AKCINĖS BENDROVĖS TURTO BANKO

TECHNINIO STANDARTO PRIEDAS TECHNET

Kibernetinio saugumo reikalavimai pastatams

Dokumento žymuo: TB-TS-TECHNET-2026
Versija: v1.0

2026 m.

Turinys

1. BENDROSIOS NUOSTATOS

1.1. Dokumento paskirtis

Šis dokumentas nustato privalomus kibernetinio saugumo reikalavimus, taikomus visoms pastatų valdymo sistemoms ir inžinerinėms valdymo sistemoms (toliau – OT), diegiamoms ar atnaujinamoms Turto banko valdomuose, projektuojamuose, prižiūrimuose objektuose. Dokumentas apibrėžia reikalavimus, kurių įgyvendinimą būtina užtikrinti visuose siūlomuose OT sprendimuose.

1.2. Taikymo sritis

Reikalavimai taikomi visiems rangovams, teikiantiems paslaugas ar įrangą, susijusią su pastatų valdymo sistemomis, ŠVOK sistemomis, apšvietimo valdymo sistemomis, gaisro aptikimo ir gesinimo sistemomis, fizinės prieigos kontrolės sistemomis, fizinio saugumo sistemomis, energijos valdymo sistemomis ir kitomis inžinerinėmis sistemomis, kurios gali būti prijungtos prie tinklo. Reikalavimai taikomi tiek naujai diegiamoms, tiek atnaujinamoms OT sistemoms Turto banko valdomuose, projektuojamuose ir prižiūrimuose objektuose.

1.3. Reikalavimų laikymasis

Rangovas turi pateikti išsamų dokumentą, kuriame aprašoma, kaip siūlomas sprendimas atitinka visus šiame dokumente nurodytus reikalavimus. Bet kokie nukrypimai nuo reikalavimų turi būti aiškiai identifikuoti, pagrįsti ir suderinti su Užsakovo atsakingais asmenimis, kartu pateikiant alternatyvius kompensuojančius kontrolės mechanizmus. Visa reikalaujama dokumentacija turi būti pateikta lietuvių kalba.

2. TINKLO ARCHITEKTŪRA IR SEGMENTAVIMAS

2.1. Tinklo segmentavimas

Rengiamuose projektuose būtina įgyvendinti tinklo architektūrą, kurioje OT tinklai yra fiziškai arba logiškai atskirti nuo įmonės IT tinklo, naudojant pramoninės klasės ugniasienę su giluminės paketų analizės galimybėmis. Reikalavimus ugniasienei pateikia Turto bankas. Rangovas turi pateikti išsamų tinklo architektūros brėžinį redaguojamu elektroniniu formatu („Microsoft Visio“, „AutoCAD“), kuriame aiškiai pažymėti visi segmentai, ugniasienės, maršrutizatoriai ir kiti OT tinklo įrenginiai, nurodant kiekvieno komponento paskirtį, ryšius tarp jų ir loginio atskyrimo konfigūraciją. Turto bankas pateikia OT tinklo loginio segmentavimo informaciją, kuri nurodoma 1 lentelėje.

1 lentelė

OT tinklo loginio segmentavimo informacija

Pateikiama informacija	Reikalavimas	Paskirtis
VLAN pavadinimas ir ID	Turi būti pateikta	Segmento identifikavimas ir atsekamumas.
VLAN paskirtis	Turi būti pateikta	Sistemos arba funkcinės zonos paskirties apibrėžimas.
IP adresų diapazonai	Turi būti pateikta	Tinklo adresavimo planavimas ir taisyklių sudarymas.
Tinklo kaukės	Turi būti pateikta	Tinklo ribų, dydžio ir segmentų atskyrimo nustatymas.

Kritinėms sistemoms, įskaitant vaizdo stebėjimo, saugos, gaisro aptikimo ir gesinimo, evakuacijos valdymo ir fizinės prieigos kontrolės sistemas, turi būti naudojami fiziškai atskirti tinklo komutatoriai, užtikrinant, kad šių sistemų veikimas nepriklausytų nuo bendros OT tinklo infrastruktūros. OT tinklo valdymui naudojamos įrangos reikalavimus pateikia Turto bankas.

2.2. Tinklo architektūros lygmenys

OT tinklo architektūra turi būti suskirstyta į ne mažiau kaip tris lygmenis, kurie pateikiami 2 lentelėje.

2 lentelė

OT tinklo architektūros lygmenys

Lygmuo	Pavyzdiniai komponentai	Komunikacijos ir atskyrimo reikalavimas
Valdymo lygmuo (Management Level)	Operatorių darbo vietos, serveriai	Leidžiama komunikacija tik su automatizacijos lygmeniu, jei ryšys būtinas sistemos veikimui.
Automatizacijos lygmuo (Automation Level)	Valdikliai, tinklo įrenginiai	Veikia kaip tarpinis lygmuo tarp valdymo ir lauko įrenginių lygmenų; tiesioginiai ryšiai ribojami taisyklėmis.
Lauko įrenginių lygmuo (Field Level)	Jutikliai, matuokliai	Negali tiesiogiai komunikuoti su valdymo lygmeniu, išskyrus Turto banko suderintus atvejus.

Kiekvienas lygmuo turi būti atskirtas naudojant loginį atskyrimo būdą, kuris riboja duomenų srautus tarp skirtingų lygmenų. Rangovas turi pateikti išsamią dokumentaciją, paaiškinančią kiekvieno lygmens paskirtį, veikimą ir saugumo kontrolės mechanizmus. Turi būti įdiegti mechanizmai, užtikrinantys, kad kompromituotas vienas lygmuo negalėtų tiesiogiai paveikti kitų lygmenų saugumo.

2.3. Saugos sistemų atskyrimas

Saugos sistemų atskyrimo, atsparumo ir avarinio veikimo reikalavimai pateikiami 3 lentelėje.

3 lentelė

Saugos sistemų atskyrimo ir atsparumo reikalavimai

Reikalavimų blokas	Privaloma užtikrinti / pateikti
Atsparumo dokumentacija	Tinklo architektūros aprašymas, prieigos kontrolės mechanizmai, autentifikacijos metodai, šifravimo protokolai ir atsarginių kopijų strategijos.
Kritinės funkcijos	Saugos sistemų kritinės funkcijos turi veikti net tada, kai kitos OT dalys yra pažeistos arba nepasiekiamos.
Avarinis režimas	Turi būti numatyti darbo režimai, leidžiantys valdyti saugos sistemas visiško tinklo ryšio praradimo atveju.
Pasiekiamumo kontrolė	Saugos sistemos turi turėti funkcionalumą, skirtą sistemų pasiekiamumui ir veikimui tikrinti.

2.4. Ugniasienės ir OT tinklo įrenginių konfigūracija

Ugniasienės turi būti sukonfigūruotos laikantis principo „uždrausti viską, išskyrus tai, kas būtina“ visuose tinklo segmentuose. Turi būti dokumentuotas kiekvienas leidžiamas ryšys. Rangovas turi pateikti išsamų ugniasienės taisyklių sąrašą su aiškiu kiekvienos taisyklės pagrindimu. Sąrašas turi būti suderintas su Turto banko atsakingu asmeniu, o taisyklių realizavimą atlieka Turto banko atsakingas asmuo. Privalomi ugniasienės taisyklių sąrašo laukai pateikiami 4 lentelėje.

4 lentelė

Ugniasienės taisyklių sąrašo privalomi laukai

Laukas	Privaloma nurodyti
Šaltinio IP adresas ar tinklas	Taip
Paskirties IP adresas ar tinklas	Taip
Protokolas ir prievadas	Taip
Veiksmas	Leisti / drausti
Taisyklės paskirtis ir pagrindimas	Taip

Ugniasienės ir OT tinklo įrenginių konfigūravimo principai pateikiami 5 lentelėje.

5 lentelė

Ugniasienės ir OT tinklo įrenginių konfigūravimo principai

Konfigūravimo principas	Reikalavimas
Įeinančio ir išeinančio ryšio ribojimas	Taisyklės turi riboti duomenų srautą tarp visų tinklo segmentų, taikant mažiausių privilegijų principą.
Būtini protokolai ir prievadai	Leidžiami tik sistemų veikimui būtini protokolai ir prievadai, o visi nenaudojami protokolai ir prievadai turi būti užblokuoti.
Pakeitimų valdymas	Ugniasienės konfigūracijos pakeitimus atlieka tik Turto banko atsakingi asmenys.
Giluminė paketų analizė	Ugniasienė turi palaikyti DPI pramoniniams protokolams, įskaitant Modbus, BACnet, KNX ir kitus taikomus protokolus.
Kelių ugniasienių veikimas	Jei architektūroje naudojamos kelios ugniasienės, turi būti užtikrinta jų sinchronizacija ir integruotas veikimas.
Lygmenų komunikacija	Komunikacija tarp skirtingų lygmenų turi būti įmanoma tik tarp gretimų lygmenų, jeigu Turto bankas nėra suderinęs kitaip.
Įrenginių autentifikavimas	OT tinkle turi būti realizuotas pajungiamų įrenginių autentifikavimas; neautorizuoti įrenginiai turi būti blokuojami ir izoliuojami.

2.5. Integravimas su Turto banko saugumo sistemomis

Visi OT tinklo komponentai turi būti integruoti su Turto banko centralizuota žurnalinių įrašų kaupimo ir valdymo sistema. Į centralizuotą žurnalų kaupimo sistemą perduodami įvykiai pateikiami 6 lentelėje.

6 lentelė

Į centralizuotą žurnalų kaupimo sistemą perduodami įvykiai

Įvykio kategorija	Turi būti perduodama
OT sistemų įjungimas, išjungimas ar perkrovimas	Taip
Naudotojų ir administratorių autentifikavimo įvykiai	Taip
Paskyrų sukūrimas ir prieigų pakeitimai	Taip
OT sistemų konfigūravimo parametrų pakeitimai	Taip
Ugniasienių taisyklių pakeitimai	Taip
Žurnalinių įrašų rinkimo funkcijos įjungimas, išjungimas	Taip

Visi OT komponentų žurnaliniai įrašai turi būti perduodami į Turto banko centralizuoto žurnalų kaupimo sprendimą. Žurnalinių įrašų perdavimo reikalavimai pateikiami 7 lentelėje.

7 lentelė

Žurnalinių įrašų perdavimo reikalavimai

Parametras	**Reikalavimas**
Protokolas	Syslog protokolas (RFC 5424)
Transportas	Šifruotas TLS transporto protokolas (Syslog over TLS, RFC 5425)
Formatas	Common Event Format (CEF) arba Structured Data formatas
Perdavimo mechanizmas	TCP protokolas
Atsparumas ryšio sutrikimams	Lokalus įrašų kaupimas ryšio sutrikimo atveju ir automatinis perdavimas atkūrus ryšį

NTP laiko sinchronizacijos reikalavimai pateikiami 8 lentelėje.

8 lentelė

NTP laiko sinchronizacijos reikalavimai

Sritis	**Reikalavimas**	**Taikymas / pastaba**
Laiko šaltinis	Visi OT komponentai turi sinchronizuoti laiką naudodami Turto banko nurodytus NTP šaltinius.	Taikoma visiems OT komponentams, kurie palaiko NTP funkcionalumą.
Laiko sinchronizacijos protokolas	Laiko sinchronizacijai turi būti naudojamas NTP protokolas.	Kiti protokolai gali būti naudojami tik suderinus su Turto banko atsakingu asmeniu.
Laiko zona	Visi OT komponentai turi būti sukonfigūruoti pagal Lietuvos Respublikos vietos laiką ir taikomą vasaros / žiemos laiko keitimą.	Taikoma sistemoms, kurios saugo arba perduoda įvykių laiką.
Žurnalinių įrašų tikslumas	Įvykių laiko žymos turi būti pakankamai tikslios, kad būtų galima atlikti įvykių sekos analizę ir incidentų tyrimą.	OT sistemoms taikoma laiko paklaida turi būti ne didesnė kaip 60 sekundžių.
Laiko sinchronizacijos stebėsena	Turi būti galimybė nustatyti, ar OT komponento laikas sinchronizuotas su nurodytu laiko šaltiniu.	Tikrinama konfigūracijos arba diagnostikos priemonėmis.
Ryšio sutrikimai	Jei ryšys su NTP šaltiniu laikinai nepasiekiamas, įrenginys turi tęsti veikimą su paskutine galiojančia laiko reikšme.	Atkūrus ryšį, laikas turi būti automatiškai sinchronizuojamas.
Įrodymas	Rangovas turi pateikti laiko sinchronizacijos konfigūracijos aprašymą arba kitą įrodymą, kad NTP reikalavimai įgyvendinti.	Pateikiama prieš perduodant sistemą eksploatacijai.

Laiko sinchronizacijos reikalavimai taikomi visiems OT komponentams, kuriuose registruojami įvykiai, saugomi žurnaliniai įrašai arba perduodami duomenys į Turto banko centralizuotą žurnalinių įrašų kaupimo ir valdymo sistemą. Jei OT komponentas nepalaiko NTP

funkcionalumo, rangovas turi pateikti pagrindimą ir suderinti alternatyvų laiko apskaitos arba įvykių koreliacijos sprendimą su Turto banko atsakingu asmeniu.

Centralizuota nuotolinio prisijungimo architektūra turi būti taikoma visiems OT sprendimams, kuriems reikalinga nuotolinė prieiga. OT sprendimai su Turto banko tinklu integruojami naudojant site-to-site VPN sprendimą, kurio reikalavimai pateikiami 9 lentelėje.

9 lentelė

Site-to-site VPN sprendimo reikalavimai

VPN parametras	**Reikalavimas**
Tunelio režimas	IPsec tunelinis režimas
Šifravimas	AES-256 ar stipresnis
Maišos algoritmas	SHA-256 ar stipresnis
Raktų sauga	Perfect Forward Secrecy (PFS)

Nuotolinės prieigos, VPN konfigūravimo ir prisijungimų stebėsenos reikalavimai pateikiami 10 lentelėje.

10 lentelė

Nuotolinės prieigos ir prisijungimų stebėsenos reikalavimai

Sritis	**Reikalavimas**
VPN konfigūravimas	VPN sprendimo konfigūravimą atlieka Turto banko atsakingas asmuo.
VPN pralaidumas	VPN sprendimas turi užtikrinti pakankamą pralaidumą operaciniams ir stebėsenos duomenims perduoti.
Naudotojai	Turto banko darbuotojai, išoriniai tiekėjai ir rangovai naudoja tik Turto banko suteiktus nuotolinės prieigos sprendimus.
Prisijungimų stebėsena	Turi būti fiksuojami visi sėkmingi ir nesėkmingi prisijungimo bandymai prie nutolusių OT sprendimų.
Nuotolinės sesijos	Nuotolinės sesijos turi būti įrašomos.
Išorinė prieiga	Prieiga prie OT sistemų iš išorinių tinklų yra draudžiama.

3. PRIEIGOS VALDYMAS

3.1. Paskyrų valdymas

Paskyrų ir prieigos valdymo reikalavimai pateikiami 11 lentelėje.

11 lentelė

Paskyrų ir prieigos valdymo reikalavimai

Sritis	Reikalavimas
Paskyrų sukūrimas ir valdymas	OT sistemos turi turėti paskyrų sukūrimo ir valdymo funkcionalumą.
Prieigos principas	Prieigos prie OT sistemų turi būti grindžiamos rolėmis ir mažiausių privilegijų principu.
Žurnalizavimas	Paskyrų naudojimas ir prieigos teisių keitimas turi būti žurnalizuojami ir perduodami į Turto banko centralizuotą žurnalinių įrašų kaupimo ir valdymo sistemą.
Nenaudojamos paskyros	Nenaudojamos paskyros blokuojamos pagal Turto banko saugos taisyklėse nurodytus reikalavimus.

3.2. Slaptažodžių politika

Būtina užtikrinti, kad OT sistemose būtų laikomasi slaptažodžių sudarymo reikalavimų ir daugiafaktorės autentifikacijos reikalavimų, kurie pateikiami 12 ir 13 lentelėse.

12 lentelė

Slaptažodžių politikos minimalūs reikalavimai

Reikalavimas	Vertė	Taikymas / pastaba
Minimalus ilgis	16 simbolių	Taikoma visoms OT paskyroms, jei nėra suderintos išimties.
Sudėtingumas	Didžiosios ir mažosios raidės, skaičiai, specialūs simboliai	Taikoma vietinėms ir administravimo paskyroms.
Galiojimo terminas	Ne ilgiau kaip 90 dienų	Išimtys galimos tik suderinus su Turto banko atsakingu asmeniu.
Istorija	Bent 6 paskutiniai slaptažodžiai	Neleidžiamas pakartotinis paskutinių slaptažodžių naudojimas.
Draudžiami slaptažodžiai	Lengvai atspėjami, dažniausiai naudojami ar pažeidžiami slaptažodžiai	Turi būti valdoma techninėmis priemonėmis arba dokumentuota procedūra.

13 lentelė

Daugiafaktorės autentifikacijos (MFA) reikalavimai

Sritis	Reikalavimas	Taikymas / pastaba
Administravimo prieiga	Kai OT sistema, įrenginys arba administravimo platforma palaiko daugiafaktorę autentifikaciją (MFA), ji privalo būti taikoma administravimo prieigoms.	Taikoma administratorių, tiekėjų, rangovų ir kitoms privilegijuotoms paskyroms.
Nuotolinė prieiga	Nuotolinei prieigai prie OT sistemų MFA privaloma, kai ji realizuojama per Turto banko suteiktą nuotolinės prieigos sprendimą.	Taikoma visiems išoriniams tiekėjams, rangovams ir Turto banko darbuotojams, kurie jungiasi nuotoliniu būdu.
Privilegijuotos paskyros	Privilegijuotos paskyros turi būti apsaugotos MFA, jei techninis sprendimas tai palaiko.	Taikoma sistemų administratoriams, aptarnavimo paskyroms ir gamintojo administravimo paskyroms, jei jos naudojamos.
Išimtys	Jei OT sistema arba įrenginys MFA nepalaiko, turi būti taikomos kompensuojančios saugumo priemonės.	Išimtis turi būti pagrįsta ir suderinta su Turto banko atsakingu asmeniu.
Kompensuojančios priemonės	Gali būti taikomas prisijungimas per Turto banko tarpinį prisijungimų serverį, VPN, IP adresų ribojimas, sesijų įrašymas ir papildomas žurnalizavimas.	Priemonės turi būti dokumentuotos ir suderintos su Turto banku.
Įrodymas	Rangovas turi pateikti MFA taikymo arba kompensuojančių priemonių aprašymą.	Pateikiama prieš perduodant sistemą eksploatacijai.

MFA reikalavimai taikomi visoms OT sistemoms, įrenginiams ir administravimo platformoms, kuriose realizuotos privilegijuotos paskyros arba nuotolinio administravimo funkcijos. Jei MFA taikymas techniškai neįmanomas, rangovas privalo pateikti pagrindimą ir suderinti kompensuojančias saugumo priemones su Turto banko atsakingu asmeniu.

3.3. Rolių valdymas

OT sistemose turi būti įdiegta rolėmis grįsta prieigos kontrolės sistema (RBAC). Rolių valdymo ir dokumentavimo reikalavimai pateikiami 14 lentelėje.

14 lentelė

Rolių valdymo ir dokumentavimo reikalavimai

Sritis	Reikalavimas	Įrodymas / dokumentacija
Rolių apibrėžimas	Turi būti palaikomas rolių apibrėžimas ir valdymas.	Rolių sąrašas.
Mažiausių privilegijų principas	Turi būti suteikiamos tik funkcijoms atlikti būtinos teisės.	Teisių matrica arba kiekvienos rolės teisių aprašymas.

Sritis	Reikalavimas	Įrodymas / dokumentacija
Rolių priskyrimo auditavimas	Turi būti vykdomas rolių priskyrimo naudotojams auditavimas.	Auditavimo žurnalai arba audito mechanizmo aprašymas.
Rolių hierarchija	Turi būti dokumentuota rolių hierarchija, nurodant pavaldumo ir paveldėjimo santykius.	Rolių hierarchijos aprašymas.
Kiekvienos rolės teisės	Turi būti dokumentuotos kiekvienai rolei suteikiamos teisės.	Kiekvienos rolės teisių aprašymas.

3.4. Fizinė įrenginių apsauga

Visi OT komponentai turi būti fiziškai apsaugoti nuo nesankcionuotos prieigos. Fizinės apsaugos reikalavimai pateikiami lentelėje.

15 lentelė

Fizinės OT komponentų apsaugos reikalavimai

Objektas	Reikalavimas	Įrodymas / dokumentacija
Serveriai ir tinklo įrenginiai	Turi būti laikomi užrakintose serverių spintose ar patalpose.	Ryšio patalpų ir serverių spintų apsaugos aprašymas.
Valdikliai ir kita įranga	Turi būti laikoma užrakintuose skyduose ar spintose.	Skydų ir spintų apsaugos aprašymas.
Lauko įrenginiai	Turi būti apsaugoti nuo neteisėtos prieigos ir vandalizmo.	Lauko įrenginių apsaugos aprašymas.
Kabeliai	Turi būti apsaugoti nuo nesankcionuotos prieigos ir pažeidimų.	Kabelių apsaugos aprašymas.
Priežiūra	Fizinė įrenginių apsauga turi būti reguliariai tikrinama ir prižiūrima.	Patikros arba priežiūros tvarka.

Fizinė įrenginių apsauga turi atitikti Turto banko fizinės saugos standartus ir gerąsias praktikas. Fizinė įrenginių apsauga turi būti reguliariai tikrinama ir prižiūrima.

4. PROGRAMINĖS ĮRANGOS IR ĮRENGINIŲ SAUGUMO VALDYMAS

Programinės įrangos, OT įrenginių saugumo valdymo, inventorizacijos ir atkūrimo reikalavimai pateikiami lentelėje.

16 lentelė

Programinės įrangos ir OT įrenginių saugumo valdymo suvestinė

Sritis	Privaloma pateikti / užtikrinti	Terminas / pastaba
Programinės įrangos pataisų valdymas	Pataisų šaltinių aprašymas, pataisų diegimo periodiškumas, pataisų diegimo ir atšaukimo procedūra.	Kritinės spragos – ne vėliau kaip per 60 dienų; ypač kritinės – per 14 dienų.
Programinės įrangos inventorizacija	Programinės įrangos pavadinimas ir versija, gamintojas, licencijos informacija, diegimo data ir vieta, palaikymo informacija.	Atnaujinama po kiekvieno pakeitimo.
OT įrenginių saugumo valdymas	Saugios nuostatos, nenaudojamų paslaugų, prievadų, protokolų ir taikomųjų programų išjungimas / pašalinimas.	Nuostatos nustatomos ir patikrinamos prieš diegimą į eksploataciją.
OT įrenginių inventorizacija	Įrenginio tipas ir modelis, gamintojas, aparatinės ir programinės įrangos versijos, IP ir MAC adresai, fizinė vieta, atsakingas asmuo, palaikymo informacija.	Atnaujinama po kiekvieno pakeitimo.
Kenkėjiškos programinės įrangos apsauga	Turto banko pateiktos apsaugos priemonės arba alternatyvių saugumo priemonių aprašymas.	Alternatyvos pateikiamos, jei OT įrenginys nepalaiko Turto banko priemonių.
Atsarginės kopijos ir atkūrimas	Atsarginių kopijų grafikas, procedūros, testavimo procedūros, atkūrimo prioritetai, RTO ir RPO.	Atkūrimo procesas turi apimti visus kritinius OT komponentus.

OT įrenginių saugios konfigūracijos reikalavimai taikomi visiems OT komponentams, kuriuose realizuotos naudotojų paskyros, administravimo funkcijos, tinklo sąsajos arba programinės įrangos konfigūravimo galimybės. Jeigu OT įrenginys nepalaiko kurio nors reikalavimo, rangovas privalo pateikti kompensuojančias saugumo priemones ir jas suderinti su Turto banko atsakingais asmenimis.

17 lentelė

OT įrenginių saugios konfigūracijos (Hardening) reikalavimai

Sritis	Reikalavimas	Įrodymas / dokumentacija
Numatytosios paskyros	Visos gamintojo numatytosios paskyros turi būti pašalintos, išjungtos arba pervadintos, jeigu tai leidžia gamintojo sprendimas.	Konfigūracijos aprašymas arba ekrano kopijos.
Numatytieji slaptažodžiai	Visi gamintojo numatytieji slaptažodžiai turi būti pakeisti prieš perduodant sistemą eksploatacijai.	Paleidimo ir konfigūravimo procedūra.
Testinės ir laikinos paskyros	Testinės, demonstracinės, laikinos arba diegimo metu naudotos paskyros negali būti naudojamos eksploatuojamoje sistemoje.	Paskyrų sąrašas.
Nenaudojamos paslaugos	Visos sistemos veikimui nereikalingos paslaugos ir procesai turi būti išjungti arba pašalinti.	Saugios konfigūracijos aprašymas.
Nenaudojami protokolai	Nenaudojami tinklo protokolai turi būti išjungti.	Konfigūracijos dokumentacija.
Nenaudojami prievadai	Nenaudojami fiziniai ir loginiai prievadai turi būti išjungti, užblokuoti arba apriboti.	Konfigūracijos dokumentacija.
Nuotolinis administravimas	Nuotolinis administravimas leidžiamas tik naudojant Turto banko patvirtintus prisijungimo būdus ir šifruotus protokolus.	Tinklo schema ir administravimo procedūra.
Šifruoti valdymo protokolai	HTTP, Telnet, FTP ir kiti nešifruoti administravimo protokolai negali būti naudojami, jeigu gamintojas palaiko saugesnes alternatyvas.	Konfigūracijos dokumentacija.
Belaidės sąsajos	Nenaudojamos Wi-Fi, Bluetooth, NFC ar kitos belaidžio ryšio sąsajos turi būti išjungtos.	Konfigūracijos dokumentacija.
USB ir išorinės laikmenos	Jei funkcionalumas nereikalingas eksploatacijai, turi būti ribojamas arba išjungiamas USB bei kitų išorinių laikmenų naudojimas.	Konfigūracijos dokumentacija.
Programinė įranga	Leidžiama naudoti tik gamintojo palaikomą programinės įrangos versiją.	Programinės įrangos inventorizacija.
Saugumo žurnalai	Visi svarbūs administravimo ir saugos įvykiai turi būti registruojami ir perduodami į centralizuotą žurnalų kaupimo sistemą.	Testavimo rezultatai ir konfigūracija.
Laiko sinchronizacija	Įrenginys turi sinchronizuoti laiką naudojant Turto banko nurodytus NTP šaltinius.	Konfigūracijos dokumentacija.
Konfigūracijos atsarginės kopijos	Turi būti numatytas konfigūracijos atsarginių kopijų sudarymas ir atkūrimo procedūra.	Atsarginių kopijų procedūra.

Lentelėje nurodyti reikalavimai laikomi minimaliais ir turi būti įgyvendinti prieš OT sistemų bei įrenginių perdavimą eksploatacijai. Pateikta dokumentacija ir inventorizacijos duomenys turi būti atnaujinami po kiekvieno reikšmingo pakeitimo.

5. GSM MARŠRUTIZATORIŲ TECHNINIAI REIKALAVIMAI

Objekte naudojami GSM maršrutizatoriai turi būti pramoninio lygio įrenginiai, užtikrinantys stabilų ir nepertraukiamą duomenų perdavimą. Reikalavimus atitinka „Teltonika“ RUT9xx serijos modeliai, įskaitant RUT951, RUT956 ar naujesnius lygiaverčius šios serijos modelius, arba technologiškai lygiaverčiai įrenginiai, suderinti su Turto banko atsakingu asmeniu. Jungiantis prie Turto banko infrastruktūros ar atliekant įrenginių autentifikavimą tinkle, GSM maršrutizatoriai privalo palaikyti XAUTH išplėstinį naudotojų autentifikavimo protokolą (angl. Extended Authentication) ir užtikrinti centralizuotą prieigos teisių validavimą prieš sukuriant duomenų perdavimo sesiją. Minimalūs techniniai reikalavimai GSM 4G LTE maršrutizatoriui pateikiami lentelėje.

18 lentelė

GSM 4G LTE maršrutizatoriaus techniniai reikalavimai

Parametras	**Minimalus reikalavimas**
Mobilus ryšys	4G LTE ryšys, ne mažiau kaip 2 SIM
VPN	IPsec VPN klientas su IKEv2 protokolu
Autentifikacija	Sertifikatai (X.509) ir XAUTH
Šifravimas ir maišos algoritmas	AES-256 šifravimas ir SHA-256 maišos algoritmas
Ethernet	Ne mažiau kaip 1 Ethernet portas
Žurnalai	Maršrutizatoriaus žurnalinių įrašų Syslog formatu siuntimas į TB centralizuotą žurnalinių įrašų kaupimo sistemą
VLAN	VLAN palaikymas
Wi-Fi	Galimybė atjungti Wi-Fi
Suderinamumas su esamomis sistemomis	Maršrutizatorius turi būti suderinamas su Turto banke naudojama GSM 4G LTE maršrutizatorių centralizuoto valdymo sistema.

Lentelėje nurodyti reikalavimai laikomi minimaliais. Jeigu siūlomas įrenginys neatitinka bent vieno reikalavimo, jo lygiavertiškumas turi būti pagrįstas ir suderintas su Turto banko atsakingu asmeniu.

6. TECHNINIAI REIKALAVIMAI UGNIASIENEI

6.1. Ugniasienės taikymo, pateikimo ir valdymo reikalavimai

Bendrieji ugniasienės taikymo, pateikimo, suderinamumo ir valdymo reikalavimai pateikiami 19 lentelėje.

19 lentelė

Bendrieji ugniasienės taikymo ir pateikimo reikalavimai

Sritis	Reikalavimas
Ryšio paslauga	Pastato valdymo technologinė įranga turi būti pasiekiama per BĮ Kertinio valstybės telekomunikacijų centro teikiamą tinklo paslaugą iš Turto banko būstinės Kęstučio g. 45, Vilniuje.
Suderinamumas	Pastate turi būti įrengtas tinklo įrenginys su ugniasienės funkcionalumu, visiškai suderinamas su Turto banke naudojama ir centralizuotai valdoma „Fortinet“ įranga.
Mobilus ryšys	Jeigu pastate nėra arba nebus teikiama KVTC tinklo paslauga, ugniasienė papildomai turi turėti galimybę duomenis perduoti naudojant mobiliojo ryšio technologijas, o SIM kortelę pateikia Turto bankas.
Konfigūravimas ir valdymas	Ugniasienę konfigūruoja ir valdo Turto bankas.
Registravimas	Ugniasienė turi būti registruota gamintojo sistemoje Turto banko vardu, pateikiant gamintojo arba įgalioto atstovo registravimo deklaraciją arba kitą tai patvirtinančią informaciją.
Gyvavimo ciklas	Ugniasienės įrangos gamintojas negali būti paskelbęs apie siūlomos ugniasienės gamybos arba tobulinimo nutraukimą, įskaitant „End of Life“ ar „Discontinued“ būsenas.
Įrangos būklė	Ugniasienė privalo būti nauja ir nenaudota; gamykliškai atnaujinti komponentai („refurbished“) neleistini.
Prijungiamos sistemos	Iki ugniasienės turi būti atvesti kompiuteriniai tinklai, fiziškai arba logiškai atskiriant PVS, šildymo ir vėsinimo sistemų valdymą, pastato apsaugos kontrolerį, vaizdo stebėjimo sistemą, elektroninės įeigos kontrolės sistemą (-as) ir kitas pastato valdymo sistemas.

6.2. Minimalūs techniniai reikalavimai ugniasienei

20 lentelė

Minimalūs techniniai reikalavimai ugniasienei

Reikalavimas	Aprašymas
Produkto surinkimo reikalavimai	Ugniasienė turi būti specializuotas aparatinis-programinis įrenginys (angl. Appliance) komplektuojamas paties gamintojo. Siūloma įranga negali būti realizuota naudojant virtualizacijos platformomis paremtus sprendimus.
Konstrukcija	Ne daugiau kaip 1U aukščio, montuojama į 19 colių komutacinę spintą, pateikiama su montavimo komponentais ir / arba lentyna, skirtais siūlomą įrangą patalpinti komutacinėje spintoje.

Reikalavimas	Aprašymas
Suderinamumas	Turi būti visiškai suderinama su Turto banke naudojamais ugniasienių centralizuoto valdymo sprendimais „FortiManager“ ir „FortiCloud“, kurių pagalba centralizuotai ir efektyviai administruojama visa Turto banko tinklo saugumo infrastruktūra iš vienos vietos.
Vidinio tinklo prievadai (portai)	Ne mažiau kaip 5 vnt. 1G RJ-45 vidinio tinklo prievadų. Kiekvienas prievadas turi palaikyti Ethernet 1G ryšį per RJ-45 jungtį. Suderinus su Turto banku ir pagrindus tinklo architektūros sprendinį, prievadų skaičius gali būti mažinamas iki 4 vnt., jeigu užtikrinamas visų prijungiamų OT tinklo segmentų, sistemų ir rezervinių jungčių poreikis pagal šios techninės specifikacijos reikalavimus.
Išorinio tinklo (WAN) prievadai (portai)	Ne mažiau kaip 1 vnt. 1G (RJ-45), lizdas privalo palaikyti RJ-45 standarto jungtis.
Dedikuoti valdymo prievadai	Turi būti ne mažiau kaip 1 konsolės prievadas RJ-45 ir ne mažiau kaip 1 USB prievadas.
Belaidis duomenų perdavimas (taikoma jeigu pastate nėra KVTC teikiamo laidinio ryšio)	Integruotas 3G / 4G / LTE / 5G belaidžio WAN modulis su išorinėmis antenomis. Esant poreikiui užtikrinti stabilų ryšį papildomai pateikiami ir antenų prailginimo kabeliai.
Našumas (ne mažiau)	Ugniasienės pralaidumas turi būti ne mažesnis kaip 3 Gbps, IPS pralaidumas – ne mažesnis kaip 2 Gbps, NGFW pralaidumas – ne mažesnis kaip 250 Mbps, SSL VPN pralaidumas – ne mažesnis kaip 150 Mbps. Įrenginys turi palaikyti iki 500 IPsec VPN ir iki 100 SSL VPN naudotojų.
Saugumo funkcijos	Turi būti integruotas SD-WAN arba lygiavertis funkcionalumas ir nulinio pasitikėjimo tinklo prieigos (ZTNA) kontrolė.
Valdymas	Ne mažiau nei: žiniatinklio sąsaja (HTTPS), SSH, konsolė RJ-45.
Galimi ugniasienės darbo režimai	L3 ir L2 pagal OSI modelį.
Ugniasienės funkcionalumas	Turi būti galimybė kurti taisykles pagal vartotojus.
Maršrutizavimas	Turi palaikyti statinį, dinaminį ir maršrutizavimą pagal taisykles (angl. policy routing) arba lygiaverčius.
Palaikomi NAT (Network Address Translation) tipai	Source NAT (SNAT), Destination NAT (DNAT), Virtual IP (VIP), One-to-One NAT, NAT Traversal, NAT-based Policy Routing arba lygiaverčius.
Integruoti serveriai	Turi turėti šiuos integruotus serverius: DHCP serverį (angl. Dynamic Host Configuration Protocol), NTP serverį (angl. Network Time Protocol), DNS tarpinį serverį (angl. DNS proxy server).
IPsec kriptavimo, maišos ir autentifikavimo algoritmai	Turi palaikyti AES-256 IPsec šifravimo algoritmą, SHA-256, SHA-384 ir SHA-512 maišos algoritmus, PSK, X.509 sertifikatus ir RSA autentifikavimo algoritmus bei IKEv2 VPN modulius. DES, 3DES ir MD5 algoritmai negali būti naudojami.
VPN funkcionalumas	Turi būti galimybė redaguoti SSL VPN portalą, naudotis SSL VPN per naršyklę be papildomų agentų ar programinės įrangos, naudoti VPN klientą, palaikantį IPsec ir SSL protokolus. Kliento programinė įranga turi būti to paties gamintojo kaip ir įranga ir turi palaikyti skaitmeninių sertifikatų naudojimą tapatybės nustatymui.

Reikalavimas	Aprašymas
Įvykių žurnalo įrašai	Turi būti fiksuojami ir kaupiami šių kategorijų žurnalų įrašai: perduoto srauto sesijos, sesijos su pažeidimais, sistemos ir administratorių veiksmų įvykiai, maršrutizavimo ir VPN įvykių įrašai (ne mažiau).
Įvykių žurnalų (event log) įrašų saugojimo pasirinkimas	Turi būti galimybė žurnalų įrašus saugoti lokaliai ir siųsti į Syslog / SIEM serverius.
Integravimas	Turi palaikyti SNMP (angl. Simple Network Management Protocol): palaikyti SNMPv1, SNMPv2c ir SNMPv3 protokolus; palaikyti SNMP trap, Get ir Set užklausas; turi būti galimybė naudoti SNMP OID duomenims gauti ir valdyti.
Galimybė užtikrinti aukšto patikimumo sprendimus	Ugniasienė turi turėti galimybę užtikrinti aukšto patikimumo sprendimus (palaikomi Active / Passive, Clustering arba lygiaverčiai įrenginių sujungimo būdai).
Palaikymo paslaugos / įrangos garantijos	Turi būti pateiktas palaikymas, apimantis techninį palaikymą, prietaiso garantiją, programinės įrangos atnaujinimus ir klaidų taisymą 5 metų laikotarpiui.

Jeigu pastate diegiami sprendimai nepalaiko kokio nors funkcionalumo arba integracinių sprendimų, tiekėjas / rangovas gali pateikti lygiavertį sprendimą ir, suderinęs jį su Turto banku, įgyvendinti. Turi būti užtikrintas visiškai veikiantis ugniasienės sprendimas, numatant visą techninę ir programinę įrangą.

Tiekėjų siūlomi sprendimai turi atitikti Bendrąjį duomenų apsaugos reglamentą (BDAR), Kibernetinio saugumo įstatymą ir kitus taikytinus nacionalinius bei tarptautinius reglamentus. Šie reikalavimai yra privalomi visiems tiekėjams, teikiantiems paslaugas ar įrangą, susijusią su Turto banko valdomuose objektuose projektuojamais ir įrengiamais OT sprendimais. Tiekėjai turi bendradarbiauti su Turto banko atsakingais asmenimis siekiant užtikrinti šių reikalavimų įgyvendinimą ir atitiktį. Turto bankas pasilieka teisę keisti ir papildyti šiuos reikalavimus pagal poreikį.

7. SĄVOKOS IR SANTRUMPOS

Toliau pateikiamos dokumente vartojamos sąvokos ir santrumpos, reikalingos vienodam techninių reikalavimų supratimui.

21 lentelė

Sąvokos ir santrumpos

Eil. Nr.	Sąvoka / santrumpa	Reikšmė
1	AES-256	Akcinė bendrovė Turto bankas.
2	Užsakovas	Turto bankas arba jo įgaliotas atstovas, nustatantis ir derinantis reikalavimus.

Eil. Nr.	Sąvoka / santrumpa	Reikšmė
3	Rangovas / tiekėjas	Asmuo ar organizacija, projektuojanti, tiekianti, diegianti arba prižiūrinti šiame dokumente nurodytus sprendinius.
4	OT	Operacinės technologijos / inžinerinių sistemų valdymo technologijos.
5	IT	Informacinės technologijos.
6	PVS	Pastato valdymo sistema.
7	Ugniasienė	Tinklo saugumo įrenginys arba sprendimas, ribojantis ir kontroliuojantis duomenų srautus tarp tinklo segmentų.
8	VLAN	Virtualus lokalus tinklas.
9	IP / MAC	Tinklo adresavimo identifikatoriai: IP adresas ir įrenginio fizinis MAC adresas.
10	WAN / Ethernet / RJ-45	Tinklo ryšio terminai: plataus masto tinklas, Ethernet ryšio technologija ir RJ-45 tinklo jungtis.
11	VPN / site-to-site VPN / SSL VPN	Virtualaus privataus tinklo sprendimai, naudojami saugiam ryšiui tarp tinklų arba nuotolinei prieigai užtikrinti.
12	IPsec / IKEv2	VPN ryšio saugos architektūra ir raktų apsikeitimo protokolas.
13	AES-256 / DES / 3DES	Šifravimo algoritmas, naudojamas duomenų konfidencialumui užtikrinti.
14	SHA-256 / SHA-384 / SHA-512	Maišos algoritmai, naudojami duomenų vientisumui tikrinti.
15	PSK / RSA / X.509 / PFS	Autentifikavimo, sertifikatų ir raktų saugos terminai, taikomi VPN ir šifruoto ryšio sprendiniuose.
16	XAUTH	Išplėstinis naudotojų autentifikavimo protokolas.
17	Syslog / CEF / Structured Data	Žurnalinių įrašų perdavimo protokolas ir įvykių duomenų formatai.
18	TLS / TCP / HTTPS / SSH	Šifruoto, patikimo arba saugaus ryšio ir valdymo protokolai.
19	SIEM	Saugumo informacijos ir įvykių valdymo sistema.
20	DPI / Deep Packet Inspection	Giluminė paketų analizė.
21	Modbus / BACnet / KNX	Pramoninių ir pastatų automatikos sistemų ryšio protokolai ar standartai.
22	NAT / SNAT / DNAT / VIP	Tinklo adresų vertimo ir virtualaus IP adreso terminai.
23	Policy routing / NAT Traversal / NAT-based Policy Routing	Maršrutizavimo ir NAT veikimo būdai, naudojami tinklo srautams valdyti.
24	SNMP / SNMP OID	Tinklo įrenginių valdymo ir stebėsenos protokolas bei jo objektų identifikatoriai.
25	DHCP / NTP / DNS	Integruotų tinklo paslaugų protokolai: adresų priskyrimas, laiko sinchronizavimas ir vardų sistema.
26	RBAC	Rolėmis grįsta prieigos kontrolė.
27	RTO / RPO	Atkūrimo laiko tikslas ir atkūrimo taško tikslas.

Eil. Nr.	Sąvoka / santrumpa	Reikšmė
28	GSM / 4G LTE / 5G / LTE / SIM	Mobiliojo ryšio technologijos ir abonento identifikavimo kortelė, naudojamos duomenų perdavimui.
29	Wi-Fi	Belaidžio ryšio technologija.
30	KVTC	Kertinis valstybės telekomunikacijų centras.
31	BDAR	Bendrasis duomenų apsaugos reglamentas.
32	Fortinet / FortiManager / FortiCloud	Ugniasienių ir jų centralizuoto valdymo sprendimų gamintojo bei valdymo platformų pavadinimai.
33	NGFW / SD-WAN / ZTNA	Pažangios tinklo saugumo ir plačiojo tinklo valdymo funkcijos.
34	OSI	Tinklo ryšio modelis, apibrėžiantis ryšio funkcijų lygmenis.
35	Appliance / refurbished / End of Life / Discontinued	Įrangos tipo, būklės ir gamintojo gyvavimo ciklo terminai.
36	Active / Passive / Clustering	Aukšto patikimumo įrenginių sujungimo ir veikimo režimai.
37	Prievadas	Fizinė arba loginė tinklo jungtis, naudojama duomenų perdavimui.
38	Komutatorius / valdiklis / maršrutizatorius	Tinklo ir valdymo įrenginiai, naudojami OT sistemų ryšiui, automatizavimui ir duomenų perdavimui.
39	Žurnaliniai įrašai / event log	Sistemos, naudotojų, administratorių, tinklo ar saugumo įvykių įrašai.
40	Autentifikacija / šifravimas	Tapatybės patvirtinimo ir duomenų apsaugos nuo neleistinos prieigos mechanizmai.