ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԿԱՌԱՎԱՐՄԱՆ ՀԱՄԱԿԱՐԳԵՐԻ ՈԼՈՐՏԱՅԻՆ ՔԱՂԱՔԱԿԱՆՈՒԹՅՈՒՆԸՆ ԱՄՊԱՅԻՆ ԾԱՌԱՅՈՒԹՅՈՒՆՆԵՐԻ ՏՐԱՄԱԴՐՄԱՆ ԺԱՄԱՆԱԿ

Ամպային ծառայությունների տրամադրման ժամանակ տեղեկատվական ակտիվների անվտանգության ապահովումը «ՋԻԷՆՍԻ-ԱԼՖԱ» ՓԲԸ-ի (այսուհետ՝ Ընկերություն) ղեկավարության կողմից սահմանվում է՝ որպես Ընկերության գործունեության իրականացման առանցքային պայման:

Տեղեկատվական անվտանգության ապահովումն Ընկերությանն անհրաժեշտ է Պատվիրատուների առջև ստանձնած պայմանագրային պարտավորությունները կատարելու, Ընկերության մրցունակությունը պահպանելու, Ընկերության տեղեկատվական անվտանգության քաղաքականության, օրենսդրության և նորմատիվ բազայի պահանջներին համապատասխանությունն ապահովելու, ինչպես նաև Ընկերության՝ որպես հուսալի Կատարողի և Գործընկերոջ գործարար համբավի ձևավորման համար:

«ՋԻԷՆՍԻ-ԱԼՖԱ» ՓԲԸ-ի կողմից ամպային ծառայությունների մատուցման ժամանակ Տեղեկատվական անվտանգության կառավարման համակարգի ոլորտի սույն Քաղաքականությունը (այսուհետ՝ Քաղաքականություն) տարածվում է Ընկերության տեղեկատվական անվտանգության կառավարման համակարգի (այսուհետ՝ ՏԱԿՀ) վրա՝ ամպային ծառայությունների մատուցման ժամանակ:

ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԿԱՌԱՎԱՐՄԱՆ ՀԱՄԱԿԱՐԳ

Ընկերությունում ներդրված ՏԱԿՀ-ն, որը համապատասխանում է ISO/IEC 27001:2022, ISO/IEC 27017:2015, ISO/IEC 27018:2019 և PCI DSS միջազգային չափորոշիչների պահանջներին, կոչված է ապահովելու տեղեկատվական անվտանգության արդյունավետ կառավարումը ամպային ծառայությունների մատուցման ժամանակ:

ՏԱԿՀ կիրառման շրջանակը ներառում է Ընկերության տեղեկատվական ակտիվները և դրա շրջանակներում գործող գործընթացները, որոնք ներկայացված են փաստաթղթավորված տեղեկատվության տեսքով և ուղղված են ինչպես Պատվիրատուների, այնպես էլ ինքնին Ընկերության տեղեկատվական ակտիվների պաշտպանությանը՝ ամպային ծառայություններ մատուցելիս:

Սույն Քաղաքականության դրույթներն իրականացնելու համար Ընկերությունում ներդրված տեղեկատվական անվտանգության ապահովման և կառավարման մասով գործընթացային մոտեցումը փաստաթղթավորված է ՏԱԿՀ գործընթացային մոդելի ձևաչափով: Յուրաքանչյուր գործընթացին համապատասխանում են տեղեկատվական անվտանգության մասով Ընկերության կոնկրետ ներքին նորմատիվ փաստաթղթեր:

ՏԱԿՀ-ը ակտիվների համատեղ անվտանգ օգտագործման, էլեկտրոնային գործառնությունների իրականացման, ինչպես նաև տեղեկատվական ռիսկերը մինչև ընդունելի մակարդակը նվազեցնելու հնարավորություն ապահովող մեխանիզմ է:

ՏԱԿՀ գործընթացների իրականացման շրջանակներում հիմնարար է հետևյալ գործունեությունը.

- Ընկերության ակտիվների, ներառյալ սահմանափակ հասանելիության տեղեկատվության կանխամտածված կամ պատահական չարտոնված մուտքի կանխարգելում,
- ակտիվների հասանելիության ապահովում նույնականացված օգտատերերի համար այն ժամանակ, երբ դրանք անհրաժեշտ են նրանց, սպառնալիքների ժամանակին հայտնաբերում և արձագանքում, որոնք կարող են հանգեցնել ակտիվների անհասանելիության,
- տվյալների դիտավորյալ կամ պատահական, մասնակի կամ լրիվ չարտոնված կերպափոխությունների կամ ոչնչացման կանխարգելում,
- բիզնեսի, վթարից հետո Ընկերության տեղեկատվական համակարգերի աշխատունակության վերականգնման ընթացակարգերի, տվյալների պահուստային պատճենման և վերականգնման ընթացակարգերի, վնասակար ԾԱ-ից և ցանցային գրոհներից պաշտպանության շարունակականության ապահովման ծրագրերի , հասանելիության վերահսկման, անվտանգության միջադեպերի կառավարման և միջադեպերի ծանուցման, փոփոխությունների և կատարելագործման ծրագրերի մշակում և կառավարում,
- ՏԱԿՀ կանոնավոր վերանայում և կատարելագործում:

Ընկերության նպատակներն են.

- Ընկերությունում պայմանների ստեղծումն ու մշտական աջակցումը, որի դեպքում Ընկերության ակտիվների անվտանգության ապահովման հետ կապված ռիսկերը, այդ թվում՝ կապված ամպային ծառայությունների տեխնիկական և շահագործման բնութագրերի հետ, մշտապես վերահսկվում և

գտնվում են ընդունելի մակարդակի վրա՝ ՏԱ հիմնական տիրույթների ՝ ամբողջականության, հասանելիության, մասնավորության և գաղտնիության ապահովման հաշվին,

- ՏԱ ապահովման միջոցների իրականացման ղեկավար սկզբունքների, այդ թվում՝ ամպային ծառայություններին հատուկ, ամպային ծառայությունների սպառողների և մատակարարների միջև փոխհարաբերություններում ՏԱ սպառնալիքների և ռիսկերի սահմանումը,
- գաղտնի տեղեկատվության պաշտպանությունը (այդ թվում՝ ամպային ծառայություններից օգտվելիս)՝ Հայաստանի Հանրապետության գործող օրենսդրության, միջազգային օրենսդրության պահանջներին, ոլորտային պահանջներին և ՏԱ կառավարման լավագույն փորձառությանը համապատասխան, այդ թվում՝ ՏԱ սպառնալիքների և ռիսկերի ամպային ծառայություններին հատուկ,
- անձնական տվյալների պաշտպանության կիրառելի օրենսդրությանը և պայմանագրային պայմաններին համապատասխանության ձեռքբերում, որոնք համաձայնեցված են Ընկերության՝ որպես ամպային ծառայությունների մատակարարի և անձնական տվյալներ մշակողի և նրա հաճախորդների (ամպային ծառայությունների սպառողների) միջև,
- ՏԱ ապահովման կատեգորիաների, միջոցների ամբողջության ստեղծում, որոնք կարող են իրականացվել Ընկերության՝ որպես ամպային ծառայությունների մատակարարի և որպես անձնական տվյալներ մշակողի կողմից,
- Ընկերության ամպային ծառայությունների մատուցման շարունակականության ապահովում,
- Ընկերության ՏԱԿՀ-ի մշտական բարելավում՝ ՏԱ պահանջներին և բիզնեսի պահանջներին համապատասխան:

Տեղեկատվական անվտանգության թիրախային ցուցանիշներն Ընկերությունում սահմանվում են հետևյալ ռազմավարական առաջադրանքների հիման վրա.

- Ընկերության կայուն գործունեություն, որը երաշխավորում է սահմանված նպատակների իրագործում,
- Ընկերությանը, նրա Պատվիրատուներին և Գործընկերներին պատկանող ակտիվների պաշտպանության ապահովում,
- Ընկերությանը վստահված անձնական տվյալների պաշտպանության ապահովում,
- տեղեկատվական անվտանգության բնագավառում Հայաստանի Հանրապետության օրենսդրության, հայկական և միջազգային չափորոշիչների պահանջներին Ընկերության գործունեության համապատասխանության ապահովում,
- Ընկերության Պատվիրատուների և Գործընկերների կողմից տեղեկատվական անվտանգության ապահովման առումով արդիական պահանջների ընդունում և կատարում,
- Ընկերության ՏԱԿՀ մշտական բարելավում՝ ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2019 և PCI DSS միջազգային չափորոշիչների պահանջներին համապատասխան:

Տեղեկատվական անվտանգության թիրախային ցուցանիշները ձեռք են բերվում հետևյալ եղանակով.

- տեղեկատվական անվտանգության ոլորտում պահանջների և ակնկալվող արդյունքների հստակ սահմանման,
- տեղեկատվական անվտանգության ռիսկերի կառավարման հիման վրա մշակված տեղեկատվական ակտիվների պաշտպանության միջոցների համալիրների իրականացման,
- ՏԱՀԿ-ն իր իրական և արդյունավետ գործառնույթան համար անհրաժեշտ պաշարներով ապահովելու,
- Տեղեկատվական անվտանգության ոլորտում սույն Քաղաքականության և Նպատակների պահանջների կատարման մասով արդյունավետության, արգասաբերության պարբերական գնահատում իրականացնելու,
- Ընկերության ղեկավարությանը գնահատման արդյունքների մասին տեղեկացնելու՝ հետագա վերլուծության և որոշումների կայացման համար,
- շարունակական կատարելագործման նպատակով ներքին աուդիտի արդյունքների կամ այլ համապատասխան տեղեկատվության վրա հիմնված շտկող և նախազգուշական գործողությունների մշտական իրականացման,
- հավաստագրման անկախ մարմնի ուժերով իրականացվող հսկիչ աուդիտի արդյունքներով

գործող ՏԱՀԿ-ի՝ ISO/IEC 27001:2022, ISO/IEC 27017:2015, ISO/IEC 27018:2019 և PCI DSS միջազգային չափորոշիչների պահանջներին համապատասխանության ամենամյա հաստատման,

«ՋԻԷՆՍԻ-ԱԼՖԱ» ՓԲԸ-ի ղեկավարությունը պատասխանատվություն է ստանձնում Ընկերության բոլոր աշխատողների կողմից սույն Քաղաքականության իրագործման և դրանում շարադրված սկզբունքների անշեղորեն կատարման համար:

ՏԱԿՀ արդիականությունն ու արդյունավետությունը և իր գործունեության պայմաններին համապատասխանությունը պահպանելու նպատակով Ընկերությունն իրականացնում է սույն Քաղաքականության կանոնավոր վերանայում:

Ընկերության կողմից կարող է նախաձեռնվել նաև սույն Քաղաքականության վերանայում՝ ռիսկերի վերլուծման, տեղեկատվական անվտանգության պահանջներին համապատասխանության աուդիտների, ՏԱԿՀ-ում փոփոխությունների ներդրման արդյունքների հիման վրա: