ELEKTRONINIŲ PASLAUGŲ TEIKIMO TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. Jungtinės centrinės kredito unijos (toliau – JCKU) Elektroninių paslaugų teikimo taisyklės (toliau – Taisyklės) reguliuoja JCKU ir jos narių kredito unijų (toliau – KU) elektroninių paslaugų sistemos (toliau – Sistema) naudojimą, teisių naudotojams suteikimą, elektroninių paslaugų sutarčių sudarymą ir JCKU/KU kaip sistemos valdytojo ir sistemos naudotojų bendrąsias teises ir įsipareigojimus.
2. Taisyklės parengtos remiantis Lietuvos Respublikos centrinių kredito unijų įstatymu, Lietuvos Respublikos bankų įstatymu, Lietuvos Respublikos kredito unijų įstatymu, Lietuvos banko valdybos teisės aktų keliamais reikalavimais bei gerąja finansų įstaigų praktika.
3. Šios Taisyklės yra neatskiriama JCKU/KU Bendrųjų finansinių paslaugų teikimo taisyklių dalis. Naudotojų instrukcijos naudojimuisi sistema, saugos reikalavimai ir kiti specialūs reikalavimai gali būti nustatyti kituose JCKU/KU vidaus dokumentuose. Sistemos naudotojai turi būti supažindinti su šiais dokumentais, kai juose yra nuostatos, reglamentuojančios naudojimąsi sistema.
4. Sistemos naudotojais gali būti:
   4.1. Kredito unijos JCKU narės;
   4.2. Kredito unijų JCKU narių nariai fiziniai ir juridiniai asmenys, taip pat klientai be privalomos narystės;
   4.3. Lietuvos Respublikoje įsteigtos kredito unijų asociacijos;
   4.4. Kitos Lietuvos Respublikoje įsteigtos finansų įstaigos.
5. Taisyklių 4.1. – 4.3. punktuose nurodyti asmenys gali naudotis sistema sudarę su JCKU/KU elektroninių paslaugų sutartį ir įvykdę JCKU/KU nustatytus kliento pažinimo ir pinigų plovimo ir teroristų finansavimo prevencijos reikalavimus. Prieš elektroninių paslaugų sutarties sudarymą JCKU/KU darbuotojas įvertina, ar paslaugų teikimas tokiam klientui neprieštarauja JCKU/KU interesams, ar klientas atitinka narystės unijoje kriterijus, ar JCKU/KU turi galimybę tinkamai įvykdyti klientų pažinimo ir pinigų plovimo ir teroristų finansavimo prevencijos reikalavimus.

II. SĄVOKOS

(a)	**Atpažinimo priemonės**	Atpažinimo kodas, skirtas prisijungimui prie Sistemos, trečiųjų šalių išduota saugi mobiliojo elektroninio parašo, SMART-ID priemonė ar trumpąja žinute (SMS) gaunamas kodas bei pradinis slaptažodis, reikalingi kliento/kliento įgalioto asmens tapatybei nustatyti, operacijoms patvirtinti sistemoje.
(b)	**Autentiškumo patvirtinimas**	Procedūra, kuria JCKU/KU tikrina Kliento tapatybę arba mokėjimo priemonės, įskaitant jos personalizuotus saugumo duomenis, naudojimo teisėtumą.
(c)	**Darbo diena**	Diena, kai JCKU/KU ir/ar atsiskaitymo centras, tarpininkaujantis JCKU/KU teikiant mokėjimo paslaugas ir apdorojantis mokėjimo atitinkama valiuta nurodymo duomenis vykdo veiklą, būtiną atliekant mokėjimo operacijas. JCKU/KU mokėjimo nurodymus pervesti lėšas iš vienos sąskaitos JCKU/KU į kitą sąskaitą JCKU/KU, momentinius mokėjimus vykdo kiekvieną dieną, o paprastus mokėjimo nurodymus pervesti lėšas į sąskaitas kitose kredito įstaigose vykdo tik darbo dienomis.
(d)	**Elektroninės paslaugos**	JCKU/KU mokėjimo paslaugų teikimas per Sistemą pagal kliento sudarytą sutartį su JCKU/KU.

(e)	**Išrašas**	JCKU/KU dokumentas, kuriame pateikiama informacija apie sąskaitoje atliktą mokėjimo operaciją (-as) per tam tikrą laikotarpį bei sąskaitos likutį tam tikrai datai.
(f)	**Klientas**	Fizinis ar juridinis asmuo, JCKU klientas, KU narys ar asocijuotas narys ir/arba be narystės KU teisėtai sudaręs JCKU/KU elektroninių paslaugų teikimo sutartį.
(g)	**Kliento įgaliotas asmuo**	Kliento, juridinio asmens Sutartyje nurodytas fizinis asmuo, kuriam suteikiamos sutartyje nurodytos teisės Sistemoje veikti kliento vardu, kliento fizinio asmens nurodytas kitas fizinis asmuo, kuriam suteikiamos Sutartyje nurodytos teisės naudotis Sistema.
(h)	**Patvarioji laikmena**	Laikmena, kurioje asmeniškai Klientui skirta informacija saugoma taip, kad su ta informacija būtų galima susipažinti informacijos paskirtį atitinkančiu laikotarpiu, ir iš kurios laikoma informacija atgaminama jos nekeičiant.
(i)	**Naudotojas**	Fizinis asmuo, kuris naudojasi Sistema.
(j)	**Sutartis**	Elektroninių paslaugų teikimo sutartis, sudaryta tarp kliento ir JCKU/KU, susidedanti iš Elektroninių paslaugų teikimo specialiosios dalies, bendrosios dalies ir Sutarties priedo - Atpažinimo priemonių naudojimo sąlygų. Neatskiriama šios Sutarties dalimi, su kuria Klientas/Naudotojas susipažįsta ir tai patvirtina pasirašydamas Sutartį, yra laikomos JCKU/KU bendrųjų finansinių paslaugų teikimo taisyklės ir šios JCKU/KU elektroninių paslaugų teikimo taisyklės.
(k)	**Unija**	JCKU ir KU

III. TECHNINĖS IR PROGRAMINĖS ĮRANGOS REIKALAVIMAI

6. Klientas, pageidaujantis naudotis Sistema, turi naudoti įrenginį (kompiuterį, telefoną, planšetę ar pan.), kuriame įdiegta interneto naršyklė, įrenginys yra prijungtas prie interneto tinklo.
7. Kliento naudojamai programinei ir techninei įrangai keliami reikalavimai, būtini siekiant tinkamai naudotis Sistema, yra pateikiami Unijos interneto svetainėje arba pateikiami klientui sudarant elektroninių paslaugų sutartį. Unija turi teisę savo nuožiūra nustatyti minimalius programinės ir techninės įrangos reikalavimus, kurių neatitinkant, klientui teisė naudotis Sistema nesuteikiama arba suteikta teisė apribojama ar panaikinama.
8. Saugaus naudojimosi Sistema reikalavimai pateikiami https://e.kreda.lt/login

IV. NAUDOJIMASIS SISTEMA

9. Sudarydamas elektroninių paslaugų teikimo sutartį, Klientas gali nurodyti neribotą skaičių Naudotojų, kurie Sistemoje tvarkys Kliento sąskaitas (būtinai pagrįsdamas tokį didelį naudotojų skaičiaus poreikį). Sistemoje užregistruotiems Naudotojams galima suteikti skirtingas operacijų atlikimo teises ir limitus.
10. Klientas elektroninių paslaugų teikimo sutarties priede - Atpažinimo priemonių nurodymo sąlygose nurodo, kokios operacijų atlikimo teisės suteikiamos ir kokie limitai nustatomi Naudotojui, kokias sąskaitas jis galės tvarkyti.

11. Unija Naudotojo (-ų) pateikto mokėjimo nurodymo sąlygas vykdo ar sutartį sudaro tik tuomet, jei mokėjimo nurodymą ar elektroniniu būdu sudaromą sutartį yra patvirtinęs naudotojas, turintis teisę tvirtinti mokėjimo nurodymą ar pasirašyti elektroniniu būdu sudaromą sutartį.

12. Naudotojams suteikiamos tokios apimties teisės:

    12.1. Jokių – atima teisę matyti sąskaitas, jų likučius;

    12.2. Peržiūra – suteikia teisę tik peržiūrėti turimas sąskaitas, jų likučius, atliktas operacijas, pasikeisti Sistemos slaptažodį;

    12.3. Įvesti mokėjimą – suteikia teisę peržiūrėti turimas sąskaitas, likučius, atliktas operacijas ir sukurti mokėjimo nurodymus, pasikeisti Sistemos slaptažodį;

    12.4. Patvirtinti mokėjimą – suteikia teisę peržiūrėti turimas sąskaitas, likučius, atliktas operacijas, sukurti mokėjimų nurodymus, tvirtinti sukurtus mokėjimų nurodymus, sudaryti ir tvirtinti sutartis, pasikeisti Sistemos slaptažodį.

    12.5. Administratoriaus – suteikia teisę peržiūrėti turimas sąskaitas, likučius, atliktas operacijas, sukurti mokėjimų nurodymus, tvirtinti sukurtus mokėjimų nurodymus, sudaryti ir pasirašyti sutartis, atnaujinti „Pažink savo klientą anketą“, suteikti ir panaikinti teises atlikti operacijas, nustatyti/keisti operacijų limitus Naudotojams.

13. Prisijungus mobiliuoju el. parašu/Smart-ID e.kreda Sistema galima:

    13.1. sužinoti savo sąskaitų likučius;

    13.2. sužinoti savo sąskaitų likučius už pasirinktą laikotarpį;

    13.3. gauti sąskaitos išrašą PDF, XML, ar Excel formatu už pasirinktą laikotarpį;

    13.4. atlikti mokėjimo pervedimus unijos viduje, momentinius ar paprastus mokėjimus į kitą Lietuvoje arba kitoje SEPA (ang. Single Euro Payments Area) erdvei priklausančioje valstybėje veikiančią kredito įstaigą;

    13.5. atšaukti mokėjimo pervedimus;

    13.6. mokėti įmokas ir komunalinius mokesčius;

    13.7. atlikti grupinius mokėjimus;

    13.8. sudaryti/nutraukti terminuoto indėlio sutartį;

    13.9. gauti/siųsti žinutes/pranešimus iš/į unijos(-ą);

    13.10. pasikeisti SMS prisijungimo slaptažodį;

    13.11. blokuoti mokėjimo kortelę;

    13.12. pasikeisti sąskaitų limitus;

    13.13. valdyti sąskaitas;

    13.14. atnaujinti „Pažink savo klientą“ anketos duomenis;

    13.15. prisijungti prie elektroninių valdžios vartų;

    13.16. peržiūrėti savo turimų kreditų mokėjimo grafikus ir pagrindines kredito sąlygas;

    13.17. atlikti kitas operacijas, kurias yra galimybė atlikti naudojantis Sistema.

14. Naudojantis Mobiliąja programėle Klientas / Kliento įgaliotas asmuo gali atlikti:

    14.1. sužinoti savo mokėjimo sąskaitų likučius ir sąskaitų išrašus už paskutines 90 dienų;

14.2. atlikti mokėjimo pervedimus unijos viduje, momentinius ar paprastus mokėjimus į kitą Lietuvoje arba kitoje SEPA (ang. Single Euro Payments Area) erdvei priklausančioje valstybėje veikiančią kredito įstaigą;

14.3. matyti einamojo mėnesio išlaidų grafiką;

14.4. peržiūrėti ir nustatyti mokėjimo kortelių limitus, nustatyti kortelių funkcionalumus bei blokuoti mokėjimo korteles;

14.5. peržiūrėti aktyvių paskolų informaciją;

14.6. peržiūrėti aktyvių indėlių informaciją;

14.7. susisiekti su savo unija programėlės dalyje „Kontaktai“ telefonu arba el. paštu.

15. Operacijų atlikimo instrukcijos yra pateikiamos Sistemoje, o Klientui pageidaujant – papildomai pateikiamos jam patvariojoje laikmenoje.

16. Klientas gali naudotis Sistema visą parą, prisijungus interneto svetainėje adresu https://e.kreda.lt

V. LIMITŲ NUSTATYMAS IR KEITIMAS

17. Naudotojui nustatomi vienos operacijos, vienos dienos ir vieno mėnesio limitai kiekvienai sąskaitai atsižvelgiant į Naudotojo naudojamų Atpažinimo priemonių saugumo lygį laikantis teisės aktų ir siekiant užtikrinti kliento lėšų bei informacijos saugumą.

18. Vienos operacijos limitas – didžiausia pinigų suma, kurios neviršydamas Naudotojas gali atlikti vienos operacijos metu.

19. Vienos dienos operacijų limitas – didžiausia pinigų suma, kurios neviršydamas Naudotojas gali atlikti per vieną unijos darbo dieną vienos ir/ar kelių operacijų metu.

20. Vieno mėnesio operacijų limitas – didžiausia pinigų suma, kurios neviršydamas Naudotojas gali pervesti per mėnesį.

21. Operacijų limitai netaikomi, jeigu Naudotojas atlieka mokėjimus tarp kliento sąskaitų unijoje.

22. Klientas, sudarydamas Sutartį, gali pasirinkti bet kokius limitus, neviršydamas Unijos nustatytų maksimalių limitų bei vėliau juos keisti Unijos nustatyta tvarka.

23. Unija turi teisę iš dalies arba visiškai apriboti Naudotojų teises bet kuriuo metu be jokio išankstinio pranešimo šiose taisyklėse nustatytais atvejais ir tvarka.

VI. KLIENTO/KLIENTO ĮGALIOTO ASMENS AUTENTIŠKUMO PATVIRTINIMO PROCEDŪRA

24. Siekiant užtikrinti saugų operacijų atlikimą ir Naudotojo autentiškumo patikrinimą, Unija suteikia personalizuotas apsaugos ir atpažinimo priemones bei sutinka, kad Naudotojas naudos savo pasirinktas priemones:

24.1. atpažinimo kodą – tai unikali skaitmenų seka, kuri naudojama asmens tapatybei nustatyti registruojantis Sistemoje;

24.2. pradinį slaptažodį – tai unikali raidžių, skaitmenų ir (ar) simbolių seka, kuri naudojama asmens tapatybei patvirtinti pirmą kartą registruojantis Sistemoje SMS būdu ir kurią Naudotojas privalo pakeisti pirmo prisijungimo prie Sistemos metu;

24.3. slaptažodį – tai Naudotojo sugalvotas slaptažodis, kuris naudojamas SMS prisijungimo būdu. Vadovaujantis geriausia saugumo praktika slaptažodžiui yra taikomi papildomi reikalavimai (ne mažiau nei 8 ženklai, bent viena didžioji ir bent viena mažoji lotyniška raidė, bent vienas skaičius ir bent vienas simbolis). Rekomendacijos slaptažodžiui skelbiamos Prisijungimo prie e.Kreda instrukcijoje:

https://e.kreda.lt/Files/KREDA/e.kreda-elektronines-bankininkystes-naudojimosi-instrukcija.pdf;

24.4. trumpąja žinute (SMS) gaunamą kodą – tai kiekvieną kartą jungiantis prie Sistemos ir /ar tvirtinant lėšų pervedimus Unijos trumpąja žinute į mobiliojo ryšio telefono numerį, kurį /Naudotojas nurodė Atpažinimo priemonių Sutartyje, siunčiamas vienkartinis kodas. Gaunamas kodas yra skirtingas kiekvieno prisijungimo prie Sistemos, mokėjimo nurodymo pervesti lėšas ar sutarties pasirašymo Sistemoje metu. Klientas pasirašydamas Sutartį pateikia galiojantį (aktyvų), išimtinai jam priklausantį ir jo naudojamą mobiliojo ryšio telefono numerį, į kurį pageidauja gauti trumpąja (SMS) žinute siunčiamą kodą;

24.5. trečiųjų šalių išduotą saugią mobiliojo elektroninio parašo, SMART ID priemonę (kvalifikuotą mobilųjį parašą).

25. Naudotojo autentiškumas laikomas patvirtintu, jei Naudotojas teisingai panaudojo Unijos suteiktų Atpažinimo priemonių duomenis arba paties Naudotojo pasirinktą identifikavimo priemonę.

26. Unija pripažįsta ir laiko Naudotojo pasirašytais bei patvirtintais Sistema gautus mokėjimo nurodymus apie kliento sąskaitose esančių lėšų panaudojimą, sutarčių sudarymą, nutraukimą ar kitą operaciją atliktą Sistemoje, jei autentiškumas buvo patvirtintas Unijos suteikta arba Naudotojo pasirinkta identifikavimo priemone.

27. Unija turi teisę savo nuožiūra nustatytais atvejais Kliento Unijai pateiktais kontaktiniais duomenimis (pvz.: el. paštu) paprašyti papildomai patvirtinti pateiktų operacijų inicijavimą. Jeigu nurodytais kontaktiniais duomenimis Klientas nepasiekiamas arba minėtos operacijos nepatvirtina, unija turi teisę tokios mokėjimo operacijos nevykdyti kaip neautorizuotos.

28. Laikoma, kad Klientas yra tinkamai atpažintas, kai Unijos Sistemoje nustatyta tvarka naudodamas tinkamas Atpažinimo priemones pateikia mokėjimo nurodymus, pranešimus, prašymus, patvirtinimus, kitus dokumentus, atlieka kitus veiksmus, susijusius su Sutarties vykdymu. Visi šiame punkte išvardinti veiksmai laikomi Kliento tinkamai pasirašytais ir patvirtintais, ir yra leistini kaip įrodinėjimo priemonė sprendžiant ginčus.

VII. JCKU/KU SUTEIKTOS IR/AR KLIENTO PASIRINKTOS IDENTIFIKAVIMO PRIEMONĖS KONFIDENCIALUMAS IR BLOKAVIMAS

29. Klientas privalo užtikrinti, kad paslaugomis, teikiamomis Sistema, Unijos suteikta ir/ar Naudotojo pasirinkta identifikavimo priemone naudotųsi tik pats klientas ir jo įgaliojimus turintys Unijai nurodyti Naudotojai, laikydamiesi Lietuvos Respublikos teisės aktų, o tuo atveju, jeigu klientas yra juridinis asmuo, ir kliento juridinio asmens vidaus norminių aktų, reglamentuojančių atsiskaitymą ir disponavimą lėšomis, reikalavimų.

30. Siekiant užtikrinti saugumą ir tai, kad Kliento sąskaitoje operacijų negalėtų atlikti kliento neįgalioti asmenys, Naudotojo turimos identifikavimo priemonės ir Naudotojo prisijungimo duomenys turi būti žinomi tik Naudotojui, kuris privalo rūpestingai juos saugoti (nelaikyti kartu visų unijos suteiktų ir/ar Naudotojo pasirinktų identifikavimo priemonių, neužsirašyti prisijungimo duomenų ant kitų su juo laikomų daiktų ir pan.). Naudotojas jokiais atvejais neturi teisės perduoti tretiesiems asmenims Unijos suteiktos identifikavimo priemonės, leisti jiems sužinoti konkrečių atpažinimo kodų, slaptažodžių, prisijungimo prie sąskaitos duomenų. Naudotojo pasirinktos identifikavimo priemonės naudojimo tvarką reglamentuoja minėtą identifikavimo priemonę išdavusi trečioji šalis.

31. Unija nedelsiant blokuoja Naudotojo naudojimąsi Sistema, jei:

31.1. yra objektyviai pagrįstos priežastys, susijusios su Sistemos ir/ar identifikavimo priemonių ir/ar Atpažinimo priemonių saugumu, įtariamu neautorizuotu ar nesąžiningu naudojimusi Sistema arba su labai padidėjusia rizika, kad Klientas gali nesugebėti tinkamai įvykdyti savo mokėjimo įsipareigojimo Unijai.

31.2. Klientas nesilaiko elektroninių paslaugų teikimo sutarties sąlygų;

31.3. Unija sužino apie identifikavimo priemonių ir/ar Atpažinimo priemonių duomenų vagystę ar praradimą, Unijai įtarus ar sužinojus apie identifikavimo priemonių ir/ar Atpažinimo priemonių duomenų neteisėtą įgijimą arba neautorizuotą jų naudojimą, taip pat apie faktus ar įtarimus, kad identifikavimo priemonių duomenis ir/ar Atpažinimo priemonių duomenis sužinojo arba jais gali pasinaudoti tretieji asmenys, Unija turi pagrįstų įtarimų, kad Sistema ir jos pagalba prieinamose Kliento sąskaitose esančiomis lėšomis ar valdomomis mokėjimo priemonėmis gali neteisėtai pasinaudoti tretieji asmenys arba kad Sistema gali būti naudojama ar yra panaudota nusikalstamai veikai vykdyti;

31.4. Klientas/Naudotojas to pareikalauja (praradus ar sugadinus kliento Atpažinimo priemonių duomenis, iškilus grėsmei, kad Naudotojo Atpažinimo priemonių duomenis gali sužinoti arba sužinojo tretieji asmenys, atsiradus kitoms priežastims, dėl kurių Naudotojas negali naudotis Sistema). Praradus Atpažinimo priemones Naudotojas privalo nedelsiant informuoti Uniją apie Atpažinimo priemonių praradimą ar saugumo pažeidimą;

31.5. Naudotojui Sistemoje 5 (penkis) kartus neteisingai panaudojus Unijos suteiktą ar Naudotojo pasirinktą identifikavimo priemonę ir (ar) pagrįstai kylant įtarimams, kad mokėjimo nurodymus Naudotojo vardu gali pateikti (pateikia) tretieji asmenys;

31.6. Lietuvos Respublikos teisės aktuose, Unijos Bendrosiose paslaugų teikimo taisyklėse, elektroninių paslaugų teikimo sutartyje, mokėjimo sąskaitos sutartyje ir kituose Unijos finansinių paslaugų teikimą reglamentuojančiuose vidaus dokumentuose (su kuriais Klientas yra supažindintas) numatytais atvejais.

31.7. Kliento/Naudotojo sukčiavimo atveju.

32. Kliento/Naudotojo prašymai blokuoti naudojimąsi Sistema pateikiami Unijai elektroniniu paštu, telefonu ar kitais kanalais. Unija gavusi tokį prašymą turi teisę atlikti papildomus veiksmus Kliento/Naudotojo identifikavimui

33. Unija panaikina naudojimosi Sistema blokavimą, kai nebelieka blokavimo priežasčių ir, jei blokavimas buvo atliktas Kliento iniciatyva, Unijai gavus atitinkamą raštišką Kliento prašymą.

34. Unija neatsako:

34.1. už Kliento nuostolius, patirtus dėl naudojimosi Sistema blokavimo, jei toks blokavimas buvo atliktas šių Taisyklių nustatyta tvarka ir esant Taisyklių 31 punkte nustatytoms sąlygoms, išskyrus šių Taisyklių 35 punkte nustatytus atvejus.

34.2. jei Naudotojas negalėjo naudotis Sistema dėl to, kad neveikė ar netinkamai veikė Naudotojo programinė ar kita įranga, trečiųjų šalių išduotos atpažinimo priemonės (pvz.: neveikė mobilus parašas, SMART ID, neveikia operatorių sistema, negavo SMS žinučių).

35. Unija:

35.1. atlygina visus nuostolius, atsiradusius po to, kai Klientas/Naudotojas pareikalavo Unijos blokuoti naudojimąsi Sistema, kaip tai numatyta 31.4. punkte, išskyrus atvejus, jei nuostoliai atsirado dėl Naudotojo nesąžiningų veiksmų ar jam tyčia ar dėl didelio neatsargumo nesilaikant Sutartyje, šiose Taisyklėse ar Mokėjimų įstatyme nurodytų Naudotojo pareigų. Jei nuostolių atsirado pasinaudojus Naudotojo apsaugos priemonėmis, Unijos Naudotojui suteiktomis atpažinimo priemonėmis arba Naudotojo prisijungimo priemone iki 31.4. punkte nurodyto pranešimo pateikimo Unijai, Naudotojui neįvykdžius Sutartyje nustatytos pareigos užtikrinti prisijungimo priemonių saugumą ir slaptumą, laikoma, kad nuostoliai atsirado dėl Naudotojo didelio neatsargumo, jei Naudotojas neįrodo kitaip;

35.2. Klientui tenkančių nuostolių, susijusių su prisijungimo priemonių praradimu ir atsiradusių iki 31.4. punkte nurodyto pranešimo pateikimo laiko, suma negali viršyti 50 eurų. Jeigu nuostolių atsirado dėl Naudotojo nesąžiningų veiksmų, tyčios, didelio neatsargumo arba Klientas yra juridinis asmuo, ši nuostata netaikoma;

35.3. Unija Klientui atlygina nuostolius, atsiradusius dėl Unijos kaltės.

VIII. PAPILDOMA INFORMACIJA

36. Klientai/Naudotojai įsipareigoja laikyti paslaptyje Unijos suteiktas Atpažinimo priemones, slaptažodžius, jų neužsirašyti ir jokia kita forma neatskleisti ar nepadaryti jų prieinamų tretiesiems asmenims.
37. Klientas yra atsakingas už nuolatinį savo kontaktinių duomenų atnaujinimą Unijos nustatyta tvarka ir terminais.
38. Jeigu keičiamas Kliento adresas, mobiliojo telefono numeris ar kiti rekvizitai, nurodyti Sutartyje, Klientas privalo tuoj pat apie tai informuoti Uniją. Neįvykdęs šio reikalavimo, Klientas negali reikšti pretenzijų ir atsikirtimų, kad Unijos veiksmai, atlikti pagal paskutinius jam žinomus Kliento rekvizitus, neatitinka Sutarties arba kad jis negavo pranešimų, siųstų pagal tuos rekvizitus.
39. Klientas juridinis asmuo įsipareigoja nedelsdamas informuoti Uniją apie prokūros (įgaliojimo) atšaukimą, jei prieš tai prokūra buvo pateikta Unijai.
40. Klientas/Naudotojas įsipareigoja užtikrinti, kad naudojantis kompiuterine, programine ar kitokia įranga, kuria jungiamasi prie Sistemos, būtų laikomasi visų įmanomų saugumo priemonių, įskaitant antivirusines programas, ir yra atsakingas už visas pasekmes, atsiradusias dėl nepakankamo Kliento/Naudotojo kompiuterinių ar kitų sistemų apsaugos.
41. Jei buvo pažeistas programinės įrangos ir duomenų, būtinų naudotis Sistema saugumas, Klientui, atvykusiam į Uniją, jo prašymu suteikiama nauja prisijungimo prie Sistemos Atpažinimo priemonė.
42. Unija turi teisę tikrinti Unijos pateiktus Kliento pranešimus ar kitus dokumentus, siunčiamus į Unijos Sistemą, ir, radusi techninių arba loginių klaidų, taip pat nustatęs, kad sąlygos prieštarauja teisės aktams, turi teisę atsisakyti vykdyti sąlygas. Apie tokį atsisakymą Unija praneša Klientui per Sistemą.

IX. BAIGIAMOSIOS NUOSTATOS

43. Unija turi teisę keisti šias Taisykles valdybos sprendimu ir tik iš anksto apie tai prieš 60 (šešiasdešimt) kalendorinių dienų viešai paskelbusi ir/ar patvariąja laikmena informavusi visus klientus. Laikoma, jog Klientas sutinka su šiais pakeitimais, jeigu jis iki pakeitimų įsigaliojimo dienos Unijai nepraneša, kad su jais nesutinka. Jei Klientas nesutinka su pakeitimais, jis turi teisę nedelsdamas ir nemokėdamas jokio komisinio atlyginimo nutraukti elektroninių paslaugų teikimo sutartį iki dienos, kurią bus pradėti taikyti pakeitimai. Pranešdama apie Taisyklių pakeitimą patvariąja laikmena, Unija užtikrina, kad:

    43.1. interneto svetainėje ir/ar Sistemoje, kurioje skelbiama informacija apie pakeitimus, leidžia Klientui saugoti šią informaciją taip, kad per reikiamą laiką jis galėtų prie jos prieiti ir atgaminti nepakitusią, o Unija neturėtų galimybės vienašališkai keisti jos turinio; ir

    43.2. perduodama šią informaciją unija imasi aktyvių veiksmų, skirtų Klientui pranešti, kad minėta informacija pateikta interneto svetainėje ir/ar Sistemoje, bei galima su ja susipažinti (teikia pranešimus per Sistemą, elektroniniu paštu, paštu ar kitu su Klientu sutartu būdu ir juos skelbia savo ir savo narių kredito unijų interneto svetainėse).

JCKU ir KU elektroninių paslaugų teikimo taisyklių

Priedas Nr.1

Internetinio banko saugumo reikalavimai

Nesiųskite el. paštu konfidencialios informacijos (prisijungimo prie elektroninės bankininkystės sistemos slaptažodžių ir pan. duomenų). Suabejoję elektroninės paslaugos ar įrenginio patikimumu, nutraukite darbą, atjunkite įrenginį nuo interneto ir nedelsdami praneškite apie tai unijai.

Kaip saugiai naudoti slaptažodį?

1. Bankininkystei naudokite unikalius slaptažodžius. Jeigu kažkas sužino jūsų daug kur naudojamą slaptažodį, jis iš karto gali patekti į visas paskyras.
2. Įsiminkite slaptažodžius, neužsirašykite jų, nesaugokite kompiuteryje (išskyrus tam skirtas ir leidžiamas programas), neatskleiskite savo asmens duomenų ar prisijungimo duomenų prie interneto banko kitiems asmenims, įskaitant šeimos narius, draugus, reguliariai keiskite slaptažodį.
3. Slaptažodžius įveskite tik tada, kai esate tikri, kad Jūsų niekas nestebi.
4. Saugokite slaptažodžius kitiems žmonėms neprieinamose vietose — ne piniginėse, rankinėse ar šalia savo kompiuterio.
5. Nepraneškite slaptažodžių telefonu, socialiniuose tinkluose, nesiųskite jų paštu ar el. paštu. Pastaruoju metu vis dažniau sukčiai slaptažodžius bando išvilioti telefonu apsimesdami, unijos, policijos, Finansinių nusikaltimų tyrimo tarnybos, Specialiųjų tyrimų tarnybos, „Sodros“ ar kitų valstybės įstaigų darbuotojais ar darbdaviais, siūlančiais patrauklų darbą. Nepasiduokite psichologiniam spaudimui — neatskleiskite telefonu konfidencialių duomenų, nes niekas neturi teisės to iš Jūsų reikalauti. Apie tokį bandymą iškart praneškite unijai ir policijai. Jeigu dvejojate, visada papildomai pasiklauskite žodžiu.
6. Sukčiai gali banko vardu siųsti jums netikrus SMS pranešimus, tam kad gautų asmens bei tapatybės patvirtinimo priemonių duomenis. Niekada neatsakykite į SMS pranešimą, kuriame prašoma pateikti slaptus duomenis.
7. Nespauskite nuorodų SMS žinutėse. Būkite itin atidūs, jeigu žinutės siuntėjai prašo atidaryti pateikiamą nuorodą. Tokiomis nuorodomis dažnai nukreipiama į netikrą interneto puslapį, skirtą duomenims surinkti.
8. Jokiu būdu nenurodykite slaptažodžių, jei prisijungiant prie elektroninės bankininkystės ar pervedant pinigus internetu Jūsų prašoma įvesti iš karto kelis slaptažodžius. Jeigu taip nutinka, vadinasi, Jūsų naudojamas kompiuteris užkrėstas — per kenksmingas programas sukčiai bando sužinoti įvestus slaptažodžius. Tokiu atveju būtinai nedelsdami:
    - baikite darbą elektroninių paslaugų sistemoje;
    - **praneškite unijai** paskambinę jos internetiniame puslapyje nurodytu kontaktiniu telefonu ir paprašykite blokuoti prieigą prie elektroninės bankininkystės sistemos.

Kokių duomenų negalima atskleisti?

1. Neatskleiskite savo paso, asmens tapatybės kortelės ar vairuotojo pažymėjimo duomenų kitiems asmenims, jeigu jie nenurodo aiškaus teisinio pagrindo šiems duomenims rinkti.
2. Nepraneškite prisijungimo prie elektroninės bankininkystės sistemos slaptažodžių telefonu, nesiųskite jų paštu ar el. paštu. Unija niekuomet nereikalauja šios informacijos pateikti minėtais būdais.
3. Atminkite, kad atpažinimo kodas yra toks pat svarbus kaip jūsų asmens kodas, tad skirkite deramą dėmesį jo apsaugai.

Kaip naršyti po internetą ir naudotis teikiamomis elektroninėmis paslaugomis?

1. Junkitės prie internetinės bankininkystės sistemos tik per oficialius unijų puslapius arba surinkę adresą: https://e.kreda.lt/. Norėdami prisijungti prie internetinės bankininkystės turite naudotis naujausiomis Internet Google Chrome , Mozilla Firefox arba Explorer naršyklių naujausiomis versijomis
2. Būkite atidūs, kai atveriate el. laiškus, naršote po internetą, kopijuojate informaciją.
3. Ypač tikrinkite nepažįstamų asmenų žinutes elektroninio pašto ir socialinių tinklų paskyrose, kuriose yra nuorodų (angl. „hyperlink“ (//bit.ly)). Niekada nespauskite įtartinų nuorodų.
4. Jeigu gavote elektroninį laišką iš unijos, kuriame prašoma prisijungti arba suvesti asmens duomenis, slaptažodžius, eikite į unijos interneto puslapį ne per nuorodą, o prisijunkite rankiniu būdu, kaip paprastai.
5. Nesilankykite nepažįstamuose tinklalapiuose — dažniausiai kenksmingos programėlės (virusai) platinamos el. paštu ir nesaugiuose tinklalapiuose.
6. Jei sąskaitoje yra daugiau pinigų, negu jums reikia kasdienėms išlaidoms, nustatykite operacijų apribojimus. Sudarant internetinės bankininkystės paslaugų sutartį, iš anksto nustatoma didžiausia pinigų suma, kurią galima išleisti naudojantis interneto banku. Jei norite pakeisti apribojimus arba pervesti didesnę sumą, atvykite į artimiausią unijos skyrių.
7. Nesinaudokite elektroninėmis paslaugomis viešose vietose, jei Jums atrodo, kad esate stebimi, ar kompiuteris kelia įtarimą.
8. Viešoje vietoje pasinaudoję elektroninių paslaugų sistema, pasikeiskite slaptažodį.
9. Nesinaudokite viešais tinklais (kavinės, parduotuvės ar kitu nesaugiu WIFI) bankinėms transakcijoms.
10. Nesinaudokite internetine bankininkyste iš svetimo kompiuterio. Svetimame ar viešai naudojamame kompiuteryje gali būti įdiegta kenkėjiška programinė įranga, renkanti asmeninius duomenis ar registruojanti klaviatūros paspaudimus. Tokiu atveju rizikuojate tretiesiems asmenims atskleisti savo asmeninius duomenis bei slaptažodžius.
11. Pirkite tik patikimose parduotuvėse. Prekes ir paslaugas visada saugu pirkti žinomose, gerą reputaciją turinčiose Lietuvos ir užsienio el. parduotuvėse. Nežinomus pardavėjus vertinkite kritiškai, pasidomėkite jų veikla. Pasidomėkite viešai internete pateikiamais atsiliepimais apie konkrečią el. parduotuvę.
12. Jei suabejojote dėl internetinės bankininkystės atvaizdavimo ar sistemos veikimo, iš karto nutraukite veiksmus. Baikite darbą internetinėje bankininkystėje ir apie tai informuokite uniją.
13. Nustatykite mažą operacijų, atliekamų elektroninės bankininkystės sistemoje, limitą ir didinkite jį tik tada, kai būtina.
14. Darbą elektroninėje bankininkystėje baikite spustelėdami „Baigti darbą“.
15. Dėl elektroninių paslaugų konsultuokitės tik su unijos darbuotojais.

Kaip apsaugoti kompiuterį?

1. Įsidiekite patikimą legalią antivirusinę programą, reguliariai atnaujinkite programinę įrangą ir naudokite naujausias naršyklių versijas.
2. Dažnai aptinkama operacinių sistemų ir kitos programinės įrangos saugumo spragų, leidžiančių sukčiams neteisėtai patekti į svetimus kompiuterius ir prisijungti prie sistemų. Šiomis spragomis naudojasi įsilaužėliai, todėl gamintojai, siekdami užtikrinti įrangos saugumą, nuolat ją koreguoja, šalina aptiktas spragas. Taigi pasirūpinkite, kad Jūsų naudojama operacinė sistema ir kita programinė įranga būtų laiku atnaujinta. Rekomenduojame nustatyti automatinius nustatymus.
3. Aptikę virusą ar pasiūlymą įsidiegti įtartiną programą, iškart baikite darbą kompiuteriu ir kreipkitės į specialistus.
4. Domėkitės ir naudokitės informacinių technologijų saugumo specialistų patarimais.
5. Jei elektroninės bankininkystės sistemos registracijos lange įvedus atpažinimo kodą ir slaptažodžius, nepavyksta prisijungti, rodomas pranešimas apie techninius nesklandumus arba ilgokai matote nesibaigiančio veiksmo piktogramą, vaizduojančią besisukantį ratą, nedelsdami praneškite apie tai unijai paskambinę jos internetiniame puslapyje nurodytu kontaktiniu telefonu.
6. Puslapis https://www.kreda.lt/ yra apsaugotas autentiškumą patvirtinančiu sertifikatu. Naršyklėje, šalia puslapio adreso atsiranda spynelė, kuri patvirtina puslapio tikrumą. Dauguma naršyklių taiko papildomus perspėjimus, jeigu sertifikatas nėra autentiškas.

Daugiau informacijos, kaip apsaugoti savo įrenginį ir kaip saugiai naudotis kitomis paslaugomis internete, rasite šioje svetainėje: https://www.esaugumas.lt/lt