1.ԸՆԴՀԱՆՈՒՐ ԴՐՈՒՅԹՆԵՐ

1.1. Տեսահսկման քաղաքականության (այսուհետ՝ Քաղաքականություն) վերաբերյալ սույն դրույթը սահմանում է «ՋԻԷՆՍԻ-ԱԼՖԱ» ՓԲԸ – ի (այսուհետ՝ Ընկերություն) տարածքներում տեսանկարահանման սարքավորումների օգտագործման և տեսահսկման համակարգի կազմակերպման կարգը (տեսահսկման անմիջական իրականացում՝ օբյեկտի և տարածքների վերաբերյալ տեսատեղեկատվություն ստանալու համար տեսախցիկների օգտագործման միջոցով, ինչպես նաև ստացված պատկերի ձայնագրում և պահպանում հետագա օգտագործման համար) և մշակվել է Ընկերության օբյեկտներում տեղադրված տեսախցիկների տեսադաշտում հայտնվող հաճախորդներին և աշխատակիցներին իրենց պատկերների մշակման նպատակների մասին տեղեկացնելու նպատակով:

1.2. Քաղաքականությունը մշակվել է Հայաստանի Հանրապետության 18.05.2015 N ՀՕ-49-Ն «Անձնական տվյալների պաշտպանության մասին» օրենքին (այսուհետ՝ Օրենք), Ընկերության տեղեկատվական անվտանգության և անձնական տվյալների մշակման քաղաքականությանը և Հայաստանի Հանրապետության այլ նորմատիվ-իրավական ակտերին համապատասխան:

1.3. Տեսահսկման համակարգը Ընկերության ընդհանուր անվտանգության համակարգի տարր է, որն ուղղված է հասարակական անվտանգության ապահովմանը, Ընկերության աշխատողների, հաճախորդների և Ընկերության գույքի նկատմամբ հնարավոր հակաօրինական դրսևորումների կանխարգելմանը, արտակարգ իրավիճակների և (կամ) պատահարների (այսուհետ՝ ոչ ստանդարտ իրավիճակներ) կանխարգելմանը և դրանց առաջացման դեպքերում հետաքննության օբյեկտիվության ապահովմանը:

1.4. Քաղաքականությունը հրապարակվում է ինտերնետում բաց հասանելիությամբ՝ Ընկերության https://ovio.am պաշտոնական կայքում, ինչպես նաև բաց հասանելիությամբ տեղակայվում է վարչական գոտում (ընդունարանում):

2.ՏԵՍԱՀՍԿՄԱՆ ԵՎ ՏԵՍԱԳՐՈՒԹՅԱՆ ՄԿՋԲՈՒՆՔՆԵՐԸ

2.1. Տեսահսկման և տեսագրման համակարգը հիմնված է օրինականության, համաչափության, թափանցիկության, բարեխղճության և անվտանգության սկզբունքների վրա:

2.1.1 **Օրինականության սկզբունք.** Ընկերությունը տեսահսկումները կազմակերպում է՝ պահպանելով օրենքի պահանջները, օրինական և որոշակի նպատակներով և չի կարող օգտագործվել այլ նպատակներով:

2.1.2 **Համաչափության սկզբունք.** Ընկերությունը տեսահսկումը օգտագործում է այն դեպքերում, երբ առանց դրա հնարավոր չէ հասնել սահմանված նպատակներին: Ընկերությունն ապահովում է հավասարակշռություն տեսահսկման հետապնդվող նպատակի և կադրում հայտնված մարդկանց անձնական կյանքի պաշտպանության միջև: Տեսագրությունները մշակվում են այն նվազագույն ծավալով, որը բավարար է օրինական նպատակներին հասնելու համար: Տեսախցիկները հնարավորության սահմաններում տեղադրվում են այնպես, որ կադրում հայտնվեն տեսահսկման նպատակներին համապատասխանող օբյեկտները:

2.1.3 **Թափանցիկության և բարեխղճության սկզբունք.** Ընկերությունը անձնական տվյալների սուբյեկտներին տեղեկացնում է տեսահսկման իրականացման մասին՝ Ընկերության գրասենյակային տարածքների մուտքի դռան վրա նախազգուշացնող ցուցանակներ տեղադրելով: Ընկերությունում արգելվում է տեղեկատվության գաղտնի ստացման համար նախատեսված սարքերի օգտագործումը: Ընկերությունը, ելնելով պահպանվող օբյեկտի կարևորության աստիճանից, կարող է չնշել տեսախցիկների տեղակայման վայրերը:

2.1.4 **Անվտանգության սկզբունք.** Ընկերությունը տվյալները մշակում է այնպիսի եղանակով, որն ապահովում է անձնական տվյալների պատշաճ անվտանգությունը, ներառյալ պաշտպանությունը չարտոնված կամ ապօրինի մշակումից, ինչպես նաև պատահական կորստից, ոչնչացումից կամ վնասումից՝ օգտագործելով համապատասխան իրավական, կազմակերպչական և տեխնիկական միջոցներ:

2.2. «ՋԻԷՆՍԻ-ԱԼՖԱ» ՓԲԸ-ում անձնական տվյալների պաշտպանության հետ կապված այլ

հարցերին, այդ թվում՝ անձնական տվյալների մշակման հետ կապված իրավունքների, ինչպես նաև դրանց իրականացման մեխանիզմի վերաբերյալ տեղեկատվությանը կարելի է ծանոթանալ «Անձնական տվյալների մշակման քաղաքականության» շրջանակներում:

3.ՏԵՍԱՀՍԿՄԱՆ ՀԱՄԱԿԱՐԳԻ ՆՊԱՏԱԿՆԵՐՆ ՈՒ ԽՆԴԻՐՆԵՐԸ

3.1. Տեսահսկման համակարգը Ընկերության ընդհանուր անվտանգության համակարգի տարր է, որն ուղղված է հասարակական անվտանգության ապահովմանը, Ընկերության աշխատողների, հաճախորդների և Ընկերության գույքի նկատմամբ հնարավոր հակաօրինական դրսևորումների կանխարգելմանը, արտակարգ իրավիճակների և (կամ) պատահարների կանխարգելմանը և դրանց առաջացման դեպքերում հետաքննության օբյեկտիվության ապահովմանը:

3.2. Ընկերությունում տեսահսկումը չի կարող ուղղված լինել անձնական տվյալների կոնկրետ սուբյեկտի վերաբերյալ տեղեկատվության հավաքագրմանը:

3.3. Ընկերությունն իրականացնում է տեսահսկում իր բոլոր շենքերում և շինություններում:

3.4. Տեսահսկման համակարգը կատարում է հետևյալ առաջադրանքները.

3.4.1 Ընկերության աշխատողների և այցելուների անձնական անվտանգության ապահովում,

3.4.2 Ընկերության գույքի, արժեքների և սահմանափակ շրջանառության տեղեկատվության պահպանություն,

3.4.3 Ընկերության օբյեկտների պահպանման ուժեղացում,

3.4.4 Արագ արձագանք Ընկերության գույքի, արժեքների, սահմանափակ շրջանառության տեղեկատվության, աշխատողների և այցելուների նկատմամբ հակաօրինական գործողություններին, ինչպես նաև Ընկերության օբյեկտներում արտակարգ իրավիճակների առաջացման դեպքում:

3.4.5 ընկերության օբյեկտների և ինքնասպասարկման սարքերի անվտանգ գործառնության ապահովում,

3.4.6 Ընկերության օբյեկտներում, ինքնասպասարկման սարքերի տեղադրման վայրերում և Ընկերության օբյեկտներին հարող տարածքում միջադեպերի, արտակարգ իրավիճակների և իրավախախտումների փաստաթղթավորում,

3.4.7 ոչ ստանդարտ իրավիճակների առաջացման դեպքում գործողությունների արդյունավետության բարձրացում, դրանց քննման և գնահատման օբյեկտիվության ապահովում,

3.4.8 Ընկերության այցելուների, աշխատողների և հաճախորդների կողմից հակաօրինական գործողությունների կանխում:

3.5. Տեսահսկումը չի կարող օգտագործվել.

3.5.1 Ընկերության աշխատողների կողմից փաստացի աշխատած աշխատաժամանակի հաշվառման,

3.5.2 Տեսագրության մեջ պատկերված անձանց նույնականացման,

3.5.3 ձայնագրության համար:

4.ՏԵՍԱՀՍԿՄԱՆ ՀԱՄԱԿԱՐԳԻ ԿԱԶՄԱԿԵՐՊՄԱՆ ԿԱՐԳԸ

4.1. Ընկերության օբյեկտներում տեսահսկման համակարգի տեղադրումն իրականացվում է նրա նպատակներին և խնդիրներին համապատասխան: Տեսախցիկների գտնվելու վայրը, դրանց տեխնիկական բնութագրերը սահմանվում են հատուկ առաջադրանքներին համապատասխան՝ ելնելով հրահանգի պահանջներից և Ընկերության այլ տեխնիկական նորմատիվ փաստաթղթերից:

4.2. Ընկերության տեսահսկման համակարգը ներառում է մի շարք սարքեր՝ տեսաձայնագրիչներ, տեսախցիկներ, տեսամոնիտորներ և այլն:

4.3. Տեսահսկումն իրականացվում է շուրջօրյա և անընդհատ՝ օգտագործելով բաց տեսահսկման տեսախցիկներ: Տեսախցիկները տեղադրվում են ճարտարապետական առանձնահատկություններից ելնելով՝ ամբողջ տարածքի պարտադիր ընդգրկման պայմանով:

4.4. Տեսահսկման խցիկները տեղադրվում են հետևյալ բաց գոտիներում:

4.4.1 Ընկերության շենքերի վրա՝ պարագծի պահպանությունն ապահովելու համար

4.4.2 սրահ՝ գրասենյակային տարածքի մուտքի կողմից և դեպի գրասենյակային տարածքի մուտքի տեսահսկման ուղղությամբ,

4.4.3 միջանցքներ՝ միջանցքի երկու կողմից տեսահսկման ուղղությամբ

4.4.4 գրասենյակային տարածքում և դեպի տարհանման ելք տեսահսկման ուղղությամբ,

4.4.5 ներքին միջանցք՝ դեպի պահեստային տարածք տեսահսկման ուղղությամբ,

4.4.6 բաց տիպի գրասենյակային տարածքներ («open space» ձևաչափ՝ լրացուցիչ տեխնիկական միջոցների կիրառմամբ՝ աշխատատեղերի պատկերների ճապաղվածությունն ապահովելու համար՝ անձնական տվյալներ, առևտրային գաղտնիք կազմող տեղեկատվության ստացումը կամ տարածումը թույլ չտալու նպատակով և այլն:

4.4.7 ելույթների անցկացման տարածք,

4.5. Տեսահսկման խցիկները տեղադրվում են ընդհանուր հասանելիության համար փակ վայրերում՝ հետևյալ գոտիներում.

4.5.1 սերվերային սենյակներում,

4.5.2 ծայրահեղ կարևոր ցանցային հանգույցներում (ՆՕԴ),

4.5.3 պահեստային տարածքներ,

4.5.4 այլ փակ տարածքներ և սահմանափակ հասանելիության տարածքներ:

4.6. Ի տարբերություն բաց տարածքների, փակ տարածքների համար Ընկերությունը կարող է չնշել տեսախցիկների տեղադրման վայրերը, և դրանք կարող են տեսանելի չլինել:

4.7. Արգելվում է Ընկերության տարածքներում անտեսանելի տեսախցիկների տեղերը բացահայտելու համար նախատեսված սարքերի օգտագործումը:

4.8. Արգելվում է տեսախցիկների տեղադրումը այն տարածքներում, որտեղ ընկերության աշխատակիցները չեն կատարում իրենց ծառայողական պարտականությունները (զուգարաններ, կենցաղային տարածքներ և այլն):

4.9. Տեսահսկման համակարգերի անխափան աշխատանքն ապահովելու, կանոնավոր տեխնիկական հսկողություն և կանխարգելիչ սպասարկում, համակարգերի վերանորոգման, արդիականացման և ընդլայնման աշխատանքներն իրականացնելու գործառույթներն իրականացնում են լիազորված աշխատողները՝ կողմնակի կազմակերպությունների ներգրավմամբ, որոնք ունեն պահնորդական գործունեություն իրականացնելու իրավունքի համապատասխան հատուկ թույլտվություններ (լիցենզիաներ)՝ պահպանության միջոցների և համակարգերի տեխնիկական սպասարկման մասով:

4.10. Արգելվում է ցանկացած անձանց, բացառությամբ լիազորված աշխատողների և կազմակերպությունների (իրավաբանական անձանց) աշխատակիցների, որոնք կատարում են Ընկերության օբյեկտների տեսահսկման համակարգերի տեխնիկական սպասարկման աշխատանքներ, չթույլատրված հասանելիությունը տեսախցիկների կարգավորումների, տեսապատկերի ձայնագրման ռեժիմների և համակարգի ծայրամասային սարքերի կառավարման նկատմամբ:

4.11. Համակարգի պարամետրերի պահպանման անվտանգության, կարգաբերման և փոփոխության ապահովման գործառույթները, համակարգի կազմաձևումը, արխիվացման պարամետրերի կառավարումը, տեսահսկման համակարգի մուտքի հաշիվների կառավարումը (մուտքանուններ/գաղտնաբառեր) և մուտքի իրավունքների նշանակումը, իրականացվում են Տեղեկատվական անվտանգության քաղաքականության և Ընկերության այլ ներքին իրավական ակտերի համաձայն:

4.12. Եթե տեղեկատվություն է ստացվել տեսահսկման խցիկների կողմից կարգապահական զանցանքի, վարչական իրավախախտման, քրեական հանցագործության նշաններ ունեցող իրավիճակի հնարավոր արձանագրման մասին, ապա Ընկերության գլխավոր տնօրենի (նրա պաշտոնակատարի), Անվտանգության ծառայության և/կամ տեղեկատվական անվտանգության գծով ղեկավարի կամ անձնական տվյալների մշակման ներքին հսկողության իրականացման համար պատասխանատուի գրավոր հանձնարարությամբ նման տեսագրությունների համար պահպանման ժամկետը կարող է երկարաձգվել համապատասխան միջոցառումների ժամանակահատվածով:

5.ՏԵՍԱՀՍԿՄԱՆ ՀԱՄԱԿԱՐԳԵՐԻ ՁԱՅՆԱԳՐՈՒԹՅՈՒՆՆԵՐԻ ՆԿԱՏՄԱՄԲ ՀԱՍԱՆԵԼԻՈՒԹՅԱՆ ԿԱՐԳԸ, ՏԵՍԱՀՍԿՄԱՆ ՀԱՄԱԿԱՐԳԵՐԻ ՁԱՅՆԱԳՐՈՒԹՅՈՒՆՆԵՐԻ ՊԱՀՊԱՆՄԱՆ ԵՎ ՈՉՆՉԱՑՄԱՆ ԺԱՄԿԵՏՆԵՐԸ

5.1. Ընկերության օբյեկտներում տեղակայված տեսահսկման համակարգերի ձայնագրությունների նկատմամբ հասանելիությունը կարգավորվում է Տեղեկատվական անվտանգության քաղաքականությամբ և Ընկերության այլ ներքին իրավական ակտերով:

5.2. Օգտատերերի կողմից տեսահսկման համակարգերի ձայնագրությունների նկատմամբ հասանելիության իրավունքի փոխանցումն այլ անձանց արգելվում է:

5.3. Ընկերության օբյեկտների տեսահսկման համակարգերի տեսատեղեկատվության ձայնագրումը (պատճենումը) արտաքին կրիչի վրա կատարվում է միայն լիազորված աշխատողի կողմից՝ Ընկերության գլխավոր տնօրենի (նրա պաշտոնակատարի), Անվտանգության ծառայության և/կամ տեղեկատվական անվտանգության գծով ղեկավարի հանձնարարությամբ:

5.4. Տեսաարխիվների պահպանման ժամկետը սահմանվում է գործող օրենսդրության պահանջներին համապատասխան: Տեսահսկման համակարգը տեղեկատվությունը ձայնագրում է տեսագրանցիչ սարքի կոշտ սկավառակի վրա: Տեսաարխիվի պահպանման ժամկետը մինչև 90 օր է՝ կախված տեղադրման վայրերից և Ընկերության տարածքների կատեգորիաներից, որը լրանալուց հետո տեղի է ունենում ինքնաշխատ հեռացում: Տեսահսկման խցիկների կողմից կարգապահական զանցանքի, վարչական իրավախախտման, քրեական հանցագործության հատկանիշներ ունեցող իրավիճակների հնարավոր արձանագրման վերաբերյալ տեղեկատվություն ստանալու դեպքում նման տեսագրությունների պահպանման ժամկետը կարող է երկարաձգվել 4.12 կետի հիման վրա՝ Հայաստանի Հանրապետության օրենսդրությամբ նախատեսված համապատասխան միջոցառումների անցկացման ժամանակահատվածով:

5.5. Տեսագրությունները աշխատողների կողմից չեն կարող օգտագործվել անձնական և մասնագիտական գործունեության հետ չկապված այլ նպատակներով, և ենթակա չեն փոփոխման, օգտագործման, տարածման և տրամադրման, բացի օրենսդրական ակտերով նախատեսված դեպքերից:

5.6. Տեսահսկման համակարգերի ձայնագրությունների գաղտնիության խախտման պատճառների մեջ մեղավոր անձը պատասխանատվություն է կրում Հայաստանի Հանրապետության գործող օրենսդրությամբ նախատեսված կարգով: Տեսահսկման համակարգերի ձայնագրությունների օգտագործումն անձնական նպատակներով արգելվում է:

6.ՏԵՍԱՀՍԿՄԱՆ ՀԱՄԱԿԱՐԳԻ ԳՐԱՆՑՈՒՄՆԵՐԸ ԵՐՐՈՐԴ ԱՆՁԱՆՑ ՓՈԽԱՆՑԵԼՈՒ ԿԱՐԳԸ, ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՄՇԱԿՄԱՆ ՀԵՏ ԿԱՊՎԱԾ ԻՐԱՎՈՒՆՔՆԵՐԻ ԻՐԱՑՈՒՄԸ

6.1. Տեսաձայնագրությունը սահմանափակ շրջանառության տեղեկատվություն է, որը ենթակա չէ փոխանցման երրորդ անձանց, բացառությամբ Հայաստանի Հանրապետության գործող օրենսդրությամբ նախատեսված դեպքերի:

6.2. Տեսահսկման միջոցով ստացված տեղեկատվությունը համապատասխան ծառայություններին և պետական մարմիններին տրամադրվում է միայն նրանց գրավոր հարցումների հիման վրա՝ Հայաստանի Հանրապետության գործող օրենսդրությամբ նախատեսված դեպքերում:

6.3. Ոչ ստանդարտ իրավիճակների դեպքում անձնական տվյալների սուբյեկտի կողմից տեսագրության պատճենի դիտումը հնարավոր է Ընկերության գրասենյակում՝ տեսագրության տվյալ պատճենի վրա անձնական տվյալների այլ սուբյեկտների պատկերի բացակայության պայմանով: Եթե հաճախորդը դիմում է Ընկերությանը՝ տեսահսկման համակարգերի արխիվային ձայնագրությունները դիտելու խնդրանքով, հաճախորդի հետ հաղորդակցություն իրականացնող Ընկերության աշխատակիցը կատարում է նրա նույնականացնում, այնուհետև ձևավորում և ուղարկում է Անվտանգության ծառայությանը և տեղեկատվական անվտանգության գծով ղեկավարին (Microsoft Outlook-ի միջոցով) հարցում՝ վերը նշված տեղեկությունների նշմամբ: Վերոնշյալ կառուցվածքային ստորաբաժանումների կողմից հարցումը հաստատվելու դեպքում լիազորված աշխատակիցը կատարում է խնդրարկվող արխիվային տեսանյութի վերբեռնում և այն տրամադրում նախաձեռնողին (Ընկերության աշխատակցին)՝

հաճախորդին ցուցադրելու համար:

6.4. Ընկերությունում անձնական տվյալների մշակման հետ կապված իրավունքների իրացմանն աջակցելու համար անձնական տվյալների սուբյեկտը կարող է դիմել նաև «ՋԻԷՆՍԻ-ԱԼՖԱ» ՓԲԸ-ի անձնական տվյալների մշակման ներքին հսկողության իրականացման համար պատասխանատու անձին՝ էլեկտրոնային հաղորդագրություն ուղարկելով pdpo@ovio.am էլեկտրոնային փոստի հասցեին:

7. ԵԶՐԱՓԱԿԻՉ ԴՐՈՒՅԹՆԵՐ

7.1. Սույն քաղաքականությունը ուժի մեջ է մտնում հաստատման պահից:

7.2. Ընկերությունն իրավունք ունի տեսահսկման խցիկների ձայնագրություններն օգտագործել որպես ապացույց քաղաքացիական, քրեական, վարչական դատավարություններում՝ հակահիրավական արարքի կատարման փաստը (փաստերը) հաստատելու, ինչպես նաև ապացուցման ենթակա այլ հանգամանքներ պարզելու համար:

7.3. Ընկերությունն իրավունք ունի իր հայեցողությամբ միակողմանի կարգով փոփոխել և (կամ) լրացնել սույն Քաղաքականության պայմանները՝ առանց անձնական տվյալների սուբյեկտներին նախապես ծանուցելու՝ Քաղաքականության նոր խմբագրությունը կայքում տեղադրելու միջոցով:

7.4. Սույն Քաղաքականության մեջ չարծարծված անձնական տվյալների մշակմանը վերաբերող հարցերը կարգավորվում են Հայաստանի Հանրապետության օրենսդրությամբ և անձնական տվյալների մշակման վերաբերյալ քաղաքականությամբ:

7.5. Այն դեպքում, երբ Քաղաքականության որևէ դրույթ ճանաչվում է Հայաստանի Հանրապետության օրենսդրությանը հակասող, մնացած դրույթները, որոնք համապատասխանում են Հայաստանի Հանրապետության օրենսդրությանը, մնում են ուժի մեջ և վավեր են, իսկ ցանկացած անվավեր դրույթ կհամարվի հեռացված (փոփոխված) այնքանով, որքանով դա անհրաժեշտ է Հայաստանի Հանրապետության օրենսդրությանը համապատասխանությունն ապահովելու համար: