«ԱՄԻՕ ԲԱՆԿ» ՓԲԸ
ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՀԱՅՏԱՐԱՐԱԳԻՐ

(քաղվածք Տեղեկատվական անվտանգության քաղաքականությունից)

Հաստատող մարմին	**Խորհուրդ**
Խմբագրություն	2.1
Ուժի մեջ մտնելու ամսաթիվ	06/04/2026

1. ԿԱՐԳԱՎՈՐՄԱՆ ԱՌԱՐԿԱ

«ԱՄԻՕ ԲԱՆԿ» ՓԲԸ-ի «Տեղեկատվական անվտանգության քաղաքականությունը» հանդիսանում է տեղեկատվական անվտանգության ոլորտում նպատակների, խնդիրների, սկզբունքների և մոտեցումների ամբողջական համակարգ, որով Բանկն առաջնորդվում է իր գործունեության ընթացքում՝ ապահովելու Բանկի կողմից մշակվող, պահպանվող, ներկայացվող, ստացվող, փոխանցվող և Բանկում շրջանառվող տեղեկատվության, համակարգերի, միջոցների, ծրագրերի, տվյալների, ցանցային համակարգերի, ֆիզիկական պաշտպանության համակարգերի և անձնակազմի պաշտպանությունը հնարավոր սպառնալիքներից՝ չթույլատրված մուտքից, օգտագործումից, հրապարակումից, խեղաթյուրումից, փոփոխումից կամ ոչնչացումից:

2. ԿԻՐԱՌՄԱՆ ՈԼՈՐՏ

Քաղաքականությունը տարածվում է Բանկի բոլոր ստորաբաժանումների վրա, որոնք տեղեկատվական ակտիվների կրողներ են:

Սույն քաղաքականության կիրառումը պարտադիր է Բանկի բոլոր կառավարման մարմինների, ղեկավարների, տարածքային և կառուցվածքային

Ստորաբաժանումների, ֆիզիկական, իրավաբանական անձերի և անհատ ձեռնարկատերերի համար, որոնց հետ Բանկն ունի կնքված համագործակցության, աշխատանքների կատարման, ծառայությունների մատուցման, առուվաճառքի, մատակարարման պայմանագրեր՝ իրենց գործառույթների և պատասխանատվությունների շրջանակներում:

3. ԱՌՆՉՎՈՂ ՓԱՍՏԱԹՂԹԵՐ

Քաղաքականությունն անմիջականորեն առնչվում է «Բանկերի և բանկային գործունեության մասին» ՀՀ օրենքի, բանկային գործունեությունը կանոնակարգող արտաքին իրավական ակտերի, «Կիբեռանվտանգության մասին» ՀՀ օրենքի, «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի, ինչպես նաև Տեղեկատվության անվտանգության համակարգի կիրառմանը առնչվող այլ օրենքների, ենթաօրենսդրական ակտերի և միջազգային ստանդարտների հետ:

4. ՆԿԱՐԱԳՐՈՒԹՅՈՒՆ

Բանկի Իրավաբանական հասցեն է՝ ՀՀ, ք. Երևան, Նալբանդյան 48, հեռ.՝ (374 10) 59-20-20, Փոստային ինդեքս՝ 0010, էլ. փոստ՝ info@amiobank.am, վեբ կայք՝ www.amiobank.am:

Տեղեկատվական անվտանգության կառավարման համակարգի հիմնական խնդիրն առկա Սպառնալիքների պայմաններում՝ Բանկի տեղեկատվական ակտիվների պաշտպանվածության ընդունելի մակարդակի ապահովումն է՝ Տեղեկատվական անվտանգության ոլորտը կանոնակարգող արդյունավետ պահանջների, կանոնների սահմանման և տեխնիկա–ծրագրային միջոցների ներդրման միջոցով:

Տեղեկատվական անվտանգության կառավարման համակարգի կառուցման հիմնական սկզբունքներն են՝ համապատասխանությունը՝

- ՀՀ գործող օրենսդրությանը և նորմատիվ իրավական ակտերին.

- Բանկի պայմանագրային պարտավորություններին՝ տեղեկատվական անվտանգության տեսանկյունից.
- Տեղեկատվականղ անվտանգությունը կարգավորող ստանդարտների պահանջներին, այդ թվում նաև՝ ISO 27001:2022, PCI DSS.

Բանկի Տեղեկատվական անվտանգության կառավարման համակարգը գործում է Բանկի գլխամասային գրասենյակի և Բանկի տարածքային ստորաբաժանումների ողջ տարածքում: Ընդգրկում է, առանց բացառությունների, Բանկի բոլոր գործառույթները, գործընթացները և ծառայությունները և ողջ անձնակազմը:

Բանկն իր տեղեկատվական ակտիվների պաշտպանության կազմակերպման՝ որպես առավել արդյունավետ մեթոդ, ընդունում է կանխարգելող մոտեցումը: Այն է՝

- Տեղեկատվական անվտանգության ապահովման տեսանկյունից Բանկի համար ամբողջությամբ, ինչպես նաև յուրաքանչյուր համակարգի համար առանձին - առանձին կատարվում է հնարավոր Սպառնալիքների համակարգային վերլուծություն, վտանգների մոդելավորում և դասակարգում, ռիսկերի համալիր գնահատում, համակարգի ողջ կենսական ցիկլի ընթացքում,
- Համակարգչային ցանցերի տարանջատում,
- անվտանգության ապահովման հարցում Բանկի բոլոր ստորաբաժանումների մասնակցություն,
- Տեղեկատվական ակտիվների անվտանգության ու պաշտպանության ապահովում,
- Վեբ զտման միջոցառումներ,
- Տվյալների քողարկման մեթոդներ,
- Տվյալների արտահոսքի կանխարգելման միջոցառումներ,
- Ֆիզիկական անվտանգության մոնիթորինգ,
- Տեղեկատվական ակտիվների գույքագրում և դասակարգում,
- Տեղեկատվության անվտանգ ջնջման մեխանիզմներ,
- Քարտապանների տվյալների և քարտային գործառությունների անվտանգության ապահովման հետ կապված միջոցառումների առկայություն,

- Տեղեկատվական անվտանգության հարցերով անձնակազմի իրազեկում, ուսուցում, որակավորման ստուգում:

Բանկն իրականացնում է ռիսկերի կառավարման ոլորտում ընդունված ընթացակարգերին համապատասխան՝ խոցելիությունների և վտանգների վերլուծության հիման վրա Տեղեկատվական անվտանգության ռիսկերի պարբերական գնահատում: Ռիսկերի գնահատման ժամանակ հաշվի են առնվում Տեղեկատվական անվտանգության սպառնալիքների հավանականությունը, բիզնես-գործընթացների վրա դրանց ազդեցության աստիճանը, Բանկի ֆինանսական վիճակը և գործարար համբավը:

Բանկի աշխատակիցների աշխատանքային պայմանագրերով, Ներքին իրավական ակտերով և ՀՀ գործող օրենսդրությամբ ամրագրվում է աշխատակցի պատասխանատվությունը՝ աշխատանքի ընթացքում նրան հասանելի դարձած սահմանափակ օգտագործման տեղեկատվության հրապարակման համար: