«ԱՄԵՐԻԱԲԱՆԿ» ՓԲԸ ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՔԱՂԱՔԱԿԱՆՈՒԹՅՈՒՆ

(քաղվածք «Ամերիաբանկ» ՓԲԸ տեղեկատվական անվտանգության քաղաքականությունից՝ ընդունված բանկի Տնօրենների Խորհրդի 21.12.2020.թ. թիվ 11-3/20/06 որոշմամբ)

1. Ընդհանուր դրույթներ

1.1. «Ամերիաբանկ» ՓԲԸ /այսուհետ՝ «Բանկ»/ կողմից որդեգրվել է «ISO 27001:2013 Տեղեկատվական Անվտանգության Կառավարման Համակարգ» ստանդարտը /այսուհետ՝ Ստանդարտ/, որը տարածվում է Բանկի կողմից իրականացվող բոլոր, ներառյալ, սակայն չսահմանափակվելով Բանկի կողմից տեղեկատվական տեխնոլոգիաների կիրառմամբ մշակվող, պահպանվող, ներկայացվող, ստացվող և Բանկին հասու ամբողջ տեղեկատվության /տեղեկատվական ակտիվների/, տեղեկատվական ենթակառուցվածքի, տեխնոլոգիաների, համակարգերի, միջոցների, ծրագրերի հետ կապված, գործառույթների վրա:

1.2. Բանկի ղեկավարությունը գիտակցում է տեղեկատվական անվտանգության ապահովմանն ուղղված միջոցների ներդրման, ապահովման և դրանց կատարելագործման կարևորությունը բանկի գործունեության անընդհատության ապահովման, հաճախորդին բարձրակարգ սպասարկման և Բանկի հեղինակության համար:

1.3. Բանկի աշխատակիցները պահպանում են ՀՀ գործող օրենսդրության և տեղեկատվական անվտանգության վերաբերյալ Բանկի ներքին իրավական ակտերի պահանջները:

1.4. Բանկը, հանդիսանալով Բանկում ձևավորված և/կամ մշակված, ինչպես նաև Բանկի կողմից օրինական ճանապարհով /ներառյալ՝ նվիրատվության, ժառանգության, իրավահաջորդության կամ այլ հիմքերով/ ձեռք բերված տեղեկատվության /ներառյալ՝ այդպիսի տեղեկատվություն պարունակող փաստաթղթերի, թղթային կամ էլեկտրոնային կրիչների և ծրագրային ապահովման իրավատերը, իրավասու է տիրապետել, օգտագործել և տնօրինել այդ տեղեկատվությունը կամ ծրագրային ապահովումը այնքանով, որքանով այդպիսի տիրապետումը, օգտագործումը և տնօրինումը չի հակասում ՀՀ օրենսդրությանը, Բանկի ներքին իրավական ակտերին, չի խախտում Բանկի պարտավորությունները:

1.5. Ստանդարտի պահանջները մանրամասն կարգավորվում և ներկայացվում են Բանկի կողմից մշակվող և հաստատվող համապատասխան ներքին ակտերով:

2. Տեղեկատվական անվտանգության ապահովման նպատակներն ու խնդիրները

2.1. Տեղեկատվական անվտանգության ապահովման գլխավոր նպատակն է ապահովել Բանկի գործունեության անընդհատությունը և պաշտպանել Բանկում մշակվող,

պահպանվող և փոխանցվող Բանկին, վերջինիս բաժնետերերին, ներդրողներին և հաճախորդներին պատկանող տեղեկատվությունը պատահական և կանխամտածված ոտնձգություններից, հրապարակումից, կորստից, արտահոսքից, խեղաթյուրումից, փոփոխությունից և ոչնչացումից՝ նվազեցնելով վերջիններիս նյութական, ֆիզիկական, բարոյական կամ այլ վնաս պատճառելու հավանականությունն ու ռիսկերը:

2.2. Բանկի տեղեկատվական անվտանգության ապահովման հիմնական խնդիրներն են.

- Բանկի տեղեկատվական անվտանգությանը սպառնացող և պոտենցիալ վտանգների և խոցելիությունների, սպառնալիքների աղբյուրների ժամանակին բացահայտումը, գնահատումը, կանխատեսումը և կանխումը,
- Հայտնաբերված խոցելիությունների և վտանգների իրագործման արգելափակումը կամ, առնվազն, իրագործման հնարավորության նվազեցումը, այդ թվում սպառնալիքներին արագ արձագանքման մեխանիզմների ներդրումը և կիրառումը,
- Բանկի տեղեկատվական համակարգերի, ռեսուրսների և դրանց գործունեության պաշտպանությունը կողմնակի անձանց մուտքից (հասանելիությունից) և անօրինական միջամտությունից (տեղեկատվական ռեսուրսների հասանելիություն պետք է ունենան միայն համապատասխան կարգով գրանցված և լիազորված օգտագործողները), Բանկի տեղեկատվական համակարգերի և ռեսուրսների օգտագործողների ամբողջական պատշաճ նույնականացման ապահովում,
- Բանկի կորպորատիվ տեղեկատվական համակարգի միջավայրում կիրառվող ծրագրային ապահովման պաշտպանությունը չլիազորված կարգաբերումներից, ձևափոխություններից, ինչպես նաև համակարգերի պաշտպանությունը չլիազորված ծրագրային ապահովման տեղադրումից, այդ թվում ծրագրային ապահովման տեղադրման, խմբագրման/ձևափոխման իրավասություններ ունեցող անձնակազմի բոլոր գործողությունների գրանցում,
- Տեղեկատվական անվտանգության կառավարման համակարգի ներդրումը, կիրառումը և շարունակական կատարելագործումը,
- Տեղեկատվական անվտանգության վերաբերյալ անձնակազմի իրազեկվածության պատշաճ մակարդակի ապահովումը և աշխատակիցների ուսուցումը,
- Բանկի՝ Տեղեկատվական ակտիվների հաշվառման ապահովումը:

3. Պատասխանատվություն

3.1. Բանկի հետ համագործակցող ֆիզիկական և իրավաբանական անձանց կողմից ստանդարտի պահանջների չկատարման/չպահպանման կամ ոչ պատշաճ կատարման/պահպանման, ներառյալ՝ համագործակցության շրջանակներում այդ անձանց հայտնի դարձած Գաղտնի (գաղտնիք կազմող) կամ փակ տեղեկատվության հրապարակման, համար պատասխանատվությունը կարգավորվում է համապատասխան անձանց հետ կնքված պայմանագրերով և կիրառելի օրենսդրությամբ: