HSBC*net* ՕՆԼԱՅՆ ԲԱՆԿԱՅԻՆ ԾԱՌԱՅՈՒԹՅԱՆ ՀԻՄՆԱԿԱՆ ՊԱՅՄԱՆՆԵՐ ԵՎ ՄՈՒՏՔԻ ՀՍԿՄԱՆ ԸՆԹԱՑԱԿԱՐԳԵՐ

Տեղեկատվական ամփոփագիր իրավաբանական անձանց համար

Հրապարակման ամսաթիվ՝ մարտ, 2023թ.:

Ամփոփագրում նշված պայմանները կարող են փոփոխված լինել:

Գործող պայմաններին ծանոթանալու, ինչպես նաև լրացուցիչ տեղեկատվություն ստանալու նպատակով այցելեք մեր ինտերնետային կայք՝ www.business.hsbc.am կամ զանգահարեք +374 60 655 200 հեռախոսահամարով:

Բանկը վերահսկվում է ՀՀ կենտրոնական բանկի կողմից:

HSBC

Բովանդակություն

E-Channels-ի Պայմաններ (E-Terms) Հիմնական Պայմաններ

1. Ներածություն

1.1 E-Channels-ով ծառայությունների մատուցումը կարգավորվում է սույն Հիմնական Պայմաններով և Ծառայությունների նկատմամբ կիրառվող պայմաններով (ստորև Ծառայությունների Պայմաններ), որոնք փոխարինելու են կողմերի միջև նախկինում կնքված E-Channels–ին վերաբերող բոլոր պայմանագրերին: Կիրառվող պայմանների միջև հակասության դեպքում գերակայությունը որոշվում է հետևյալ հերթականությամբ

(ա) տեղական Բանկի պայմաններ,
(բ) այլ Լրացուցիչ Հիմնական Պայմաններ,
(գ) հիմնական Պայմաններ,
(դ) ծառայությունների Պայմաններ:

1.2 E-Terms-ը կարող է կնքվել ցանկացած քանակի օրինակներից՝ համապատասխան Դիմումի Ձևի հետ միասին, որոնք բոլորը միասին կազմում են մեկ փաստաթուղթ:

1.3 Սույն Հիմնական Պայմաններում օգտագործված եզակի թվով արտահայտությունները ներառում են հոգնակի թվով օգտագործված նույն արտահայտությունները և հակառակը, իսկ պայմանագրի կետերի վերնագրերը տրված են միայն հարմարության նպատակներից ելնելով և չեն ազդում դրանց մեկնաբանման վրա:

2. Սահմանումներ

- Հաշվետեր հաճախորդ նշանակում է կողմ, որ համաձայնվում է իր հաշիվները և/կամ ծառայություններն ընդգրկել Հիմնական հաճախորդի E-Channels-ում:
- Դիմումի ձև նշանակում է ցանկացած դիմում, որով Հիմնական հաճախորդը համաձայնվում է Հիմնական բանկի կողմից E-Channels ծառայության տրամադրմանը:
- Լիազորված անձ նշանակում է անձ, որին Հիմնական Հաճախորդը լիազորել է (միանձնյա կամ այլ անձանց հետ միասին) տալ հանձնարարականներ և/կամ Հիմնական Հաճախորդի անունից կատարել գործողություններ:
- Տեղական Բանկի Պայմանները՝ յուրաքանչյուր երկրի օրենսդրության համար, հատուկ պայմաններ, որոնք լրացնում և/կամ փոփոխում են ցանկացած E-Terms-ը:
- E-Channels նշանակում է Խմբի էլեկտրոնային բանկային համակարգերը:
- E-Terms նշանակում է Հիմնական Պայմաններ, ցանկացած կիրառելի Լրացուցիչ E-Terms և Տեղական Բանկի Պայմաններ:
- Հիմնական Պայմաններ նշանակում է սույն պայմանները:

- Խումբ նշանակում է Էյչ-Էս-Բի-Սի Հոլդինգս Փի Էլ Սի-ն, վերջինիս դուստր ընկերությունները, փոխկապցված ընկերությունները, կից կորպորատիվ անձինք, և դրանց ցանկացած մասնաճյուղերը:
- Ենթակառուցվածքներ տրամադրող նշանակում է որևէ երրորդ անձ, որն ապահովում է Կողմերի համար անհրաժեշտ հասանելի ենթակառուցվածք, որն անհրաժեշտ է կողմի համար E-Terms-ով ստանձնած պարտավորությունները կատարելու համար, ներառյալ հաղորդակցությունը, քլիրինգը, վճարահաշվարկային համակարգերը կամ միջնորդ կամ թղթակից բանկը:
- Հանձնարարական նշանակում է ցանկացած հաղորդագրություն, որը E-Channels-ի միջոցով ստացվել է Հիմնական Բանկի կողմից և որն ուղարկվել է Լիազորված Անձի կողմից:
- Կորուստ նշանակում է ցանկացած կորուստ, վնաս, պատասխանատվություն, ծախս, պահանջ և, կանխատեսված կամ չկանխատեսված ցանկացած բնույթի ծախս:
- Կողմ նշանակում է Հիմնական հաճախորդ կամ Հիմնական Բանկ:
- Հիմնական Բանկ նշանակում է Խմբի անդամ, որը Հիմնական հաճախորդին մատուցում է E-Channels ծառայությունը:
- Հիմնական հաճախորդ նշանակում է Կողմ, որին Հիմնական Բանկի կողմից տրամադրվել է E-Channels ծառայությունից օգտվելու հնարավորություն:
- Անվտանգության Միջոցներ նշանակում է E-Channels-ի անվտանգության ապահովման համար անհրաժեշտ միջոցներ, որոնք ժամանակ առ ժամանակ կարող են տրամադրվել Հիմնական Հաճախորդին Հիմնական Բանկի կողմից:
- Ծառայություններ նշանակում է ցանկացած բանկային կամ դրա հետ կապված ծառայություններ, որոնք մատուցվում և ստացվում են E-Channels-ի միջոցով
- Լրացուցիչ E-Terms նշանակում է ցանկացած պայմաններ, որոնք վերաբերում են տվյալ E-Channels-ի ծառայությանը և ներառում են սույն պայմանները:

3. Հանձնարարականներ

3.1 Հիմնական Հաճախորդը համաձայնվում է ժամանակ առ ժամանակ հանձնարարականներ տրամադրել Հիմնական Բանկի կողմից ընդունելի ձևով, որոնք Հիմնական Բանկը պարտավոր չէ կատարել այլ կերպ, քան նախատեսված է հանձնարարականներում:

3.2 Հիմնական Բանկն իրավունք ունի առաջնորդվել ցանկացած հանձնարարականով, և Հիմնական Բանկն իրավունք ունի բոլոր ստացված հանձնարարականները համարել հաստատված և վավեր, պայմանով որ, Անվտանգության միջոցները պահպանվել են: Հիմնական հաճախորդը պարտավոր է E-Channels-ում ստեղծել իր էջը սեփական իրավասությունների և ներքին վերահսկողությանը համապատասխան: Ո՛չ Հիմնական Բանկը, ո՛չ Խմբի մեկ այլ անդամ պարտավոր չեն ստուգելու, արդյո՞ք հանձնարարականը հակասում է Հիմնական հաճախորդի կամ Հաշվետեր

հաճախորդի մեկ այլ հանձնարարականի կամ իրավասության հետ: Հիմնական Բանկն իրավունք ունի մերժել կամ հետաձգել հանձնարարականի կատարումը, եթե հիմքեր ունի կասկածելու հանձնարարականի օրինականության, ծագման կամ հաստատման կապակցությամբ:

3.3 Կողմերը համաձայնվում են պահպանել Անվտանգության Միջոցները: Հիմնական հաճախորդը պետք է սահմանի, պահպանի և վերանայի իր համապատասխան սեփական ներքին անվտանգության միջոցները E-Channels-ի օգտագործման և համակարգ մուտք գործելու նպատակով՝ ներառյալ հակավիրուսային ծրագրային ապահովման տեղադրումը և շարունակական թարմացումը: Հիմնական հաճախորդը պարտավոր է Հանձնարարականների ներկայացման ընթացքում ապահովել Անվտանգության միջոցների պատշաճ կիրառումը:

3.4 Հիմնական հաճախորդը պարտավոր է պատշաճ կերպով ձեռք բերել, պահպանել, թարմացնել և տեղադրել (անհրաժեշտության դեպքում) ցանկացած սարքավորում, ծրագրային ապահովում, հեռահաղորդակցման միջոցներ, ցանցեր, միացումներ, ծրագրային լրացումներ և/կամ թարմացումներ, որը Հիմնական Բանկը կպահանջի տեղադրել կամ օգտագործել, կամ որը Հիմնական Բանկը տրամադրում է Հիմնական հաճախորդին՝ E-Channels մուտք գործելու համար: Հիմնական հաճախորդը պատասխանատու է համակարգչային ծրագրային ապահովման և սարքավորումների տեղադրման և պահպանման համար, որոնք անհրաժեշտ են E-Channels մուտք գործելու համար:

3.5 Հիմնական հաճախորդը պարտավորվում է չփոփոխել, չձևափոխել, չպատճենել (բացառությամբ օգտագործման համար անհրաժեշտ և թույլատրելի դեպքերի), չհրատարակել կամ երրորդ անձանց չհայտնել Հիմնական Բանկի կողմից տրամադրված ծրագրերի կամ նյութերի վերաբերյալ տեղեկությունները, ներառյալ E-Channels-ի կամ այլ ծրագրի և նյութերի վերաբերյալ, որոնք տրամադրվել են որպես վերջինիս մաս կազմող ծառայություն կամ պրոդուկտ:

4. Երաշխիքներ, Հավաստումներ և Պարտավորություններ

4.1 Հիմնական հաճախորդը պարտավոր է՝
(ա) Հիմնական Բանկին տրամադրել E-Channels-ին վերաբերող բոլոր փաստաթղթերը և այլ տեղեկատվություն, որը պատշաճ կերպով ժամանակ առ ժամանակ պահանջվում է Հիմնական Բանկի կողմից, և
(բ) ծանուցել Հիմնական Բանկին իրեն հայտնի դառնալու պահից հնարավորինս սեղմ ժամկետում՝ E-Channels-ի հետ կապված ցանկացած գողության, զեղծարարության, ապօրինի գործողության, կորստի, վնասի կամ այլ չարաշահման, կամ սխալ օգտագործման դեպքերի մասին:

4.2 Եթե Հիմնական հաճախորդը մուտք է գործում կամ օգտագործում է E-Channels-ը երրորդ անձի հաշվի կապակցությամբ, ապա վերջինս հավաստում և երաշխավորում է, որ պատշաճ կերպով լիազորված է երրորդ անձի կողմից նման գործողություններ կատարելու համար:

4.3 Ո՛չ Հիմնական Բանկը, և ո՛չ էլ Խմբի մեկ այլ անդամ պատասխանատվություն չեն կրում Ենթակառուցվածքների տրամադրողի գործողությունների կամ անգործության պատճառով առաջացած վնասի համար, բայց կհամագործակցեն Հիմնական հաճախորդի հետ այդպիսի վնասի հատուցման համար:

4.4 Հիմնական Բանկը կարող է կասեցնել E-Channels-ի ծառայությունների մատուցումը տեխնիկական աշխատանքներ կատարելու պատճառով կամ Հիմնական Բանկի համար ողջամտորեն անհրաժեշտ որևէ այլ պատճառով: Հիմնական Բանկը հնարավորության դեպքում նախապես պատշաճ կծանուցի Հիմնական հաճախորդին նման կասեցման մասին:

5. Վճարներ և գանձումներ

Հիմնական Հաճախորդը պարտավոր է Հիմնական Բանկին վճարել E-Channels-ի առնչությամբ բոլոր վճարները, ծախսերը, գանձումները, տոկոսները, որոնք նախատեսված են Ծառայությունների մատուցման պայմաններով կամ համաձայնեցված Հիմնական Բանկի հետ:

6. Փոփոխություններ

Հիմնական Բանկը իրավունք ունի փոփոխություններ կատարել E-Terms-ում, որոնք ուժի մեջ կմտնեն Հիմնական հաճախորդին պատշաճ ծանուցելուց 45 օր հետո: Ներկայացվող ցանկացած ծանուցում պետք է տրամադրվի գրավոր Հիմնական հաճախորդին կամ հրապարակվի www.hsbcnet.com կայքում: Հիմնական Բանկը, այդուհանդերձ, բացառիկ հանգամանքներում, օրենքի կամ կանոնակարգի պահանջներին համապատասխանությունն ապահովելու նպատակով, կարող է ցանկացած ժամանակ փոփոխություններ կատարել E-Terms-ում, որոնք ուժի մեջ կմտնեն անմիջապես Հիմնական հաճախորդին ծանուցելու պահից:

7. Դադարեցում

7.1 Յուրաքանչյուր կողմ կարող է դադարեցնել E-Terms-ը և/կամ E-Channels-ը մասամբ կամ ամբողջությամբ՝ մյուս կողմին նախապես 30 օր առաջ գրավոր ծանուցելով: E-Terms-ի դադարեցման դեպքում Հիմնական Բանկի նկատմամբ E-Channels-ին վերաբերող բոլոր ֆինանսական պարտավորությունները ենթակա են անհապաղ վճարման:

7.2 Որևէ իրավական կամ կանոնակարգային սահմանափակումների կիրառման դեպքում, ցանկացած Կողմ կարող է անմիջապես դադարեցնել E-Terms-ը և/կամ E-Channels-ը մասամբ կամ ամբողջությամբ, եթե՝

(ա) մյուս Կողմը էականորեն խախտել է E-Terms- ը, որը հնարավոր չէ վերացնել կամ չի վերացվում ողջամիտ ժամկետում,

(բ) մյուս Կողմը ճանաչվում է անվճարունակ, կամ

(գ) Կողմի համար E-Terms-ի կատարումն անօրինական է կամ կարող է անօրինական դառնալ:

7.3 7.3 և 3.5 կետերը ուժի մեջ են մնում E-Terms-ի դադարեցումից հետո:

7.4 Ծառայությունների դադարեցման դեպքում, Ծառայությունների Պայմանները ուժի մեջ են մնում անկախ Ծառայությունների դադարեցումից, եթե դա անհրաժեշտ է E-Terms-ը գործողության մեջ պահելու համար:

Անվտանգության Միջոցներ

Այս փաստաթուղթը սահմանում է անվտանգության չափանիշներ (որոնք ժամանակ առ ժամանակ կարող են վերանայվել կամ թարմացվել HSBC Խմբի կողմից) HSBC խմբի ցանկացած անդամի («Հիմնական Բանկ») կողմից իր հաճախորդներին («Հիմնական Հաճախորդ») տրամադրվող ցանկացած էլեկտրոնային բանկային համակարգի («E-channels»-ի) համար:

Հիմնական Բանկի անվտանգության միջոցներ

1. Հիմնական Բանկը պարտավոր է միջոցներ կիրառել՝ արգելելու երրորդ անձանց չթույլատրված մուտքը այն միջավայր, որում գործում է Բանկի ինտերնետային ծառայությունը:

2. Հիմնական Բանկը պետք է ապահովի, իր համակարգերի նկատմամբ խիստ վերահսկողությունը, ներառյալ գործունեության շարունակականությունն ապահովող ծրագրերի առկայությունը:

3. Որպես Հիմնական Բանկի անվտանգության չափանիշների մի մաս՝ Հիմնական Հաճախորդի կողմից լիազորված օգտագործողների մուտքը համակարգ կարող է ժամանակավորապես կասեցվել, երբ նրանք մուտք չեն գործել HSBC*net* 6 ամիս շարունակ: Եթե 18 ամսվա ընթացքում HSBC*net* համակագ ընդհանրապես որևէ օգտագործող մուտք չի գործել, HSBC*net*-ը կարող է կասեցվել ամբողջությամբ:

4. Եթե կենսաչափական վավերացման միջոցները (օրինակ՝ մատնահետքերի կամ դեմքի ճանաչում) օգտագործվում են բջջային սարքից E-Channels մուտք գործելու համար, Հիմնական Բանկը և բջջային սարքերի հավելված տրամադրող HSBC-ի հետ փոխկապակցված կազմակերպությունը իրավունք ունեն հեռացնել կենսաչափական վավերացումը ցանկացած պահի և անհրաժեշտության դեպքում առանց նախազգուշացման, եթե սարքի անվտանգության հետ կապված մտահոգություններ կան: Այդ պայմաններում հնարավոր կլինի նույնականացում բջջային սարքի միջոցով օգտագործելով առկա այլ մեթոդներ:

Հիմնական Հաճախորդի անվտանգության միջոցները

1. Հիմնական հաճախորդը պարտավոր է մուտք գործել E-Channels միայն Հիմնական Բանկի կողմից սահմանված հավաստագրման եղանակներով:

2. Հիմնական հաճախորդը երաշխավորում է, որ բոլոր օգտագործողները մշտապես խստորեն պահպանում են իրենց անվտանգության տվյալները (գաղտնաբառ, հիշվող պատասխան, անվտանգության պատասխաններ, անվտանգության սարքի ծածկագիր կամ E-Channels մուտք գործելու համար անհրաժեշտ անվտանգության այլ տվյալներ), և չեն նպաստելու դրանց որևէ չարտոնված օգտագործմանը: Մասնավորապես, Հիմնական Հաճախորդը չի կարող տրամադրել իր E-Channels-ի անվտանգության տվյալները երրորդ անձանց, բացառությամբ կարգավորվող երրորդ կողմի ծառայություններ մատուցողի՝ լիազորված Հիմնական Հաճախորդի կողմից:

3. Հիմնական հաճախորդը պարտավոր է զգուշությամբ ընտրել իր Օգտագործողներին, հաշվի առնելով, որ այդ Օգտագործողները օժտվում են լայն հնարավորություններով՝ ներառյալ հաշիվների կամ այլ ծառայությունների նկատմամբ իրավասությունների տրամադրումը և այդ հաշիվներին կամ ծառայություններին վերաբերող հանձնարարականների ուղարկումը:

4. Հիմնական հաճախորդը իր անվտանգության սարքերի կորստի կամ գողության դեպքում պետք է անհապաղ տեղեկացնի Հիմնական Բանկին:

5. Հիմնական հաճախորդը պետք է՝

(ա) անհապաղ գործողություններ ձեռնարկի որևէ Օգտատիրոջ տվյալները պահպանելու նպատակով, եթե կասկածներ ունի, որ Օգտագործողի տվյալները որևէ կերպ ամբողջությամբ կամ մասամբ հասանելի են դարձել այլ անձանց;

(բ) ստուգի իր հաշվով կատարված վերջին գործողությունները և Օգտագործողների տվյալները, եթե կասկածներ կան, որ իր որևէ Օգտագործողի տվյալները

հասանելի են դարձել այլ անձանց և անհապաղ տեղյակ պահի Հիմնական Բանկին ցանկացած անհամապատասխանության մասին; և

(գ) պարբերաբար ստուգի հաշիվների և օգտագործողների ակտիվությունը և լիազորությունները, համոզված լինելու համար, որ չկան անհամապատասխանություններ, հակառակ դեպքում անհապաղ տեղեկացնի Հիմնական Բանկին:

6. Հիմնական Հաճախորդը պետք է անհապաղ հեռացնի E-Channels-ից կազմակերպությունից դուրս եկած Օգտագործողներին: Հիմնական Հաճախորդը պետք է անհապաղ կասեցնի մուտքը E-Channels համակարգ ցանկացած Օգտագործողի համար, երբ որևէ անհանգստություն կա այդ Օգտագործողի վարքի կամ լիազորությունների վերաբերյալ: Հիմնական Հաճախորդը երաշխավորում է, որ անվտանգության տվյալները և Անվտանգության Սարքերը կօգտագործվեն միայն այն Օգտագործողների կողմից, որոնց լիազորել է:

7. Հիմնական հաճախորդը երաշխավորում է, որ բոլոր Օգտագործողները տրամադրել են ամբողջական և ոչ կրճատ տվյալներ, ինչպես պահանջվում է HSBC Խմբի կողմից: Հաճախորդը հետագայում կապահովի, որպեսզի Օգտագործողները պարբերաբար վերանայեն և փոփոխությունների դեպքում թարմացնեն իրենց տվյալները և չօգտվեն մեկից ավել Օգտագործողի անունից կամ անվտանգության տվյալներից:

8. Հիմնական Հաճախորդը պետք է տեղեկացնի Հիմնական Բանկին Անվտանգության Սարքերի ուղարկելուց յոթ օրվա ընթացքում, որ նա չի ստացել ուղարկված փաթեթը, պայմանով, որ Հաճախորդը տեղեկացված է եղել փաթեթի ուղարկման մասին:

9. Հիմնական հաճախորդը պարտավոր է Հիմնական Բանկի պահանջի դեպքում անհապաղ վերադարձնել բոլոր Անվտանգության Սարքերը:

10. Հիմնական Հաճախորդը կանոնավոր կերպով պետք է հետևի իր ներքին անվտանգության համակարգերի թարմացմանը՝ համաձայն համապատասխան կարգավորող մարմինների և արդյունաբերության լավագույն փորձի ուղեցույցների: Դա պետք է ներառի, բայց չսահմանափակվի միայն վնասաբեր ծրագրերից պաշտպանությամբ, ցանցի, աշխատավայրի, հեռակառավարման հասանելիության սահմանափակումներով, համակարգչային անվտանգության կարգավորումներով, համակարգերի ոչ պատշաճ օգտագործման մոնիտորինգով, վստահելի զննարկիչների և էլ. փոստի օգտագործմամբ:

11. Հիմնական Հաճախորդը պետք է ունենա համապատասխան գործընթացներ կանխելու էլեկտրոնային խարդախությունները և կեղծ հաղորդակցությունները: Սա նպատակ ունի կանխելու էլեկտրոնային փոստի միջոցով իրականացվող խաբեությունները և նմանատիպ այլ գործողությունները, երբ խաբեբան էլ. փոստի միջոցով նամակ է ուղարկում E-Channels-ի լիազորված օգտագործողի հասցեին՝ պահանջելով փոփոխություններ կատարել բանկային փոխանցման տվյալների մեջ: Նման գործընթացները պետք է կիրառվեն օրինակ այն դեպքերում, երբ Օգտագործողը հաղորդակցություններ է ստանում, որոնք, կարծես ուղարկված են ծանոթ հասցեից բայց պարունակում են կեղծ տվյալներ: Պետք է ապահովվի այդ հաղորդակցությունների իսկության ստուգումը:

12. Եթե Օգտագործողը E-Channels մուտք է գործել շարժական սարքի միջոցով, ապա Հիմնական հաճախորդը պարտավոր է պահանջել Օգտագործողից, որպեսզի նա՝

(ա) ցանկացած E-Channels համակարգ մուտք գործելիս բջջային սարքերը չթողնի առանց հսկողության,

(բ) սեղմի «Ելք/Logout» կոճակը, երբ Օգտագործողը ավարտել է իր աշխատանքը E-Channels-ում,

(գ) ակտիվացնի շարժական սարքերի

ավտոմատ արգելափակումը գաղտնաբառի միջոցով,

(դ) չտրամադրի ուրիշներին բջջային սարքերը, որոնցով մուտք եք գործում E-Channels համակարգ,

(ե) Օգտագործողը բջջային սարքի կենսաչափական հավելվածների (դեմքի, մատնահետքի, ձայնի ճանաչում) միակ գրանցված անձն է,

(զ) քայլեր ձեռնարկի ապաակտիվացնելու բջջային սարքերը, որոնք այլևս չեն օգտագործվում նույնականացման համար, ինչպես նախատեսված է 15-րդ կետով, և

(է) մուտք չգործի E-Channels համակարգ բջջային սարքերով, որոնց գործարանային ծրագրային ապահովումը փոխվել է, շրջանցվել է կամ այլ կերպ վնասվել:

13. Հիմնական Հաճախորդը ընդունում և համաձայնվում է, որ այն դեպքում, երբ E-Cnannels համակարգը որևէ պատճառով կասեցված է, հետագա վերաակտիվացումից հետո ավտոմատ կերպով կվերականգնվեն բոլոր նախնական լիազորությունները, իրավունքները, սահմանաչափերը և ծառայությունները, ինչպես եղել է նախկինում, մինչև կասեցումը;

14. Հիմնական Հաճախորդը պետք է տեղյակ լինի, որ բջջային սարքերի միջոցով E-Channels մուտք գործող օգտվողները կարող են իրականացնել լայնածավալ գործողություններ այդ սարքերի միջոցով: Սա ներառում է (օրինակ՝ Անվտանգության Սարքի փոխարեն) բջջային սարքի օգտագործումը համակարգչի միջոցով իրականացվող գործողությունները հաստատելու համար:

15. Այն դեպքում, երբ օգտագործողները մուտք են գործում E-Channels որոշակի բջջային սարքերում առկա կենսաչափական նույնականացման միջոցով (օրինակ՝ մատնահետքերի սկաներ կամ դեմքի ճանաչում), Հիմնական Հաճախորդը ընդունում է, որ այդ նույնականացման եղանակները դեռևս վտանգ են ներկայացնում չարտոնված մուտքի համար (օրինակ, երբ ներգրավված են ընտանիքի անդամներ):

Մուտքի Հսկման Ընթացակարգեր

Այս բաժնում նկարագրվում են Մուտքի Հսկման Ընթացակարգերը, որոնց հղում է արված HSBC*net* Հաճախորդի Պայմանագրում:

Այս բաժնի հիմնական նպատակն է սահմանել Հաճախորդների՝ Ձեր և Ձեր կողմից նշանակված Օգտագործողների անվտանգության հետ կապված պարտականությունները: Մուտքի Հսկման Ընթացակարգերը նաև նպատակ ունեն սահմանել այն մեխանիզմներն ու ընթացակարգերը, որոնց պետք է հետևեն Օգտագործողները Համակարգ մուտք գործելիս կամ ծառայություններից օգտվելիս, նկարագրել այն բոլոր լիազորությունները/իրավասությունները, որոնք տրվելու են Օգտագործողներին, ինչպես նաև Համակարգի և Ծառայությունների օգտագործման հետ կապված բոլոր սահմանափակումները:

Մուտքի Հսկման Ընթացակարգերի այս տարբերակը թարմացվել է և ընդգրկում է անվտանգության հետ կապված այն լրացուցիչ առանձնահատկությունները, որոնք ներմուծվել են HSBC*net*-ով կատարվող գործարքների համար:

Այս բաժինը նպատակ չունի տրամադրել համապարփակ տեղեկություններ Համակարգի և Ծառայությունների վերաբերյալ, և ցանկացած լրացուցիչ տեղեկություն կարելի է գտնել Հաճախորդի Ձեռնարկներում: Մուտքի Հսկման Ընթացակարգերի և Հաճախորդի Ձեռնարկների միջև անհամապատասխանությունների դեպքում գերակայում է Մուտքի Հսկման Ընթացակարգերը:

Այս բաժնում օգտագործվող մեծատառերով գրված բոլոր բառերն ունեն նույն նշանակությունը, ինչ որ HSBC*net* Հաճախորդի Պայմանագրում օգտագործված հասկացությունները: Բացի այդ, հարկ է նշել, որ վերոհիշյալ Հաճախորդի Պայմանագրի 6.1. կետով Հաճախորդները պարտավորվում են հետևել և կատարել Մուտքի Հսկման Ընթացակարգի պահանջները:

1. Համակարգ

HSBC*net*-ը Էյչ-Էս-Բի-Սի Բանկի ինտերնետ պորտալն է, որի միջոցով Դուք հնարավորություն ունեք օգտվելու Ձեր կողմից ընտրված Ծառայություններից: HSBC*net*-ին միանալու համար Ձեզ անհրաժեշտ է զննարկիչ ծրագիր և ինտերնետ կապ, որը միանում է կամ զանգահարելու կամ տեղական ցանցի միջոցով:

2. Ծառայություններ

HSBC*net*-ն առաջարկում է բազմաթիվ ծառայություններ, որոնք հասանելի են վավերացման մի շարք մեթոդների կիրառմամբ: Այս մեթոդները հիմնականում կիրառվում են գաղտնաբառի կամ Բանկի կողմից Ձեզ տրամադրված անվտանգության սարքերի միջոցով (երկաստիճան վավերացում):

Էյչ-Էս-Բի-Սի Բանկը կարող է փոփոխել վավերացման այս մեթոդների բնույթը և ժամանակ առ ժամանակ հզորացնել ծառայություններից յուրաքանչյուրի կամ բոլոր ծառայությունների անվտանգությունը: Բացի այդ, հնարավոր է վավերացման ոչ բոլոր մեթոդները հասանելի լինեն բոլոր Օգտագործողների համար:

HSBC*net*-ի հիմնական Ծառայությունների նույնականացման աստիճանները

ԾԱՌԱՅՈՒԹՅՈՒՆ	ՎԱՎԵՐԱՑՈՒՄ
Հաշվի վերաբերյալ տեղեկությունների ստացում	Ծածկագիր և հիշվող պատասխան կամ մեկանգամյա գաղտնաբառ գեներացնող անվտանգության սարք (համակարգ մուտք գործելիս)
Տեղեկանքների/քաղվածքների ստացում	
Վճարման կամ գործարքի նախապատրաստում	
Վճարման կամ գործարքի հաստատում	Ծածկագիր և հիշվող պատասխան և ծածկագրով պաշտպանված սմարթ քարտ կամ մեկանգամյա գաղտնաբառ գեներացնող անվտանգության սարք (համակարգ մուտք գործելիս և սերվերի մեկնարկի ժամանակ)
Լրացուցիչ Օգտագործողի հաշվի կարգավորում	
Համակարգում ֆայլերի վերբեռնում	

3. Օգտագործողներ

Օգտագործողներ

Օգտագործողներ են համարվում բոլոր այն անձինք, ովքեր Ձեր կողմից լիազորված են օգտվել Համակարգից: Օգտագործողները ստեղծվում են Ձեր առաջադրած Համակարգի Ադմինիստրատորների կողմից: Համակարգի սկզբնական ադմինիստրատորներից բացի, որոնք նշանակվում են Բանկի կողմից, բոլոր հետագա Օգտագործողները հաստատվում և հսկվում են ուղղակիորեն Համակարգային Ադմինիստրատորների կողմից:

Համակարգի Ադմինիստրատորներ

Համակարգի ադմինիստրատորները պատասխանատվություն են կրում Օգտագործողների հաստատման, լիազորման և հսկման համար (ներառյալ համակարգի այլ ադմինիստրատորների): Համակարգի Ադմինիստրատորները հաստատում են այն անձանց (ներառյալ այլ Համակարգի Ադմինիստրատորների), որոնք պետք է օգտվեն համակարգից: Նրանք սահմանում են, թե ինչ ծառայություններից կարող են օգտվել Օգտագործողները և այդ ծառայությունների ներքո նրանց լիազորությունների համապատասխան շրջանակները: Օրինակ, համակարգի ադմինիստրատորը կարող է Օգտագործողին տալ համապատասխան լիազորություն օգտվելու արտասահմանում գտնվող հաշիվների վերաբերյալ տեղեկություններ ստանալու ծառայությունից և այնուհետև Ծառայության ներքո սահմանել, թե կոնկրետ որ հաշիվների վերաբերյալ տվյալ Օգտագործողը կարող է ստանալ տեղեկություններ: Համակարգային ադմինիստրատորները կառավարում/հսկում են բոլոր Օգտագործողների կողմից Համակարգի օգտագործումը: Նրանք պետք է ապահովեն Օգտագործողի օգտահաշվի կասեցումը, երբ նա գտնվում է արձակուրդում և անհրաժեշտության դեպքում ջնջեն այն: Համակարգային Ադմինիստրատորները նույնպես լիազորված են փոխելու / վերահաստատելու Օգտագործողների ծածկագրերը և անհրաժեշտության դեպքում պահպանել նրանց օգտահաշիվները: Համակարգի ադմինիստրատորների կողմից Օգտագործողների հաստատումն ու լիազորումը և օգտվելու որոշակի ծառայությունների մասին տեղեկատվություն կարելի է գտնել HSBC*net*-ի հաճախորդների ուղեցույցում:

Օգտագործողի նույնականացում

Դուք պատասխանատու եք Օգտագործողների ինքնությունն ստուգելու համար, մասնավորապես այն Օգտագործողներինը, ովքեր լիազորված են Ձեր անունից գործարքներ կատարել: Համակարգի ադմինիստրատորները սովորաբար պետք է պաշտոնապես նույնականացվեն և նրանց հասցեները հաստատվեն Բանկի կողմից՝ փողերի լվացումը կանխարգելելու նպատակով: Ձեր(կամ Տվյալ) երկրի Էյչ-Էս-Բի-Սի Բանկի աշխատակիցը Ձեզ կտեղեկացնի, թե ինչ փաստաթղթեր են անհրաժեշտ ներկայացնել և արդյոք գործում են արտոնություններ որոշ ընկերությունների համար:

4. Գրանցումը Համակարգում

HSBC*net*-ում գրանցումը բաղկացած է հետևյալ պարզ քայլերից.

Հաճախորդի պայմանագրի լրացում

Սա իրենից ներկայացնում է այն ստանդարտ HSBC*net* հաճախորդների պայմանագիրը, որը պետք է ստորագրվի համաձայն ընկերության ստորագրությունների կարգի: Այն ընդգրկում է հետևյալ տվյալները՝

- ընկերության վերաբերյալ տեղեկություններ,
- այն հաշիվների ցանկը, որոնց վերաբերյալ տեղեկություններ են ստացվելու HSBC*net*-ի միջոցով,
- տվյալներ համակարգի սկզբնական ադմինիստրատորների վերաբերյալ:

Եթե ցանկանում եք, որ Ձեր դուստր ձեռնարկություններից մեկը հաշվետվություններ ներկայացնի Ձեզ HSBC*net*-ի միջոցով, Դուք նաև պետք է ապահովեք, որ այն լրացնի և ստորագրի Հաճախորդների պայմանագրի Հաճախորդների գործընկեր բաժինը, որը թույլ կտա Ձեր դուստր ձեռնարկության խմբային գրասենյակին կամ այլ բանկերին հաշվետվություններ ներկայացնել HSBC*net*-ի միջոցով:

Նախնական Համակարգի ադմինիստրատորի գրանցում

Ձեր նախնական համակարգի ադմինիստրատորին գրանցելու համար, պետք է Բանկին տրամադրեք համակարգի նախնական ադմինիստրատորների (առավելագույնը չորս հոգու) անունները և տեղեկատվություն նրանց մասին: Բանկը կստեղծի համակարգի նախնական ադմինիստրատորների պրոֆիլները Ձեզ համար: Դրանից հետո Դուք եք պատասխանատու լինելու համակարգի լրացուցիչ ադմինիստրատորների և Օգտագործողների պրոֆիլների ստեղծման բոլոր փուլերի համար:

Լրացուցիչ Օգտագործողի Գրանցում

Լրացուցիչ Օգտագործողների (այդ թվում՝ լրացուցիչ ցանցային ադմինիստրատորների) գրանցումը կատարվում է Ցանցային ադմինիստրատորների կողմից, մինչդեռ նախնական համակարգային Ադմինիստրատորները գրանցվում են Բանկի կողմից:

Լրացուցիչ օգտագործողների գրանցման գործընթացը նման է վերոնշյալ առցանց Համակարգի Ադմինիստրատորի գրանցման կարգին, երբ Օգտագործողները պետք է լրացնեն ինտերնետում դիմումի ձև, որն էլ այնուհետև հաստատվում է Համակարգային Ադմինիստրատորների կողմից: Հարկ է նշել, որ լրացուցիչ համակարգային ադմինիստրատորների ինքնությունը պետք է ստուգվի Բանկի կողմից «Օգտագործողի Նույնականացում» բաժնում նկարագրված կարգով:

Գրանցման նոր հայտը մշակելիս, Համակարգի Ադմինիստրատորներին, բոլոր դեպքերում, խորհուրդ է տրվում ստուգել դիմումի օրինականությունը՝ հիմնվելով համցանցից բացի այլ աղբյուրի վրա:

Իրենց բնույթով, գրանցման նոր հայտերը չեն ներկայացվում անվտանգ աղբյուրից:

5. Նույնականացուցիչներ

Այս բաժնում նկարագրվում են HSBC*net* ծառայություններ մուտք գործելու համար օգտագործվող տարբեր նույնականացուցիչները:

Խնդրում ենք նկատի ունենալ, որ այս բոլոր մեթոդները ամբողջական կամ մասնակիորեն կարող են կիրառվել HSBC*net* ծառայություններից Ձեր կողմից գրանցված օգտվողներին վավերացնելու համար, ընդ որում՝անվտանգության նկատառումներից ելնելով դրանց օգտագործումը երբեմն կարող է կարգավորվել Բանկի հայեցողությամբ:

Բացի այդ, վավերացման ոչ բոլոր մեթոդներն են մատչելի լինելու Ձեզ համար, և որտեղ կա վավերացման մեթոդի հնարավոր ընտրություն, Բանկը իրավունք է վերապահում որոշել անվտանգության մեթոդաբանությունը՝ ըստ Ձեր գործունեության տեսակի:

Գաղտնաբառ

Գաղտնաբառը նվազագույնը 8 նիշից բաղկացած տառերի և թվերի համակցություն է, որն ընտրվում է Օգտագործողի կողմից գրանցման ժամանակ:

Հիշվող պատասխան

HSBC*net*-ում գրանցման ժամանակ Օգտագործողներից կպահանջվի ընտրել Հիշվող Հարց և Պատասխան: Հիշվող պատասխանը կարող է անհրաժեշտ լինել համակարգ մուտք անելիս, որպես ապահովության լրացուցիչ միջոց:

Ծածկագրով Պաշտպանված Սմարթ Քարտ

Սա իրենից ներկայացնում է սմարթ քարտ, որը պարունակում է նախապես բեռնված թվային սերտիֆիկատ: Որոշակի ծառայություններից օգտվելու համար Օգտագործողները, ինչպես նկարագրված է վերոհիշյալ 2-րդ բաժնում, պետք է մուտքագրեն իրենց սմարթ քարտը՝ հատուկ սմարթ քարտ ընթերցող սարքի մեջ և մուտք անեն լրացուցիչ ծածկագիրը: Բաժին 2-ում նկարագրված ծառայություններից օգտվելու համար Օգտատերերը պետք է սմարթ քարտը մուտք անեն ընթերցող սարքի մեջ և մուտքագրեն PIN կոդը:

Ծածկագրով Պաշտպանված Անվտանգության Սարք

Սա ծածկագրով պաշտպանված սարք է, որը գեներացնում է մեկանգամյա օգտագործման գաղտնաբառեր HSBC*net* մուտք գործելու համար: Այդ գաղտնաբառերը կարող են օգտագործվել միայն մեկ անգամ. այն անվավեր կճանաչվի կարճ ժամանակ անց: Հիշյալ գաղտնաբառերը յուրահատուկ են յուրաքանչյուր սարքի համար, հետևաբար յուրահատուկ են յուրաքանչյուր Օգտագործողի հաշվի համար:

Անվտանգության սարքը օգտագործվում է և համակարգ մուտք գործելիս, և որոշ բաժիններ մուտք գործելու ժամանակ վերահավաստագրման ժամանակ (տես՝ բաժին 2):

Սմարթ քարտը և Անվտանգության սարքը իրենցից ներկայացնում են երկաստիճան հավաստագրման մի ձև, որը պահանջում է, որ Օգտատերը ոչ միայն իմանա սարքի գաղտնաբառը, այլ նաև ֆիզիկապես ունենա այն իր մոտ:

6. Անվտանգության Նպատակով ձեռնարկվող միջոցներ

Դուք պատասխանատու եք համակարգի և Բանկի հետ Ձեր հաղորդակցության համար, ուստի պետք է հետևեք այս քայլերին առավելագույն պաշտպանություն ապահովելու համար:

Անվտանգության միջոցներ

Օգտագործողները պետք է պահեն իրենց անվտանգության միջոցները (գաղտնաբառը, հիշվող պատասխանը, անվտանգության պատասխանները, սմարթ քարտի ծածկագիրը, անվտանգության սարքը կամ ցանկացած այլ անվտանգության միջոց, որն անհրաժեշտ է HSBC*net* մուտք գործելու համար) ապահով տեղում և բացառեն դրանց օգտագործումը կամ օգտագործման փորձերը ոչ լիազորված անձանց կողմից: Մասնավորապես՝

- երբեք մի գրեք այդ տվյալները որևէ տեղ կամ մի հայտնեք դրանք երրորդ անձանց,
- ոչնչացրեք Բանկից կամ որևէ այլ տեղից ստացված ծածկագրի վերաբերյալ տեղեկանքը,
- խուսափեք այնպիսի ծածկագրերից, հիշվող պատասխաններից, որոնք ուրիշները կարող են հեշտությամբ կռահել (օրինակ անձնական տվյալներ, թվերի պարզ համադրություն) և հետևեք HSBC*net* կայքում տեղակայված ծածկագրերի նշանակման ուղեցույցին,
- երբևէ մի գրանցեք Ձեր ծածկագրերը կամ հիշվող պատասխանները որևէ համակարգչային ծրագրում, որը կարող է ավտոմատ հիշվել (օրինակ համակարգիչը կարող է առաջարկել «հիշել ծածկագիրը» կամ ունենալ դրան նման որևէ այլ գործառույթ),
- համոզվեք, որ համակարգ մուտք գործելիս ոչ մեկ չի հետևում ձեզ անձամբ կամ տեսախցիկի միջոցով,
- ստանալուն պես անմիջապես փոխեք ծածկագիրը, և պարբերաբար փոխեք ծածկագիրն ու գաղտնաբառը,
- երբևէ մի հայտնեք Ձեր գաղտնաբառերը Էյչ-Էս-Բի-Սի-ի աշխատակիցներին: Դուք պետք է զգույշ լինեք, եթե ստանում եք որևէ գրություն, որտեղ Ձեզնից պահանջվում է տրամադրել Ձեր ծածկագիրը կամ բանկային որևէ այլ տվյալ, և կասկածներ ունենալու դեպքում անմիջապես կապվեք Բանկի հետ,
- եթե Դուք կասկածում եք, որ Ձեր գաղտնաբառերը մասնակիորեն կամ ամբողջությամբ հայտնի են դարձել, անմիջապես ձեռնարկեք միջոցներ Ձեր հաշիվը պաշտպանելու համար՝ փոխելով տվյալները, գաղտնաբառը կամ ժամանակավորապես փակելով հաշիվը՝ մինչև կձեռնարկվեն անվտանգության անհրաժեշտ միջոցառումներ,
- Դուք նաև պետք է վերհիշեք հաշվի վերջին գործարքները՝ չարտոնված գործարքները բացահայտելու նպատակով:

Ֆիզիկական անվտանգության Թոքեններ. Սմարթ քարտեր և Անվտանգության սարքեր

- Անվտանգության սարքերը (և անհրաժեշտության դեպքում դրանց ծածկագրերը) Ձեզ տրամադրվում են տարբեր եղանակներով: Դուք պետք է անհապաղ տեղեկացնեք Բանկին, եթե ողջամիտ ժամկետում (սովորաբար յոթ օր) չեք ստացել համապատասխան փաթեթը,

- այն դեպքում, երբ անվտանգության սարքեր պարունակող փաթեթները չեն կարող ուղղակիորեն առաքվել Ձեր ընկերության համապատասխան աշխատակցին (օրինակ, երբ առաքումը կատարվում է փոստի միջոցով), Դուք պատասխանատու եք, որ երրորդ կողմը հանձնի փաթեթը անմիջապես տվյալ աշխատակցին,
- անվտանգության սարքի միջոցով HSBC*net* ծառայություններից օգտվելիս բացվում է անվտանգ աշխատաշրջան, որը մնում է բաց մինչև Օգտագործողն ինքը դուրս չգա համակարգից: Հետևաբար չափազանց կարևոր է բաց չթողնել ծրագիրը սարքից հեռանալիս, նույնիսկ եթե այն ծառայությունը, որից օգտվել եք արդեն փակ է,
- անվտանգության սարքերը չթողնել առանց հսկողության կամ որտեղ դրանք կարող են յուրացվել, անկախ այն հանգամանքից, որ դրանք պաշտպանված են ծածկագրով,
- պետք է հետևել նաև, որ անվտանգության սարքերը պահվեն անվտանգ վայրում, երբ դրանք չեն օգտագործվում,
- Դուք չպետք է տաք կամ ժամանակավորապես հանձնեք Ձեր անվտանգության սարքը որևէ երրորդ անձի,
- եթե Ձեր անվտանգության սարքը կորել կամ գողացվել է, պետք է անհապաղ տեղեկացնեք կամ հետևեք այն ուղեցույցներին, որոնք սահմանված են անվտանգության սարքերի օգտագործման համար,
- անվտանգության սարքերը պետք պահվեն ապահով տեղում: Խուսափեք՝

– բարձր ջերմաստիճանից,

– էլեկտրական հոսանքի սխալ լարումից,

– բարձր խոնավությունից,

– քայքայիչ կամ այլ քիմիական նյութերից,

– արևի ուղիղ ճառագայթներից

– ջրից, լվացող և սպիտակեցնող միջոցներից, ալկոհոլից և այլն:

- մշտապես հետևեք ինտերնետ կայքում տեղադրված կամ Էյչ-Էս-Բի-Սի Բանկի կողմից հրատարակված օգտագործման ուղեցույցներին և անվտանգության կանոններին:

Խնդրում ենք հաշվի առնել, որ Բանկն իրավունք ունի ետ վերցնել Անվտանգության սարքը, եթե գտնում է, որ այն օգտագործվում է ոչ պատշաճ:

Թվային Սերտիֆիկատի Կառավարում

Սմարթ քարտի վրա պահվող թվային սերտիֆիկատները չպետք է ուղարկվեն որևէ երրորդ կողմի կամ օգտագործվեն HSBC*net* մուտք գործելուց բացի այլ նպատակներով:

Համակարգի Համատեղելիություն

Համակարգ մուտք գործելու համար Դուք պետք է ունենաք համատեղելի սարք և ծրագիր:

Նվազագույն տեխնիկական պահանջները մանրամասն ներկայացված են HSBC*net* հաճախորդի ուղեցույցներում:

Անվտանգության Չափանիշներ

Դուք պետք է վերանայեք անվտանգության Ձեր ներքին ընթացակարգերը՝ համոզվելու համար, որ պատշաճ կերպով պաշտպանված եք: Մասնավորապես Դուք պետք է երաշխավորեք/համոզվեք, որ.

- համակարգում Բանկի կողմից օգտագործվող կամ պահանջվող գաղտնագրման տեխնոլոգիան համապատասխանում է այն երկրի ազգային օրենսդրության պահանջներին, որտեղ օգտագործում եք Համակարգը,

- HSBC*net* մուտք գործելիս Դուք հաստատում և պահպանում եք համակարգի անվտանգության ստանդարտները և դրա համար օգտագործվող բաղադրիչների համար, համապատասխան ոլորտի կողմից ճանաչված ստանդարտները և վաճառողի ցուցումներին և ընդունում եք Բանկի կամ ծրագրային ապահովման մատակարարների կողմից սահմանված կամ առաջարկված շահագործման կամ անվտանգության հետ կապված բոլոր համապատասխան միջոցները:

  Սա ներառում է թարմացված արգելապատնեշների և վիրուսներից պաշտպանող ծրագրերի կիրառումը և համապատասխան սպասարկումը, ծառայությունների ժխտումը կանխարգելող միջոցները և անվտանգության այլ միջոցները, ինչպիսիք են համակարգիչ ոչ լիազորված ներխուժումը ճանաչող ծրագրային ապահովումը՝ Ձեր տեղեկատվական տեխնոլոգիայի գործողությունների չափի և բարդության համապատասխան,

- Դուք օգտագործում եք տեղեկատվական տեխնոլոգիաները և համակարգային տարրերը համապատասխան կարգավորող չափորոշիչների համաձայն (օրինակ Sarbanes Oxley):

Մուտք համակարգ

Համակարգ ոչ լիազորված անձանց կողմից մուտքը կանխելու համար Դուք պետք է երաշխավորեք/համոզվեք, որ.

- Օգտագործողները միշտ դուրս են գալիս համակարգից և համակարգին միացված ժամանակ չեն հեռանում իրենց համակարգիչների մոտից,

- Օգտագործողները պատշաճ կերպով դուրս են գալիս համակարգից օգտագործելով էկրանի վերին աջ անկյունում գտնվող «Logout» կոճակը և ոչ թե փակելով զննարկիչ պատուհանը,

- Դուք պետք է անմիջապես տեղյակ պահեք բանկին ոչ լիազորված անձանց կողմից Համակարգի օգտագործման փորձի կամ կասկածներ ունենալու դեպքում կամ որևէ ոչ լիազորված, Ձեզ համար ոչ հայտնի կամ կասկածելի գործարքի կամ հանձնարարականի մասին,

- Դուք անմիջապես պետք է արգելափակեք համակարգ մուտք գործելու իրավունքը և տեղյակ պահեք Բանկին որևէ Օգտագործողի կողմից Ծառայությունների օգտագործման հետ կապված փաստացի կամ թվացյալ որևէ խախտման վերաբերյալ կամ այն դեպքում, երբ տվյալ Օգտագործողը այլևս լիազորված չէ օգտվել Համակարգից (աշխատանքից դուրս գալու կամ որևէ այլ պատճառով),

- Դուք կատարում եք Բանկի, ոստիկանության կամ այլ կարգավորող մարմինների կողմից օգնության բոլոր ողջամիտ պահանջները անվտանգության իրական կամ հավանական խախտումները հայտնաբերելու համար:

Ֆայլերի Վերբեռնում

Հաճախորդի հրահանգներ պարունակող ֆայլը Բանկին փոխանցելու համար նախքան նշված վայրից ֆայլ ընտրելը, Դուք պետք է լրացնեք պահանջվող տեղեկատվությունը File Upload գործիքում, որը ներառում է ֆայլի տեսակը, ձևաչափը, թույլտվության աստիճանը և երկիրը (անհրաժեշտության դեպքում): Երբ Դուք սեղմեք «Go» կոճակը և Բանկը ստանա համապատասխան ֆայլը, Ձեր էկրանին կհայտնվի Բանկի կողմից ուղարկված հաստատում առ այն, որ բանկը ստացել է համապատասխան ֆայլը: Այնուհետև ֆայլի ճանաչման հաստատում տալուց առաջ Բանկը պետք է կատարի նույնականացման որոշակի գործընթաց, որը պետք է կատարվի Report and File Download գործիքի միջոցով:

Դուք պետք է տեղյակ պահեք Բանկին ֆայլի ճանաչման հաստատում ստանալու մասին, եթե Ձեր կողմից որևէ ֆայլ չի ուղարկվել, հայտնաբերել եք որևէ անճշտություն նշված հաստատման մեջ, կամ եթե որոշակի ժամանակաշրջանի ընթացքում չեք ստացել որևէ նման հաստատում: HSBC*net*-ի ֆայլերի վերբեռնման գործիքի միջոցով Հաճախորդի հանձնարարականի ֆայլը կվերցվի Ձեր կողմից նշված տեղից և կուղարկվի Բանկին: Ուստի կարևոր է, որ միջոցներ ձեռնարկվեն բացառելու շփոթմունքի արդյունքում այլ ֆայլ ուղարկելու հավանականությունը:

- Ֆայլը պետք է պահվի ապահով տեղում՝ սահմանափակելով դրա հասանելիությունը:
- Ֆայլը պետք է ստեղծվի միայն վավերացված ընթացակարգով և կարդացվի HSBC*net* համակարգի միջոցով:
- Բոլոր մուտքերը դեպի ֆայլ պետք է լինեն անվտանգ կերպով, որպեսզի անհրաժեշտության դեպքում հնարավորություն տրվի ուսումնասիրություններ իրականացնելու:

Չափազանց կարևոր է պահպանել վերոնշյալ կանոնները բոլոր դեպքերում, մասնավորապես, երբ Բանկին ուղարկվում են նախապես լիազորված Հաճախորդի Հանձնարարականները:

Այս Մուտքի Հսկման Ընթացակարգերի որևէ դրույթ չի սահմանափակում HSBC*net*-ի Հաճախորդի պայմանագրի 3-րդ կետի պայմանները և, մասնավորապես, Բանկին Հաճախորդի հրահանգների ճիշտ փոխանցումը ապահովելու Ձեր պարտավորությանը:

7. Առաջացած խնդիրների լուծում

Ծառայությունների առկայություն/ հասանելիություն

Սովորաբար Ծառայություններից կարելի է օգտվել ցանկացած ժամանակ, սակայն լինում են դեպքեր, երբ Բանկը իր հայեցողությամբ ամբողջությամբ կամ մասնակիորեն կարող է դադարեցնել Համակարգի հասանելիությունը կամ Ծառայությունների տրամադրումը:

Խնդրում ենք հաշվի առնել, որ կատարվող գործարքի կատարումը միշտ չէ, որ տեղի է ունենում հրահանգի պահին: Որոշ հարցումների մշակումը կարող է ժամանակ պահանջել, ավելին՝ որոշ գործարքներ կարող են մշակվել միայն Բանկի աշխատանքային ժամերին, չնայած որ Ծառայությունները կարող են հասանելի լինել այդ ժամերից դուրս:

Տեխնիկական աջակցություն

Բոլոր Օգտագործողները կարող են ստանալ Համակարգի կամ Ծառայությունների հետ կապված տեխնիկական աջակցություն Բանկից.

- առցանց Օժանդակող Տեքստ,
- համակարգում հասանելի է օժանդակող տեքստը, որն Օգտագործողին կօգնի հաճախ հանդիպող տեխնիկական խնդիրներին լուծում տալ,
- Համակարգային Ադմինիստրատորի օժանդակություն:

HSBC*net*-ի հետ կապված խնդիրների մեծ մասի դեպքում Օգտագործողները պետք է կապվեն իրենց Համակարգային ադմինիստրատորների հետ: Համակարգային Ադմինիստրատորներն ունեն բազմաթիվ լիազորություններ՝ այդ թվում՝ ծածկագրերի փոփոխումը:

- Զանգերի Կենտրոնի աջակցություն

Եթե կան հարցեր, որոնք չեն կարող լուծվել Համակարգային Ադմինիստրատորների կողմից, ապա Օգտագործողները կարող են ստանալ աջակցություն հեռախոսազանգի միջոցով: Էյչ-Էս-Բի-Սի Բանկի հայեցողությամբ Օգտագործողներից, աշխատողներից կարող է պահանջվել հաստատել իրենց ինքնությունը:

- Բանկի Աջակցությունը

Եթե Հաճախորդը չի կարող օգտագործել համակարգը, նա պետք է կապվի Տեղեկատվական կենտրոնի համապատասխան աշխատակցի հետ: Բանկը կարող է պահանջել, որպեսզի Օգտագործողը հաստատի իր ինքնությունը:

- Օգտագործողների գործառույթների կասեցում

Համակարգը հնարավորություն է տալիս Համակարգի ադմինիստրատորներին կասեցնել այլ Օգտագործողներին տրված լիազորությունները: Սրա անհրաժեշտությունն առաջանում է այն դեպքերում, երբ Օգտագործողի մուտքը Համակարգ պետք է ժամանակավորապես արգելափակվի, օրինակ՝ նրա արձակուրդում գտնվելու ժամանակ: Այն նախատեսված չէ օգտագործման համար այն իրավիճակում, երբ լուրջ մտահոգություններ կան Օգտագործողի վարքագծի հետ կապված: Այդ դեպքում, Համակարգի ադմինիստրատորը պետք է անհապաղ ջնջի Օգտագործողին համակարգից և չեղյալ համարի օգտագործողի սմարթ քարտը (եթե այն առկա է): Եթե կասեցումը միակ հնարավոր տարբերակն է (օրինակ, եթե անհրաժեշտ է անհապաղ արգելափակել Օգտագործողին և որևէ այլ Համակարգի ադմինիստրատոր չկա, ով կկարողանա հաստատել այդ արգելափակումը), ապա այն պետք է օգտագործվի՝ այլ պաշտպանական միջոցների հետ մեկտեղ, ինչպիսիք են օրինակ Օգտագործողի սմարթ քարտի առբերում (retrieval): Եթե կասկածներ կան, ապա կապվեք Բանկի հետ օժանդակություն ստանալու նպատակով:

Կասեցվելուց առաջ Օգտագործողը պետք է լինի «Ակտիվ» (Active) կամ «Հաստատված» (Approved) կարգավիճակում: Կասեցվելուց հետո անհրաժեշտ է, որ տվյալ Օգտագործողի պրոֆիլում որևէ հետագա տեխնիկական սպասարկում չիրականացվի՝ նրանց վերաակտիվացման կամ ջնջելուց առաջ:

Նշումներ՝

- «HSBC*net* օնլայն բանկային ծառայության» նկարագրությունը, ընձեռած հնարավորությունները և սակագները ներկայացված են համանուն տեղեկատվական ամփոփագրում, ինչպես նաև business.hsbc.am կայքում:
- Իրավաբանական անձանց մատուցվող ծառայությունների տրամադրման հիմնական պայմաններին կարող եք ծանոթանալ business.hsbc.am կայքում և «Հաճախորդների բանկային հաշիվների, բանկային ավանդների, էլեկտրոնային բանկային ծառայությունների և բանկային այլ ծառայությունների մատուցման հիմնական պայմաններ իրավաբանական անձանց համար» տեղեկատվական ամփոփագրում:

Թողարկված է «էյչ-էս-Բի-Սի Բանկ Հայաստան» ՓԲԸ-ի կողմից
«էյչ-էս-Բի-Սի Բանկ Հայաստան» ՓԲԸ-ն հանդիսանում է էյչ-էս-Բի-Սի Խմբի անդամ, որն աշխարհի ֆինանսական և բանկային ծառայություններ տրամադրող խոշորագույն կազմակերպություններից մեկն է: էյչ-էս-Բի-Սի Խմբի միջազգային ցանցը ներառում է 63 երկիր և տարածաշրջան:

www.business.hsbc.am
+374 60 655 200

Իրավաբանորեն հաստատված է
Հայաստանի Հանրապետություն, Երևան 0009, Տերյան փողոց 66
Գրանցման համար 67