ՔԱՂԱՔԱԿԱՆՈՒԹՅՈՒՆ
ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ

Կոդ POL14-0001-17 PUB		Խմբագրություն 08
Կազմեց	Հավանության արժանացավ	Հաստատված
Բիզնես գործընթացների կառավարման բաժին	Վարչության 29/10/2024թ. թիվ 40 արձանագրություն Վարչության նախագահ՝ Կարեն Եղիազարյան_____	Խորհրդի 27/11/2024թ. թիվ 13 արձանագրությամբ Խորհրդի նախագահ՝ Խոսե Մարիա Մորենո Դե Բարրեդա _____

Կիրառման ոլորտ	Բանկի կառավարման բոլոր մարմիններ, ղեկավարներ, կառուցվածքային և տարածքային ստորաբաժանումներ, ինչպես նաև Բանկին ծառայություն մատուցող Երրորդ անձինք
Վերանայման համար պատասխանատու ստորաբաժանում	Տեղեկատվական անվտանգության բաժին
Ուժի մեջ մտնելու ամսաթիվ	06/12/2024թ.
Ուժը կորցնելու ամսաթիվ	

1. Նպատակը

Սույն քաղաքականության նպատակն է սահմանել Բանկի Տեղեկատվական անվտանգության սկզբունքները, ոլորտի նպատակները, խնդիրները և մոտեցումները, որոնցով Բանկը ղեկավարվում է իր գործունեության ընթացքում:

2. Սահմանումներ և հապավումներ

- **Բանկ** – «ԷՎՈԿԱԲԱՆԿ» ՓԲԸ:
- **Քաղաքականություն** – Տեղեկատվական անվտանգության քաղաքականություն:
- **Տեղեկատվական անվտանգություն** – Բանկին պատկանող տեղեկատվությունը չթույլատրված մուտքից, օգտագործումից, հրապարակումից, խեղաթյուրումից, փոփոխումից կամ ոչնչացումից պահպանում/պաշտպանություն:
- **ՏԱԿՀ** – Բանկի Տեղեկատվական անվտանգության կառավարման համակարգ, որը նկարագրվում է հետևյալ կերպ. Պաշտպանել Բանկի համար կարևոր նշանակություն ունեցող տեղեկատվական ռեսուրսները և Բանկի ներքին իրավական ակտերով սահմանված գաղտնիք պարունակող տեղեկատվությունը, բացառել այդ տեղեկատվության տարածումը: Իրականացնել և իրագործել տեղեկատվական ռեսուրսների և տեղեկատվության գաղտնիությունը, ամբողջականությունը, հասանելիությունը:
- **Տեղեկատվական ակտիվ** – Բանկի համար արժեք ունեցող՝ տվյալներ պարունակող տեղեկատվություն, որը գտնվում է Բանկի տիրապետության տակ և համարվում է Բանկի սեփականությունը:
- **Երրորդ անձ** – Բանկին ժամանակավոր և/կամ անժամկետ պայմանագրային հիմունքներով ծառայություններ մատուցող ընկերություն կամ անձ, որը որևէ կերպ առնչվում է, կարող է առնչվել կամ հասանելիության իրավասություններ ձեռք բերել Բանկի կողմից դասակարգված տեղեկատվությանը:
- **Խախտող** – անձ, որը սխալմամբ, չհմացությամբ կամ գիտակցաբար՝ օգտագործելով դրա համար տարբեր հնարավորություններ, մեթոդներ և միջոցներ, փորձում է կատարել արգելված գործողություններ:
- **ԱԲՀ** – Ավտոմատացված բանկային համակարգ:
- **Համակարգչային ցանց** – Բանկի միասնական տեղեկատվական համակարգի մի մաս, որի գործունեությունը պահանջում է կազմակերպչական և տեխնիկական միջոցառումների իրականացում՝ օգտագործողների և աջակցող անձնակազմի խիստ կարգապահությամբ:
- **Համակարգի ադմինիստրատոր** – SS բաժնի աշխատակից, որի վրա համաձայն Բանկի ներքին իրավական ակտերի դրված է նման պարտականություն:
- **Արտաքին տեղեկատվական համակարգեր –** Բանկի այն համակարգերը, որոնք ներգրավված չեն Բանկի համակարգչային (գլոբալ և լոկալ) ցանցերի մեջ:

3. Ընդհանուր դրույթներ

3.1. Բանկի նպատակը տեղեկատվական անվտանգության ոլորտում հետևյալն է՝
- Ապահովել Բանկի համար Տեղեկատվական ակտիվ հանդիսացող տեղեկատվության գաղտնիությունը, հասանելիությունը, ամբողջականությունը,
- Տեղեկատվական անվտանգության ապահովման միջոցով բարելավել Բանկի գործարար համբավը և կորպորատիվ մշակույթը,
- Ձեռնարկել համապատասխան միջոցառումներ Տեղեկատվական անվտանգության սպառնալիքներից պաշտպանվելու համար,
- Տեղեկատվական անվտանգության հնարավոր սպառնալիքներից կանխարգելում, հնարավոր վնասի նվազեցում,
- Աշխատակիցների շրջանում իրազեկության բարձրացում, ուսուցում:

3.2. Տեղեկատվությունը Բանկի համար հանդիսանում է կարևոր ակտիվ, այդ իսկ պատճառով Բանկը ֆինանսական գործառնությունների իրականացման հետ մեկտեղ իրականացնում է տեղեկատվության կառավարում (Տեղեկատվական ակտիվների գաղտնիության, ամբողջականության և հասանելիության ապահովում):

3.3. Յուրաքանչյուր տեղեկատվական ակտիվ պետք է օգտագործվի նպատակային (զուտ աշխատանքային անհրաժեշտությունից ելնելով):

3.4. Քաղաքականության նպատակաուղղվածությունը հետևյալն է՝
- Բանկի գործարար գործընթացների անընդհատության ապահովում,
- հասցնել նվազագույնի Տեղեկատվական անվտանգության ոլորտի հնարավոր կորուստները և վնասները:

3.5. Բանկի ՏԱԿՀ պահպանման հիմնական օբյեկտներ են հանդիսանում՝

- **Տեղեկատվական ռեսուրսները** - տվյալների բազաները և ֆայլերը, համակարգերի նկարագրման փաստաթղթերը, օգտագործողի փաստաթղթերը, ուսումնական նյութերը, բիզնեսի անընդհատության պահպանման պլանները, դրանց պատճենները և այլն:
- **Ծրագրային ռեսուրսները** - օպերացիոն համակարգերը, կիրառական/ծրագրային համակարգերը, ներքին մշակման ծրագրային ապահովման միջոցները և այլ ծրագրային միջոցները, որոնք նախատեսված են կրկնօրինակման, մշակման, պահպանման և տեղեկատվության փոխանցման համար:
- **Սարքավորումները** - համակարգչային տեխնիկան (պրոցեսորներ, մոնիտորներ, փոխադրելի համակարգիչներ), կոմունիկացիոն սարքավորումները (հեռախոսային կայաններ, մարշրուտիզատորներ, ֆաքսեր, ինքնապատասխանիչներ, մոդեմներ), մագնիսական և արտաքին այլ կրիչները (CD, DVD, մագնիսական ժապավեններ, ֆլեշ կրիչներ, հիշողության քարտեր), այլ տեխնիկական սարքավորումները (հոսանքի աղբյուրներ, օդամղիչներ և այլն):
- **Մարդկային ռեսուրսները** - Բանկի կառուցվածքային և տարածքային ստորաբաժանումների աշխատակիցները և Բանկին ծառայություն մատուցող Երրորդ անձիք:

3.6. Բանկի Տեղեկատվական անվտանգության քաղաքականությունը պետք է վերանայվի առնվազն 3 տարին մեկ անգամ, ինչպես նաև հետևյալ դեպքերում՝

- Տեղեկատվական անվտանգության քաղաքականությունը հաստատած անձի փոփոխության կամ վերջինիս իրավասությունների փոփոխության դեպքում,
- Տեղեկատվական անվտանգության վրա մեծ ազդեցություն ունեցող պատահարների դեպքում,
- նոր խոցելիությունների հայտնաբերման դեպքում,
- Բանկի տեղեկատվական ենթակառուցվածքների փոփոխությունների դեպքում:

3.7. Քաղաքականությունը կարող է փոփոխության ենթարկվել նաև հետևյալ չափանիշների գնահատման կամ վերագնահատման արդյունքում՝

- Քաղաքականության արդյունավետության (կախված Տեղեկատվական անվտանգության պատահարների քանակից և Տեղեկատվական անվտանգության վրա ազդեցության չափից),
- Բանկի կազմակերպական կառուցվածքի էական փոփոխության դեպքում,
- Բանկի գործունեության արդյունավետության վրա հակազդեցության դեպքում,
- տեխնոլոգիական փոփոխության դեպքում:

4. Տեղեկատվական անվտանգության կառավարում

4.1. Բանկի Տեղեկատվական անվտանգության ապահովումը իրականացվում է ՀՀ ԿԲ կողմից սահմանված և ISO27001 միջազգային ստանդարտների պահանջներին համապատասխան:

4.2. Բանկում ներդրվում է ՏԱԿՀ, որի գործունեությունը կարգավորվորելու նպատակով մշակվում են համապատասխան ներքին իրավական ակտեր (ներքին իրավական ակտերի մշակման գործընթացը սահմանվում է Բանկում գործող «Ներքին իրավական ակտերի մասին» կարգով (PRD14-0001-09)), որոնք հասանելի են Բանկի բոլոր աշխատակիցներին և որոնց պահանջները ենթակա են պարտադիր կատարման:

4.3. Բանկում ՏԱԿՀ համար պատասխանատու ստորաբաժանում է համարվում Տեղեկատվական անվտանգության բաժինը:

4.4. Բանկի բոլոր Տեղեկատվական ակտիվները ենթակա են գույքագրման, հաշվառման և դասակարգման՝ յուրաքանչյուրը իր կարևորության և հասանելիության աստիճանի:

4.5. Բանկում իրականացվում է Տեղեկատվական անվտանգության պարբերաբար գնահատում և ռիսկերի վերլուծություն, որի համար մշակվում են Տեղեկատվական անվտանգության ռիսկերի կառավարման ներքին իրավական ակտեր:

4.6. Ռիսկերի գնահատման մեթոդոլոգիան կիրառում է գաղտնիության, ամբողջականության և հասանելիության, սպառնալիքի և խոցելիության վտանգի գնահատման մոտեցումը: Գնահատումը իրականացնելիս հաշվի է առնվում Տեղեկատվական անվտանգության ռիսկերի հավանականությունը և դրա ազդեցությունը Բանկի բիզնես գործընթացների, ֆինանսական վիճակի և բարի համբավի վրա:

4.7. Բանկի ներքին իրավական ակտերով սահմանվում են Տեղեկատվական անվտանգության սպառնալիքների և խոցելիության բնորոշ ցանկեր:

4.8. Տեղեկատվական անվտանգության ռիսկերի գնահատման արդյունքների հիման վրա ձեռնարկվում են միջոցառումներ տեղեկատվության պահպանման արդյունավետ կառավարում իրականացնելու ուղղությամբ, այդ թվում՝ կազմակերպչական, ֆիզիկական, տեխնիկական, ծրագրային և այլն:

4.9. Տեղեկատվական ակտիվների ֆիզիկական անվտանգության համար Բանկն իր գործունեության վայրերում (գլխամասային գրասենյակ և մասնաճյուղեր) ներդնում է անվտանգության գոտիներ՝

հաստատված Բանկի Վարչության կողմից, և ձեռնարկվում է համապատասխան միջոցառումներ չարտոնագրված մուտքերը կանխելու ուղղությամբ:

4.10. Բանկը Տեղեկատվական անվտանգության ոլորտում գործող իրավական ակտերի համապատասխան պետք է ցանկացած պատահար բացահայտի, քննարկի, արձագանքի և կառավարի դրանք:

4.11. Բանկում ներդրվում է ուղղիչ և կանխարգելիչ գործողությունների իրականացման ընթացակարգ:

4.12. Բանկում իրականացվում է տեղեկատվական ռեսուրսների և տեխնիկածրագրային համակարգերի կառավարում, տեղեկատվության մշակման, փոխանցման և տրամադրման վերաբերյալ:

4.13. Բանկում ներդրվում են արտակարգ իրավիճակներում գործունեության անընդհատության ապահովման և արտակարգ իրավիճակներում Տեղեկատվական ակտիվների տարահանման գործընթացները նկարագրող ներքին իրավական ակտեր:

4.14. Բանկի աշխատակիցներին տրվում է իրավասություն միայն այն տեղեկատվություններին, որոնք անհրաժեշտ են իրենց աշխատանքային պարտականությունների կատարման համար:

4.15. Բանկում ցանկացած նախագծի իրականացման և դրա կառավարման ընթացքում պետք է կիրառվեն Բանկում գործող Տեղատվական ավտանգության պահանջները:

4.16. Բանկի և բոլոր տեղեկատվական համակարգերի համար օրենսդրական, նորմատիվ, պայմանագրային պահանջները պետք է լինեն հստակ որոշված, փաստաթղթավորված և գտնվեն արդիական վիճակում:

4.17. Բանկում ներդրվում են տեղեկատվական անվտանգության ոլորտում կիրառվող առաջադեմ և արդիական ծրագրեր, սարքավորումներ և տեխնիկական լուծումներ:

4.18. Բանկի ներքին իրավական ակտերով սահմանվում են աշխատակիցների կողմից Տեղեկատվական անվտանգության պահանջների չկատարման դեպքում նրանց պատասխանատվության ենթարկելու ընթացակարգեր:

4.19. Բանկն անձնակազմ ընտրելիս իրականացնում է վստահելիության ստուգման գործընթաց, որը սահմանվում է Բանկի ներքին իրավական ակտերով:

4.20. Բանկը իրականացնում է Տեղեկատվական անվտանգության ոլորտին՝ աշխատակիցների տեղեկացվածություն, վերապատրաստում և հմտությունների բարձրացում:

4.21. Բանկում ստեղծվում է Տեղեկատվական անվտանգության կոմիտե, որի գործունեությունը կարգավորվում է կոմիտեի կանոնակարգով:

4.22. Բանկում յուրաքանչյուր ստորաբաժանման ղեկավար իր պատասխանատվության շրջանակներում պարբերաբար վերանայում է տեղեկատվության մշակման և ընթացակարգերի համապատասխանությունը սույն Քաղաքականության, սահմանված ստանդարտների և Տեղեկատվական անվտանգության այլ պահանջներին: Իրականացված վերանայումների գծով կազմվում են հաշվետվություններ:

4.23. Բանկի տեղեկատվական համակարգերը պարբերաբար վերանայվում են սույն Քաղաքականության, սահամանված ստանդարտների և Տեղեկատվական անվտանգության այլ պահանջներին համապատասխան: Իրականացված վերանայումների գծով կազմվում են հաշվետվություններ:

4.24. Բանկում կիրառվող ծրագրային կոդերի պահպանման համար պետք է կիրառվեն անվտանգ համակարգեր: Ծրագրային կոդերին իրավասությունները տրամադրվում են միայն աշխատակցի կողմից իր աշխատանքային պարտականությունները կատարելու նպատակով: Ծրագրային կոդերին իրավասություն ունեցող Բանկի աշխատակիցների աշխատանքային պայմանագրերով սահմանվում են աշխատանքային պայմանագիրը լուծվելու դեպքում Բանկի ծրագրային կոդերը չհրապարակելու վերաբերյալ դրույթներ, ինչպես նաև աշխատանքային պայմանագիրը լուծվելուց նվազագույնը 6 ամսվա ընթացքում տվյալ աշխատակցի կողմից գրված ծրագրային կոդերում թաքնված թերություններ հայտնաբերելու դեպքում, այդ թերությունները վերացնելու վերաբերյալ դրույթներ: Ծրագրային կոդերի անվտանգ պահպանման համար պատասխանատու է Ծրագրավորման բաժնի պետը:

5. Երրորդ անձանց հետ հարաբերություններ

5.1. Երրորդ անձանց հետ Բանկը կնքում է գաղտնիության պահպանման վերաբերյալ պայմանագիր:

5.2. Պայմանագրով պետք է սահմանվի մատուցվող ծառայությունների որակի մակարդակը, այդ թվում հստակ սահմանվում է մատուցվող ծառայության ձախողման դեպքում արձագանքման հստակ ժամկետը:

5.3. Երրորդ անձանց հետ կնքված պայմանագիրը կարող է խզվել, եթե ծառայություն մատուցող Երրորդ անձը չի կատարում կամ խախտում է Բանկում գործող Տեղեկատվական անվտանգության պահանջները:

6. ՏԱԿՀ շահագրգիռ կողմեր

6.1. ՏԱԿՀ շահագրգիռ կողմեր կարող են հանդիսանալ Բանկի բաժնետերերը, Բանկի կառավարման մարմինները, աշխատակիցները, Բանկի գործընկերները, Բանկի հաճախորդները, մատակարարները, Երրորդ անձինք և այլն:

6.2. **Շահագրգիռ կողմերի պահանջները և ակնկալիքները**

6.2.1. Բանկը սահմանում է ՏԱԿՀ հետ կապ ունեցող շահագրգիռ կողմերին, ինչպես նաև, ՏԱԿՀ համար պատասխանատու ստորաբաժանմանը ներկայացվող՝ շահագրգիռ կողմերի կողմից ներկայացվող պահանջները: Շահագրգիռ կողմերի կողմից ներկայացվող պահանջները կարող են իրենց մեջ ներառել.

1) Օրենսդրական, կարգավորիչ և պայմանագրային պարտավորություններ,
2) Սահմանված պահանջների համապատասխանելիություն, հուսալիություն,
3) Ապահովել տեղեկատվության ամբողջականությունը, հասանելիությունը և գաղտնիությունը,
4) Տեղեկատվական ակտիվների խնամքով օգտագործելու պահանջ,
5) Տեղեկատվական անվտանգության կանոնների պահպանման պահանջ,
6) Ակտիվների դասակարգում, ռիսկերի գնահատում,
7) Տեղեկատվական պատահարների կառավարում,
8) Փոփոխությունների կառավարում,
9) Անվտանգության մշտադիտարկում,
10) Ծրագրային ապահովում և համակարգերի մշակում

7. Տեղեկատվական անվտանգության ռիսկերի կառավարում

7.1. Տեղեկատվական անվտանգության պոտենցիալ ռիսկերը ըստ առաջացման բնույթի բաժանվում են հետևյալ տեսակների.

7.1.1. **Անթրոպոգեն.** Կարող է առաջանալ Տեղեկատվական անվտանգության ոչ կայուն կառավարման հետ կապված մարդկային գործոնի ազդեցությամբ, այն կարող է առաջանալ ոչ դիտավորյալ գործողություններով (տեղեկատվական համակարգի կամ դրա տարրերի սխալ նախագծում, սխալներ անձնակազմի գործողություններում և այլն) և դիտավորյալ գործողություններով (շահադիտական, մտածված կամ այլ նպատակների հետապնդում):

7.1.2. **Տեխնածին.** ՏԱԿՀ խափանումը կամ ոչնչացումը, որը կարող է պայմանավորված լինել սպառնալիքի օբյեկտի վրա տեխնածին բնույթի օբյեկտիվ ֆիզիկական գործընթացների ազդեցությամբ:

7.1.3. **Բնական.** Օդերևութաբանական, մթնոլորտային, երկրաֆիզիկական, գեոմագնիսական և այլն, այդ թվում ծայրահեղ կլիմայական պայմանները, եղանակային իրադարձությունները, բնական աղետները և այլն: Վերջինիս առաջացումը պայմանավորված է սպառնալիքի օբյեկտի վրա բնական բնույթի օբյեկտիվ ֆիզիկական գործընթացների ազդեցությամբ, աղետալի բնական երևույթների, որը ուղակիորեն պայմանավորված չէ մարդկային գործոնի հետ:

7.2. Բանկի համար նշանակալից են համարվում հետևյալ խմբերի ռիսկերի տեսակները՝

1) Գաղտնիության խախտում (գաղտնի տեղեկատվության հրապարակում, արտահոսք և այլն),
2) աշխատունակության խախտում (գործարար գործընթացների ապակազմակերպում),
3) ամբողջականության խախտում (տեղեկատվության խեղաթյուրում, փոփոխում, հափշտակում, ոչնչացում և այլն),
4) տեղեկատվության հասանելիության խախտում:

7.3. Տեղեկատվական անվտանգության ռիսկերի գնահատման և վերլուծության գործընթացում Տեղեկատվական անվտանգության ռիսկերի հնարավոր աղբյուրները դասակարգվում են ըստ ներքին և արտաքին ռիսկերի, ինչպես նաև նկարագրվում է խախտողի մոդելը:

7.4. Տեղեկատվական անվտանգության ռիսկերի կառավարման նպատակով Բանկում իրականացվում է հետևալ միջոցառումները

7.4.1. **Ներքին ներթափանցման թեստ (Internal network penetration testing)՝** միջոցառումների ամբողջություն, որն ուղղված է ստուգելու Բանկի ներքին տեղեկատվական ցանցի պաշտպանվածությունը ներքին ռիսկերից:

7.4.2. **Արտաքին ներթափանցման թեստ (External network penetration testing)՝** միջոցառումների ամբողջություն, որն ուղղված է ստուգելու Բանկի ներքին տեղեկատվական ցանցի պաշտպանվածությունը արտաքին ռիսկերից:

7.4.3. **Սոցիալական ինժինիրինգ (Social engineering)՝** ներքին տեղեկատվական ցանցի լիազորված օգտագործողին մոլորեցնելու ճանապարհով գաղտնի տեղեկատվության ձեռքբերում:

7.4.4. **Բարձր վտանգ պարունակող կայուն սպառնալիք (Advanced persistent threat - APT)՝** ցանցային գրոհ, որի ժամանակ չլիազորված անձը ձեռք է բերում հասանելիություն Բանկի ներքին տեղեկատվական ցանցին և որոշակի ժամանակ մնում է չհայտնաբերված:

7.4.5. **Բարձր վտանգ պարունակող կայուն սպառնալիքի թեստ (Advanced persistent threat test – APT, Red-teaming)՝** առկա բոլոր պաշտպանական միջոցների (այդ թվում՝ կազմակերպչական)

արդյունավետությունը ստուգելու նպատակով իրականացվող արտոնված գրոհ:

7.4.6. **Բարձր վտանգ պարունակող կայուն սպառնալիքի առկայության թեստ (APT hunting exercise)՝** մինչև մեկ շաբաթ տևողությամբ առավել կրիտիկական սերվերների և աշխատակայանների ուղղությամբ ցանցային հոսքի վերլուծության միջոցով Բանկի ենթակառուցվածքում արդեն իսկ հաջողված բարձր վտանգ պարունակող կայուն սպառնալիքի գրոհի դրսևորման բացահայտում:

7.4.7. **Ներքին տեղեկատվական ցանցի խոցելիության սքանավորում (զննում)՝** խոցելիության զննիչների կիրառմամբ կատարվող սերվերների, աշխատակայանների, ցանցային սարքավորումների, ինչպես նաև ներքին տեղեկատվական ցանցի այլ ակտիվների ծրագրային և (կամ) տեխնիկական ապահովման մեջ չարտոնված մուտքի պոտենցիալ հնարավորություն ընձեռող անվտանգության բացերի հայտնաբերում:

7.4.8. **Խոցելիության զննիչ՝** ծրագրային և (կամ) տեխնիկական ապահովման խոցելիությունների հայտնաբերման հատուկ համակարգի կիրառում:

8. Մտավոր սեփականության և հեղինակային իրավունքներ

8.1. Բանկում մտավոր սեփականության, արտոնագրային հարաբերությունների, լիցենզավորման, հեղինակային իրավունքների հետ կապված հարաբերությունները կարգավորվում են ՀՀ օրենսդրությամբ և այլ իրավական ակտերով մասնավորապես՝ ՀՀ Սահմանադրությամբ, ՀՀ քաղաքացիական օրենսգրքով, ՀՀ Կենտրոնական բանկի 2012թ. նոյեմբերի 13-ի 309-Ն որոշմամբ, որով կարգավորվում են ՀՀ ԿԲ կողմից գրանցվող բանկերի ֆիրմային անվանումների գրանցման և փոփոխությունների կարգը, «Հեղինակային իրավունքների և հարակից իրավունքների մասին» ՀՀ օրենքով, «Ֆիրմային անվանումների մասին» ՀՀ օրենքով, «Լիցենզավորման մասին» ՀՀ օրենքով, 20.07.1999թ. ուժի մեջ մտած մտավոր սեփականության բնագավառում իրավախախտումները կանխելու նպատակով համագործակցության մասին միջազգային համաձայնագրով:

8.2. Բանկը ձեռք է բերում ծրագրեր միայն ճանաչված և լիցենզավորված աղբյուրներից՝ ապահովելով հեղինակային իրավունքի պաշտպանությունը: Նաև իրականացնում է աշխատակազմի վերապատրաստումը և զգոնությունը: Բանկի աշխատակիցները ծանոթ են կարգապահական և այլ կանոններին, պարբերաբար ներքին հսկողություն է իրականացվում չլիցենզավորված ծրագրերը բացահայտելու և սահմանված օգտատերերի քանակը չգերազանցելու ուղղությամբ:

9. Անվտանգության համակարգի ապահովման քաղաքականություն

9.1. Բանկի անվտանգության ապահովումը հանդիսանում է նրա գործունեության անբաժանելի մասը:

9.2. Բանկի անվտանգության ապահովումը՝ Բանկի նյութական արժեքների և տեղեկատվական ռեսուրսների պաշտպանվածությունն է ներքին և արտաքին սպառնալիքներից:

9.3. Բանկի անվտանգության ապահովման օբյեկտներն են հանդիսանում՝

1) ֆինանսական միջոցները և նյութական արժեքները;
2) տեղեկատվական ակտիվները;
3) Բանկի անձնակազմը, Բանկի տարածքում գտնվող հաճախորդները;
4) Բանկի գործունեության շենքերը և շինությունները:

9.4. Անվտանգության համակարգի նպատակն է՝ կոորդինացնել և կենտրոնացնել անվտանգության ապահովման ուղղությամբ Բանկում իրականացվող բոլոր աշխատանքները, ապահովել Բանկի հուսալի և անվտանգ գործունեությունը և պաշտպանվածությունը:

9.5. Բանկի անվտանգության ապահովումը պետք է ապահովի Բանկի հետևյալ խնդիրների լուծումը.

1) պահվող դրամական և նյութական արժեքների պաշտպանության ապահովում;
2) Բանկի աշխատակիցների անվտանգության ապահովում Բանկի տարածքում;
3) Բանկի շենքի, շինությունների և տարածքի պատշաճ պաշտպանվածության ապահովում;
4) Բանկի տեղեկատվական ակտիվների անվտանգության ապահովում:

9.6. **Անվտանգության համակարգի կառուցվածքը**

9.6.1. Բանկի Անվտանգության համակարգն իր գործունեության ընթացքում հիմնվում է հետևյալ սկզբունքների վրա՝

1) անվտանգության վիճակի համալիր գնահատում, հնարավոր սպառնալիքների համակարգային վերլուծություն և վտանգների կանխատեսում;
2) անվտանգության կենսականորեն կարևոր գոտիների որոշում, պաշտպանական միջոցների և միջոցառումների մշակում;
3) պաշտպանության միջոցառումների և միջոցների ընտրություն և ներդրում;
4) պաշտպանության մեխանիզմների անընդհատության ապահովում;

5) անվտանգության ապահովման հարցում Բանկի բոլոր ստորաբաժանումների մասնակցություն (իրենց վերապահված խնդիրների շրջանակում);
6) անվտանգության համակարգի աստիճանաբար զարգացում:

9.6.2. Բանկի անվտանգության համակարգի ապահովման նպատակով իրականացվում է՝
1) Բանկի տարածքի (Գլխամասային գրասենյակ և մասնաճյուղեր) գոտիավորում, ըստ հասանելիությունների՝ հաստատված Բանկի Վարչության կողմից, որտեղ պետք է հստակ տարրանջատվի մուտքերի իրավասությունները;
2) խոցելի տեղամասերի պաշտպանություն և վերահսկողություն;
3) հայտնաբերման, հեռուստադիտարկման և պաշտպանական միջոցների ու համակարգերի տեղադրում պաշտպանվող գոտիներում;
4) նորմալ և արտակարգ իրավիճակներում պաշտպանական համակարգերի աշխատանքային գործունեության ապահովում:

9.6.3. Պաշտպանական միջոցների անվտանգության աստիճանը պետք է աճի Բանկի հասանելի գոտիներից դեպի սահմանափակ հասանելիությամբ գոտիներ:

9.6.4. Պաշտպանական միջոցառումները չպետք է էական դժվարություններ առաջացնեն Բանկի ամենօրյա գործունեությանը և պետք է լինեն առավելագույնս անտեսանելի:

9.7. **Անվտանգության համակարգի սպառնալիքները**

9.7.1. Բանկի գործունեությանը վտանգող հնարավոր սպառնալիքները դասակարգվում են՝ որպես ներքին և արտաքին:

9.7.2. **Ներքին սպառնալիքները հետևյալն են՝**
1) գաղտնի տեղեկատվության բացահայտում (երրորդ անձանց /ոչ թույլատրելի/ տեղեկատվության ոչ թույլատրված տրամադրում, փոփոխում կամ ոչնչացում);
2) կեղծ և սխալ փաստաթղթերի կազմում;
3) տեղեկատվության ոչ դիտավորյալ փոփոխում կամ ոչնչացում;
4) ներթափանցելու անթույլատրելի փորձերի իրագործում;
5) համակարգում օգտագործողների արտոնությունների անթույլատրելի վերաբախշում;
6) տեղեկատվության կորուստ կամ թերի հասցնում (հասցեատիրոջը);
7) տրամադրվող ծառայությունների նվազում կամ մերժում;
8) տեղեկատվությունից հրաժարվում;
9) տեղեկատվական համակարգերում կամ համակարգչային ցանցում սխալ/կեղծ փաստաթղթերի բարձր ինտենսիվության տեղեկատվական հոսքերի ներմուծում;
10) պաշտպանական տեխնիկական համակարգերի աշխատանքներին ոչ թույլատրված միջամտում;
11) համակարգչային վիրուսների տարածում;
12) խոցելի տեղամասերում աշխատանքների տարանջատման սկզբունքի խախտում, աշխատակցի փոխարինելիության բացակայություն;
13) ծրագրային ապահովման ոչ արտոնված փոփոխում և այլն:

9.7.3. **Արտաքին սպառնալիքները հետևյալն են՝**
1) արտակարգ իրավիճակներ (հրդեհ, տարերային աղետներ, պատերազմական գործողություններ);
2) տարածքի ապօրինի ներխուժում (հարձակում, կողոպուտ);
3) համակարգչային հանցագործություններ (վնասարար ծրագրեր, կեղծ էլեկտրոնային վճարագրեր, չարտոնված միջամտություն և կեղծիքներ);
4) չհրահանգավորված ձայնագրում, նկարահանում, պատճենահանում:

9.7.4. Բանկին սպառնացող վտանգներից խուսափելու և դրանց հետևանքով առաջացող վնասները նվազեցնելու համար՝ կարող են կիրառվել անվտանգության ապահովման հետևյալ ծրագրատեխնիկական միջոցները.
1) ձայնագրող սարքերի հայտնաբերման միջոցներ;
2) հարձակման հետ մղման միջոցներ;
3) պայթուցիկ սարքերի բլոկավորման միջոցներ;
4) համակարգիչների հատուկ ստուգման միջոցներ;
5) տեղեկատվության պաշտպանության ծրագրաապարատային միջոցներ և այլն:

9.7.5. Թղթային փաստաթղթերի պաշտպանության սպառնալիքներից խուսափելու, նրանց պահպանությունը ապահովելու և վտանգները նվազեցնելու համար՝ անհրաժեշտ է.
1) Բանկում գաղտնի փաստաթղթաշրջանառության իրականացում;
2) չլիազորված անձանց փաստաթղթերին հասանելիության կանխարգելում:

9.7.6. **Անվտանգության համակարգի կառուցվածքը**

1) Բանկի Անվտանգության համակարգի գործունեության հիմնական ենթակառուցվածքներն են.
   - տեխնիկական անվտանգության ենթահամակարգը;
   - ֆիզիկական անվտանգության ենթահամակարգը;
   - տեղեկատվական անվտանգության ենթահամակարգը;

9.7.7. **Տեխնիկական անվտանգության ենթահամակարգը** նպատակ ունի բարձրացնելու համակարգի ինժեներատեխնիկական ապահովածությունը և նախատեսվում է ապահովել Բանկի շենքերի և տարածքների անվտանգությունը տեխնիկական միջոցներով և սարքերով: Ենթահամակարգի հիմնական ֆունկցիաները հետևյալն են.
   - անվտանգության գոտիների վերահսկում;
   - ահազանգման համակարգի ապահովում և շահագործում;
   - տեսադիտարկման համակարգի ապահովում և շահագործում:

9.7.8. Պահպանիչ ահազանգող համակարգը պետք է ապահովի պաշտպանական գոտիների սահմանների ամբողջականության ապահովման ավտոմատ վերահսկում, այդ գոտիների ներսում կայուն պահպանում, ազդանշանի թողարկում գործարկման փաստի վերաբերյալ: Համակարգը ապահովում է ահազանգման նյութերի ամենօրյա գրանցում՝ հետագա թողարկման պատճառների ուսումնասիրման և վերլուծական աշխատանքների իրականացման համար:

9.7.9. Հակահրդեհային ահազանգող համակարգը պետք է ապահովի համապատասխան ծառայությունների հուսալի տեղեկացում (ազդարարում) հրդեհային կամ նախահրդեհային իրավիճակի ստեղծման մասին: Համակարգը ապահովում է ահազանգման նյութերի ամենօրյա պահուստավորում (արխիվացիա)՝ հետագա թողարկման պատճառների ուսումնասիրման և վերլուծական աշխատանքների իրականացման համար:

9.7.10. Հեռուստադիտարկման համակարգը պետք է թույլատրի տեսողականորեն վերահսկել իրավիճակը Բանկի տարբեր պաշտպանական գոտիներում՝ խախտման կատարման փաստը ճշգրիտ հաստատելու կամ հերքելու նպատակով:

9.7.11. Համակարգը ապահովում է տեսագրված նյութերի ամենօրյա պահուստավորում (արխիվացիա) դրանց հետագա ուսումնասիրման և վերլուծական աշխատանքների իրականացման համար:

9.7.12. **Ֆիզիկական անվտանգության ենթահամակարգը** նպատակ ունի ապահովելու Բանկի անձնակազմի պաշտպանվածությունը, արժեքանյութական ապահովածությունը, բարձրացնել համակարգի հուսալիությունը և ապահովել Բանկի շենքերի և տարածքների ֆիզիկական պահպանությունը: Ենթահամակարգի հիմնական ֆունկցիաները հետևյալն են.
   - Բանկի ներքին ռեժիմի վերահսկում;
   - արժեքների պահպանության ինժեներատեխնիկական ապահովում;
   - անվտանգության գոտիներում գտնվող հաճախորդների տեղաշարժի վերահսկում;
   - համագործակցություն ՀՀ Ոստիկանության և համապատասխան պետական մարմինների հետ (կապի հաստատման տվյալների ցուցակի առկայություն (հեռախոսահամարներ և այլն)):

9.7.13. Ենթահամակարգը պետք է ապահովի ֆինանսական միջոցների, անձնակազմի, տարածքների ու շինությունների պահպանությունը,
   - Բանկի գործունեության տարածքներում անցագրային ռեժիմների ապահովում և վերահսկում (ըստ սահմանված գոտիների);
   - Բանկի աշխատակիցների անձնական անվտանգության ապահովում;
   - դրամական և նյութական արժեքների պահպանության կազմակերպում և ապահովում;
   - հատուկ կանխարգելիչ միջոցառումների կազմակերպում և իրականացում;
   - աշխատակիցների անվտանգության պահանջների կատարման տեղեկացում և ուսուցման կազմակերպում:

9.7.14. **Տեղեկատվական անվտանգության ենթահամակարգը** նպատակ ունի ապահովել Բանկի տեղեկատվական ակտիվների անվտանգությունը: Բանկում տեղեկատվական անվտանգության ապահովման նպատակով գործում է Տեղեկատվական անվտանգության կառավարման համակարգ (ՏԱԿՀ):

9.7.15. Տեղեկատվական անվտանգության համակարգի օգտագործման ժամանակ կիրառվում են միջազգային չափանիշներին համապատասխանող նոր տեխնոլոգիաններ, սարքավորումներ, որոնք բավարարում են վճարային համակարգերի կողմից սահմանված անվտանգության պահանջներին, մասնավորապես.

1) SSL արձանագրությունների կիրառում, որը թույլ է տալիս ավտոմատ կերպով ծածկագրել ողջ փոխանցվող տեղեկատվությունը;

2) Թվային հավաստագրի տրամադրում /certificate/;
3) Էլեկտրոնային ստորագրության կիրառում;
4) Նույնականացման վավերականացում;
5) Երկփուլանի նույնականացման իրականացում;
6) Token մեկանգամյա գաղտնաբառերի կիրառում;
7) 3d secure sms հաղորդագրությունների օգտագործում;
8) Encryption ծածգարման կիրառում:

10. Իրավասությունների կառավարման քաղաքականություն

10.1. ԱԲՀ-ում տեղեկատվական անվտանգության ապահովման համար, ինչպես նաև Բանկի տեղեկատվությանը չարտոնագրված մուտքերից պաշտպանելու նպատակով Բանկում ներդրվում է տեղեկատվական համակարգի անհատական համակարգիչների իրավասությունների կառավարում:

10.2. Համակարգի օգտագործողներին իրավասությունները տրամադրվում են՝ յուրաքանչյուրին իր աշխատանքային պարտականություններին համապատասխան:

10.3. Բանկի ստորաբաժանման ղեկավարները Տեղեկատվական անվտանգության բաժնի հետ համատեղ պարտավոր են որոշել իրենց ենթակայության տակ գտնվող աշխատակիցների հաստիքներին համապատասխան տեղեկատվական ռեսուրսների պահանջարկը և դրա հիման վրա սահմանել ԱԲՀ-ում նրանց իրավասությունների շրջանակը:

10.4. Բանկի ցանցային ռեսուրսների իրավասությունների կառավարումը իրականացնում է SS բաժինը, իսկ դրա վերահսկողությունը՝ Տեղեկատվական անվտանգության բաժինը:

10.5. Տեղեկատվական համակարգի յուրաքանչյուր օգտագործող պարտավոր է պահպանել իր իրավասությունների շրջանակներում տեղեկատվական համակարգի օգտագործման համար սահմանված ներքին իրավական ակտերի պահանջները, որի պատշաճ օգտագործման համար կրում է անձնական պատասխանատվություն:

10.6. ԱԲՀ համակարգչային համակարգին չարտոնագրված մուտքերից խուսափելու համար, Բանկում ներդրվում են տեղեկատվական համակարգերին իրավասությունների տրամադրման ընթացակարգ, որը ներառում է օգտագործողների իրավասությունների կառավարման կյանքի ցիկլի բոլոր փուլերը, սկսված նոր օգտագործողների սկզբնական գրանցումից մինչև օգտագործողի տվյալների հեռացում, որոնց այլևս տեղեկատվական համակարգերի իրավասությունների տրամադրման անհրաժեշտություն չկա: Ընթացակարգով նվազագույնը պետք է սահմանվի՝

1) Օգտագործողներին և նրանց խմբերին իրենց իրավասությունների տրամադրման ձևը:
2) Հսկողությունը, թե տեղեկատվական համակարգի օգտագործողները ունեն արդյոք դրանց օգտագործման իրավասությունը:
3) Ստուգումը, թե բավարար է արդյոք օգտագործողին տրամադրված իրավասության շրջանակը իր վրա դրված պարտականությունների կատարման համար և չի հակասում արդյոք տրամադրված իրավասության շրջանակները Բանկի Տեղեկատվական անվտանգության քաղաքականությանը:
4) Օգտագործողին իր հիմնական իրավասություններից բացի, լրացուցիչ իրավասությունների տրամադրման վերաբերյալ դրույթներ:
5) Տեղեկատվական համակարգի օգտագործողների հաշվառման վերաբերյալ դրույթներ:
6) Բանկից ազատված կամ հաստիքային փոփոխության ենթարկված օգտագործողների իրավասությունների դադարման կամ փոփոխման վերաբերյալ դրույթներ:
7) Օգտագործողների գրանցումների և նույնականացուցիչների, որոնք այլևս անհրաժեշտ չեն, պարբերաբար ստուգման և ջնջման վերաբերյալ դրույթներ:
8) Հսկողությունը, թե օգտագործողների կողմից տրամադրվում է արդյոք տեղեկատվական համակարգի իրենց նույնականացուցիչները այլ օգտագործողների:

10.7. Օգտագործվում է տեղեկատվական համակարգի անվտանգության պահպանման հետևյալ մեթոդները՝

1) Ծրագրային մուտքերի գաղտնաբառերի օգտագործում:
2) Իրավասության ժամանակային սահմանափակումների ներդրում, օրինակ՝ տվյալների փոփոխություն կամ ջնջում իրականացնելու ժամանակային սահմանափակում:
3) Ծրագրային օգտագործման բոլոր դեպքերի գրանցում:
4) Ծրագրային օգտագործման իրավասութունյունների շրջանակների փաստաթղթավորում:
5) Բոլոր ոչ անհրաժեշտ ցանցային ծրագրերի հեռացում:

10.8. Վերահսկման նպատակով տեղեկատվական բոլոր համակարգերում օգտագործողներին տրամադրվում է ունիկալ անհատական նույնականացման կոդեր, տվյալ օգտագործողին նույնականացնելու համար:

10.9. Անհրաժեշտ է սահմանափակել դեպքերը, որոնք հնարավորություն կունենան ադմինիստրատիվ

եղանակով շրջանցել հսկողության միջոցները, որի համար պետք է իրականացվի ադմինիստրատիվ ծրագրերի պատշաճ վերահսկողություն:

10.10. Չարտոնագրված մուտքերից խուսափելու համար սահմանափակվում է տվյալ պահին չօգտագործվող և մուտք գործած տեղեկատվական համակարգի բաց մնալու ժամանակը:

10.11. Չարտոնագրված մուտքերին ժամանակին արձագանքելու նպատակով, անհրաժեշտ է իրականացնել պարբերաբար վերահսկողություն՝ օգտագործելով արդյունավետ մեթոդներ:

10.12. Բանկին ծառայություններ մատուցող երրորդ անձանց կողմից Բանկի տեղեկատվական համակարգի օգտագործման անվտանգությունը պահպանելու համար պատասխանատու է Բանկի Տեղեկատվական անվտանգության կառավարման համակարգի համար պատասխանատու ստորաբաժանումը:

10.13. Օգտագործողների նույնականացման և վավերականացման համար կիրառվում է Active Directory կատալոգների համակարգը:

11. Համակարգչային ցանցի օգտագործման քաղաքականություն

11.1. Բանկի Համակարգչային ցանցը հանդիսանում է կառավարման համակարգի անբաժանելի մաս և ներդրված է ժամանակակից տեղեկատվական տեխնոլոգիաների հիման վրա, կառավարչական խնդիրների լուծման համար՝ ապահովելով որոշումների արագ ընդունում, մասնավորապես՝

1) Բանկի տարածքային և կառուցվածքային ստորաբաժանումների միջև տեղեկատվության արագ փոխանակում,
2) ընդհանուր տեղեկատվական ցանցային ռեսուրսների օգտագործումը,
3) միասնական համակարգչային ցանցի միջոցով այլ տվյալների իրավասությունների տրամադրում,
4) Էլեկտրոնային փոստի և ինտերնետի օգտագործում,
5) Բանկի տվյալների բազայի կենտրոնացում տեղեկատվության հասանելիության տարբեր մակարդակներով:
6) Տվյալների փոփոխության վերահսկում:

11.2. **Կազմը**

11.2.1. Բանկի ներքին իրավական ակտերով սահմանվում են Համակարգչային ցանցի կառուցվածքը և սկզբունքները:

11.2.2. Համակարգչային ցանցը ձևավորվում է սարքավորումների հիմնական բաղադրիչներից՝ ծրագրային ապահովմամբ և ցանցային ու ոչ ցանցային պարամետրերի փոխազդեցությամբ:

11.2.3. Սերվերներ.[1]

- ֆայլեր,
- տվյալների բազաներ,
- դիմումներ,
- փոստային,
- արխիվային,
- հեռահար իրավասություն,
- տպագրություն,

11.2.4. Հեռահաղորդակցության ենթակառուցվածք.

- մալուխներ,
- միացման սարքավորումներ,
- իրավասությունների ընդլայնման և սահմանափակման սարքավորումներ,

11.2.5. Աշխատանքային կայաններ, ապահովված անհրաժեշտ ցանցային ադապտերներով:

11.2.6. Կրկնօրինակման և տեղեկատվության պահպանման համակարգեր:

11.2.7. Սերվերների և աշխատանքային կայանների անխափան սնուցման համակարգեր:

11.2.8. Տեղեկատվական ենթակառուցվածքներ.

- օպերացիոն համակարգեր,
- ցանցային և արտացանցային համգործակցության արձանագրություններ,
- կոլեկտիվ իրավասությունների համար կիրառվող ծրագրային ապահովում,
- աշխատանքային կայանների համար կիրառվող ծրագրային ապահովում:

11.3. **Գործողության սկզբունքը**

11.3.1. Ցանցի շահագործումը ապահովվում է աշխատանքային կայաններին, սերվերներին և համատեղ սերվերներին միացմամբ՝ կապող սարքավորումների միջնորդությամբ:

[1] *Թույլատրվում է օգտագործել մեկ սերվեր, մի քանի տարբեր նպատակների համար*

11.3.2. Ցանցի ընդլայնումը կատարվում է լրացուցիչ սեգմենտների միացման ճանապարհով ուղղորդիչների, վերահաղորդիչների և տարբեր տեսակի կապուղիների միջոցով:

11.3.3. Համացանցին միացումը կատարվում է հատուկ սարքավորումների և ներքին ցանցը դրսի (հաքերային) չարտոնագրված մուտքերից ապահովելու նպատակով ստեղծված հատուկ ծրագրային ապահովումների միջոցով:

11.3.4. Տեղեկատվության պաշտպանությունը կատարվում է իրավասությունների տրամադրման տարբեր մակարդակների գործողությամբ, որը իրականացվում է ֆայլ սերվերների և տվյալների բազաների սերվերների ադմինիստրացմամբ և հատուկ կազմակերպչական և տեխնիկական միջոցառումների իրականացմամբ:

11.4. **Աջակցություն**

11.4.1. Սերվերներ.

1) Սերվերների ադմինիստրավորումը իրականացվում է Համակարգի ադմինիստրատորի կողմից:
2) Գաղտնի տեղեկատվություն օգտագործողների իրավասությունների մակարդակը կառավարվում է Տեղեկատվական անվտանգության բաժնի կողմից և իրականացվում է միայն Համակարգի ադմինիստրատորի կողմից:
3) Տեխնիկական նպատակներով սերվերների և աշխատանքային կայանների անջատումը իրականացվում է միայն Համակարգի ադմինիստրատորի կողմից, լրացուցիչ տեղեկացնելով տվյալ սերվերները և աշխատանքային կայանները օգտագործողներին:
4) Սերվերների անջատման կամ նրա վրա առաջացած անսարքությունների վերացման դեպքում, ցանցային ադմինիստրատորները պարտավոր են առաջին հերթին իրականացնել կազմակերպչական, տեխնիկական միջոցառումներ ստորաբաժանումների գործընթացների անընդհատությունը ապահովելու նպատակով:

11.4.2. Հեռահաղորդակցություն.

1) Հեռահաղորդակցության ներքին ցանցային ուղիների ստեղծումը և սպասարկումը հանդիսանում է Բանկի բացառիկ իրավասությունը: Համակարգչային ցանցի տեղաբանությունները փաստաթղթավորվում են:
2) Համակարգի ադմինիստրատորի կողմից միացման որոշումը ընդունվում է դիմումի հիման վրա՝ Տեղեկատվական անվտանգության բաժնի գիտությամբ՝ առկա ռեսուրսների և տեխնիկական հնարավորությունների սահմաններում:
3) Անհատական համակարգիչների միացումը ցանցին իրականացվում է Համակարգի ադմինիստրատորի կամ իրավասու տեխնիկական մասնագետի կողմից, համապատասխան դիմումի հիման վրա՝ Տեղեկատվական անվտանգության բաժնի գիտությամբ:
4) Այլ կազմակերպությունների կամ օգտագործողների կողմից ինքնուրույն համակարգչային ցանցի տեղաբանությունների փոփոխությունները, ցանցին ցանկացած տարրի միացումը կամ պարամետրերի փոփոխությունը առանց Համակարգի ադմինիստրատորի և Տեղեկատվական անվտանգության բաժնի թույլտվության և Վարչության նախագահի գիտության արգելվում է:
5) Արտաքին ցանցին իրավասություն ունենալու նպատակով, մոդեմների և այլ սարքավորումների միացումը աշխատանքային կայաններին արգելվում է: Բացառիկ դեպքերում վերը նշվածը կարող է իրականացվել միայն Համակարգի ադմինիստրատորի կողմից տվյալ աշխատանքային կայանների պարտադիր վերահսկմամբ:

11.4.3. Անհատական համակարգիչներ (աշխատանքային կայաններ).

1) Ցանցի ճշգրիտ աշխատանքի նպատակով աշխատանքային կայանների օպերացիոն համակարգերի կարգավորումները իրականացվում են Համակարգի ադմինիստրատորի կողմից:
2) Աշխատանքային կայանների համակարգերում պարամետրերի փոփոխությունը, նոր ծրագրերի և տեխնիկական միջոցների տեղադրումը, որոնք կարող են փոփոխության ենթարկել համակարգի կարգավորումները ինքնուրույն կամ երրորդ անձանց միջամտությամբ, առանց Համակարգի ադմինիստրատորի մասնակցության և Տեղեկատվական անվտանգության բաժնի գիտության արգելվում է:
3) Ցանցային ռեսուրսներից, օգտագործողի անջատումը իրականացվում է տվյալ օգտագործողին պարտադիր ծանուցելուց հետո:
4) Օգտագործողի միացման պարամետրերի ցանկացած փոփոխության դեպքում, Համակարգի ադմինիստրատորը ստուգում է կապուղիների գործողությունները և իրավասությունը ցանցային ռեսուրսներին:

5) Ցանցային ռեսուրսները օգտագործողներին խստիվ արգելվում է երրորդ անձանց տրամադրել ցանցային տարրերի կարգաբերումների վերաբերյալ տեղեկություններ (օգտագործողի անուններ, գաղտնաբառեր և այլն):
6) Օգտագործողներին, իրենց և այլ անձանց իրավունքների տարածումը արգելվում է:
7) Արգելվում է համակարգչային ցանցում օգտագործել չլիցենզավորված ծրագրային ապահովումներ:
8) Աշխատակայանների տեղափոխությունը իրականացվում է համաձայն Բանկում գործող ներքին իրավական ակտերի:

11.5. **Համակարգչային ցանցի զարգացման վերաբերյալ դրույթներ**

11.5.1. Ցանցին միացումը իրականացվում է ցանկացած հեռահաղորդակցման ուղիով կախված տեխնիկական նպատակահարմարությունից:
11.5.2. Պարբերաբար իրականացվում է աշխատակայանների արդիականացում SS բաժնի կողմից տրամադրվող առաջարկների հիման վրա:
11.5.3. Նոր ձևավորվող ստորաբաժանումները համակարգչային տեխնիկայով ապահովվում են համակարգի ադմինիստրատորի և Տեղեկատվական անվտանգության բաժնի աշխատակցի մասնակցությամբ:
11.5.4. Բոլոր այն հարցերը, որոնք վերաբերվում են համակարգչային ցանցի գործունեությանը և զարգացմանը, լուծվում են SS բաժնի կողմից, որը կարգավորվում է սույն Քաղաքականությամբ և Բանկի այլ ներքին իրավական ակտերով:
11.5.5. Համակարգչային ցանցի գործունեության օպտիմիզացման նպատակով SS և Տեղեկատվական անվտանգության բաժինների աշխատակիցները իրավունք ունեն իրականացնել վերլուծություններ, ցանցի մաս կազմող ցանկացած տարրի վերաբերյալ:
11.5.6. Բոլոր տեսակի փոփոխությունները և անսարքությունները պարտադիր գրանցվում են համաձայն Բանկում գործող ներքին իրավական ակտերի:

11.6. **Համակարգչային ցանցի անվտանգությանը ներկայացվող պահանջներ**

11.6.1. Բանկի համակարգչային ցանցի կառուցվածքը հաստատվում է Բանկի Վարչության կողմից:
11.6.2. Բանկի համակարգչային ցանցերի հետ կապված փաստաթղթերը հանդիսանում են գաղտնի և պետք է հասանելի լինեն միայն արտոնագրված օգտագործողներին:
11.6.3. Համակարգչային յուրաքանչյուր լարանցում պետք է կատարվի գետնի տակով (հնարավորություն դեպքում), այլապես անհրաժեշտ է կիրառել համապատասխան պաշտպանական միջոցներ:
11.6.4. Ցանցային լարանցումները պետք է պաշտպանված լինեն անօրինական միացումներից կամ վնասվածքներից: Դրան կարելի հասնել՝ այդ լարանցումները անցկացնելով ոչ բոլորին հասանելի վայրերով:
11.6.5. Էլեկտրոմագնիսական ազդեցություններից զերծ մնալու նպատակով հեռահաղորդակցման լարանցումները պետք է առանձնացված լինեն հոսանքի՝ հատկապես բարձրավոլտ լարանցումներից:
11.6.6. Բանկի բոլոր լարանցումները պետք է փակված լինեն պաշպանիչ տուփերով: Բոլոր տեսակի լարանցումների կենտրոնացման վայրերը պետք է ամփոփվեն արկղերի մեջ, որոնք պետք է կողպվեն և կնքվեն:
11.6.7. Բանկի համակարգչային ցանցը պետք է կառուցված լինի այնպես, որ ցանցին կամայական արտաքին հարցում անցնի առնվազն մեկ միջցանցային էկրանի միջով:
11.6.8. Բանկի SS բաժնի կողմից պետք է մշակվեն և պարբերաբար վերանայվեն համակարգչային ցանցերում տեղեկատվության հոսքի ֆիլտրացման կանոնները:
11.6.9. Բանկի ներքին ցանցին միացված համակարգիչները համացանցին կարող են միանալ միայն Բանկի ինտերնետային պրովայդերների միջոցով օգտագործելով միայն Բանկի ներքին տեղեկատվական ցանցը: Արգելվում է Բանկի ներքին ցանցի համակարգիչների ուղիղ միացումը համացանցին, օրինակ՝ տարբեր տեսակի շարժական մոդեմների կիրառմամբ:
11.6.10. Բանկի Վարչության նախագահի կողմից սահմանված պարբերականությամբ պետք է ուսումնասիրվեն համակարգչային ցանցի աշխատունակությունը գերծանրաբեռնված ռեժիմներում:
11.6.11. Բանկի կողմից պետք է դիտարկվեն միջցանցային էկրանների համար Բանկի կողմից սահմանված բոլոր նախազգուշական ցուցումները:
11.6.12. Բանկի կողմից պետք է բացահայտվեն ներքին ցանցի բոլոր վտանգավոր կետերը, ներքին ցանցին արտաքին ցանկացած միացման հնարավոր տեղերը:
11.6.13. Բանկի տարածքային ստորաբաժանումների միջև տեղեկատվական ցանցերով շրջանառվող տեղեկատվությունը պետք է լինի առնվազն ծածկագրված:
11.6.14. Անլար ցանցի կիրառման դեպքում Բանկի ներքին իրավական ակտերով սահմանվում են՝

1) Անլար միացումների նպատակները և անլար միացումները թույլատրող սարքերի կարգաբերումները:
2) Անլար միացումների համար կիրառվող անվտանգության միջոցները և միջոցառումները:

11.6.15. Ցանցերը սպասարկող աշխատակիցների կողմից համակարգի խափանման ռիսկը կանխելու կամ նվազեցնելու համար Բանկը՝
1) որպես ցանցային ադմինիստրատորներ աշխատանքի է ընդունում միայն համապատասխան կրթություն ունեցող մասնագետների,
2) բացառում է ադմինիստրատորի կողմից ֆինանսական գործարքներ կատարելու հնարավորությունը, ինչպես նաև գործառնական օրվա բացման/փակման իրականացումը
3) աշխատանքները կազմակերպում է այնպես, որ նվազեցնի մարդկային գործոնը և չարտոնված գործողությունների թիվը (իրավասությունների տարանջատում, գործողությունների գրանցում, վերահսկում և այլն):

12. Գաղտնաբառերի օգտագործման քաղաքականություն

12.1. Գաղտնաբառերը հանդիսանում են համակարգչային անվտանգության կարևոր մաս: Պարզ գաղտնաբառերի օգտագործումը կարող է հանգեցնել չարտոնագրված մուտքերի և/կամ Բանկի ռեսուրսների օգտագործման: Բանկի տեղեկատվական ռեսուրսներին հասանելիություն ունեցող բոլոր օգտագործողները կրում են պատասխանատվություն իրենց գաղտնաբառերի ընտրության և դրանք անվտանգ պահպանման համար:

12.2. Տեղեկատվական անվտանգության համակարգերում Բանկի աշխատակիցներին տրամադրվում են հետևյալ մակարդակների գաղտնաբառեր՝
1) **Ադմինիստրատորներ** - աշխատակիցներ, որոնք համաձայն Բանկի ներքին իրավական ակտերի ունեն ադմինիստրատորի իրավասություններ:
2) **Օգտագործողներ** - Բանկի բոլոր հիմնական աշխատակիցները:
3) **Ժամանակավոր օգտագործողներ** - ստաժորները և բոլոր այն անհատները, որոնց Բանկում գտնվելը կրում է ժամանակավոր բնույթ:

12.3. Բոլոր ադմինիստրատորի մակարդակի գաղտնաբառերը (root, enable, Windows Administrator, application administration accounts և այլն) պետք է փոփոխվեն նվազագույնը 60 օրը մեկ անգամ:

12.4. Բոլոր օգտագործողի մակարդակի գաղտնաբառերը (web, desktop, computer և այլն) պետք է փոփոխվեն նվազագույնը 90 օրը մեկ անգամ:

12.5. **Գաղտնաբառ ստեղծելու ընդհանուր ցուցումներ**

12.5.1. Ապահով գաղտնաբառերը ունեն հետևյալ բնութագրերը.

12.5.1.1. Պարունակում են ներքոնշված 4 դասերի նիշերից նվազագույնը 3-ը՝
1) Մեծատառեր
2) Փոքրատառեր
3) Թվեր
4) Հատուկ նիշեր (@#$%^&*()_+|~-=\`{}[]:";'<>/ և այլն):

12.5.1.2. Օգտագործողի մակարդակի գաղտնաբառերը պետք է պարունակեն նվազագույնը 8 տառերից և թվերից բաղկացած նիշեր:

12.5.1.3. Ադմինիստրատորի մակարդակի գաղտնաբառերը պետք է պարունակեն նվազագույնը 16 տառերից և թվերից բաղկացած նիշեր:

12.5.2. Պարզ գաղտնաբառերը ունեն հետևյալ բնութագրերը
1) Պարունակում են 8-ից պակաս նիշեր,
2) Գաղտնաբառ է հանդիսանում որևէ բառ,
3) Գաղտնաբառ է հանդիսանում ընդհանուր օգտագործվող բառերը, ինչպիսիք են՝
   - ընտանիքի անդամների, ընկերների, կոլեգաների անունները, կենդանիների անուններ և այլն,
   - համակարգչային տերմինների, կայքերի, կազմակերպությունների, սարքավորումների անվանումներ,
   - ծննդյան ամսաթվեր կամ այլ անձնական տվյալներ, ինչպիսիք են՝ հասցե, հեռախոսահամար և այլն,
   - ստեղնաշարի վրա իրար մոտ գտնվող կամ կրկնվող նիշեր (օրինակ՝ aaaa, qwer, zxc123, bbbb1111 և այլն):

12.6. **Գաղտնաբառերի պաշտպանության ստանդարտներ**

12.6.1. Միշտ օգտագործել տարբեր գաղտնաբառեր տարբեր կազմակերպչական կարիքների համար:

12.6.2. Չհայտնել գաղտնաբառը այլ անձանց ներառյալ SS բաժնի աշխատակիցներին: Բոլոր

գաղտնաբառերը համարվում են Բանկի համար զգայուն կոնֆիդենցիալ տեղեկատվություն:

12.6.3. Գաղտնաբառերը երբեք չպետք է արձանագրվեն կամ պահվեն առցանց առանց կոդավորման:

12.6.4. Չհայտնել գաղտնաբառը էլեկտրոնային փոստով կամ այլ էլեկտրոնային հաղորդագրությունների միջոցով:

12.6.5. Այլ անձանց ներկայությամբ չխոսել գաղտնաբառի վերաբերյալ:

12.6.6. Չակնարկել կիրառվող գաղտնաբառերի ձևաչափերի վերաբերյալ:

12.6.7. Եթե ինչ որ մեկը պահանջում է գաղտնաբառ ապա հայտնել այդ մասին Տեղեկատվական անվտանգության բաժնին, բացառությամբ այն դեպքերի, երբ Տեղեկատվական անվտանգության բաժինը կամ աուդիտ իրականացնող անձը ստուգում է գաղտնաբառի համապատասխանությունը սույն Քաղաքականության պահանջներին կամ լուծում է անվտանգության գծով ստեղծված միջադեպը (նշված դեպքում գաղտնաբառը ենթակա է փոփոխման աշխատանքները վերջացնելուց հետո՝ անմիջապես):

12.6.8. Ոչ մի դեպքում չնշել «հիշել գաղտնաբառը» նշումը:

12.6.9. Եթե առկա է կասկածներ գաղտնաբառի վտանգի վերաբերյալ հայտնել այդ մասին Տեղեկատվական անվտանգության բաժնին:

13. Տեղեկատվության փոխանակման քաղաքականություն

13.1. Արտաքին տեղեկատվական համակարգերով տեղեկատվության փոխանակման պաշտպանական միջոցների տեղադրումը և շահագործումը իրականացվում է SS բաժնի կողմից, իսկ դրանց վերահսկումը իրականացվում է Տեղեկատվական անվտանգության բաժնի կողմից:

13.2. Արտաքին միացումների անհրաժեշտությունը դադարելու դեպքում դրանք անմիջապես հեռացվում են՝ իրենց պարագաներով:

13.3. Տեղեկատվական անվտանգության բաժնի կողմից եռամսյակային պարբերականությամբ ուսումնասիրվում են անօրինական արտաքին միացումները կամ նման միացումների փորձերը՝ գրառում կատարելով համապատասխան գրանցամատյանում, և հետագայում դրանք կանխելու կամ այդ հասցեները բլոկավորելու ուղղությամբ միջոցներ են ձեռնարկվում:

13.4. Ինտերնետ ռեսուրսների և Էլեկտրոնային փոստի իրավասությունների տրամադրումը օգտագործողներին իրականացվում է Ինտերնետ ռեսուրսների և Էլեկտրոնային փոստի իրավասությունների տրամադրման ընթացակարգով:

13.5. Վարչության նախագահի կողմից սահմանված պարբերականությամբ Բանկում իրականացվում է Բանկի տեղեկատվական կայքի անվտանգության և ամբողջականության պարբերական ուսումնասիրություն, ինչպես նաև համացանցում Բանկի մասին հրապարակումների ուսումնասիրություն:

13.6. Բանկի ինտերնետային կայքի միջոցով հաճախորդների անձնական տվյալների առցանց ստացման դեպքում, Բանկը պետք է ունենա Գաղտնիության քաղաքականություն, որը պետք է հրապարակվի Բանկի ինտերնետային կայքում:

13.7. **Ինտերնետ**

13.7.1. Ինտերնետը օգտագործվում է հետևյալ նպատակներով՝

- Բանկի մասին տեղեկատվության ներկայացում պաշտոնական կայքում,
- անհրաժեշտ տեղեկատվության ստացում:

13.7.2. Բանկի ներքին օգտագործողներին որպես կանոն թույլատրվում է օգտվել ինտերնետ ռեսուրսների հետևյալ խմբից՝

- Բանկի կորպորատիվ կայք www.evocabank.am,
- ՀՀ ֆինանսաբանկային կազմակերպությունների կայքեր (www.banks.am, www.cba.am, www.arca.am, www.banki.ru և այլն),
- ՀՀ պետական կառույցների կայքեր (www.arlis.am, www.parliament.am և այլն/;
- լրատվական կայքեր /www.tert.am, www.cnn.com և այլն),
- տեղեկատվա-որոնողական կայքեր՝ (www.google.com, www.yahoo.com և այլն):

13.7.3. Բանկի ներքին օգտագործողներին խստիվ արգելվում է օգտվել/դիտարկել ինտերնետ ռեսուրսների հետևյալ խմբից՝

- սոցիալական և զվարճալի կայքեր (www.odnoklassniki.ru, www.vkontakte.ru և այլն),
- խաղային և դրույքադրման կայքեր (www.casino.com, www.vivaro.am և այլն),
- ազատ Proxy-սերվերների միջոցով ինտերնետ կայքերի այցելումը (www.myproxy.com, www.zeroproxy.com և այլն),
- գնումների համար նախատեսված կայքերը,

- մեծահասակների համար նախատեսված կայքերի այցելումը/դիտումը, տվյալ կայքերից տեսանյութերի (ֆիլմերի, հոլովակների, նկարների) բեռնավորումը և տարածումը:

13.7.4. Բանկի ներքին օգտագործողներին խստիվ արգելվում է իրականացնել հետևյալ գործողությունները՝

- ինտերնետ կայքերին միացումը՝ շրջանցելով Բանկի www-սերվերը, բացառությամբ ուղիղ միացման (Direct Connection) անհրաժեշտության դեպքերի՝ Բանկի Վարչության նախագահի կարգադրությամբ,
- ծառայողական ինտերնետի միջոցով անձնական մեդիա-ֆայլերի՝ .avi, .mpeg, .wmv և այլ լայնացումով տեսանյութերի, ինչպես նաև .mp3, .mp4, .wma և այլ լայնացումով ձայնանյութերի բեռնավորումը,
- ծառայողական ինտերնետի օգտագործումը աշխատակցի անձնական փոստարկղի դիտարկման և նամակների փոխանցման համար (@mail.ru, @google.com, @gmail.com և այլն),
- օգտվել ֆայլերի ազատ փոխանակման կայքերից (www.rapidshare.com, www.depositfiles.com, ամպային տիրույթներ և այլն):

13.7.5. Հաշվի առնելով աշխատակիցների ինտերնետային ռեսուրսներից օգտվելու ծառայողական անհրաժեշտությունը և այդ տեղեկատվական հոսքերի հասանելիությունը, Բանկի ներքին օգտագործողները դասակարգվում են ըստ հետևյալ խմբերի.

1) **Նվազագույն հասանելիություն -** օգտագործողների համար հասանելի են սույն գլխի 13.6.2 ենթակետով ներկայացված տեղական (.am տիրույթի) կայքերը:
2) **Միջին հասանելիություն** - օգտագործողների համար հասանելի են սույն գլխի 13.6.2 ենթակետով ներկայացված կայքերը:
3) **Առավելագույն հասանելիություն** - օգտագործողների համար հասանելի են բոլոր կայքերը, բացառությամբ սույն գլխի 13.6.3 ենթակետում նշվածներից:
4) **Հասանելիություն առանց սահմանափակումների** - օգտագործողների վրա տարածվում են սույն գլխի 13.6.3 ենթակետով նշված սահմանումները, սակայն թույլատրվում է անհրաժեշտ ծրագրերի և ծրագրային թարմացումների բեռնավորում:

13.7.6. Սույն գլխի 13.6.5 ենթակետում ներկայացված 1-ին, 2-րդ և 3-րդ խմբերի ցուցակները թարմացվում և վերահսկվում են Տեղեկատվական անվտանգության բաժնի կողմից՝ նախապես համաձայնեցնելով Բանկի ղեկավարության հետ:

13.8. **Կորպորատիվ էլեկտրոնային փոստ**

13.8.1. Էլեկտրոնային փոստի օգտագործման կանոնները հանդիսանում են Բանկի տեղեկատվական անվտանգության քաղաքականության կարևոր և անբաժան տարր:

13.8.2. Էլեկտրոնային փոստը հանդիսանում է Բանկի սեփականությունը և կարող է միայն օգտագործվել ծառայողական նպատակներով: Այլ նպատակներով էլեկտրոնային փոստի օգտագործումը խստիվ արգելվում է:

13.8.3. Յուրաքանչյուր աշխատակցի էլեկտրոնային փոստի պարունակությունը կարող է ստուգվել անմիջական ղեկավարի պահանջով կամ Տեղեկատվական անվտանգության բաժնի կողմից առանց աշխատակցին նախօրոք ծանուցելու:

13.8.4. Էլեկտրոնային փոստային համակարգի հետ աշխատելու ընթացքում Բանկի աշխատակիցներին արգելվում է.

1) Օգտագործել էլեկտրոնային փոստի հասցեն բաժանորդագրությունների գրանցման համար առանց Տեղեկատվական անվտանգության բաժնի նախնական համաձայնության:
2) Հրապարակել իր կամ Բանկի այլ աշխատակիցների հասցեները ընդհանուր հասանելի ինտերնետ միջավայրերում (ֆորումներ, կոնֆերենցիաներ և այլն):
3) Ուղարկել կցված ֆայլերով հաղորդագրություններ, որոնց ընդհանուր ծավալը գերազանցում է 10 մեգաբայթը:
4) Մուտք եղած հաղորդագրությունների ժամանակ, կցված ֆայլեր առկա լինելու դեպքում բացել դրանք առանց հակավիրուսային համակարգերի միջոցով լրացուցիչ ստուգման, նաև այն դեպքում եթե ուղարկողը հայտնի է:
5) Օգտագործել մուտք եղած հաղորդագրության կցված ֆայլերը կամ հղումները դեպի ինտերնետ ռեսուրսներ, եթե ուղարկողը հայտնի չէ:
6) Իրականացնել փոստային հաղորդագրությունների զանգվածային ուղղարկում (10-ից ավել) արտաքին հասցեատերերի առանց իրենց համաձայնության: Այդ գործողությունները դասակարգվում են որպես սպամ և հանդիսանում են անօրինական:
7) Իրականացնել գովազդային բնույթի փոստային հաղորդագրությունների զանգվածային ուղղարկում առանց Տեղեկատվական անվտանգության բաժնի նախնական համաձայնության:

8) Ուղարկել էլեկտրոնային փոստի միջոցով նյութեր, որոնք պարունակում են վիրուսներ կամ այլ համակարգչային կոդեր, ֆայլեր կամ ծրագրեր, որոնք նախատեսված են խախտել, ոչնչացնել կամ սահմանափակել ցանկացած համակարգչային կամ հեռահաղորդակցության սարքավորումների աշխատունակությունը՝ չարտոնագրված մուտքեր իրականացնելու նպատակով, ինչպես նաև ուղղարկել սերիական համարներ, առևտրային ծրագրային պրոդուկտների կամ դրանց գեներացման ծրագրերի գաղտնաբառեր այլ միջոցներ ինտերնետում վճարովի ռեսուրսներին չարտոնագրված մուտքի իրավունք ստանալու համար կամ հղումներ վերը նշված տեղեկատվությունը ստանալու համար:
9) Հեղինակային իրավունք պարունակող նյութերի տարածումը, որը խախտում է որևէ արտոնագիր, ապրանքային նշան, առևտրային գաղտնիք, հեղինակային իրավունք և այլ գույքային, և/կամ հեղինակային և նրան կապակցված երրորդ անձանց իրավունքները:
10) Տարածել տեղեկատվություն, որի պարունակությունը և ուղղվածությունը արգելված է օրենսդրությամբ, այդ թվում նյութեր, որոնք պարունակում են վնասակար, սպառնացող, զրպարտող անպարկեշտ տեղեկատվություն, ինչպես նաև արժանապատվությունը վարկաբեկող, ատելություն և բռնություն հրահրող և այլ նմանատիպ տեղեկատվություններ:
11) Բանկից դուրս տարածել բանկային, առևտրային և ծառայողական գաղտնիք կազմող տեղեկություններ: Խիստ անհրաժեշտության դեպքում կոնֆիդենցիալ տեղեկատվությունը կարող է ուղղարկվել միայն ամուր կոդավորված ալգորիթմների կիրառմամբ և Տեղեկատվական անվտանգության բաժնի թույլտվությամբ՝ համաձայն Բանկում գործող Տեղեկատվական ակտիվների դասակարգման կարգի:

13.9. **Հեռակա աշխատանքների իրականացում**

13.9.1. Բանկի հաճախորդները Բանկի հեռակառավարման համակարգերից օգտվելու նպատակով գրանցվում են որպես «Հեռավոր դիմելու սերվերի» օգտագործողներ: Հաճախորդների գրանցումն իրականացվում է հեռակառավարման համակարգի օգտագործման համաձայնություն տալու դեպքում:

13.9.2. Բանկի տարածքից դուրս հեռակա աշխատանքները կատարվում են նախապես որոշված շրջանակների հիման վրա, որոնք պլանավորվում և համաձայնեցվում են Բանկի Վարչության նախագահի հետ: Տրամադրվում են անհատական և/կամ սահմանափակ արտոնություններ՝ կախված որոշված աշխատանքի տեսակից, որի վերաբերյալ կատարվում է գրանցում հատուկ գրանցամատյանում:

13.9.3. Բանկի տարածքից դուրս կատարված հեռակա աշխատանքների ավարտից անմիջապես հետո Տեղեկատվական անվտանգության բաժնի կողմից կատարվում է հեռակա աշխատանքների լոգ-ֆայլերի դիտարկում և կազմվում է արձանագրություն: Այն դեպքում, երբ կատարված հեռակա աշխատանքները դուրս են եկել Բանկի Վարչության նախագահի հետ նախապես համաձայնեցված շրջանակներից, Տեղեկատվական անվտանգության բաժինը արձանագրության մեջ մանրամասն նկարագրում է այն և ներկայացնում Բանկի Վարչության նախագահին:

13.10. **Արտաքին տեղեկատվական համակարգերին միացման պաշտպանություն**

13.10.1. Բանկի պաշտոնական www-սերվերը, ներքին ցանցում գտնվող համակարգիչները (ինտերնետից և էլեկտրոնային փոստի օգտվողները) առանձնացված են ինտերնետ ցանցից միջցանցային պաշտպանիչ էկրանով (Firewall), որն ապահովում է.

1) հարցման անցկացումը միջցանցային էկրանի (Firewall) միջով,
2) ցանցային անունների ու կառուցվածքի չբացահայտումը արտաքին օգտագործողներին,
3) ցանց մուտք գործելու տեղերի կարգավորումը,
4) արտաքին միացման իսկության հաստատումը,
5) նախանշված վայրից ցանցի ամբողջությամբ կառավարումը,
6) ցանցի կառավարման հաշվետվությունների հնարավորությունների ակտիվացումը,
7) էլեկտրոնային փոստից ստացված նամակների և դրանց կցված ֆայլերի ստուգումը՝ հեռացնելով վարակված ֆայլերով նամակները,
8) կապի այն միջոցների ստուգման հնարավորությունը, որոնք կարող են հեշտությամբ կեղծվել (DNS, FTP, NNTP, RIP, SMTP, Telnet, UUCP),
9) փաթեթների բլոկավորումը, որոնք օգտագործվում են ծառայության մերժման DoS-հարձակումների համար (ICMP Echo, UDP և TCP Echo, Chargen և Discard),
10) ինֆորմացիոն հոսքի (Traffic) մերժումն այնպիսի հասցեներից, որոնք կարող են լինել ապօրինի ձեռք բերված (Spoofed, այսինքն հասցեն պատկանում է ցանցին, բայց ստեղծումը եղել է ցանցից դուրս),

11) կասկածելի հասցեներից ուղարկվող հարցումների փակումը:

13.10.2. Միջցանցային էկրանը (Firewall) ունակ է բլոկավորելու կապի որոշակի հարցումները՝ հիմնվելով.
1) հասցեի վրա (կոնկրետ IP-հասցե),
2) պորտի վրա (FTP 20 և FTP 21 կամ Telnet 23),
3) նոր կամ փոփոխված կանոնները կարող են կիրառվել միայն դրանց թեստավորումից հետո:

13.10.3. Ինտերնետ ցանցի տրանսպորտային միջավայրի օգտագործման և հեռավոր միացումների սերվերին միանալու ժամանակ օգտագործվում են գաղտնագրային ֆունկցիաներ: Պարբերաբար կատարվում է գաղտնագրման բանալիների փոփոխում, սակայն ոչ պակաս, քան վեց ամիսը մեկ անգամ:

13.10.4. Ցանցի մասին տեղեկատվության բացահայտումը սահմանափակվում է ցանցային մակարդակում հասցեները ձևափոխելու միջոցով (հասցեի փոփոխություն ցանցից դուրս գալու դեպքում) և ծրագրային մակարդակում սերվերների (Proxy Server) օգտագործմամբ (HTTP հարցումները անցկացվում են HTTP Proxy-սերվերի միջով):

13.10.5. Միջցանցային էկրանի (Firewall) թերությունների հայտնաբերման և վերացման նպատակով Բանկն իրականացնում է միջցանցային էկրանի (Firewall) պարբերական դիտարկումներ և թեստավորումներ՝ համապատասխան ծրագրերի միջոցով կամ բոլոր նախազգուշական ցուցումների դիտարկումների միջոցով:

13.10.6. Ադմինիստրատորների կողմից պարբերաբար ուսումնասիրվում են գործող ցանցային սարքավորումների շահագործումը նորմալ և զբաղված վիճակում, կիրառելով.
1) ցանցի ավտոմատ մոնիթորինգ իրականացնող ծրագրեր,
2) ցանցի լոգ ֆայլերի պարբերական ուսումնասիրություններ,
3) ցանցի խցանումների և գերծանրաբեռնվածության հետազոտություն,
4) համապատասխան համակարգերի միջոցով (Nessus, Pingware կամ այլ) ցանցի և ցանցային սարքավորումների խոցելիության ստուգում,
5) չհավատարմագրված անլար (Wireless) ցանցերի փնտրում:

13.11. **Տեղեկատվության ոչ էլեկտրոնային փոխանակման պահանջներ**

13.11.1. Բանկի աշխատակիցները պետք է պահպանեն նախազգուշական միջոցներ հեռախոսային զանգերի և բանակցությունների ժամանակ:

13.11.2. Մասնավորապես արգելվում է՝
1) Կոնֆիդենցիալ հեռախոսազրույցներ կամ երես առ երես բանակցություններ վարել կողմնակի անձանց ներկայությամբ:
2) Թողնել գաղտնիք կազմող տեղեկատվություն ինքնապատասխանիչի վրա:
3) Թողնել տպված փաստաթղթերը աշխատասեղանի կամ տպիչի վրա:
4) Ֆաքսերի հետ աշխատանքի ժամանակ անհրաժեշտ է հաշվի առնել հետևյալ խնդիրները.
   - չավտորիզացված մուտքը հաղորդագրություններ ստանալու վայր.
   - հաղորդագրությունների ուղարկում սխալ համարներով:

13.11.3. Տեղեկատվության թղթային փոխանակման գործընթացը իրականացվում է Բանկի այլ ներքին իրավական ակտերով:

14. Մաքուր սեղանի և մաքուր էկրանի քաղաքականություն

14.1. **Մաքուր սեղան**

14.1.1. Բանկում տեղեկատվական ակտիվ պարունակող փաստաթղթերը երբ որ չեն օգտագործվում, մասնավորապես՝ ոչ աշխատանքային ժամերին, պետք է պահվեն աշխատանքային սենյակներում համապատասխան փակ չհրկիզվող կամ այլ անվտանգ պահարաններում:

14.1.2. Այն աշխատասենյակներում որտեղ առկա է փակվող չհրկիզվող պահարաններ, պահարաններ և այլն, դրանք առանց հսկողության թողնելու ընթացքում տվյալ աշխատասենյակի դռները պետք է լինեն փակված:

14.1.3. Յուրաքանչյուր աշխատանքի վերջում բոլոր զգայուն տեղեկատվությունը պետք է հեռացվի աշխատանքային սեղանից և պահվի փակի տակ, մասնավորապես՝ այն փաստաթղթերը, որոնց գաղտնիության աստիճանը համաձայն Բանկի ներքին իրավական ակտերի կոնֆիդենցիալ է կամ ներքին:

14.1.4. Կոնֆիդենցիալ կամ զգայուն տեղեկատվությունը տպելուց հետո այն պետք է անմիջապես վերցվի պրինտերի վրայից: Հնարավորության դեպքում օգտագործվում է պրինտերներ, որոնք աշխատում են գաղտնաբառերով:

14.1.5. Աշխատակիցների բացակայության ընթացքում կամ ոչ աշխատանքային ժամերին աշխատասենյակների դռները պետք է լինեն փակ:

14.1.6. Բոլոր տեղեկատվական ակտիվները, որոնք չեն օգտագործվում պետք է լինեն փակի տակ:
14.1.7. Հաճախորդների սպասարկում իրականացնող աշխատակիցների աշխատանքային սեղանները կարող են լինել ավելի խոցելի, այդ պատճառով հաճախորդի անձնական տեղեկատվություն պարունակող փաստաթղթերը չպետք է պահվեն սեղանի վրա՝ հաճախորդների համար տեսանելի վայրում:
14.1.8. Սեղանի վրա թողնված տեղեկատվական ակտիվների ոչնչացման հավանականությունը ավելի բարձր է:

14.2. **Մաքուր էկրան**

14.2.1. Համակարգ մուտք եղած ժամանակ, համակարգիչները կամ համակարգչային տերմինալները չպետք է թողնվեն առանց հսկողության, առանց հսկողության թողնելու դեպքում, «Lock» գործողությամբ պետք է փակել համակարգչի իրավասությունը:
14.2.2. Համակարգչային էկրանները պետք է տեղադրված լինեն այնպես, որպեսզի կողմնակի անձանց համար էկրանի տեղեկատվությունը լինի անհասանելի:
14.2.3. Պետք է սահմանվի համակարգչի ոչ ակտիվ լինելու ժամանակահատված, որից հետո համակարգիչը պետք է ավտոմատ արգելափակվի:
14.2.4. Արգելափակված համակարգիչը կրկին ակտիվացնելու համար պետք է կիրառվի գաղտնաբառ:
14.2.5. Օգտագործողները համակարգչից հեռանալու դեպքում «Lock» գործողությամբ պետք է արգելափակեն դրանք:
14.2.6. Աշխատանքային օրվա վերջում օգտագործողները պետք է ելք լինեն բոլոր տեղեկատվական համակարգերից:

15. Համակարգիչների և դրանց հարակից սարքավորումների քաղաքականություն

15.1. **Սարքավորումների անվտանգություն**

15.1.1. Սարքավորումները պետք է տեղակայված լինեն այնպես, որ սահմանափակվի հասանելիությունը դրանց օգտագործումն ու սպասարկումն անմիջականորեն չիրականացնող անձանց համար:
15.1.2. Տեղեկատվության վերամշակումն ու պահպանումն ապահովող սարքավորումները պետք է տեղակայված լինեն այնպես, որ զերծ լինեն կողոպուտից, հրդեհից, ծխից, ջրից և փոշուց:
15.1.3. Կարևոր ցանցային սարքավորումների և ծրագրային ապահովումների խափանման ռիսկի նվազեցման նպատակով Բանկում ձեռնարկվում են հետևյալ միջոցառումները՝
1) արտոնագրված, որակյալ սարքավորումների և ծրագրային ապահովումների ձեռքբերում,
2) պարբերական թարմացումների կատարում,
3) կարևոր սարքավորումների և ծրագրային ապահովումների կարճ ժամանակահատվածում փոխարինելիության ապահովում,
4) ցանցի նպատակին և կառուցվածքին համապատասխանող արձանագրությունների (protocol) օգտագործում,
15.1.4. Բոլոր տեսակի սարքավորումները պարբերաբար պետք է ենթարկվեն դիտարկման և հեռակա վերահսկման:
15.1.5. Բանկի SS բաժինը վարում է Բանկի բոլոր աշխատակայանների համակարգչային բազայի էլեկտրոնային գրանցամատյան, որտեղ լրացված են աշխատակայանում տեղադրված համակարգչի և/կամ հարակից սարքավորումների մասին տեղեկատվություն (տեխնիկական կազմը, ձեռքբերման ամսաթիվը, մեկ աշխատակայանից այլ աշխատակայան տեղափոխման ամսաթիվը, եթե տեղափոխություն եղել է):
15.1.6. Սահմանված պարբերականությամբ SS բաժնի համապատասխան աշխատակիցները պետք է իրականացնեն Բանկում տեղադրված բոլոր համակարգիչների տեխնիկական վիճակի ստուգում՝ ստուգման արդյունքները ներկայացնելով Բանկի Վարչության նախագահին:
15.1.7. Բանկի բոլոր համակարգիչները անխտիր պետք է ապահովված լինեն UPS /Uninterruptable Power Supply/ անխափան սնուցման սարքերով՝ արտակարգ իրավիճակների դեպքում աշխատակայանի աշխատանքի անընդհատությունն ապահովելու և համակարգչում առկա տեղեկատվության կորստի ռիսկերից խուսափելու նպատակով:
15.1.8. Բանկի բոլոր տեսակի սարքավորումների մոտ ուտելը, ծխելը և խմելը խստիվ արգելվում է:
15.1.9. Բանկի բոլոր տեխնիկական սարքավորումները պետք է հողանցվեն:
15.1.10. Բանկի տեխնիկածրագրային սարքավորումները պետք է ունենան նույնականացուցիչներ:
15.1.11. Ցանցային միացման կետերը պետք է ֆիզիկապես պաշտպանված լինեն:
15.1.12. Բանկում գործում է Համակարգչային տեխնիկայի շահագործման և շահագործումից դուրս բերման ընթացակարգ:

15.2. **Սերվեր հանդիսացող համակարգիչներ**

15.2.1. Բանկի սերվեր հանդիսացող համակարգիչները պետք է պահպանվեն համապատասխան առանձնացված (սերվերային) սենյակներում, որը պետք է համապատասխանի հետևյալ չափանիշներին՝

1) լինի առանձնացված հարակից տարածքներից ոչ թափանցիկ նյութերից (օրինակ՝ չլինի ապակուց) պատրաստված պատերով,
2) սերվերային սենյակի դուռը պետք է հանդիսանա միակ ճանապարհը այնտեղ մուտք գործելու կամ դուրս գալու համար,
3) ունենա հակահրդեհային պաշտպանության համակարգ,
4) ունենա շարժման գրանցման/հայտնաբերման համակարգ և/կամ տվիչներ,
5) ունենա համակարգիչների բնականոն աշխատանքն ապահովելու համար անհրաժեշտ ջերմաստիճանը (18-24C), օդի խոնավությունը կարգավորող և պահպանող համակարգ (օդի խոնավությունը պետք է լինի 20%-55%), ինչպես նաև օդափոխության համակարգ,
6) ունենա տեսահսկման համակարգ, որը պետք է տեղադրված լինի այնպես, որ հնարավորություն լինի հսկելու սերվերային սենյակում տեղի ունեցող ցանկացած իրադարձություն,
7) ունենա դռան ինքնաբերաբար փակման համակարգ,
8) սերվերային սենյակը պետք է ունենա անխափան էլեկտրասնուցման համակարգեր, որը պետք է ապահովի ինչպես սերվերների անխափան աշխատանքը, այնպես էլ այս գլխում նշված տեսահսկման, հակահրդեհային պաշտպանության, շարժման գրանցման և հայտնաբերման, ջերմաստիճանը պահպանող, օդափոխության համակարգերի անխափան աշխատանքը, առնվազն հիմնական սերվերներից այլ վայրում գտնվող պահուստային սերվերներին անցնելու ժամանակահատվածում,
9) չպետք է ունենա պատուհան
10) սերվերային սենյակի մուտքի դուռը բացվում է հատուկ կոդերի կամ քարտերի կիրառմամբ:
11) սերվերային սենյակ մուտքի իրավասություն ունեցող անձանց ցուցակը սահմանվում է Վարչության նախագահի կարգադրությամբ:
12) սերվերային սենյակ միաժամանակ մուտք կարող են լինել առավելագույնը 5 անձ՝ SS բաժնի պետի կամ Տեղեկատվական անվտանգության բաժնի պետի ուղեկցությամբ, իսկ նրանց բացակայության դեպքում Անվտանգության բաժնի պետի ուղեկցությամբ:
13) սերվերային սենյակ մուտքի/ելքի համար վարվում է գրանցամատյան, որտեղ գրանցվում է մուտք/ելք գործողի անուն-ազգանունը, մուտքի/ելքի ժամը և ամսաթիվը:

15.3. **Շարժական սարքավորումներ**

15.3.1. Շարժական սարքավորումները հանդիսանում են Բանկի բիզնես գործընթացի կարևոր գործիք, սարքավորման շարժական լինելը դարձնում է նրան ավելի խոցելի:

15.3.2. Շարժական սարքավորման ֆիզիկական անվտանգության համար պատասխանատվություն է կրում սարքավորման օգտագործողը:

15.3.3. Երբ շարժական սարքավորումը չի օգտագործվում, ցանկալի է նրան պահել փակի տակ:

15.3.4. Օգտագործողը պետք է իր մոտ պահպանի շարժական սարքավորման գույքագրման համարը և սարքավորման կորուստի կամ հափշտակման դեպքում անմիջապես այդ մասին պետք է հայտնի Տեղեկատվական անվտանգության բաժին:

15.3.5. Շարժական սարքավորումների հակավիրուսային ծրագրերը պետք է թարմացվեն նվազագույնը ամիսը մեկ անգամ:

15.3.6. Տարբեր աղբյուրներից ներմուծված ֆայլերի ստուգումը՝ հակավիրուսային ծրագրերով պարտադիր է (CD/DVD, USB, հիշողության քարտ, համացանցից ներբեռնումներ և այլն):

15.3.7. Պետք է անմիջապես արձագանքել վիրուսի նախազգուշացմանը կամ վիրուսային վարակի կասկածի դեպքում կապնվել Տեղեկատվական անվտանգության բաժնի հետ:

15.3.8. Չուղարկել ֆայլեր կամ չներբեռնել տվյալներ ցանց, եթե կա կասկած, որ շարժական սարքավորումը կարող է վարակված լինել:

15.3.9. Շարժական սարքավորումներում կոնֆիդենցիալ տեղակատվություն պահելը արգելվում է: Խիստ անհրաժեշտության դեպքում շարժական սարքավորումներում կոնֆիդենցիալ տեղակատվություն կարող է պահվել միայն ամուր կոդավորմամբ ալգորիթմների օգտագործման և Տեղեկատվական անվտանգության բաժնի թույլտվության դեպքում:

15.3.10. Շարժական սարքավորման օգտագործողը կրում է անձնական պատասխանատվություն իր նույնականացման տվյալներով համակարգի հասանելիության համար:

15.3.11. Կորպորատիվ շարժական սարքավորումները նախատեսված է օգտագործել միայն Բանկի

լիազորված աշխատակիցների կողմից: Այլ անձանց կողմից դրանց օգտագործումը խստիվ արգելվում է (օրինակ՝ ընտանիքի անդամներ, ընկերներ և այլն):

16. Գաղտնագրման և բանալիների կառավարման քաղաքականություն

16.1. Գաղտնագրում

16.1.1. Բանկի բոլոր կոդավորումները պետք է իրականացված լինեն FIPS-140 գաղտնագրային մոդուլների հիմքի վրա:

16.1.2. Բանկում կիրառվում է AES 256, Triple DES и RSA գաղտնագրման ալգորիթմները:

16.1.3. Գաղտնագրված բանալու երկարությունը պետք է փոքր չլինի 128 բիթից:

16.1.4. Գաղտնագրված բանալու երկարության չափը պետք է պարբերաբար վերանայվի, Բանկում գործող ՏԱԿՀ վերանայման շրջանակներում և տեխնոլոգիաների արդիականացման հետ համահունչ արդիականացվի:

16.2. Բանալիների կառավարում

16.2.1. Բանալիի կյանքի ցիկլի գործընթացի կառավարումը և հավաստագիրը պետք անցնի հետևյալ փուլերով.

16.2.2. Կարգաբերումներ՝

- Գրանցում
- Զույգ Բանալիների գեներացում
- Հավաստագրի ստեղծում
- Բանալու և հավաստագրի բաշխում
- Հավաստագրի տարածում
- Բանալու պահուստավորում

16.2.3. Բանալիների և հավաստագրերի ադմինիստրավորում

- Հավաստագրի ստուգում և վերականգնում
- Բանալու վերականգնում և թարմացում

16.2.4. Հավաստագրի և Բանալու պատմության չեղյալ համարում

- Հավաստագրի կիրառման ժամկետի ավարտ
- Հավաստագրի չեղյալացում
- Բանալու պատմություն
- Բանալու արխիվացում

16.2.5. Բանալու կայանքի ցիկլը պետք լինի առավելագույնը 6 ամիս: Փակ բանալու արատավորման կամ կասկածի դեպքում այն պետք է չեղյալացվի:

16.2.6. Բանալիների ընդունումը և հանձնումը պետք փաստաթղթավորվի:

16.2.7. Բանալիները պետք է լինեն պահպանված, իսկ հասանելիությունը օգտագործողներին տրամադրվում է սահմանված կարգով:

16.2.8. Բանկի Վարչության նախագահի կարգադրությամբ սահմանվում է՝ օգտագործողներին Բանալիների տրամադրման, վերադարձման և դրանց ակտիվացման դեպքերը:

16.2.9. Բանալիների փոփոխման և թարմացման յուրաքանչյուր դեպք, Տեղեկատվական անվտանգության բաժնի կողմից պետք է գրանցվի համապատասխան գրանցամատյանում:

16.2.10. Բանալիները պետք է չեղյալացվեն, և հետ կանչվեն կամ անջատվեն, երբ Բանալին արատավորված է կամ օգտագործողը հեռանում է աշխատանքից:

17. Տվյալների քողարկման քաղաքականություն

17.1. Բանկի քարտապան հաճախորդների քարտային տվյալների քողարկման (masking) կամ կրճատման (truncation) քաղաքականությունը նախատեսում է հետևյալ հիմնական սկզբունքները՝

17.1.1. **Քողարկման պահանջ**

Պետք է ցուցադրվեն քարտի դիմերեսի թվանշանների առաջին վեց և վերջին չորս թվերը: Միջին թվերը պետք է քողարկվեն՝ ապահովելու զգայուն տեղեկատվության արտահոսքը,

17.1.2. **Հասանելիության վերահսկում**

Հաշվեհամարի հասանելիություն պետք է ունենա միայն իրավասու աշխատակիցները, ընդ որում վերջինները ամբողջական հաշվեհամարը դիտելու համար պետք է ունենան օրինական հիմնավորում

17.1.3. **Գաղտնագրում**

Քարտի փոխանցման կամ պահպանման ժամանակ պետք է գաղտնագրվեն քարտապանի տվյալները՝ կանխելու դրանց չարտոնված հասանելիությունը,

17.1.4. **Թոքենացում**

Կարող են օգտագործվել թոքեններ, որոնց միջոցով հնարավոր կլինի իրականացնել գործարքներ առանց բացահայտելու քարտերի տվյալները

17.1.5. **Կանոնավոր աուդիտ**

Պետք է իրականացվի սույն քաղաքականության կանոնների և պահանջների պահպանման հաճախակի աուդիտ:

18. Պատասխանատվություն

18.1. Բանկի ղեկավարությունը իրականացնում է Տեղեկատվական անվտանգության ընդհանուր ղեկավարում և ապահովում է ընդհանուր պայմաններ՝

1) Տեղեկատվական անվտանգության և տեղեկատվության պահպանման ռիսկերի գնահատման միջոցառումների իրականացման համար,
2) ՏԱԿՀ-ի մոնիթորինգների և վերլուծությունների իրականացման և աշխատանքի անընդհատության բարելավման համար,
3) Տեղեկատվական անվտանգության ոլորտում Բանկի աշխատակիցների պարբերաբար վերապատրաստումներ իրականացնելու համար:

18.2. Սույն Քաղաքականության պահանջների կատարման հսկողությունը իրականացվում է Բանկի տարածքային և կառուցվածքային ստորաբաժանումների ղեկավարների կողմից:

18.3. Բանկի աշխատակիցները կրում են անձնական պատասխանատվություն ՏԱԿՀ-ը կարգավորող իրավական ակտերի պահանջների կատարման համար և պարտավոր են Տեղեկատվական անվտանգության ոլորտում ՏԱԿՀ-ի համար պատասխանատու ստորաբաժանմանը տեղեկացնել հայտնաբերված բոլոր խախտումների վերաբերյալ: Բանկի յուրաքանչյուր աշխատակից պատասխանատվություն է կրում սույն Քաղաքականության պահանջների խախտման համար, որի դեպքում կարող է կիրառվել ՀՀ օրենսդրությամբ սահմանված ինչպես նաև Բանկի ներքին իրավական ակտերով սահմանված պատժամիջոցներ:

18.4. Բանկում առկա է աշխատակիցների և Երրորդ անձանց կողմից իրենց աշխատանքային պարտականությունների կատարման ընթացքում հայտնի դարձած տեղեկատվության պահպանման վերաբերյալ պարտավորագիր, որը ստորագրվում է Բանկի յուրաքանչյուր աշխատակցի և Երրորդ անձի կողմից: