t. y. jų tiekėjams ir subtieėjams (toliau kartu – Paslaugų teikėjas), veikiantiems Turto banko informacinių technologijų ir telekomunikacijų įrenginiuose ar sistemose (toliau – IT).

2. Neteisėto atskleidimo, korupcinio pobūdžio ir kitų neteisėtų veikų prevencijos, taip pat informacinių sistemų bei informacijos saugos ir Reikalavimų kontrolės bei paslaugų suteikimo kontrolės tikslu Paslaugų teikėjo veiksmai, atliekami jungiantis ir prisijungus prie Turto banko IT, gali būti stebimi ir įrašomi, o įrašai saugomi neilgiau nei galioja sutartis su Paslaugų teikėju.

3. Paslaugų teikėjas yra atsakingas už savo darbuotojų, tiekėjų ir subtieėjų darbuotojų, kurie turi prieigą prie Turto banko IT ar gali būti susiję su prieigos prie Turto banko IT suteikimu ar naudojimu ir supažindinimą su Reikalavimais, iki jiems suteikiant prieigą ir turi gebėti tai įrodyti.

4. Paslaugų teikėjas privalo užtikrinti ir kontroliuoti, kad jo darbuotojų ir kitų pasitelktų šalių veiksmai, naudojama programinė ir aparatinė įranga nepažeis, neteisėtai nekeis ar kitaip nesutrikdys Turto banko IT veiklos, nebus nesankcionuotai atskleista konfidenciali ar komercinę (gamybos) paslaptį sudaranti informacija, asmens duomenys ar padaryta žala Turto bankui arba tretiesiems asmenims.

5. Paslaugų teikėjo darbuotojų, tiekėjų ir subtieėjų darbuotojų, kurie turi prieigą prie Turto banko IT ar gali būti susiję su prieigos prie Turto banko IT suteikimu ar naudojimu, informacinių technologijų ir informacijos saugos žinios turi būti pakankamos paslaugoms atlikti. Paslaugų teikėjas turi vertinti šių žinių lygį ir, jei reikia, organizuoti papildomus mokymus.

6. Turto bankui pateikus oficialų prašymą ar įvykus reikšmingam incidentui, siekiant patvirtinti, jog Paslaugų teikėjas laikosi Reikalavimų, Paslaugų teikėjas suteikia Turto bankui ar Turto banko pasirinktai trečiajai šaliai, veikiančiai Turto banko pavedimu, leidimą atlikti visų Paslaugų teikėjo aplinkoje taikytų valdymo priemonių, susijusių su Turto banko duomenų tvarkymu ir/ar paslaugų Turto bankui teikimu, vertinimą, auditą, tikrinimą ar peržiūrą. Atliekant tokį vertinimą, Paslaugų teikėjas turi visapusiškai bendradarbiauti, t. y. suteikti galimybę susipažinti su kompetentingais darbuotojais, dokumentais, infrastruktūra ir programine įranga, kuri naudojama apdorojant, saugant ar perduodant Turto bankui duomenis. Reikiamą informaciją Paslaugų teikėjas pateikia ne vėliau, nei per 24 valandas nuo prašymo gavimo dienos. Tuo atveju, jeigu audito metu nustatomi trūkumai, Paslaugų teikėjas privalo pašalinti rastus trūkumus per Turto banko nurodytą protingą terminą.

7. Turto bankas neprivalo padengti jokių Paslaugų teikėjo išlaidų, kurias Paslaugų teikėjas patiria bendradarbiaudamas audito metu arba šalindamas nustatytus trūkumus.

8. Paslaugų teikėjas privalo nedelsiant, bet ne vėliau kaip per 24 val. nuo momento, kai jam tapo žinoma, pranešti el. paštu infosauga@turtas.lt apie visus pastebėtus ar įtariamus informacijos saugos incidentus ir įvykius, bei Reikalavimų laikymosi pažeidimus (net jei jų faktas dar nėra patvirtintas), įskaitant, bet neapsiribojant, šiais įvykiais: Paslaugų teikėjo IT nustatyta kenkėjiška programinė įranga,

aptiktas kibernetinės atakos ar įsilaužimo faktas ar galimybė, pastebėti Paslaugų teikėjo IT pažeidžiamumai, prarasta įranga ar įrenginiai, kuriuose yra Turto banko informacija, neteisėtai atskleisti Turto banko duomenys, prarasti prisijungimo duomenys ir t.t. Jeigu incidentas įvyko Paslaugų teikėjo infrastruktūroje, jis turi imtis priemonių incidento suvaldymui ar galimų pasekmių sumažinimui, pvz. nedelsiant pakeisti prarastus slaptažodžius ar kreiptis dėl jų pakeitimo ir pan.

II SKYRIUS ĮRANGOS SAUGOS REIKALAVIMAI

9. Paslaugų teikėjas privalo užtikrinti, kad jo darbuotojai ar tiekėjų ir subtiektėjų darbuotojai, prie Turto banko IT jungtųsi iš įrenginių, kuriems būtų taikomos atitinkamos jų keliamai rizikai informacijos saugos priemonės, įskaitant, bet neapsiribojant, šias minimalias priemones:

9.1. turi būti naudojama gamintojų palaikoma aparatinė įranga, užtikrinant savalaikį naujausių aparatinės programinės įrangos saugos pataisų diegimą;

9.2. turi būti įdiegta antivirusinė programinė įranga, užtikrinant, kad antivirusinės programinės įrangos naujinimai būtų diegiami ne rečiau kaip kartą per parą;

9.3. turi būti nuolat diegiamos operacinės sistemos ir naudojamos programinės įrangos gamintojų išleistos kritinės ir svarbios saugos pataisos;

9.4. naudotojo ir administratorių paskyros turi būti atskirtos, t.y. administratorių paskyros naudojamos tik konfigūravimo ir kitiems administratoriaus teisių reikalaujantiems veiksams atlikti;

9.5. naudojami slaptažodžiai turi atitikti Reikalavimų V skyriaus nuostatas;

9.6. turi būti aktyvuotas automatinis naudotojo paskyros užrakinimas, įsijungiantis ne vėliau kaip po 15 min. naudotojo neveiklumo;

9.7. turi būti įjungta ir naudojama kompiuterinės darbo vietos ugniasienė;

9.8. kompiuterinės darbo vietos vidinė atmintis turi būti užšifruota (pvz.: naudojant „Bitlocker“ arba lygiavertę programinę įrangą);

9.9. naudojamos išorinės atminties laikmenos turi būti šifruojamos (pvz.: naudojant „Bitlocker“ arba lygiavertę programinę įrangą).

10. Paslaugų teikėjas turi imtis deramų priemonių užtikrinant, kad Turto banko IT aptarnavimui naudojama programinė įranga yra saugi ir tinkamai licencijuota. Draudžiama naudoti nelegalią, nelicencijuotą programinę įrangą.

11. Turto bankas turi teisę, be išankstinio perspėjimo, blokuoti Paslaugų teikėjo turimą prieigą prie Turto banko IT ar naudojamus įrenginius, jei nustatyta, kad Paslaugų teikėjo veiksmai ar naudojami įrenginiai kelia grėsmę Turto banko informacijai, neatitinka Reikalavimų nuostatų arba Paslaugų teikėjo darbuotojų ar jo pasitelktų tiekėjų arba subtiektėjų darbuotojų elgesys Turto banko IT infrastruktūroje kelia įtarimų arba gali sukelti grėsmes Turto banko informacijai arba IT (pvz.: DDoS atakos, spam žinutės ir pan.).

12. Prieš suteikiant prieigą prie Turto banko IT, Turto bankas turi teisę patikrinti Paslaugų teikėjo darbo priemonių, su kuriomis ketinama jungtis prie Turto banko IT, atitiktį Reikalavimų nuostatoms.

III SKYRIUS IDENTIFIKAVIMO PRIEMONĖS IR RIBOJIMAI

13. Prisijungimo paskyros prie Turto banko IT yra unikalios, jei tai neriboja techninės galimybės, ir suteikiamos asmeniškai tik Paslaugų teikėjo įgaliotiems asmenims.

14. Paslaugų teikėjas įsipareigoja užtikrinti, kad paskyrų naudotojai laikysis Reikalavimų, suteiktus prisijungimo duomenis naudos tik pagal tiesioginę paskirtį sutartoms paslaugoms atlikti, saugos paslapyje ir neatskleis tretiesiems asmenims. Paslaugų teikėjas privalo supažindinti paskyrų naudotojus su Reikalavimais.

15. Nustačius bet kokius paslaugų sutarties, kuriai įgyvendinti buvo suteikta prieiga, ar Reikalavimų pažeidimus, suteikta prieiga gali būti nedelsiant panaikinama ir apie tokius veiksmus informuojamas Paslaugų teikėjas.

IV SKYRIUS

DARBO SU TURTO BANKO IT REIKALAVIMAI

16. Paslaugų teikėjai, teikdami paslaugas, susijusias su Turto banko IT, visiškai atsako už Reikalavimų laikymąsi, praktikų, užtikrinančių kibernetinį ir konfidencialios ar komercinės (gamybos) paslaptį sudarančios informacijos saugumą, taikymą. Jei Paslaugų teikėjas dėl informacijos stokos ar kitų priežasčių to negali užtikrinti, jis privalo nedelsdamas stabdyti teikiamas paslaugas ir nedelsdamas, bet ne vėliau kaip per 24 val., apie tai pranešti Turto bankui el. paštu infosauga@turas.lt.

17. Paslaugas teikti leidžiama tik tokia apimtimi ir tik tokioje Turto banko IT, kiek tai yra numatyta ar reikalauja paslaugų teikimo sutartis, pateiktas užsakymas ar kita forma išreikštas Turto banko poreikis. Bet kokie kiti veiksmai turi būti suderinti su Turto banko darbuotojais atsakingais už sutarties vykdymą, o jų nesuderintas atlikimas yra draudžiamas.

18. Dirbant su Turto banko IT draudžiama:

18.1. savavališkai perduoti Turto banko IT aparatinę įrangą naudoti tretiesiems asmenims;

18.2. savavališkai ardyti, remontuoti ar keisti Turto banko IT aparatinės įrangos komplektaciją, jei tai nėra Paslaugų teikimo dalis ir tai nėra suderinta su Turto banko darbuotoju atsakingu už IT infrastruktūrą;

18.3. prie Turto banko IT jungti nesankcionuotus duomenų perdavimo tinklo įrenginius (pvz. 3/4/5G ryšio modemus ir pan.), taip pat bet kokius kitus, tiesioginių paslaugų atlikimui neskirtus įrenginius;

18.4. Turto banko IT diegti, saugoti ar joje paleidinėti Turto banko nelicencijuotą, neautorizuotą programinę įrangą ar autorių teisėmis apsaugotus kūrinius ar juos naudoti pažeidžiant licencijavimo sąlygas ar autorių teises;

18.5. išnešti Turto banko IT aparatinę įrangą, nesuderinus šių veiksmų su už atitinkamos sutarties vykdymą atsakingu Turto banko darbuotoju;

18.6. kopijuoti, saugoti, perduoti Turto banko informacinėse sistemose esančius duomenis ir informaciją į kitą, Turto banko nevaldomą, IT infrastruktūrą, nesuderinus šių veiksmų su už atitinkamos sutarties vykdymą atsakingu Turto banko darbuotoju (pvz. draudžiama testavimo ar kitais tikslais perkelti duomenų bazes, sistemas ar kitus informacinius išteklius į paslaugos teikėjo valdomą, turimą infrastruktūrą, kopijuoti Turto banko informaciją į failų mainų sistemas Wetransfer, Google Drive ir pan.);

18.7. blokuoti antivirusines programas, ugniasienes ir kitas Turto banko IT naudojamas saugos priemones ar keisti jų nustatymus;

18.8. naudoti bet kokias priemones, įrangą ir paslaugas (pvz. proxy, VPN, SSH tunneling, DNS tunneling ir pan.), siekiant apeiti Turto banko naudojamas saugos sistemas, pasiekti blokuojamus interneto išteklius/paslaugas, bei atlikti kitus, su teikiamomis paslaugomis nesusijusius, veiksmus ar slėpti savo atliekamus veiksmus, išskyrus tuos atvejus, kai jų naudojimas yra reikalingas atlikti paslaugų teikimo sutartyje numatytas funkcijas ir yra suderintas su Turto banko darbuotoju atsakingu už kibernetinį saugumą;

18.9. naudoti Turto banko IT išteklius su teikiamomis paslaugomis nesusijusiais tikslais komercinei veiklai, taip pat smurto, amoralaus elgesio skatinimui, įžeidžiančių dalykų sklaidimui ir pan. Paslaugų teikėjo darbuotojai privalo laikytis etikos normų ir atsako už informaciją, pateiktą naudojant Turto banko kompiuterinius tinklus;

18.10. užsiimti veikla, kuri pažeidžia Lietuvos Respublikos įstatymus;

18.11. nesankcionuotai naudotis svetimais ištekliais (pvz. dirbti kitam naudotojui suteiktais prisijungimo duomenimis, kopijuoti ir naudotis programomis ir duomenimis be išteklių savininko žinios ir sutikimo, jungtis prie kompiuterių be atitinkamo leidimo ir pan.);

18.12. griežtai draudžiama savavališkai keisti Turto banko IT parametrus, nesuderinus pokyčių su Turto banko darbuotoju atsakingu už IT infrastruktūrą (pvz. IP adresą, įrangos vardus ir pan.);

18.13. savo paslaugų teikimui skirtuose įrenginiuose naudoti programas, kurios apsunkina ar trikdo Turto banko IT veikimą (pvz. kompiuteriniai virusai, tinklo ar sistemų skenavimo programos, tinklo ar sistemų blokavimo programos ir pan.);

18.14. vykdyti Turto banko IT, tame tarpe kompiuterių tinklą, pažeidžiamumų skenavimą. Pažeidžiamumų skenavimo priemonių naudojimas galimas tik suderinus jų naudojimą su Turto banko darbuotoju atsakingu už kibernetinį saugumą.

V SKYRIUS

SLAPTAŽODŽIŲ SAUGOS REIKALAVIMAI

19. Reikalavimuose pateikti slaptažodžių saugos reikalavimai taikomi Paslaugų teikėjo IT ištekliams (įrenginiams ir sistemoms), kurie skirti aptarnauti Turto banko IT ar juose yra talpinama Turto banko informacija.

20. Kiekvienam Paslaugų teikėjo arba jo subtiektėjo darbuotojui, jei neriboja techninės galimybės, suteikiamas unikalus, asmeninis prisijungimo prie Turto banko IT vardas.

21. Paslaugų teikėjas privalo įpareigoti savo darbuotojus saugoti jiems suteiktus prisijungimo duomenis, neperduoti jiems suteiktų prieigos teisių kitiems asmenims, įskaitant ir kitą Paslaugų teikėjo personalą. Paslaugų teikėjo arba jo subtiektėjo darbuotojai negali naudotis kitiems asmenims išduotais prisijungimo duomenimis.

22. Paslaugų teikėjas yra tiesiogiai atsakingas už visus Paslaugų teikėjo darbuotojų arba jo subtiektėjų prisijungimo vardu Turto banko IT atliktus žalingus veiksmus ir Turto bankui padarytus nuostolius.

23. Paslaugų teikėjas, kurdamas slaptažodžius (net ir laikinus), privalo laikytis šių reikalavimų:

23.1. slaptažodžius draudžiama sudarinėti naudojant lengvai nuspėjamas sekas (pvz. qwerty, ABC123 ir pan.) ar naudoti asmeninio pobūdžio informaciją (pvz. gimimo data, šeimos narių vardai ir pan.);

23.2. slaptažodžius turi sudaryti ne mažiau kaip 12 simbolių, kurių sudarymui turi būti panaudotos didžiosios ir mažosios raidės, skaičiai bei specialieji simboliai;

23.3. slaptažodžiai turi būti keičiami ne rečiau kaip kartą per tris mėnesius. Keičiant slaptažodį, turi būti užtikrinta, kad naujo slaptažodžio negalima nuspėti, žinant prieš tai buvusį slaptažodį.

24. Prisijungimo slaptažodžiai gali būti saugomi ar esant būtinybei, perduodami tik šifruotu pavidalu, naudojant specialią slaptažodžių saugojimui skirtą programinę įrangą (pvz.: KeePass arba lygiavertę). Draudžiama saugoti ar perduoti prisijungimo slaptažodžius nešifruotus, užrašytus atviru tekstu (pvz. popieriuje, failuose, programinėje įrangoje ir pan.).

25. Draudžiama prieigai prie Turto banko IT naudojamus slaptažodžius naudoti kitur (pvz. internetinėse sistemose, asmeninio naudojimo sistemose arba įrenginiuose, kitų klientų įrenginiuose ir pan.).

26. Kai dėl techninių ar organizacinių ribojimų būtina taikyti slaptažodžių sudėtingumo išimtis, turi būti gautas Turto banko darbuotojo, atsakingo už kibernetinę saugą, patvirtinimas ir įgyvendintos pateiktos papildomos priemonės skirtos sumažinti informacijos saugos rizikas, kylančias dėl išimties.

VI SKYRIUS

TEISIŲ SUTEIKIMO REIKALAVIMAI

27. Paslaugų teikėjas turi nedelsdamas, bet ne vėliau nei per 24 valandas informuoti apie savo darbuotojų ir tiekėjų bei subtiektėjų darbuotojų darbo ir kitų sutarčių nutraukimus ir kitus pasikeitimus, siekiant užtikrinti, kad prieiga prie Turto banko IT būtų panaikinta ir/ar išduota įranga būtų grąžinta ne vėliau, kaip paskutinę sutarties su tais asmenimis galiojimo dieną.

28. Iki paslaugų teikimo pradžios Paslaugų teikėjas turi būti įdiegęs formalią procedūrą prieigos teisių suteikimui ir panaikinimui ir ją taikyti prieigos prie Turto banko IT valdymui ir, Turto bankui pareikalavus, gebėti tai įrodyti.

29. Paslaugų teikėjo prieigos valdymo formali procedūra turi apimti ir užtikrinti šių reikalavimų laikymąsi:

29.1. pasirašytos paslaugų teikimo ar kitos sutarties, kurios įgyvendinimas reikalauja prieigos suteikimo, pagrindu, ne ilgesniam, negu reikia, sutartinių įsipareigojimų įvykdymo terminui ir mažiausia konkrečioms veiksmams atlikti reikalinga apimtimi;

29.2. pasirašius konfidencialumo įsipareigojimą, atitinkantį konfidencialumo susitarimo su Turto banku sąlygas, jeigu jis nenumatytas aukščiau nurodytoje sutartyje;

29.3. trečiųjų šalių prieigos teisės prie visų informacinių išteklių turi būti panaikinamos ne vėliau, kaip paskutinę sutarties ar paslaugų, kurioms suteikti buvo reikalinga prieiga, teikimo dieną;

29.4. įpareigojus trečiąją šalį laikytis reikalavimų, atitinkančių šiuos Reikalavimus.

VII SKYRIUS

NUOTOLINĖS PRIEIGOS REIKALAVIMAI

30. Nuotolinei prieigai prie Turto banko IT galima naudoti tik Turto banko suteiktus prisijungimo metodus ir priemones. Savavališka nuotolinė prieiga prie Turto banko IT griežtai draudžiama. Nuotolinė prieiga suteikiama griežtai tik tais atvejais, kai tai yra būtina tiesioginių pareigų atlikimui arba tai yra numatyta paslaugų teikimo sutartyje.

31. Nuotolinis prisijungimas prie Turto banko IT per viešuosius tinklus (internetą), realizuojamas tik naudojant Turto banko VPN arba taikant kelių faktorių autentifikacijos principą, papildomai patvirtinant besijungiančiojo asmens tapatybę naudojant mobiliojo ryšio telefono numerį ar kitą kelių faktorių autentifikavimo priemonę.

32. Nesankcionuotas Turto banko VPN prisijungimas ar jo panaudojimas ne atitinkamoje sutartyje numatytais tikslais griežtai draudžiamas.

33. VPN naudotojai atsako už tai, kad tretieji asmenys VPN prisijungimo sesijos metu neprieitų prie Turto banko IT (pvz. paliekant savo darbo vietą, privaloma atsijungti nuo Turto banko VPN, aktyvuoti kompiuterio ekrano užrakino funkciją ir pan.).

34. Nuotolinė prieiga suteikiama Paslaugų teikėjui arba jo subtiekejui tik:

34.1. pateikus nuotolinės prieigos gavėjo pasirašytą konfidencialumo pasižadėjimą;

34.2. pateikus Paslaugų teikėjo įgalioto asmens užpildytą nuotolinės prieigos prie Turto banko išteklių užsakymo formą;

34.3. nuotolinės prieigos užsakymą patvirtinus Turto banko darbuotojui, atsakingam už kibernetinį saugumą, ir suteikus prisijungimo duomenis;

34.4. ne ilgesniam nei paslaugoms suteikti reikalinga terminui, bet ne ilgiau nei 1 metai, kuriam praėjus, procedūra kartojama.

35. Paslaugų teikėjas, prisijungęs prie Turto banko IT, privalo laikytis šių Reikalavimų nuostatų.

VIII SKYRIUS

ŠALIŲ ATSAKOMYBĖ

36. Turto bankas turi teisę tikrinti kaip Paslaugų teikėjas laikosi Reikalavimų nuostatų, įskaitant, bet neapsiribojant, Paslaugų teikėjo prisijungimui prie Turto banko IT naudojamų darbo priemonių atitikties Reikalavimams patikrinimą be išankstinio įspėjimo.
