Տեղեկատվական անվտանգության քաղաքականությունը (այսուհետ՝ Քաղաքականություն) «ՋԻԷՆՍԻ-ԱԼՖԱ» ՓԲԸ-ի (այսուհետ՝ Ընկերություն) տեղեկատվական անվտանգության (ՏԱ) կառավարման համակարգի (ՏԱԿՀ) մասն է:

Քաղաքականությունը սահմանում է Ընկերության ՏԱ ապահովման բարձր մակարդակի նպատակները, բովանդակությունը և գործունեության հիմնական ուղղությունները: Քաղաքականության դրույթները հիմնարար են և մանրամասն ներկայացված են ՏԱ մեկ կամ մի քանի ոլորտների, Ընկերության գործունեության տեսակների և տեխնոլոգիաների և ՏԱ ապահովման այլ նորմատիվ փաստաթղթերում:

Քաղաքականության ազդեցությունը տարածվում է Ընկերության բոլոր տեղեկատվական ակտիվների վրա՝ անկախ դրանց տեղակայման և օգտագործման վայրից: Քաղաքականության պահանջները պարտադիր են Ընկերության ողջ անձնակազմի, ինչպես նաև Ընկերության տեղեկատվական ակտիվներին հասանելիություն ունեցող գործընկեր կազմակերպությունների անձնակազմի կատարման համար:

Քաղաքականությունը մշակվել է ՏԱ մասով միջազգային չափորոշիչներին և հանձնարարականներին, միջազգային իրավունքի կիրառելի նորմերին, Ընկերության ներկայության երկրների օրենսդրության, ներառյալ ընկերության գտնվելու վայրի երկրին, Ընկերության ներքին նորմատիվ-իրավական բազայի դրույթներին համապատասխան, այդ թվում՝

- Ընկերության տեղեկատվական անվտանգության և ռիսկերի կառավարման հայեցակարգին,
- Ընկերությունում անձնական տվյալների մշակման քաղաքականությանը,
- ISO/IEC 27001:2022, Տեղեկատվական անվտանգություն, կիբերանվտանգություն և անձնական տվյալների պաշտպանություն, Տեղեկատվական անվտանգության կառավարման համակարգ, Պահանջներ
- PCI DSS 4.0 չափորոշչի պահանջներին:

Սույն Քաղաքականությունը տեղեկատվական անվտանգության ոլորտի առաջին մակարդակի կորպորատիվ փաստաթուղթ է:

Տեղեկատվական անվտանգության մեկ կամ մի քանի ոլորտների, Ընկերության գործունեության տեսակների և տեխնոլոգիաների հետ կապված կորպորատիվ քաղաքականության դրույթները մանրամասնող փաստաթղթերն են՝ Անձնական տվյալների մշակման քաղաքականությունը, ՏԱԿՀ-ի Քաղաքականությունն ու Ուղեցույցը, ինչպես նաև կանոնակարգերը, որոնք հանդիսանում են տեղեկատվական անվտանգության երկրորդ մակարդակի փաստաթղթեր, ձևակերպվում են՝ որպես Ընկերության առանձին ներքին նորմատիվ փաստաթղթեր, մշակվում, համաձայնեցվում և հաստատվում են Ընկերությունում սահմանված կարգին համապատասխան:

1. ԸՆԴՀԱՆՈՒՐ ԴՐՈՒՅԹՆԵՐ

Քաղաքականությունը մշակվել է տեղեկատվական անվտանգության, կիբերանվտանգության ոլորտում հիմնական սկզբունքներն ու ուղղությունները սահմանելու նպատակով և ընդգրկում է այն բոլոր բիզնես գործընթացները, տեղեկատվական համակարգերը և փաստաթղթերը, որոնց սեփականատերը և օգտատերը Ընկերությունն է:

Ընկերությունում տեղեկատվական անվտանգության և կիբերանվտանգության կառավարման գործունեության նպատակը տեղեկատվական հարաբերությունների սուբյեկտների պաշտպանությունն է վերջինիս շոշափելի նյութական, ֆիզիկական, բարոյական կամ այլ վնասների հնարավոր պատճառելուց՝ տեղեկատվական համակարգի գործունեության գործընթացքում պատահական կամ կանխամտածված չարտոնված միջամտության կամ Ընկերությունում (իր համակարգերում) շրջանառվող տեղեկատվության չարտոնված մուտքի և դրա ապօրինի օգտագործման միջոցով:

Ընկերությունում տեղեկատվական անվտանգության համակարգի պաշտպանության հիմնական օբյեկտներն են՝

- առևտրային գաղտնիք, գաղտնի տեղեկատվություն պարունակող տեղեկատվական ռեսուրսները, ներառյալ ֆիզիկական անձանց անձնական տվյալները, սահմանափակ շրջանառության տեղեկությունները, ինչպես նաև Ընկերության աշխատանքի համար անհրաժեշտ բացահայտորեն շրջանառվող տեղեկատվությունը՝ անկախ դրա ներկայացման ձևից և տեսակից,

- Ընկերության տեղեկատվական ակտիվների և համակարգերի օգտատեր հանդիսացող Ընկերության աշխատողները,
- Հատուկ վերահսկվող գոտիներ, որոնց շարքին են դասվում ռեսուրսների հետևյալ խմբերը. հիմնական տեղեկատվական սերվերներ և հաշվողական տեխնիկայի միջոցներ, որոնց վրա իրականացվում է սահմանափակ շրջանառության տեղեկատվության մշակումն ու պահպանությունը, ցանցային սարքավորումներ և սերվերներ, որոնք ապահովում են կրիտիկական համակարգերի աշխատանքը, ֆայլային սերվերներ, որոնց վրա պահվում են տվյալները, այդ թվում նաև՝ պահուստային, Ընկերության գործունեության համար կրիտիկական համակարգեր ու հաղորդակցական սարքավորումներ, որոնք ապահովում են արտաքին հաղորդակցությունը, տեղեկատվության պաշտպանության համակարգեր ու միջոցներ, օբյեկտներ ու տարածքներ, որտեղ տեղակայված են այդպիսի համակարգեր,
- Հաճախորդների ու Գործընկերների կողմից Ընկերությանը վստահված տեղեկատվական ակտիվները,
- Ընկերությանը վստահված անձնական տվյալները:

Ընկերությունում տեղեկատվական անվտանգության կառավարման համակրգի խնդիրներն են.

- տեղեկատվական ակտիվների դասակարգումը՝ դրանցում պահվող և մշակվող տեղեկատվության կրիտիկականության առավելագույն մակարդակի հիման վրա դրանք կրիտիկականի և ոչ կրիտիկականի բաժանելու միջոցով,
- տեղեկատվական անվտանգության հնարավոր սպառնալիքների և Ընկերության տեղեկատվական ակտիվների խոցելիության ժամանակին բացահայտում,
- բացահայտված սպառնալիքների բացառում կամ նվազագույնի հասցնում,
- տեղեկատվական անվտանգության միջադեպերի կանխարգելում կամ դրանց հետևանքների նվազագույնի հասցնում:

Ընկերության տեղեկատվական ակտիվների գաղտնիության, ամբողջականության և հասանելիության հիմնական միջոցներն են՝

- ցանցային անվտանգության կառավարումը,
- խոցելիությունների և անվտանգության քաղաքականությունների կառավարումը,
- վերջնական սարքերի անվտանգության կառավարումը,
- նույնականացման և հասանելիության կառավարումը,
- տեղեկատվության անվտանգության միջադեպերի կառավարումը,
- պաշտպանության ծածկագրային միջոցների կառավարումը,
- պաշտպանության հակավիրուսային միջոցների կառավարումը,
- տեղեկատվական ակտիվների ֆիզիկական անվտանգության ապահովումը,
- անվտանգության ապահովումը կոնտրագենտների հետ փոխգործակցելիս,
- անձնակազմի ուսուցումը և իրազեկվածության բարձրացումը ՏԱ հարցերում,
- համացանցային-ռեսուրսների անվտանգության ապահովումը:

Առաջադրված հիմնական նպատակներն ու վերևում թվարկված լուծումներն ձեռք են բերվում՝

- պաշտպանության ենթակա բոլոր տեղեկատվական ակտիվների խստագույն հաշվառմամբ,
- պաշտպանության ենթակա տեղեկատվության մշակման գործընթացների կանոնակարգմամբ՝ օգտագործելով ավտոմատացման միջոցներ և Ընկերության կառուցվածքային ստորաբաժանումների աշխատողների գործողությունները, ինչպես նաև անձնակազմի գործողությունները, որոնք իրականացնում են Ընկերության ծրագրային և տեխնիկական միջոցների սպասարկումն ու փոխակերպումը՝ տեղեկատվական անվտանգության ապահովման հարցերի շուրջ Ընկերության գլխավոր տնօրենի կողմից հաստատված կազմակերպչակարգադրական փաստաթղթերը
- տեղեկատվական անվտանգության ապահովման հարցերի շուրջ Ընկերության կազմակերպչակարգադրական փաստաթղթերի պահանջների ամբողջականությամբ, իրական իրագործելիությամբ և անհակասականությամբ,
- տեղեկատվական անվտանգության ապահովման և դրա մշակման գործընթացների գործնական միջոցառումների կազմակերպման և իրականացման համար պատասխանատու պաշտոնատար անձանց

(աշխատողների) նշանակմամբ և պատրաստմամբ,

- Ընկերության տեղեկատվական ակտիվի յուրաքանչյուր օգտատիրոջ՝ իր ֆունկցիոնալ պարտականությունները կատարելու համար նվազագույն անհրաժեշտ մուտքի լիազորություններով օժտմամբ,
- Ընկերության ապարատային և ծրագրային միջոցները օգտագործող և սպասարկող բոլոր աշխատողների կողմից տեղեկատվական անվտանգության ապահովման հարցերի շուրջ կազմակերպչակարգադրական փաստաթղթերի պահանջների հստակ իմացությամբ և խիստ պահպանմամբ,
- իր ֆունկցիոնալ պարտականությունների շրջանակներում տեղեկատվության մշակման գործընթացներին մասնակցող և Ընկերության տեղեկատվական ակտիվների նկատմամբ հասանելիություն ունեցող յուրաքանչյուր աշխատողի՝ իր գործողությունների համար անձնական պատասխանատվությամբ,
- ծրագրային ապահովման, տեխնիկական միջոցների և տվյալների պաշտպանության կազմակերպչատեխնիկական միջոցների համալիրների օգտագործմամբ տեղեկատվության մշակման տեխնոլոգիական գործընթացների իրագործմամբ,
- տեխնիկական միջոցների ֆիզիկական ամբողջականության ապահովման արդյունավետ միջոցների ձեռնարկմամբ և Ընկերության տեղեկատվական ակտիվների պաշտպանվածության անհրաժեշտ մակարդակի շարունակական պահպանմամբ,
- Ընկերության ակտիվների պաշտպանության ֆիզիկական և տեխնիկական (ծրագրաապարատային) միջոցների կիրառմամբ,
- գաղտնիության տարբեր մակարդակների տեղեկատվության հոսքերի սահմանազատմամբ, ինչպես նաև չպաշտպանված կապուղիներով սահմանափակ շրջանառության տեղեկատվության փոխանցման արգելմամբ,
- Ընկերության ստորաբաժանումների աշխատակիցների կողմից տեղեկատվության և անվտանգության ապահովման պահանջների պահպանման արդյունավետ վերահսկմամբ,
- Արտաքին կազմակերպությունների հետ փոխգործակցելիս (կապված տեղեկատվության փոխանակման հետ) անօրինական գործողություններից Ընկերության շահերի իրավաբանական պաշտպանությամբ, ինչպես այդ կազմակերպությունների կողմից, այնպես էլ սպասարկող անձնակազմի և երրորդ անձանց չարտոնված գործողություններից,
- ձեռնարկված միջոցների և տեղեկատվության պաշտպանության կիրառվող միջոցների արդյունավետության և բավարարության շարունակական վերլուծության իրականացմամբ, Ընկերության տեղեկատվական ակտիվների պաշտպանության համակարգի կատարելագործմանն ուղղված առաջարկությունների մշակմամբ և իրականացմամբ:

2. ՏԱ ԱՊԱՀՈՎՄԱՆ ՍԿԶԲՈՒՆՔՆԵՐՆ ՈՒ ՊԱՀԱՆՋՆԵՐԸ

Օրինականություն: Ընկերության ՏԱ ապահովման միջոցները պետք է համապատասխանեն միջազգային իրավունքի կիրառելի նորմերին, Ընկերության ներկայության երկրների օրենսդրությանը, ներառյալ Ընկերության գտնվելու վայրի երկրի, ընկերության ներքին նորմատիվ-իրավական բազային:

Բիզնես կողմնորոշվածությունը. Տեղեկատվական անվտանգությունը դիտվում է՝ որպես բիզնես գործընթացների աջակցման գործընթաց: Տեղեկատվական անվտանգության ապահովման ցանկացած միջոց չպետք է հանգեցնի Ընկերության գործունեության լուրջ խոչընդոտների:

Համալիրություն և համակարգում: ՏԱ ապահովմանը պետք է մասնակցեն Ընկերության ղեկավար մարմինները, կառուցվածքային ստորաբաժանումները և անձնակազմը: ՏԱ ապահովման համար անհրաժեշտ է բոլոր հասանելի իրավական, կազմակերպչական և տեխնիկական միջոցների համաձայնեցված կիրառում, որոնք ընդհանուր առմամբ փակում են ՏԱ սպառնալիքների իրագործման բոլոր էական ուղիները: ՏԱ ապահովման գործունեության կազմակերպման և համակարգման պատասխանատվությունը պետք է դրվի հատուկ լիազորված անձի վրա:

Իրավասություն և մասնագիտացում: ՏԱ ապահովման մակարդակի վրա ազդող որոշումները, ներառյալ տեղեկատվայնացման և տեղեկատվության պաշտպանության միջոցների ընտրությունը,

անձնակազմի պարտականությունների բաշխումը, բիզնես գործընկերների հետ տեղեկատվական փոխգործակցությունը և այլն, պետք է համաձայնեցվեն ՏԱ գծով լիազորված անձի հետ:

Շարունակականություն: ՏԱ ապահովումը պետք է լինի շարունակական գործընթաց, որն իրականացվում է գործընթացների և տեղեկատվական համակարգի կենսացիկլի բոլոր փուլերում: ՏԱ ապահովման գործընթացը պետք է ներառի համակարգի պլանավորման, իրականացման, վերահսկման և վերլուծության, աջակցության և կատարելագործման փուլերը:

Իրազեկվածություն: Ընկերության անձնակազմը, ինչպես նաև արտաքին կազմակերպությունների՝ Ընկերության հաճախորդների և կոնտրագենտների, աշխատակիցները պետք է իրազեկված լինեն ՏԱ ապահովման պահանջների մասին այն ծավալով, որը պահանջվում է նրանց ծառայողական պարտականությունները կատարելու համար: ՏԱ վերաբերյալ նորմատիվ փաստաթղթերը պետք է ամբողջությամբ ներկայացնեն, ինչպես Ընկերության, այնպես էլ իրազեկվող անձի կամ կազմակերպության համար կարգավորման առարկան, պարտավորությունները և պատասխանատվության միջոցները: ՏԱ ոլորտում անձնակազմի իրազեկվածության մակարդակը ենթակա է պարբերաբար վերահսկողության ՏԱ մասով լիազորված անձանց կողմից:

Հաճախորդների, աշխատակիցների և կոնտրագենտների իմացությունը: Ընկերությունը պետք է տիրապետի իր հաճախորդների, աշխատակիցների և կոնտրագենտների վերաբերյալ ՏԱ ապահովման համար անհրաժեշտ տեղեկատվության: Այս տեղեկատվությունը պետք է պահպանվի արդիական վիճակում և օգտագործվի ՏԱ-ի ապահովման վերաբերյալ որոշումներ կայացնելիս:

Մակարդակների ստեղծում (էշելոնավորում) : Պաշտպանվածության մակարդակը բարձրացնելու համար պաշտպանության համակարգը պետք է կառուցվի էշելոնացված: ՏԱ սպառնալիքների հայտնաբերումն ու հակազդումը պետք է ապահովվի պաշտպանության անկախ մակարդակներով (էշելոններով) այնպես, որ մեկ մակարդակի խոցումը չի հանգեցնում պաշտպանական միջոցների ամբողջ համակարգի խոցելիության: Ընկերության պարագիծը արտաքին սպառնալիքներից պաշտպանելու հետ մեկտեղ պետք է ապահովվի՝ կրիտիկական տեղեկատվական ակտիվների տեղաբաշխման վայրերի, ներքին պարագծերի կազմակերպումն ու պաշտպանությունը: ՏԱ համակարգը պետք է ներառի պաշտպանության անկախ էշելոններ հետևյալ համակարգերում. տվյալների կրիչների, սերվերների, պահուստային պատճենման համակարգերի և այլ սարքավորումների ֆիզիկական հասանելիության, Ընկերության միջցանցային միացումների և ներքին հաշվողական ցանցի հասանելիության, գործառնական համակարգերի հասանելիության, հավելվածների և տվյալների հասանելիության:

Հատուկ միջոցներ պետք է ձեռնարկվեն ՏԱ կառավարման, մշտադիտարկման, հաշվետվողականության և աուդիտի համակարգերի պաշտպանության համար:

Նախազգուշացման միջոցների առաջնահերթություն: Ընկերության ՏԱ ապահովման գործընթացը պետք է ուղղված լինի ՏԱ սպառնալիքների առաջացման և իրագործման նախադրյալների կանխարգելմանն ու ժամանակին բացահայտմանը:

Արտոնությունների նվազեցում, լիազորությունների տարանջատում: Յուրաքանչյուր օգտագործողի պետք է տրամադրվեն տեղեկատվական ակտիվներին հասանելիության նվազագույն իրավունքներ, որոնք անհրաժեշտ են իր աշխատանքային պարտականությունների կատարման համար: Մեկ օգտատիրոջ իրավունքները չպետք է ՏԱ խախտման հնարավորություն ընձեռեն:

Պաշտպանության նվազագույն ընդհանուր ռեսուրս: Բոլոր հնարավոր դեպքերում պետք է օգտագործվեն տեղեկատվական համակարգերի օգտատերերի նույնականացման և հավաստիացման անձնավորված միջոցներ:

Վերահսկողության ամբողջականություն: ՏԱ համակարգը՝ յուրաքանչյուր պաշտպանվող տեղեկատվական ակտիվին դիմելիս, պետք է ապահովի սահմանված անվտանգության քաղաքականության իրականացումը: Անվտանգության քաղաքականությունը պետք է կառուցվի «Այն ամենը, ինչ ակնհայտորեն թույլատրված չէ, ապա արգելված է» սկզբունքի հիման վրա:

Ծառայությունների և սպասարկման հասանելիություն: Տեղեկատվական ակտիվները՝ նորմատիվ փաստաթղթերով սահմանված ժամանակահատվածում, պետք է հասանելի լինեն իրավասու օգտատերերին: Ծայրահեղ կարևոր տեղեկատվական ակտիվների համար պետք է մշակվեն գործունեության շարունակականության ապահովման և ընդհատումներից հետո աշխատունակության

վերականգնման պլաններ:

Կառավարման կենտրոնացում: Ընկերության ՏԱ ապահովման կազմակերպչական և տեխնիկական միջոցները պետք է առավելագույնս կենտրոնացված լինեն և ապահովեն անվտանգության համակարգի գործունեությունը միասնական իրավական, կազմակերպչական, ֆունկցիոնալ և մեթոդաբանական սկզբունքներով: ՏԱ միջոցների կառավարման կենտրոնացումը պետք է ապահովի անձնակազմի առավելագույն տեղեկացվածությունը, հիմնավորվածությունը, օպերատիվությունը և որոշումների համակարգման նվազագույն ծախսերը:

Կառավարման և կիրառման ճկունություն: ՏԱ համակարգը՝ բիզնես գործընթացների և պաշտպանության պահանջների փոփոխության դեպքում, պետք է վերակառուցվի ժամանակի և ռեսուրսների նվազագույն ծախսերով, ինչպես նաև ապահովի պաշտպանություն ոչ միայն ՏԱ հայտնի սպառնալիքներից, այլև ապագայում առաջացող հնարավոր սպառնալիքներից:

Հիմնավորվածություն և տնտեսական նպատակահարմարություն: Պաշտպանության կիրառվող հնարավորություններն ու միջոցները պետք է իրականացվեն գիտության և տեխնիկայի զարգացման համապատասխան մակարդակում, հիմնավորված լինեն անվտանգության տվյալ մակարդակի տեսանկյունից և պետք է համապատասխանեն ներկայացված պահանջներին ու նորմերին, անհրաժեշտ է հաշվի առնել դրանց իրագործման ծախսերի և սպառնալիքների տեղի ունենալու հնարավոր վնասների հարաբերակցությունը:

3. ՏԱ ԱՊԱՀՈՎՄԱՆ ԳՈՐԾՈՒՆԵՈՒԹՅԱՆ ԿԱԶՄԱԿԵՐՊՈՒՄ

Ընկերությունն ապահովում է տեղեկատվական անվտանգության կառավարման համակարգի ստեղծումը և գործունեությունը, որը Ընկերության կառավարման ընդհանուր համակարգի մի մասն է և նախատեսվում է տեղեկատվական անվտանգության ապահովման գործընթացը կառավարելու համար:

Ընկերությունը մշակում է իր տեղեկատվական համակարգերում տեղեկատվության ստեղծման, հավաքման, պահպանման և մշակման ներքին ընթացակարգեր: Ընկերությունը տեղեկատվական համակարգերի մեխանիզմների և անվտանգության ապահովման տեխնիկական միջոցների օգնությամբ իրականացնում է տեղեկատվության ստեղծման, պահպանման և մշակման և դրանց հասանելիության գործընթացների մշտադիտարկում: Ընկերության տեղեկատվական համակարգերում ստեղծվող, պահվող և մշակվող տեղեկատվության հասանելիությունը տրամադրվում է աշխատողներին ըստ իրենց գործառութային պարտականությունների՝ արտոնությունների նվազագույն մակարդակի սկզբունքին համապատասխան:

Ընկերության տեղեկատվական անվտանգության կառավարման համակարգի մասնակիցներն են.

1) Մենեջմենթ,
2) Տեղեկատվական անվտանգության հարցերով խորհուրդ,
3) տեղեկատվական անվտանգության ստորաբաժանում,
4) տեղեկատվական տեխնոլոգիաների գծով ստորաբաժանում,
5) անվտանգության գծով ստորաբաժանում,
6) անձնակազմի հետ աշխատանքի գծով ստորաբաժանում,
7) Ընկերության իրավական աջակցության ստորաբաժանում,
8) ներքին աուդիտի ստորաբաժանում:

Մենեջմենթը հաստատում է պաշտպանության ենթակա տեղեկատվության ցանկը, որը ներառում է այդ թվում՝ ծառայողական, առևտրային կամ օրենքով պահպանվող այլ գաղտնիք կազմող տեղեկությունների վերաբերյալ տեղեկատվությունը (այսուհետ՝ պաշտպանվող տեղեկատվություն), և պաշտպանվող տեղեկատվության հետ աշխատելու կարգը: Հաստատում է նաև տեղեկատվական անվտանգության կառավարման գործընթացը կանոնակարգող ներքին փաստաթղթերը, վերանայման կարգը և պարբերականությունը:

Ընկերությունը ստեղծում է Տեղեկատվական անվտանգության հարցերով խորհուրդ, որի կազմում ընդգրկված են տեղեկատվական անվտանգության հարցերով ստորաբաժանման, տեղեկատվական տեխնոլոգիաների գծով ստորաբաժանման, ինչպես նաև անհրաժեշտության դեպքում Ընկերության այլ ստորաբաժանումների ներկայացուցիչներ: Տեղեկատվական անվտանգության հարցերով խորհրդի

ղեկավար է նշանակվում ընկերության գլխավոր տնօրենը կամ գլխավոր տնօրենի առաջին տեղակալը, որը վերահսկում է տեղեկատվական անվտանգության գծով ստորաբաժանման գործունեությունը:

Տեղեկատվական անվտանգության հարցերով խորհուրդը տարեկան առնվազն մեկ անգամ իրականացնում է տեղեկատվական անվտանգության ապահովման գործունեության և սպառնալիքների հայտնաբերման և վերլուծության, գրոհների հակազդման և տեղեկատվական անվտանգության միջադեպերի հետաքննության միջոցառումների պարբերական մշտադիտարկում: Տեղեկատվական անվտանգության ապահովման գործունեության, սպառնալիքների հայտնաբերման և վերլուծության, ինչպես նաև գրոհներին հակազդելու միջոցառումների մշտադիտարկման գործընթացը պետք է ներառի հաշվետվություն սպառնալիքների հայտնաբերման, վերլուծության և գրոհների հակազդման վերաբերյալ՝ հիմնվելով տեղեկատվական անվտանգության գծով ստորաբաժանման կողմից տրամադրված տվյալների վրա՝ հայտնաբերված սպառնալիքների քանակի, ձեռնարկված միջոցների և տեղի ունեցած տեղեկատվական անվտանգության միջադեպերի մասով: Տեղեկատվական անվտանգության միջադեպերի հետաքննությանն ուղղված միջոցառումների մշտադիտարկումը ներառում է միջադեպերի հետևանքների գնահատումը, դրանց առաջացման պատճառները և տեղեկատվական անվտանգության միջադեպերի ազդեցության նվազեցմանն կամ կանխմանն ուղղված միջոցառումների պլանը:

Գլխավոր տնօրենն իրականացնում է ռազմավարական պլանավորում, Ընկերության բոլոր ստորաբաժանումների գործունեության համակարգում՝ տեղեկատվական անվտանգության համապատասխան մակարդակը կազմակերպելու և պահպանելու համար:

Տեղեկատվական անվտանգության ստորաբաժանման ղեկավարն ապահովում է տեղեկատվական անվտանգության և տեղեկատվական անվտանգության ռիսկերի կառավարման ոլորտում փաստաթղթավորված չափորոշիչների և ընթացակարգերի մշակումը, ներդրումը և կատարելագործումը:

Տեղեկատվական անվտանգության ստորաբաժանումն ապահովում է տեղեկատվական անվտանգության միջադեպերի վերաբերյալ տեղեկատվության ժամանակին վերլուծություն, որը պետք է ներառի այն իրադարձության հանգամանքների բացահայտումը, որոնց դեպքում հնարավոր է դարձել տեղեկատվական անվտանգության միջադեպի իրագործումը, անհրաժեշտության դեպքում, ձևավորում է հանձնարարականներ պաշտպանական միջոցների ներդրման ուղղությամբ: Ստորաբաժանումը պատասխանատու է տեղեկատվական ակտիվների դասակարգման իրականացման համար՝ դրանք բաժանելով կրիտիկականի և ոչ կրիտիկականի՝ դրանցում պահվող և մշակվող տեղեկատվության կրիտիկականության առավելագույն մակարդակի հիման վրա:

Տեղեկատվական տեխնոլոգիաների գծով ստորաբաժանումն ապահովում է տեղեկատվական ենթակառուցվածքների գործունեության շարունակականության, Ընկերության տեղեկատվական համակարգերի տվյալների գաղտնիության, ամբողջականության և հասանելիության (ներառյալ տեղեկատվության պահուստավորումը և (կամ) արխիվացումը և տեղեկատվության պահուստային պատճենումը) սահմանված պահանջների կատարումը՝ Ընկերության ներքին նորմատիվ փաստաթղթերին համապատասխան, ինչպես նաև ապահովում է տեղեկատվական անվտանգության պահանջների պահպանումը տեղեկատվական համակարգերի ընտրության, ներդրման, մշակման և փորձարկման ժամանակ:

Անվտանգության գծով ստորաբաժանումն իրականացնում է ֆիզիկական և տեխնիկական անվտանգության միջոցներ, այդ թվում՝ կազմակերպում է անցագրային և ներօբյեկտային ռեժիմ, ինչպես նաև իրականացնում է կանխարգելիչ միջոցառումներ, որոնք ուղղված են Ընկերության աշխատողներին աշխատանքի ընդունելիս և ազատելիս տեղեկատվական անվտանգության սպառնալիքների առաջացման ռիսկերը նվազագույնի հասցնելուն:

Անձնակազմի հետ աշխատանքի գծով ստորաբաժանումն ապահովում է Ընկերության աշխատողների, ինչպես նաև ծառայությունների մատուցման պայմանագրով աշխատանքի մեջ ներգրավված անձանց, փորձնակների, պրակտիկանտների կողմից գաղտնի տեղեկատվության չբացահայտման և անձնական տվյալների մշակման վերաբերյալ համաձայնության ստորագրումը, ինչպես նաև մասնակցում է տեղեկատվական անվտանգության ոլորտում Ընկերության աշխատողների իրազեկության բարձրացման գործընթացի կազմակերպմանը:

Իրավաբանական ստորաբաժանումն իրականացնում է ներքին նորմատիվ փաստաթղթերի և

Ընկերության ներքին փաստաթղթերի իրավական փորձաքննություն տեղեկատվական անվտանգության ապահովման հարցերի շուրջ:

Ներքին աուդիտի ստորաբաժանումն իրականացնում է Ընկերության տեղեկատվական անվտանգության կառավարման համակարգի վիճակի գնահատում աուդիտորական ստուգումների իրականացման ժամանակ:

Տեղեկատվական համակարգերի կամ ենթահամակարգերի սեփականատերերը ապրանքներ և ծառայություններ ստեղծելիս, ներդնելիս, կերպափոխելիս, հաճախորդներին տրամադրելիս պատասխանատու են տեղեկատվական անվտանգության պահանջների պահպանման համար, ինչպես նաև ձևավորում և պահպանում են տեղեկատվական համակարգերի հասանելիության մատրիցների արդիականությունը:

Ընկերության կառուցվածքային ստորաբաժանումների ղեկավարները ապահովում են աշխատողների ծանոթացումը ընկերության ներքին նորմատիվ փաստաթղթերին, որոնք պարունակում են տեղեկատվական անվտանգության պահանջներ, ինչպես նաև պատասխանատու են ենթակա ստորաբաժանումներում տեղեկատվական անվտանգության պահանջների կատարումն ապահովելու, նոր ապրանքների, ծառայությունների, բիզնես հավելվածների, բիզնես գործընթացների և տեխնոլոգիաների մշակման ժամանակ պաշտպանական միջոցների ներդրման համար:

4. ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՌԻՍԿԵՐԻ ԿԱՌԱՎԱՐՈՒՄ

Տեղեկատվական անվտանգության ապահովման և արդյունավետ կառավարման համար Ընկերությունն ապահովում է տեղեկատվական անվտանգության ռիսկերի կառավարումը, որը ներառում է.

- Ընկերության տեղեկատվական անվտանգության վրա Ընկերության գործունեության մեջ կիրառվող տեխնոլոգիաների, ինչպես նաև Ընկերության նկատմամբ արտաքին իրադարձությունների ազդեցության վերլուծություն,
- տեղեկատվական անվտանգության ապահովման խնդիրների բացահայտում, դրանց ծագման պատճառների վերլուծություն և դրանց զարգացման կանխատեսում,
- տեղեկատվական անվտանգության սպառնալիքների մոդելների սահմանում,
- Ընկերության համար նշանակալի տեղեկատվական անվտանգության սպառնալիքների բացահայտում, վերլուծություն և գնահատում,
- Ընկերության համար հնարավոր բացասական հետևանքների բացահայտում, որոնք առաջանում են տեղեկատվական անվտանգության ռիսկի գործոնների դրսևորման արդյունքում, այդ թվում՝ կապված Ընկերության տեղեկատվական ակտիվների անվտանգության խախտման հետ,
- տեղեկատվական անվտանգության ռիսկային իրադարձությունների նույնականացում և վերլուծում,
- տեղեկատվական անվտանգության ռիսկերի գնահատում և Ընկերության համար անընդունելի ռիսկերի որոշում,
- տեղեկատվական անվտանգության ռիսկերի գնահատման արդյունքների մշակում՝ գործառնական ռիսկերի կառավարման մեթոդների կիրառմամբ,
- տեղեկատվական անվտանգության ռիսկերի օպտիմալացում՝ պաշտպանական միջոցների ընտրության և կիրառման հաշվին, որոնք հակազդում են ռիսկի գործոնների դրսևորումներին և նվազագույնի հասցնում Ընկերության համար հնարավոր բացասական հետևանքները ռիսկային իրադարձությունների առաջանալու դեպքում,
- Ընկերության հիմնական գործունեության նպատակների վրա պաշտպանական միջոցների ազդեցության գնահատում,
- պաշտպանական միջոցառումների իրականացման ծախսերի գնահատում,
- տեղեկատվական անվտանգության ապահովման խնդիրների լուծման տարբեր տարբերակների քննարկում և գնահատում,
- ռիսկերի կառավարման պլանների մշակում, որոնք նախատեսում են տարբեր պաշտպանիչ միջոցներ և դրանց կիրառման տարբերակներ, և դրանցից այնպիսինի ընտրություն, որի իրականացումը

առավելագույնս դրականորեն կազդի Ընկերության հիմնական գործունեության նպատակների վրա և օպտիմալ կլինի կատարված ծախսերի և ակնկալվող արդյունքի տեսանկյունից,

5. ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՍՊԱՌՆԱԼԻՔՆԵՐ

Տեղեկատվության անվտանգության հնարավոր սպառնալիքների ամբողջ բազմազանությունը ըստ առաջացման բնույթի բաժանվում է երեք դասի՝ մարդածին, տեխնածին և բնական:

Մարդածին սպառնալիքների առաջացումը պայմանավորված է մարդու գործունեությամբ: Տեղեկատվական համակարգի և դրա տարրերի նախագծման սխալների հետևանքով առաջացած սպառնալիքները, անձնակազմի գործողությունների սխալները և այլն, ինչպես նաև սպառնալիքներ, որոնք առաջանում են ինչպես ոչ կանխամտածված (ոչ դիտավորյալ) գործողությունների հետևանքով՝ տեղեկատվական համակարգի և դրա տարրերի նախագծման սխալների հետևանքով առաջացած սպառնալիքներ, անձնակազմի սխալ գործողություններ և այլն, այնպես էլ սպառնալիքներ, որոնք առաջանում են դիտավորյալ գործողությունների հետևանքով, որոնք կապված են մարդկանց շահադիտական, գաղափարական կամ այլ նկրտումների հետ:

Տեխնածին սպառնալիքների առաջացումը պայմանավորված է սպառնալիքի օբյեկտի վրա տեխնածին բնույթի օբյեկտիվ ֆիզիկական գործընթացների ազդեցությամբ, սպառնալիքի օբյեկտի կամ դրա շրջապատի տեխնիկական վիճակով, որոնք ուղղակիորեն պայմանավորված չեն մարդու գործունեությամբ:

Տեխնածին սպառնալիքների շարքին կարող են դասվել խափանումները, այդ թվում՝ աշխատանքային, կամ մարդու կողմից ստեղծված համակարգերի փլուզումը:

Բնական (բնական) սպառնալիքների առաջացումը պայմանավորված է սպառնալիքի օբյեկտի վրա բնական բնույթի օբյեկտիվ ֆիզիկական գործընթացների, բնական տարերային երևույթների, ֆիզիկական միջավայրի վիճակների ազդեցությամբ, որոնք ուղղակիորեն պայմանավորված չեն մարդու գործունեությամբ:

Բնական սպառնալիքներին են դասվում օդերևութաբանական, մթնոլորտային, երկրաֆիզիկական, երկրամագնիսական և այլ սպառնալիքներ, ներառյալ ծայրահեղ կլիմայական պայմանները, օդերևութաբանական երևույթները, բնական աղետները:

Ընկերության ենթակառուցվածքների նկատմամբ սպառնալիքների աղբյուրները կարող են լինել ինչպես արտաքին, այնպես էլ ներքին:

6. ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՀՆԱՐԱՎՈՐ ԽԱԽՏՈՂՆԵՐԻ ՈՉ ՖՈՐՄԱԼ ՄՈԴԵԼ

Խախտողները կարող են բաժանվել արտաքին և ներքին խախտողների:

Խախտողն այն անձն է, որը սխալմամբ, անտեղյակությամբ կամ գիտակցաբար չար մտադրությամբ (շահադիտական հետաքրքրությունից ելնելով) կամ առանց դրա (խաղի կամ հաճույքի համար, ինքնահաստատման նպատակով և այլն) փորձել է կատարել արգելված գործառնություններ (գործողություններ) և դրա համար օգտագործել է տարբեր հնարավորություններ, մեթոդներ և միջոցներ:

Ընկերության տեղեկատվական ակտիվների պաշտպանության համակարգը կառուցվում է ենթադրությունների հիման վրա՝ խախտողների հետևյալ հնարավոր տեսակների վերաբերյալ (հաշվի առնելով անձանց կատեգորիան, շահադրդումը, որակավորումը, հատուկ միջոցների առկայությունը և այլն):

«Անփորձ (անուշադիր) աշխատող»՝ Ընկերության (կամ այլ կազմակերպության աշխատող, որը ընկերության տեղեկատվական համակարգերում գրանցված է՝ որպես օգտատեր), որը կարող է ձեռնակել արգելված գործողությունների իրականացման, Ընկերության պաշտպանված ռեսուրսներ մուտք գործելու՝ իր լիազորությունների գերազանցմամբ, սխալ տվյալներ մուտքագրելու և այլ սխալմունքի, ոչ կոմպետենտության կամ անփութության պատճառով, առանց չար դիտավորության այլ գործողությունների փորձեր՝ միևնույն ժամանակ օգտագործելով միայն հաստիքային (իրեն հասանելի) ապարատային և ծրագրային միջոցներ:

«Ոչ պրոֆեսիոնալ»՝ Ընկերության (կամ այլ կազմակերպության աշխատող, որը ընկերության տեղեկատվական համակարգերում գրանցված է՝ որպես օգտատեր), որը փորձում է հաղթահարել պաշտպանության համակարգը՝ առանց շահադիտական նպատակների և չար դիտավորության,

ինքնահաստատման կամ «սպորտային հետաքրքրության» համար: Պաշտպանության համակարգը հաղթահարելու և արգելված գործողություններ կատարելու համար նա կարող է օգտագործել ռեսուրսների (այլ օգտատերերի անուններ, գաղտնաբառեր և այլն) հասանելիության լրացուցիչ լիազորությունների ստացման տարբեր մեթոդներ, պաշտպանության համակարգի կառուցման թերություններ և իրեն հասանելի հաստիքային (աշխատատեղում տեղադրված) ծրագրեր (չարտոնված գործողություններ՝ թույլատրելի միջոցների օգտագործման իր լիազորությունները գերազանցելու միջոցով):

Բացի այդ, նա կարող է փորձել օգտագործել լրացուցիչ ոչ հաստիքային գործիքներ և տեխնոլոգիական ծրագրային միջոցներ (կարգաբերիչներ, ծառայողական ուտիլիտներ (օժանդակ ծրագրեր), ինքնուրույն մշակված ծրագրեր կամ ստանդարտ լրացուցիչ տեխնիկական գործիքներ:

«Խարդախ»՝ Ընկերության (կամ այլ կազմակերպության աշխատող, որը ընկերության տեղեկատվական համակարգերում գրանցված է՝ որպես օգտատեր), որը կարող է ձեռնարկել ապօրինի տեխնոլոգիական գործողություններ կատարելու, կեղծված տվյալներ մուտքագրելու և նման գործողություններ կատարելու փորձեր՝ շահադիտական նպատակներով, հարկադրանքով կամ չար մտադրությունից դրդված, բայց օգտագործելով միայն հաստիքային (աշխատատեղին և իրեն հասանելի) ապարատային և ծրագրային միջոցներ՝ իր անվամբ կամ այլ աշխատողի անվամբ (իմանալով նրա անունն ու գաղտնաբառը՝ օգտվելով աշխատատեղից նրա կարճաժամկետ բացակայությունից և այլն):

«Ներքին չարագործ»՝ ընկերության տեղեկատվական համակարգերում որպես օգտատեր գրանցված Ընկերության աշխատող, որը գործում է նպատակաուղղված՝ շահադիտական շահերից կամ հասցված վիրավորանքի համար վրեժխնդրությունից ելնելով, հնարավոր է՝ Ընկերության աշխատող չհանդիսացող անձանց հետ դավադրությամբ: Նա կարող է օգտագործել պաշտպանության համակարգը կոտրելու մեթոդների և միջոցների ամբողջ հավաքածուն, ներառյալ մուտքի վավերապայմանների ստացման գործակալական մեթոդները, պասիվ միջոցները (գաղտնալսման տեխնիկական միջոցներ՝ առանց համակարգի բաղադրիչների ձևափոխման), ակտիվ ազդեցության մեթոդներ ու միջոցներ (տեխնիկական միջոցների ձևափոխում, տվյալների փոխանցման ուղիների միացում, ծրագրային էջանիշների ներդնում և հատուկ գործիքային և տեխնոլոգիական ծրագրերի օգտագործում), ինչպես նաև ներազդման համակցություններ ինչպես ներսից, այնպես էլ դրսից՝ ընդհանուր օգտագործման ցանցերից:

Ներքին խախտողներից կարող է լինել անձ՝ Ընկերության անձնակազմի հետևյալ կատեգորիաներից.

- ընկերության տեղեկատվական համակարգերում գրանցված վերջնական օգտագործողներ (Ընկերության աշխատողներ),
- Ընկերության տեղեկատվական ակտիվների հետ աշխատելու թույլտվություն չունեցող աշխատողներ,
- տեղեկատվական ակտիվների տեխնիկական միջոցները սպասարկող անձնակազմ (ինժեներներ, տեխնիկներ),
- ծրագրային ապահովման մշակման և աջակցության ստորաբաժանումների աշխատողներ (կիրառական և համակարգային ծրագրավորողներ),
- շենքերը սպասարկող տեխնիկական անձնակազմ (հավաքարարներ, էլեկտրիկներ, սանտեխնիկներ և այլ աշխատողներ, որոնք մուտք ունեն շենքեր և տարածքներ, որտեղ գտնվում են ծայրահեղ կարևոր տեղեկատվական համակարգեր և ակտիվներ),
- տեղեկատվական անվտանգության և SS ստորաբաժանման աշխատողներ,
- տարբեր մակարդակների ղեկավարներ:

«Արտաքին խախտող (չարագործ)»՝ կողմնակի անձ կամ Ընկերության կամ այլ կազմակերպության նախկին աշխատող, որը գործում է նպատակաուղղված՝ շահադիտական շահերից ելնելով, վրեժխնդրությունից կամ հետաքրքրասիրությունից դրդված, հնարավոր է այլ անձանց հետ դավադրությամբ: Կարող է օգտագործել ընդհանուր օգտագործման ցանցերին (հատկապես IP պրոտոկոլի վրա հիմնված ցանցերին) բնորոշ տեղեկատվական անվտանգության խախտման ռադիոէլեկտրոնային եղանակների, պաշտպանության համակարգերի կոտրման մեթոդների և միջոցների ամբողջ հավաքածուն, ներառյալ՝ ծրագրային էջանիշների հեռավար ներդնումը և հատուկ գործիքների և տեխնոլոգիական ծրագրերի օգտագործումը՝ օգտվելով փոխանակման արձանագրությունների և

Ընկերության ցանցային հանգույցների պաշտպանության համակարգի առկա թուլություններից:

Անձանց կատեգորիաներ, որոնք կարող լինել արտաքին խախտողներ.

- Աշխատանքից ազատված աշխատողներ,
- կազմակերպությունների ներկայացուցիչներ, որոնք համագործակցում են կազմակերպության կենսագործունեության ապահովման հարցերով (էներգա-, ջրա-, ջերմամատակարարման և այլն),
- այցելուներ (կազմակերպությունների հրավիրված ներկայացուցիչներ, քաղաքացիներ), տեխնիկա, ծրագրային ապահովում, ծառայություններ մատակարարող ֆիրմաների ներկայացուցիչներ և այլն,
- հանցավոր կազմակերպությունների անդամներ, հատուկ ծառայությունների աշխատողներ կամ նրանց առաջադրանքով գործող անձինք,
- հեռահաղորդակցության արտաքին (ընկերության նկատմամբ) ցանցերից պատահաբար կամ դիտավորությամբ Ընկերության ցանց ներթափանցած անձինք («հաքերներ»):

Օգտատերերն ու Ընկերության սպասարկող անձնակազմն ունեն չարտոնված գործողություններ իրականացնելու ամենալայն հնարավորությունները՝ ռեսուրսների նկատմամբ հասանելիության որոշակի լիազորությունների առկայության և տեղեկատվության մշակման տեխնոլոգիայի և պաշտպանական միջոցների լավ իմացության պատճառով: Անձանց այս խմբի գործողություններն ուղղակիորեն կապված են գործող կանոնների և հրահանգների խախտման հետ: Խախտողների այս խումբը հատուկ վտանգ է ներկայացնում հանցավոր կառույցների կամ հատուկ ծառայությունների հետ փոխգործակցության դեպքում:

Աշխատանքից ազատված աշխատողները կարող են իրենց նպատակներին հասնելու համար օգտագործել իրենց գիտելիքները աշխատանքային տեխնոլոգիայի, պաշտպանական միջոցների և մուտքի իրավունքների վերաբերյալ: Ընկերությունում ձեռք բերված գիտելիքներն ու փորձը նրանց առանձնացնում են արտաքին սպառնալիքների այլ աղբյուրներից:

Հանցավոր կառույցները իրենցից ներկայացնում են արտաքին սպառնալիքների առավել ագրեսիվ աղբյուր: Իրենց մտահղացումներն իրականացնելու համար այդ կառույցները կարող են օրենքի բացահայտ խախտման դիմել և իրենց հասանելի բոլոր ուժերով ու միջոցներով իրենց գործունեության մեջ ներգրավել Ընկերության աշխատակիցներին:

Արհեստավարժ «հաքերներն» ունեն ամենաբարձր տեխնիկական որակավորումն ու գիտելիքները ծրագրային և ապարատային միջոցների խոցելիության վերաբերյալ: Ամենամեծ վտանգը ներկայացնում են ընկերության աշխատող և աշխատանքից ազատված աշխատակիցների և հանցավոր կառույցների հետ փոխգործակցությամբ:

Այն կազմակերպությունները, որոնք զբաղվում են սարքավորումների, տեղեկատվական համակարգերի մշակմամբ, մատակարարմամբ և վերանորոգմամբ, արտաքին սպառնալիք են ներկայացնում այն պատճառով, որ դիպվածային կերպով անմիջական հասանելիություն ունեն տեղեկատվական ռեսուրսների նկատմամբ: Հանցավոր կառույցներն ու հատուկ ծառայությունները կարող են այդ կազմակերպություններն օգտագործել իրենց անդամներին ժամանակավորապես աշխատանքի տեղավորելու համար՝ պաշտպանված տեղեկատվության և տեղեկատվական ակտիվների նկատմամբ հասանելիության նպատակով:

7. ՊԱՇՏՊԱՆՈՒԹՅԱՆ ՀԱՄԱԿԱՐԳԻ ԱՐԴՅՈՒՆԱՎԵՏՈՒԹՅԱՆ ՎԵՐԱՀՍԿՈՂՈՒԹՅՈՒՆ

Տեղեկատվության պաշտպանության արդյունավետության վերահսկողությունն իրականացվում է տեխնիկական ուղիներով տեղեկատվության արտահոսքը ժամանակին հայտնաբերելու և կանխելու հաշվին, ինչպես նաև տեղեկատվության ոչնչացմանը, տեղեկատվայնացման միջոցների ոչնչացմանն ուղղված հնարավոր հատուկ ազդեցությունների նախազգուշացման նպատակով:

Վերահսկողությունը կարող է իրականացվել ինչպես տեղեկատվական անվտանգության առանձնացված աշխատողների, այնպես էլ այդ նպատակով ներգրավված իրավասու կազմակերպությունների կողմից, որոնք ունեն գործունեության այս տեսակի լիցենզիա:

Տեղեկատվության պաշտպանության միջոցների արդյունավետության գնահատումն իրականացվում է սահմանված պահանջներին համապատասխանության տեխնիկական և ծրագրային հսկողության

միջոցների օգտագործմամբ:

Վերահսկողությունը կարող է իրականացվել ինչպես չարտոնված մուտքից տեղեկատվության պաշտպանության համակարգի հաստիքային միջոցների, այնպես էլ հսկողության հատուկ ծրագրային միջոցների օգնությամբ:

8. ԱՈՒԴԻՏ

Տեղեկատվական անվտանգության գծով ստորաբաժանումը պետք է ներքին և արտաքին աուդիտի օգնությամբ ապահովի և ստուգի տվյալ Քաղաքականության դրույթների և դրանից բխող ներքին նորմատիվ փաստաթղթերի կատարման աստիճանը, ճշգրտությունը և օպերատիվությունը, ինչպես նաև ապահովի սահմանված ուղղիչ միջոցների իրականացումը՝ գործունեության շարունակական կատարելագործման նպատակով:

9. ՊԱՏԱՍԽԱՆԱՏՎՈՒԹՅՈՒՆ ՔԱՂԱՔԱԿԱՆՈՒԹՅԱՆ ԴՐՈՒՅԹՆԵՐԻ ՊԱՀՊԱՆՄԱՆ ՀԱՄԱՐ

Սույն Քաղաքականության դրույթները արդի վիճակում պահելու, համակարգումը, ներդնումը կազմակերպելու, և ընկերության տեղեկատվական անվտանգության կառավարման համակարգի գործընթացներում փոփոխություններ կատարելու պատասխանատվությունը դրվում է տեղեկատվական անվտանգության գծով ստորաբաժանման վրա:

Սույն Քաղաքականությունը չկատարելու համար Ընկերության աշխատողների պատասխանատվությունը որոշվում է Ընկերության աշխատողների հետ աշխատանքային պայմանագրերում ներառված համապատասխան դրույթներով, ինչպես նաև Ընկերության ներքին նորմատիվ փաստաթղթերի դրույթներով:

10. ԵԶՐԱՓԱԿԻՉ ԴՐՈՒՅԹՆԵՐ

Սույն քաղաքականության պահանջները կարող են լրացվել և ճշգրտվել Ընկերության այլ ներքին նորմատիվ փաստաթղթերով:

Գործող օրենսդրության և այլ նորմատիվ ակտերի, ինչպես նաև Ընկերության Կանոնադրության փոփոխության դեպքում սույն Քաղաքականությունը և դրա փոփոխությունները կիրառվում են այն մասով, որը չի հակասում նոր ընդունված օրենսդրական և այլ նորմատիվ ակտերին, ինչպես նաև Ընկերության Կանոնադրությանը: Այս դեպքում Պատասխանատու ստորաբաժանումը պարտավոր է անհապաղ նախաձեռնել համապատասխան փոփոխությունների կատարումը:

Սույն Քաղաքականության մեջ փոփոխությունների կատարումն իրականացվում է պարբերական և արտապլանային հիմունքներով.

- սույն Քաղաքականության մեջ պարբերաբար փոփոխություններ կատարելը պետք է իրականացվի օրենսդրության և նորմատիվ ակտերի, ոլորտային սկզբունքների և տեխնիկական կանոնակարգերի փոփոխություններն արտացոլելու համար,
- սույն Քաղաքականության մեջ արտապլանային փոփոխությունները կարող են կատարվել՝ տեղեկատվական անվտանգության միջադեպերի, տեղեկատվական անվտանգության ապահովման միջոցների արդիականության, բավարարության և արդյունավետության վերլուծության արդյունքներով, տեղեկատվական անվտանգության ներքին աուդիտի անցկացման և այլ վերահսկիչ միջոցառումների արդյունքներով:

Քաղաքականության կողմից սահմանված պահանջների կատարման նկատմամբ վերահսկողությունը դրվում է Տեղեկատվական անվտանգության գծով խորհդի վրա:

Քաղաքականությամբ չկարգավորված հարցերը լուծվում են Հայաստանի Հանրապետության օրենսդրությանը համապատասխան: