

«ՀԱՍՏԱՏՎԱԾ»
ԱՐԱՐԱՏՔԱՆԿ ԲԲԸ
խորհրդի «10» հուլիսի 2019թ.
թիվ 27/05Լ-Հ որոշմամբ
խորհրդի նախագահի
Արզիկ Սուվարյան _____



ՔԱՂԱՔԱԿԱՆՈՒԹՅՈՒՆ

ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ

Ուժի մեջ է՝ 2019թ-ի հուլիսի «10»-ից

	Քաղաքականություն Տեղեկատվական անվտանգության	Կոդ: ՔԱՂ05 - 01 Խմբագրություն: 03 Դաս: ՀՊ Ամսաթիվ: «10» հուլիսի 2019թ.
---	--	---

ԲԱԺԻՆ Ի. ՆՊԱՏԱԿԸ, ԿԻՐԱՌՄԱՆ ՇՐՋԱՆԱԿԸ, ԱՌՆՉՎՈՂ ՓԱՍՏԱԹՂԹԵՐԸ ԵՎ ՍԱՀՄԱՆՈՒՄՆԵՐԸ

ԳԼՈՒԽ 1. ՆՊԱՏԱԿԸ

1. ԱՐԱՐԱՏԲԱՆԿ ԲԲԸ-ն հանդիսանում է Հայաստանի Հանրապետությունում գործող առևտրային բանկ, որն իրականացնում է գործունեություն ֆինանսական և իրավաբանական անձանց ֆինանսական ծառայությունների մատուցման բնագավառում: Նշված գործունեության իրականացումը կապված է տեղեկատվության կառավարման հետ, որը հանդիսանում է ԱՐԱՐԱՏԲԱՆԿ ԲԲԸ կարևորագույն ակտիվներից մեկը և կախված է տեղեկատվական անվտանգության ապահովումից, որն իրենից ներկայացնում է մի շարք այլ միջոցառումների համախումբ ուղղված տեղեկատվական ակտիվների գաղտնիության, ամբողջականության և հասանելիության ապահովմանը, տեղեկատվական անվտանգության կառավարման համակարգի շարունակական զարգացմանը և բարելավմանը:

ԳԼՈՒԽ 2. ԿԻՐԱՌՄԱՆ ՇՐՋԱՆԱԿԸ

2. Տեղեկատվական անվտանգության քաղաքականությունը տարածվում է ԱՐԱՐԱՏԲԱՆԿ ԲԲԸ-ի բոլոր աշխատողների և բոլոր շահագրգիռ երրորդ կողմերի վրա:

ԳԼՈՒԽ 3. ԱՌՆՉՎՈՂ ՓԱՍՏԱԹՂԹԵՐ

3. Տեղեկատվական անվտանգության քաղաքականությունն առնչվում է հետևյալ հիմնական փաստաթղթերի հետ.
 - 1) ՀՀ կենտրոնական բանկի խորհրդի 2013 թվականի հուլիսի 9-ի թիվ 173-Ն որոշմամբ հաստատված «Տեղեկատվական անվտանգության ապահովման նվազագույն պահանջների սահմանման վերաբերյալ կարգ»:
 - 2) ԱՐԱՐԱՏԲԱՆԿ ԲԲԸ բաժնետերերի արտահերթ ընդհանուր ժողովի 2008 թվականի դեկտեմբերի 29-ի N04/01 որոշմամբ հաստատված «ԱՐԱՐԱՏԲԱՆԿ ԲԲԸ Կանոնադրություն» (փոփոխություններով):
 - 3) ԱՐԱՐԱՏԲԱՆԿ ԲԲԸ Խորհրդի 2015 թվականի նոյեմբերի 10-ի թիվ 15/03Լ-Հ որոշմամբ հաստատված «Ռիսկերի կառավարման քաղաքականություն»:

	Քաղաքականություն Տեղեկատվական անվտանգության	Կոդ: ՔԱՂ05 - 01 Խմբագրություն: 03 Դաս: ՀՊ Ամսաթիվ: «10» հուլիսի 2019թ.
---	--	---

- 4) ԱՐԱՐԱՏԲԱՆԿ ԲԲԸ Խորհրդի 2017 թվականի սեպտեմբերի 14-ի թիվ 11/09Լ որոշում՝ «ԱՐԱՐԱՏԲԱՆԿ ԲԲԸ վարչակազմակերպական կառուցվածքի հաստատման մասին»:
- 5) ԱՐԱՐԱՏԲԱՆԿ ԲԲԸ Խորհրդի 2013 թվականի հունվարի 8-ի թիվ 01/01Լ որոշում՝ «ԱՐԱՐԱՏԲԱՆԿ ԲԲԸ-ի նոր հաստիքացուցակի հաստատման մասին»:
- 6) ԱՐԱՐԱՏԲԱՆԿ ԲԲԸ Խորհրդի 2017 թվականի հունիսի 22-ի թիվ 23/01Լ-Հ որոշում՝ «ԱՐԱՐԱՏԲԱՆԿ ԲԲԸ Գլխամասային դրասենյակի հաստիքացուցակի հաստատման մասին»:
- 7) ԱՐԱՐԱՏԲԱՆԿ ԲԲԸ Խորհրդի 2014 թվականի նոյեմբերի 4-ի թիվ 11/01Լ որոշմամբ հաստատված «Իրավական ակտերի նախագծերի պատրաստման և ընդունման կարգ»:
- 8) ԱՐԱՐԱՏԲԱՆԿ ԲԲԸ Խորհրդի 2014 թվականի նոյեմբերի 4-ի թիվ 11/02Լ որոշմամբ հաստատված «Բանկի տեղեկատվական ակտիվների դասակարգման և նույնականացման կարգ»:
- 9) ԻՍՕ/ԻԷԿ 27001 «Տեղեկատվական տեխնոլոգիաներ. Անվտանգության ապահովման մեխանիզմներ. Տեղեկատվական Անվտանգության Կառավարման Համակարգեր. Պահանջներ» ստանդարտ:

ԳԼՈՒԽ 4. ՍԱՀՄԱՆՈՒՄՆԵՐ ԵՎ ՀԱՊԱՎՈՒՄՆԵՐ

4. Տեղեկատվական անվտանգության քաղաքականությունում օգտագործվում են հետևյալ հիմնական հասկացությունները՝
 - 1) **Քանկ՝** ԱՐԱՐԱՏԲԱՆԿ ԲԲԸ:
 - 2) **Քաղաքականություն՝** Տեղեկատվական անվտանգության քաղաքականություն:
 - 3) **ՏԱՊ՝** Անվտանգության վարչության տեղեկատվական անվտանգության համար պատասխանատու:
 - 4) **ՏԱԿՀ՝** Տեղեկատվական անվտանգության կառավարման համակարգ:

ԳԼՈՒԽ 5. ՓՈՓՈԽՈՒԹՅՈՒՆՆԵՐ ԵՎ ԼՐԱՑՈՒՄՆԵՐ

5. Խմբագրություն 03, փոփոխություններ են կատարվել Քաղաքականության 3-րդ կետի 3-րդ, 4-րդ և 6-րդ ենթակետերում, 9-րդ կետում:

ԳԼՈՒԽ 6. ՀԱՎԵԼՎԱԾՆԵՐ

	Քաղաքականություն Տեղեկատվական անվտանգության	Կոդ: ՔԱՂ05 - 01 Խմբագրություն: 03 Դաս: ՀՊ Ամսաթիվ: «10» հուլիսի 2019թ.
---	--	---

6. Քաղաքականությունը հավելվածներ չունի:

ԲԱԺԻՆ II. ՆԿԱՐԱԳՐՈՒԹՅՈՒՆ

ԳԼՈՒԽ 1. ԸՆԴՀԱՆՈՒՐ ԴՐՈՒՅԹՆԵՐ

7. Քաղաքականությունը սահմանում է նպատակները, խնդիրները և մոտեցումները տեղեկատվական անվտանգության բնագավառում, որով Բանկը ղեկավարվում է իր գործունեության մեջ:
8. ՏԱԿՀ-ի ներդրման և բարելավման շահագրգիռ կողմեր են հանդիսանում.
- 1) Բանկի Խորհուրդը,
 - 2) Բանկի Վարչությունը,
 - 3) Բանկի Տնօրինությունը,
 - 4) Բանկի Հաճախորդները,
 - 5) Բանկի Գործընկերները:
9. ՏԱԿՀ-ի շրջանակներում իրականացվող գործառույթները տարածվում են Բանկի բոլոր կառուցվածքային և տարածքային ստորաբաժանումների վրա: Կառուցվածքային ստորաբաժանումների ցանկը հաստատվել է Բանկի Խորհրդի 2017 թվականի սեպտեմբերի 14-ի «ԱՐԱՐԱՏԲԱՆԿ ԲԲԸ վարչակազմակերպական կառուցվածքի հաստատման մասին» թիվ 11/09Լ որոշմամբ և տեղադրված է Բանկի ինտերնետային կայքում հետևյալ հասցեով՝ <https://www.araratbank.am/տեղեկություններ-մեր-մասին/>: Մասնաճյուղերի ցանկը տեղադրված է Բանկի ինտերնետային կայքում հետևյալ հասցեով՝ <https://www.araratbank.am/hy/branches>: Բանկի Գլխամասային գրասենյակի աշխատողների հաստիքացուցակը հաստատվել է Բանկի Խորհրդի 2017 թվականի հունիսի 22-ի «ԱՐԱՐԱՏԲԱՆԿ ԲԲԸ Գլխամասային գրասենյակի հաստիքացուցակի հաստատման մասին» թիվ 23/01Լ-Հ որոշմամբ: Բանկի տարածքային ստորաբաժանումների հաստիքացուցակը հաստատվել է Բանկի Խորհրդի 2013 թվականի հունվարի 8-ի «ԱՐԱՐԱՏԲԱՆԿ ԲԲԸ նոր հաստիքացուցակի հաստատման մասին» թիվ 01/01Լ որոշմամբ:
10. Քաղաքականությունն ուղղված է հետևյալ նպատակների և մոտեցումների իրականացմանը՝
- 1) Բանկի հիմնական բիզնես-գործընթացների անընդհատության ապահովում,

	Քաղաքականություն Տեղեկատվական անվտանգության	Կոդ: ՔԱՂ05 - 01 Խմբագրություն: 03 Դաս: ՀՊ Ամսաթիվ: «10» հուլիսի 2019թ.
---	--	---

- 2) տեղեկատվական անվտանգության ոլորտում խախտումների արդյունքում հնարավոր կորուստների և վնասի հնարավորինս նվազեցում,
- 3) տեղեկատվական անվտանգության ոլորտում խախտումների կանխարգելում,
- 4) տեղեկատվության գաղտնագրման վերահսկում,
- 5) գաղտնագրման բանալիների կառավարում,
- 6) տեղեկատվության հասանելիության վերահսկում,
- 7) մաքուր սեղանի մոտեցում,
- 8) մաքուր էկրանի մոտեցում,
- 9) տեղեկատվական կրիչների ոչնչացման մոտեցում,
- 10) շարժական սարքերի անվտանգության մոտեցում,
- 11) համակարգչային ցանցերի անվտանգության մոտեցում,
- 12) գաղտնաբառերի կառավարման մոտեցում,
- 13) տեղեկատվության դասակարգում,
- 14) ֆիզիկական անվտանգություն,
- 15) ակտիվների ընդունելի շահագործում,
- 16) տեղեկատվության փոխանցում,
- 17) ծրագրային ապահովման տեղադրման և օգտագործման սահմանափակումներ,
- 18) կրկնօրինակում,
- 19) պաշտպանություն չարամիտ ծրագրերից,
- 20) խոցելիությունների կառավարում,
- 21) անձնական տեղեկատվության գաղտնիություն և պաշտպանություն,
- 22) Բանկին ծառայություններ մատուցող կազմակերպությունների հարաբերությունների մոտեցում:

ԳԼՈՒԽ 2. ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԿԱՌԱՎԱՐՈՒՄ

11. Քաղաքականության 10-րդ կետում նշված նպատակների իրականացման համար Բանկում ներդրվում է ՏԱԿՀ, որը պետք է համապատասխանի.

- 1) ԻՍՕ/ԻԷԿ 27001:2013 «Տեղեկատվական տեխնոլոգիաներ. Անվտանգության ապահովման մեխանիզմներ. Տեղեկատվական Անվտանգության Կառավարման Համակարգեր. Պահանջներ» ստանդարտի պահանջներին,
- 2) Հայաստանի Հանրապետության օրենսդրության և Բանկի ներքին իրավական ակտերի պահանջներին ու պայմանագրային պարտավորություններին,
- 3) Բանկի ռիսկերի կառավարման քաղաքականությանը:

12. ՏԱԿՀ-ը կանոնակարգվում է Քաղաքականությամբ և դրա շրջանակներում

	Քաղաքականություն Տեղեկատվական անվտանգության	Կոդ: ՔԱՂ05 - 01 Խմբագրություն: 03 Դաս: ՀՊ Ամսաթիվ: «10» հուլիսի 2019թ.
---	--	---

ընդունված ներքին իրավական այլ ակտերով:

13. Բանկի ՏԱԿՀ-ի տարածման շրջանակները ներառում են Բանկի Գլխամասային գրասենյակը, տարածքային և կառուցվածքային ստորաբաժանումները, Բանկի գործունեության հետ առնչվող գործընթացները, Բանկի անձնակազմը, տեղեկատվության մշակման և պահպանման համակարգերը:
14. Բանկի բոլոր տեղեկատվական ակտիվները, ակտիվների տնօրինողները, ակտիվների պահպանողները և օգտագործողները՝ ներառյալ սարքավորումները, ծրագրային ապահովումը, թղթային և էլեկտրոնային կրիչներում առկա տեղեկատվական ռեսուրսները, ենթակա են հաշվառման և դասակարգման՝ համաձայն իրենց կարևորության և հասանելիության մակարդակի:
15. Տեղեկատվական անվտանգության ռիսկերի պարբերաբար գնահատումն իրականացվում է համաձայն Բանկի «Տեղեկատվական անվտանգության ռիսկերի կառավարման» ընթացակարգի: Դրա իրականացման ժամանակ հաշվի են առնվում տեղեկատվական անվտանգության խոցելիության և սպառնալիքների հնարավորությունները և նրանց ազդեցության աստիճանը Բանկի բիզնես-գործընթացների, ֆինանսական դրության և գործարար համբավի վրա:
16. Տեղեկատվական անվտանգության ռիսկերի գնահատման արդյունքում մշակվում է ռիսկերի կառավարման պլան, ընտրվում և կիրառվում են տեղեկատվության պաշտպանության կառավարման միջոցներ, այդ թվում՝ ՏԱԿՀ-ի անվտանգության ապահովման կազմակերպչական, ֆիզիկական, տեխնիկական, ծրագրային և ծրագրաապարատային միջոցներ:
17. Բանկի տեղեկատվական ակտիվների ֆիզիկական պաշտպանության համար ՏԱԿՀ-ի գործունեության սահմաններում սահմանվում են անվտանգության գոտիներ և միջոցներ են ձեռնարկվում չթույլատրված մուտքի կանխարգելման նպատակով:
18. Բանկը ձգտում է հայտնաբերել, հաշվի առնել և արձագանքել տեղեկատվական անվտանգության բնագավառում տեղի ունեցած միջադեպերին՝ համաձայն սահմանված ընթացակարգերի:
19. Բանկում սահմանված են տեղեկատվական համակարգերի էական խափանումներից կամ արտակարգ իրավիճակներից կրիտիկական բիզնես գործընթացների անընդհատության ապահովման և ՏԱԿՀ-ի աշխատունակության հսկողության ընթացակարգեր:
20. Բանկի աշխատողները ստանում են այն տեղեկատվությանը հասանելիության

	Քաղաքականություն Տեղեկատվական անվտանգության	Կոդ: ՔԱՂ05 - 01 Խմբագրություն: 03 Դաս: ՀՊ Ամսաթիվ: «10» հուլիսի 2019թ.
---	--	---

հնարավորություն, որն անհրաժեշտ է իրենց ֆունկցիոնալ պարտականությունների կատարման համար: Բանկը պարբերաբար իրականացնում է տեղեկատվական անվտանգության բնագավառում աշխատողների տեղեկացում, ուսուցում և որակավորման բարձրացում:

ԳԼՈՒԽ 3. ՏԵՂԵԿԱՏՎՈՒԹՅԱՆ ԳԱՂՏՆԱԳՐՄԱՆ ՎԵՐԱՀՍԿՈՒՄ

21. Բանկում իրականացվում է տեղեկատվության գաղտնագրում:

22. Գաղտնագրման բանալիների կիրառելի երկարությունը առնվազն 128 բիտ է (инициализация):

23. Գաղտնագրման բանալիների երկարությունը պարբերաբար վերանայվում է անվտանգության ապահովման և արդիականացման շրջանակներում, որքանով որ թույլատրում է ընտրված գաղտնագրման տեխնոլոգիան:

ԳԼՈՒԽ 4. ԳԱՂՏՆԱԳՐՄԱՆ ԲԱՆԱԼԻՆԵՐԻ ԿԱՌԱՎԱՐՈՒՄ

24. Բանկում գործող գաղտնագրման բանալիների և հավաստագրերի կառավարումը կատարվում է հետևյալ փուլերով՝

- 1) բանալիի գեներացում գաղտնագրման համակարգերի համար,
- 2) բաց բանալիների հավաստագրերի տրամադրում և ստացում,
- 3) բանալիների տարածում,
- 4) բանալիների պահպանում,
- 5) բանալիների փոխարինում կամ թարմացում,
- 6) վտանգված բանալիների հետ վարման որոշում,
- 7) բանալիների չեղյալ հայտարարում,
- 8) վնասված կամ կորցված բանալիների վերականգնում,
- 9) բանալիների կրկնօրինակում և արխիվացում,
- 10) բանալիների ոչնչացում,
- 11) բանալիների հիմնական միջոցառումների լոգավորում:

25. Բանկում գործող գաղտնագրման բանալիների փոփոխվում են առնվազն վեց ամիսը մեկ անգամ:

ԳԼՈՒԽ 5. ՏԵՂԵԿԱՏՎՈՒԹՅԱՆ ՀԱՍԱՆԵԼԻՈՒԹՅԱՆ ՎԵՐԱՀՍԿՈՒՄ

26. Տեղեկատվության, տեղեկատվության մշակման համակարգերին չարտոնված հասանելիության պաշտպանության նպատակով Բանկում կազմակերպվում է

	Քաղաքականություն Տեղեկատվական անվտանգության	Կոդ: ՔԱՂ05 - 01 Խմբագրություն: 03 Դաս: ՀՊ Ամսաթիվ: «10» հուլիսի 2019թ.
---	--	---

տեղեկատվության և տեղեկատվության մշակման համակարգերի հասանելիության վերահսկում:

27. Բանկի աշխատակիցներին և անհրաժեշտության դեպքում պայմանագրային հիմունքներով սպասարկման անձնակազմին տեղեկատվությանը և տեղեկատվության մշակման համակարգերին հասանելիությունը տրվում է համաձայն Բանկում ընդունված համապատասխան իրավական ակտերի:
28. Չարտոնված հասանելիության կանխման նպատակով Բանկում կիրառվում է անգործության ժամանակային սահմանափակում, որի արդյունքում ավտոմատ եղանակով արգելափակվում է համակարգը:
29. Բանկում առնվազն տարեկան կտրվածքով ստեղծվում է հանձնաժողով բաղկացած տարբեր ստորաբաժանումների ղեկավարներից և իրականացվում է իրավասությունների վերանայում՝ ստեղծելով տիպային իրավասությունների ցանկ՝ աշխատակիցների պաշտոնական պարտականություններին համապատասխան:

ԳԼՈՒԽ 6. ՄԱՔՈՒՐ ՍԵՂԱՆ ԵՎ ՄԱՔՈՒՐ ԷԿՐԱՆ

30. Տեղեկատվության չարտոնված հասանելիության պաշտպանության և արտահոսքի կանխման նպատակով Բանկում կիրառվում են հետևյալ մոտեցումները՝

- 1) Ոչ աշխատանքային ժամերին Բանկի գլխավոր գրասենյակում և ստորաբաժանումներում բոլոր փաստաթղթերը պետք է պահվեն համապատասխան երկաթյա կամ այլ փակվող պահարաններում:
- 2) Այն վայրերում, որտեղ անհասանելի են երկաթյա կամ այլ պահարաններ պետք է փակվեն սենյակների դռները՝ սենյակից դուրս գալու ժամանակ:
- 3) Մուտք եղած համակարգիչները և այլ տեղեկատվության մշակման համակարգերը չպետք է լինեն առանց հսկողության:
- 4) Համակարգիչների էկրանները պետք է տեղադրված լինեն այն դիրքով, որ կողմնակի անձանց հնարավոր չլինի դիտել էկրանի պարունակությունը:
- 5) Համակարգից հեռանալիս անհրաժեշտ է բլոկավորել համակարգիչը:
- 6) Բանկի աշխատողները աշխատանքային օրվա վերջում պետք է դուրս գան համակարգիչներում ակտիվացրած բոլոր համակարգերից և անջատեն համակարգիչները:

ԳԼՈՒԽ 7. ՏԵՂԵԿԱՏՎՈՒԹՅԱՆ ԿՐԻՉՆԵՐԻ ՈՉՆՉԱՑՈՒՄ

31. Տեղեկատվության կրիչ է համարվում այն կրիչը, որի մեջ պահվում է

	Քաղաքականություն Տեղեկատվական անվտանգության	Կոդ: ՔԱՂ05 - 01 Խմբագրություն: 03 Դաս: ՀՊ Ամսաթիվ: «10» հուլիսի 2019թ.
---	--	---

տեղեկատվությունը: Այդ կրիչների ցանկին են պատկանում՝

- 1) փաստաթղթերը,
- 2) կոշտ սկավառակները,
- 3) CD և DVD սկավառակները,
- 4) մագնիսական կրիչները,
- 5) ֆլեշ կրիչները,
- 6) հիշողության քարտերը և այլն:

32. Համաձայն Բանկում գործող ընթացակարգի և տեղեկատվությունը վերականգնելու հնարավորությունը բացառելու նպատակով կիրառվում է տեղեկատվության կրիչների ոչնչացման հետևյալ մոտեցումը՝

- 1) տեղեկատվության մաքրում/ջնջում, որն իրականացվում է DoD 5220.22-M ստանդարտի համապատասխան ծրագրային ապահովմամբ,
- 2) ֆիզիկական ոչնչացում, որն իրենից ներկայացնում է տեղեկատվության կրիչի այնպիսի կործանում, որի արդյունքում անհնար է դառնում տեղեկատվության վերականգնումը և կրիչի երկակի օգտագործումը:

ԳԼՈՒԽ 8. ՇԱՐԺԱԿԱՆ ՄՈՔԱՅԼ ՍԱՐՔԵՐԻ ԱՆՎՏԱՆԳՈՒԹՅՈՒՆ

33. Շարժական (մոբայլ) սարքերը հանդիսանում են Բանկի բիզնես գործընթացի կարևորագույն տարր, սակայն նրանց շարժական լինելը դարձնում է նրանց ավելի խոցելի սարքերի գողության և տեղեկատվության արտահոսքի տեսանկյունից:

34. Նման խոցելիությունների նվազեցման և բացառման նպատակով և Բանկում գործող ընթացակարգի համաձայն կիրառվում է շարժական (մոբայլ) սարքերի պաշտպանության հետևյալ մոտեցումները՝

- 1) շարժական (մոբայլ) սարքերի ֆիզիկական անվտանգության հսկողություն,
- 2) վիրուսներից և այլ վնասակար ծրագրերից հակավիրուսային պաշտպանություն,
- 3) շարժական (մոբայլ) սարքերի միջոցով Բանկի տեղեկատվության չարտոնված մուտքի վերահսկում:

ԳԼՈՒԽ 9. ՀԱՄԱԿԱՐԳՉԱՅԻՆ ՑԱՆՑԵՐԻ ԱՆՎՏԱՆԳՈՒԹՅՈՒՆ

35. Բանկի համակարգչային ցանցը հանդիսանում է կառավարման համակարգի, տեղեկատվության մշակման և փոխանցման կարևորագույն և անբաժանելի մաս, որի անվտանգության ապահովման նպատակով համաձայն գործող ընթացակարգերի Բանկում կիրառվում են վիրտուալ լոկալ ցանցեր (VLAN), միջցանցային էկրաններ, վիրտուալ մասնավոր ցանցեր, հակավիրուսային

	Քաղաքականություն Տեղեկատվական անվտանգության	Կոդ: ՔԱՂ05 - 01 Խմբագրություն: 03 Դաս: ՀՊ Ամսաթիվ: «10» հուլիսի 2019թ.
---	--	---

պաշտպանության համակարգ և այլ անվտանգության միջոցներ:

ԳԼՈՒԽ 10. ԳԱՂՏՆԱԲԱՌԵՐԻ ԿԱՌԱՎԱՐՈՒՄ

36. Գաղտնաբառերի պաշտպանության և կառավարման նպատակով Բանկում կիրառվում են հետևյալ մոտեցումները՝

- 1) արգելվում է պահպանել գաղտնաբառերը թղթի վրա, ծրագրային ֆայլի կամ շարժական սարքի մեջ,
- 2) այլ անձանց կողմից գաղտնաբառը կռահելու կասկածի դեպքում անհրաժեշտ է փոխել գաղտնաբառը,
- 3) Գաղտնաբառերի ստեղծման նվազագույն պահանջներն են՝
 - ա. պետք է լինի հեշտ հիշվող ստեղծողի համար,
 - բ. արգելվում է գաղտնաբառի ստեղծման ժամանակ հիմնվել անվան, հեռախոսահամարի կամ այլ տվյալի վրա, որը հեշտ կռահվող է այլ անձանց կողմից,
 - գ. չպետք է լինի զգայուն բառարանային հարձակումների հանդեպ,
 - դ. պետք է պարունակի թվային և տառային սիմվոլներ,
 - ե. պետք է փոխարինվի առաջին գրանցման ժամանակ,
- 4) արգելվում է գաղտնաբառի տրամադրումը այլ աշխատակցի,
- 5) արգելվում է հիշեցնել գաղտնաբառերը համակարգչային ծրագրերում ավտոմատ մուտք գործելու նպատակով,
- 6) արգելվում է օգտագործել նույն գաղտնաբառը մի քանի համակարգերի համար:

37. Տեղեկատվական անվտանգության ապահովման նպատակով Բանկում համակարգչային տեխնիկայի և տեղեկատվության մշակման համակարգերի գաղտնաբառերը փոփոխվում են համաձայն Բանկում գործող ընթացակարգի:

ԳԼՈՒԽ 11. ՏԵՂԵԿԱՏՎՈՒԹՅԱՆ ԴԱՍԱԿԱՐԳՈՒՄ

38. Տեղեկատվության պաշտպանության նպատակով, համաձայն Բանկում ընդունված կարգի, կիրառվում է տեղեկատվության դասակարգում:

ԳԼՈՒԽ 12. ՖԻԶԻԿԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅՈՒՆ

39. Ֆիզիկական անվտանգության ապահովման նպատակով համաձայն Բանկում ընդունված ընթացակարգի կիրառվում է անվտանգության գոտիներ:

	Քաղաքականություն Տեղեկատվական անվտանգության	Կոդ: ՔԱՂ05 - 01 Խմբագրություն: 03 Դաս: ՀՊ Ամսաթիվ: «10» հուլիսի 2019թ.
---	--	---

ԳԼՈՒԽ 13. ԱԿՏԻՎՆԵՐԻ ԸՆԴՈՒՆԵԼԻ ՇԱՀԱԳՈՐԾՈՒՄ

40. Տեղեկատվական ակտիվների պաշտպանության նպատակով՝ համաձայն Բանկում ընդունված ընթացակարգի կիրառվում է ակտիվների ընդունելի շահագործման կանոններ:

ԳԼՈՒԽ 14. ՏԵՂԵԿԱՏՎՈՒԹՅԱՆ ՓՈԽԱՆՑՈՒՄ

41. Տեղեկատվության պաշտպանության նպատակով, համաձայն Բանկում ընդունված ընթացակարգի, կիրառվում է տեղեկատվության փոխանցման կանոններ:

ԳԼՈՒԽ 15. ԾՐԱԳՐԱՅԻՆ ԱՊԱՀՈՎՄԱՆ ՏԵՂԱԴՐՄԱՆ ԵՎ ՕԳՏԱԳՈՐԾՄԱՆ ՍԱՀՄԱՆԱՓԱԿՈՒՄՆԵՐ

42. Չարամիտ ծրագրերի տեղադրումից և օգտագործումից խուսափելու նպատակով Բանկում, համաձայն ընդունված ընթացակարգի, կիրառվում է ծրագրային ապահովման տեղադրման և օգտագործման սահմանափակումներ:

ԳԼՈՒԽ 16. ԿՐԿՆՕՐԻՆԱԿՈՒՄ

43. Տեղեկատվության կորստի բացառելու նպատակով, համաձայն Բանկում ընդունված ընթացակարգի, կիրառվում է տեղեկատվության կրկնօրինակում:

ԳԼՈՒԽ 17. ՉԱՐԱՄԻՏ ԾՐԱԳՐԵՐԻՑ ՊԱՇՏՊԱՆՈՒԹՅՈՒՆ

44. Չարամիտ ծրագրերից պաշտպանության նպատակով Բանկում կիրառվում է ծրագրային ապահովման թույլատրելի ցուցակ՝ համաձայն Բանկում ընդունված ընթացակարգերի:

ԳԼՈՒԽ 18. ԽՈՑԵԼԻՈՒԹՅՈՒՆՆԵՐԻ ԿԱՌԱՎԱՐՈՒՄ

45. Խոցելիությունների կառավարման նպատակով Բանկում կիրառվում են խոցելիությունների հայտնաբերման համակարգեր, որոնց հայտնաբերած տվյալների հիման վրա գնահատվում են տեղեկատվական անվտանգության ռիսկերը և արդյունքում, համաձայն Բանկում ընդունված ընթացակարգերի, այդ

	Քաղաքականություն Տեղեկատվական անվտանգության	Կոդ: ՔԱՂ05 - 01 Խմբագրություն: 03 Դաս: ՀՊ Ամսաթիվ: «10» հուլիսի 2019թ.
---	--	---

ռիսկերը կառավարվում և նվազեցվում են:

ԳԼՈՒԽ 19. ԱՆՁՆԱԿԱՆՏԵՂԵԿԱՏՎՈՒԹՅԱՆ ԳԱՐՏՆԻՈՒԹՅՈՒՆ ԵՎ ՊԱՇՏՊԱՆՈՒԹՅՈՒՆ

46. Անձնական տեղեկատվության գաղտնիությունը և պաշտպանությունը Բանկում կիրառվում է համաձայն ՀՀ օրենսդրության պահանջների:

ԳԼՈՒԽ 20. ԲԱՆԿԻՆ ԾԱՌԱՅՈՒԹՅՈՒՆՆԵՐ ՄԱՏՈՒՑՈՂ ԿԱԶՄԱԿԵՐՊՈՒԹՅՈՒՆՆԵՐԻ ՀԵՏ ՀԱՐԱՔԵՐՈՒԹՅՈՒՆՆԵՐ

47. Այն կազմակերպությունների հետ, որոնք Բանկին մատուցում են ծառայություն և ունեն տեղեկատվությանը կամ տեղեկատվության մշակման համակարգերին հասանելիություն, պետք է կնքվեն տեղեկատվության չբացահայտման և գաղտնիության համաձայնագրեր:

ԲԱԺԻՆ III. ՊԱՏԱՍԽԱՆԱՏՎՈՒԹՅՈՒՆԸ ՔԱՂԱՔԱԿԱՆՈՒԹՅԱՆ ՊԱՀԱՆՋՆԵՐԸ ԽԱԽՏԵԼՈՒ ՀԱՄԱՐ, ԵԶՐԱՓԱԿԻՉ ԴՐՈՒՅԹՆԵՐ

ԳԼՈՒԽ 1. ՊԱՏԱՍԽԱՆԱՏՎՈՒԹՅՈՒՆԸ ՔԱՂԱՔԱԿԱՆՈՒԹՅԱՆ ՊԱՀԱՆՋՆԵՐԸ ԽԱԽՏԵԼՈՒ ՀԱՄԱՐ

48. Բանկի աշխատողները կրում են անհատական պատասխանատվություն ՏԱԿՀ-ի պահանջների պահպանման համար և պարտավոր են տեղեկացնել ՏԱՊ-ին տեղեկատվական անվտանգության ոլորտում հայտնաբերված ցանկացած խախտման վերաբերյալ:

49. Աշխատողների աշխատանքային պայմանագրերում և պաշտոնեական հրահանգներում սահմանվում է պատասխանատվություն ծառայողական փաստաթղթերի և գաղտնի տեղեկատվության պահպանման համար, որն աշխատողներին հայտնի է դառնում իրենց աշխատանքային պարտականությունների կատարման ընթացքում:

50. Բանկի ղեկավարությունն իրականացնում է Բանկի տեղեկատվական անվտանգության ընդհանուր կառավարում և ապահովում է անհրաժեշտ

	Քաղաքականություն Տեղեկատվական անվտանգության	Կոդ: ՔԱՂ05 - 01 Խմբագրություն: 03 Դաս: ՀՊ Ամսաթիվ: «10» հուլիսի 2019թ.
---	--	---

պայմաններ հետևյալի համար՝

- 1) տեղեկատվական անվտանգության ռիսկերի գնահատմանը և տեղեկատվության պաշտպանությանն ուղղված միջոցառումների իրականացման,
- 2) ՏԱԿՀ աշխատանքի արդյունավետության,
- 3) տեղեկատվական անվտանգության ոլորտում Բանկի աշխատողների պարբերաբար ուսուցման և վերապատրաստման,
- 4) ՏԱԿՀ բնականոն գործունեության համար անհրաժեշտ ռեսուրսների հատկացման:

ԳԼՈՒԽ 2. ԵԶՐԱՓԱԿԻՉ ԴՐՈՒՅԹՆԵՐ

51. Բանկը կարևորում է ՏԱԿՀ շարունակական զարգացումը և բարելավումը:

52. Բանկի ղեկավարությունն ուղղակի պատասխանատվություն է կրում Քաղաքականության պահանջների կատարման և իրենց ենթակայության տակ գտնվող աշխատողների, ներառյալ պայմանագրային հիմունքներով աշխատանքներ իրականացնող և/կամ ծառայություններ մատուցող անձանց կողմից սահմանված պահանջներին համապատասխանության համար, ովքեր ունեն հասանելիություն Բանկի ենթակառուցվածքներին և իրենց պարտականությունների կատարման ընթացքում օգտվում են դրանցից:

53. Քաղաքականությունը կարող է տրամադրվել բոլոր շահագրգիռ կողմերին և տեղադրվել Բանկի պաշտոնական տեղեկատվական կայքում՝ քաղվածքի կամ ամբողջական տեսքով:

54. Քաղաքականության դրույթների կատարման նկատմամբ ընդհանուր հսկողությունն իրականացնում է Անվտանգության վարչությունը, իսկ վերահսկողությունը՝ Ներքին աուդիտի վարչությունը: