Մուտքի Հսկման Ընթացակարգեր

HSBCnet
www.hsbcnet.com

HSBC
The world's local bank

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 (1) սահմանել այն մեխանիզմներն ու ընթացակարգրեը, որոնց պետք է հետևեն Օգտագործողները Համակարգ մուտք գործելիս կամ ծառայություններից օգտվելիս, (2) նկարագրել այն բոլոր լիազորությունները/իրավասությունները, որոնք տրվելու են Օգտագործողներին, ինչպես նաև Համակարգի և Ծառայությունների օգտագործման հետ կապված բոլոր սահմանափակումները:

Մուտքի Հսկման Ընթացակարգերի այս տարբերակը (տարբերակ 3) 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 տեղեկություններ 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:

Մուտքի Հսկման Ընթացակարգեր

1. Համակարգ

HSBC*net*-ը դա էյչ-էս-Բի-Սի-ի ինտերնետ պորտալն է, որի միջոցով դուք հնարավորություն ունենք օգտվել ձեր կողմից ընտրված Ծառայություններից: HSBC*net*-ին միանալու համար ձեզ անհրաժեշտ է զննարկիչ ծրագիր և ինտերնետ կապ, որը միանում է կամ զանգահարելու կամ էլ տեղական ցանցի միջոցով:

2. Ծառայություններ

HSBC*net*-ն առաջարկում է զանազան ծառայություններ, որոնք հասանելի են հավաստագրման մի շարք մեթոդների կիրառմամբ: Ընդհանուր առմամբ դրանք հիմնված են գաղտնաբառի վրա կամ Բանկի կողմից ձեզ տրամադրված անվտանգության սարքերի վրա (երկաստիճան հավաստագրում):

էյչ-էս-Բի-Սի-ն կարող է փոփոխել հավաստագրման այս մեթոդների բնույթը և ժամանակ առ ժամանակ հզորացնել ծառայություններից յուրաքանչյուրի կամ բոլոր ծառայությունների անվտանգությունը: Բացի այդ, հավաստագրման բոլոր մեթոդները կարող է նախատեսված չլինեն բոլոր Օգտագործողների համար:

HSBC*net*-ի հիմնական Ծառայությունների նույնականացման աստիճաններ

ԾԱՌԱՅՈՒԹՅՈՒՆ	ՆՈՒՅՆԱՑՈՒՑԻՉ
Ստանալ տեղեկություններ հաշվի վերաբերյալ	Ծածկագիր և հիշարժան պատասխան կամ միանգամյա գաղտնաբար գեներացնող անվտանգության սարք (համակարգ մուտք գործելիս)
Համակարգից հանել տեղեկանքներ/քաղվածքներ	
Վճարման կամ գործարքի նախապատրաստում	
Վճարման կամ գործարքի հաստատում	Ծածկագիր և հիշարժան պատասխան և ծածկագրով պաշտպանված սմարտ քարտ կամ միանգամյա գաղտնաբար գեներացնող անվտանգության սարք (համակարգ մուտք գործելիս և սերվերի մեկնարկման ժամանակ)
Լրացուցիչ Օգտագործողի պրոֆիլների սահմանում	
Համակարգ վերբեռնել ֆայլեր	

3. Օգտագործողներ

Օգտագործողներ

Օգտագործողներ են համարվում բոլոր այն անձինք, որոնք ձեր կողմից լիազորված են օգտվել Համակարգից: Օգտագործողները հաստատվում են ձեր համապատասխան 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 սահմանի, 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, որ երբ որ տվյալ Օգտագործողը արձակուրդում է գտնվում, նրա պրոֆիլները կասեցվում են և անհրաժեշտության դեպքում՝ ջնջվում: Համակարգային Ադմինիստրատորները նույնպես լիազորված են փոխելու/ վերահաստատելու Օգտագործողների ծածկագրերը և պահանջված դեպքերում՝պահպանել նրանց պրոֆիլները: Լրացուցիչ տեղեկություններ, թե ինչպես են համակարգի ադմինիստրատորները հաստատում և լիազորում Օգտագործողներից օգտվելու որոշակի ծառայություններին կարելի է գտնել HSBC*net*-ի հաճախորդների ուղեցույցում:

Մուտքի Հսկման Ընթացակարգեր

Օգտագործողի նույնականացում

Դուք պատասխանատու եք Օգտագործողների ինքնությունն ստուգելու համար, մասնավորապես այն Օգտագործողներինը, որոնք ձեր անունից լիազորված են գործարքներ կատարել: Սովորաբար անհրաժեշտ է լինում, որպեսզի համակարգային ադմինիստրատորները ֆորմալ կերպով նույնականացվեն և իրենց հասցեներն ստուգվեն Բանկի կողմից՝ փողերի լվացման կանխարգելման նպատակներով: Էյչ-Էս-Բի-Սի-ի տեղական գրասենյակի համապատասխան աշխատակիցը ձեզ կտեղեկացնի, թե ի՞նչ փաստաթղթեր են անհրաժեշտ ներկայացնել և արդյո՞ք որոշ ընկերությունների համար գործում են բացառություններ, թե՝ ոչ:

4. Գրանցումը Համակարգում

HSBC*net* համակարգում գրանցումը մի քանի պարզ քայլերից է բաղկացած:

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 դուք ցանկանում եք, որ ձեր դուստր ընկերությունների հաշիվների վերաբերյալ տեղեկությունները ձեզ տրամադրվեն HSBC*net*-ի միջոցով, ապա պետք է ապահովեք, որ տվյալ դուստր ձեռնարկությունը լրացնի և ստորագրի Հաճախորդի Պայմանագրի՝ Հաճախորդի դուստր ընկերություն բաժինը, որով տվյալ ընկերությունը կստանա լիազորություն տրամադրելու ձեզ HSBC*net* համակարգի միջոցով տեղեկություններ համապատասխան հաշվի վերաբերյալ:

Մուտքի Հսկման Ընթացակարգեր

Սկզբնական Համակարգի ադմինիստրատորի գրանցում

Ձեր նախնական համակարգի ադմինիստրատորին գրանցելու համար, պետք է Բանկին տրամադրեք համակարգի նախնական ադմինիստրատորի (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

Մինչդեռ նախնական համակարգային ադմինիստրատորները գրանցվում են Բանկի կողմից, բոլոր հետագա Օգտագործողները (ներառյալ լրացուցիչ համակարգային ադմինիստրատորները) գրանցվում են Համակարգային Ադմինիստրատորների կողմից: Լրացուցիչ Օգտագործողների համար գրանցման գործընթացը նման է վերը նկարագրված համակարգային ադմինիստրատորների գրանցման գործընթացին, 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 դիմումի ընթացք տալուց առաջ Համակարգի Ադմինիստրատորներն ամեն դեպքում պետք է ստուգեն այդ դիմումի ծագման աղբյուրը՝ Ինտերնետից բացի այլ ճանապարհով: Իրենց բնույթով, գրանցման նոր դիմումները չեն ներկայացվում ապահով ճանապարհով:

Մուտքի Հսկման Ընթացակարգեր

5. Նույնացուցիչներ

Այս բաժնում նկարագրված են HSBC*net*-ի ծառայությունների օգտագործման ժամանակ կիրառվող զանազան նույնացուցիչները: Կցանկանայինք նշել, որ Ձեր Օգտագործողների՝ HSBC*net*-ի ծառայություններից օգտվելիս կարող են օգտագործվել բոլոր այդ մեթոդները կամ դրանցից մի քանիսը. Դրանց կիրառումը ժամանակի ընթացքում Բանկի հայեցողությամբ անվտանգության նկատառումներով կարող է փոփոխվել: Բացի այդ, հավաստագրման ոչ բոլոր մեթոդներն են հասանելի լինելու Ձեզ համար, և հավաստագրման մեթոդի ընտրության հնարավորության դեպքում Բանկն իրեն իրավունք է վերապահում որոշելու անվտանգության այն մեթոդոլոգիան, որը Բանկի կարծիքով առավել հարմար է Ձեր գործունեության համար:

Գաղտնաբառ

Գաղտնաբառն իրենից ներկայացնում է նվազագույնն ութանիշ թվերի և տառերի շարան, որը Օգտագործողի կողմից ընտրվում է գրանցման ժամանակ:

Հիշվող պատասխան

HSBC*net*-ում գրանցման ժամանակ Օգտագործողներից կպահանջվի ընտրել Հիշվող Հարց և Պատասխան: Հիշվող պատասխանը կարող է անհրաժեշտ լինի մուտք անել համակարգին միանալիս, որպես ապահովության լրացուցիչ միջոց:

Ծածկագրով պաշտպանված սմարտ քարտ

Սա իրենից ներկայացնում է սմարտ քարտ, որը պարունակում է նախապես բեռնված թվային վկայագիր: Որոշակի ծառայություններից օգտվելու համար Օգտագործողները, ինչպես նկարագրված է ներոհիշյալ 2-րդ բաժնում, պետք է մուտք անեն իրենց սմարտ քարտը՝ հատուկ սմարտ քարտ ընթերցող սարքի մեջ և մուտք անեն լրացուցիչ ծածկագիրը:

Մուտքի Հսկման Ընթացակարգեր

Ծածկագրով պաշտպանված անվտանգության սարք

Սա ծածկագրով պաշտպանված սարք է, որը գեներացնում է միանգամյա 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):

Սմարտ քարտը և անվտանգության սարքը իրենցից ներկայացնում են երկաստիճան հավաստագրում, հավաստագրման մի ձև, որը պահանջում է, որ Օգտագործողը ոչ միայն իմանա ինչ-որ բան (սարքի գաղտնաբառը), այլ նաև ֆիզիկապես ունենա այն:

6. Անվտանգության նպատակով ձեռնարկվող միջոցներ

Դուք պատասխանատվություն եք կրում ձեր համակարգի և բանկի հետ ձեր հաղորդակցության համար, ուստի պետք է ձեռնարկեք հետևյալ քայլերը ձեզ պաշտպանելու համար, որոնք ընդգրկում են.

Մուտքի Հսկման Ընթացակարգեր

Անվտանգության միջոցներ

Օգտագործողները պետք է պահեն իրենց անվտանգության միջոցները (գաղտնաբառը, հիշարժան պատասխանը, անվտանգության պատասխանները, սմարտ 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, հիշարժան 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 հիշարժան պատասխանները որևէ համակարգչային ծրագրիում, որը կարող է ավտոմատ կերպով հիշողության մեջ պահել դրանք (օրինակ համակարգիչը կարող է առաջորկել «հիշել ծածակագիրը» կամ ունենալ դրան նման որևէ այլ գործառույթ),
- համոզվեք, որ համակարգ մուտք գործելիս ոչ մեկը 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 աշխատողներին: Դուք պետք է զգույշ լինեք, եթե ստանում եք որևէ գրություն, որտեղ ձեզ խնդրում են հայտնել ձեր ծածկագիրը կամ բանկային որևէ այլ տվյալ և կասկածներ ունենալու դեպքում անմիջապես կապվել բանկի հետ,
- եթե Դուք կասկած ունեք, որ Ձեր գաղտնաբառերը մասնակիորեն կամ ամբողջությամբ հայտնի են դարձել այլ անձանց, անմիջապես պաշտպանեք Ձեր հաշիվը գաղտնաբառերը փոխելու կամ հավիշը ժամանակավորապես դադրեցնել Ձեր հաշվի գործունեությունը մինչ այն պաշտպանվի: Նման կասկածներ ունենալու դեպքում Դուք նաև կարող եք դիտարկել Ձեր հաշվի վերջին գործարքները՝ ոչ լիազորված գործողությունները բացահայտելու նպատակով:

Մուտքի Հսկման Ընթացակարգեր

Անվտանգության սարքեր և սմարտ քարտեր

- Անվտանգության սարքերը (անհրաժեշտության դեպքում նաև դրանց ծածկագրերը) առաքվում են Ձեզ մատակարարման տարբեր ճանապարհներով: Եթե խելամիտ ժամանակահատվածում (սովորաբար 7 օր) Դուք չեք ստացել այդ փաթեթները, անմիջապես տեղեկացրեք էյչ-էս-Բի-Սի-ին այդ մասին:
- Այն դեպքերում, երբ անվտանգության նյութեր պարունակող փաթեթները չեն կարող առաքվել անմիջապես Ձեր ընկերության համապատասխան աշխատակցին (օրինակ, եթե փոստն ընդունում է համապատասխան բաժինը), Դուք եք պատասխանատու այն բանի համար, որ երրորդ կողմը հանձնի համապատասխան փաթեթն անմիջապես աշխատակցին:
- HSBC*net* ծառայություններից օգտվելու համար անվտանգության սարքի միջոցով նույնականացումից հետո բացվում է անվտանգ աշխատաշրջան, որը մնում է բաց մինչև Օգտագործողը դուրս չգա համակարգից: Հետևաբար չափազանց կարևոր է, որ համակարգչից հեռանալուց դուրս գաք համակարգից, նույնիսկ եթե այն ծառայությունը, որից օգտվել եք անվտանգության սարքի միջոցով, արդեն փակվել է ինքն իրեն:
- Չնայած, որ անվտանգության սարքերը պաշտպանված են ծածկագրերով, երբեք մի թողեք Ձեր անվտանգության սարքերն առանց հսկողության: Հետևեք, որ անվտանգության սարքերը պահվեն անվտանգ վայրում երբ դրանք չեն օգտագործվում:
- Երբեք մի տվեք Ձեր անվտանգության սարքը որևէ երրորդ անձի:
- Եթե Ձեր անվտանգության սարքը կորել կամ գողացվել է, անմիջապես տեղեկացրեք Բանկին այդ մասին կամ տետևեք այն ուղեցույցներին, որոնք սահմանված են անվտանգության սարքերի օգտագործման համար:

Մուտքի Հսկման Ընթացակարգեր

- Անվտանգության սարքերը պետք պահվեն ապահով տեղում: Խուսափեք՝
  - բարձր ջերմաստիճանից,
  - բարձր խոնավությունից,
  - արևի ուղիղ ճառագայթներից,
  - էլեկտրական հոսանքի սխալ լարվածությունից,
  - քայքայիչ կամ այլ քիմիական նյութերից,
  - ջրից, ժավելից, ալկոհոլից, և այլն:
- Մշտապես հետևեք ինտերնետ կայքում տեղակայված կամ էյչ-էս-Բի-Սի-ի կողմից հրատարակված օգտագործման և անվտանգության կանոններին:

Բանկն իրավունք է վերապահում ետ պահանջել անվտանգության սարքը, եթե կարծում է, որ այն օգտագործվում է ոչ իր նպատակով:

Մուտքի Հսկման Ընթացակարգեր

Թվային սերտիֆիկատի կառավարում

Սմարտ քարտի վրա պահվող թվային սերտիֆիկատները չպետք է ուղղարկվեն որևէ երրորդ կողմին կամ օգտագործվեն HSBC*net* մուտք գործելուց բացի այլ նպատակներով:

Համակարգի համատեղելիություն

Համակարգին մուտք գործելու համար պետք է համոզվեք, որ ձեր համակարգիչն ու ծրագրերը համատեղելի են միմյանց հետ: HSBC*net*-ի հաճախորդի ուղեցույցներում նկարագրված են մինիմալ տեխնիկական պահանջները:

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:
- Ստեղծել եք կամ հետևում եք համակարգային անվտանգության չափորոշիչները HSBC*net*-ի կողմից օգտագործվող տարրերի համար, հետևում եք ճանաչված չափորոշիչների և ուղեցույցների, ընդունում եք Բանկի կամ համակարգչային սարքավորումների և ծրագրային ապահովման մատակարարողների կողմից սահմանված կամ առաջարկած թարմացումների: 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 ներծուժումը 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):

Մուտքի Հսկման Ընթացակարգեր

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 վերաբերյալ:
- 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 պետք է կատարեք բանկի, ոստիկանության կամ այլ վերահսկող մարմինների կողմից ներկայացված բոլոր պահանջները՝ ողջամտության սահմաններում, անվտանգության փաստացի կամ պոտենցիալ խախտումները հայտնաբերելու համար:

Ֆայլերի վերբեռնում (upload)

Հաճախորդի հանձնարարականներ պարունակող ֆայլը Բանկին առաքելու նպատակով դուք պետք է, որոշակի ֆայլը որոշակի տեղից ընտրելուց առաջ, լրացնեք համապատասխան ֆայլերի վերբեռնման գործիքով (file upload tool) պահանջվող տեղեկությունները, որոնք ընդգրկում են ֆայլի տեսակը, ֆորմատը, անհրաժեշտ լիազորման աստիճանը և երկիրը (անհրաժեշտության դեպքում): Հենց որ դուք սեղմեցիք «Go» կոճակը և Բանկը ստացավ համապատասխան ֆայլը, ձեր էկրանին կհայտնվի Բանկի կողմից ուղարկված հաստատում առ այն, որ բանկը ստացել է ամապատասխան ֆայլը: Այնուհետև ֆայլի ճանաչման հաստատում տալուց առաջ Բանկը պետք է կատարի նույնականացման որոշակի գործընթաց, որը պետք է գնահատվի Report and File Download գործառույթի միջոցով:

Մուտքի Հսկման Ընթացակարգեր

Դուք պետք է տեղյակ պահեք Բանկին ֆայլի ճանաչման հաստատման ստանալու մասին, եթե ձեր կողմից որևէ ֆայլ չի ուղարկվել, կամ եթե 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 դուք ձեռնարկեք համապատասխան միջոցներ բացառելու ֆայլի հետ կատարվող որևէ գործողություն՝ մինչև դրա ուղղարկելը:

- Ֆայլը պետք է պահվի ապահով տեղում՝ սահմանափակելով դրա հասանելիությունը
- Ֆայլը պետք է պատրաստվի լիազորված կերպով և ուղարկվի HSBC*net* Համակարգ
- Ֆայլի բոլոր օգտագործումները պետք է գրանցվեն ապահով կերպով՝ անհրաժեշտության դեպքում քննություն անցկացնելու համար

Կարևոր է, որ բոլոր իրադրություններում, բայց մասնավորապես Բանկին նախապես լիազորված Հաճախորդի Հանձնարարականի ֆայլեր ուղարկելիս, պահպանվեն վերոհիշյալ կանոնները: Այս Մուտքի Հսկման Ընթացակարգերի որևէ դրույթ չի սահմանափակում HSBC*net*-ի Հաճախորդի պայմանագրի 3-րդ կետի պայմանները և մասնավորապես ձեր պարտականությունը երաշխավորելու, որ Հաճախորդի Հանձնարարականները պատշաճ կերպով ուղարկվում են բանկին:

7. Առաջացած խնդիրների լուծում

Ծառայությունների առկայությունը/մատչելիություն

Սովորաբար Ծառայություններից կարելի է օգտվել ցանկացած ժամանակ, սակայն լինում են դեպքեր, երբ մենք մեր հայեցողությամբ կարող ենք դադարեցնել Ծառայությունների տրամադրումը կամ Համակարգի առկայությունը ամբողջությամբ կամ մասամբ:

Ի նկատի ունեցեք, որ կատարվող գործարքը միշտ չէ, որ տեղի են ունենում հանձնարարականի տրման հետ միաժամանակ: Որոշ գործարքներ կատարելու համար կարող է ժամանակ պահանջվել և որոշ հանձնարարականներ կարող են կատարման ներկայացվել/կատարվել միայն սովորական բանկային ժամերի ընթացքում, չնայած որ Ծառայությունները կարող են մատչելի լինել այդ ժամերից դուրս ևս:

Տեխնիկական աջակցություն

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

- Օժանդակության տեքստ

  Համակարգի վրա կարելի է գտնել օժանդակության տեքստ, որը Օգտագործողի համար կարող է օգտակար լինել սովորական տեխնիկական հարցերը լուծելիս:
- Համակարգի ադմինիստրատորի օժանդակությունը

  HSBC*net*-ի հետ կապված խնդիրների մեծ մասի դեպքում Օգտագործողները պետք է կապվեն իրենց Համակարգի ադմինիստրատորների հետ: Համակարգի Ադմինիստրատորներն ունեն բազմաթիվ լիազորություններ՝ ներառյալ ծածկագրերի փոխումը:

Մուտքի Հսկման Ընթացակարգեր

- Աջակցություն հեռախոսակապի միջոցով

  Եթե կան հարցեր, որոնք չեն կարող լուծվել Համակարգի Ադմինիստատորների կողմից, ապա Օգտագործողենը կարող են ստանալ աջակցություն հեռախոսակապի միջոցով: Էյչ-Էս-Բի-Սի-ի հայեցողությամբ Օգտագործողներից, աշխատողներից կարող է պահանջվել հաստատել իրենց ինքությունը:

- Բանկի Աջակցությունը

  Եթե Հաճախորդը չի կարող օգտագործել համակարգը, Հաճախորդները պետք է կապվեն համապատասխան լիազոր աշխատակիցների հետ: Բանկը կարող է պահանջել, որպեսզի Օգտագործողը հաստատի իր ինքնությունը վերը նկարագրված կարգով:

- 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 չի նախատեսված այնպիսի դեպքերի համար, երբ լուրջ մտահոգություններ կան Օգտագործողի վարքագծի հետ կապված: Տվյալ դեպքում Համակարգի Ադմինիստրատորները կարող են անմիջապես ջնջել Օգտագործողին համակարգից և չեղյալ համարել տվյալ Օգտագործողի սմարտ քարտը (եթե առկա է): Եթե կասեցումը միակ հնարավոր տարբերակն է (օրինակ, եթե անհրաժեշտ է անհապաղ արգելափակել Օգտագործողին և որևէ այլ Համակարգի ադմինիստրատոր չկա, որը կկարողանա հաստատի այդ արգելափակումը), ապա այն պետք է օգտագործվի՝ այլ պաշտպանական միջոցների հետ մեկտեղ, ինչպիսիք են օրինակ Օգտագործողի սմարտ 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: