РОСГОССТРАХ

«ՌՈՍԳՈՍՍՏՐԱԽ-ԱՐՄԵՆԻԱ» ԱՊԱՀՈՎԱԳՐԱԿԱՆ ՓԱԿ ԲԱԺՆԵՏԻՐԱԿԱՆ ԸՆԿԵՐՈՒԹՅՈՒՆ

ՈՐԱԿԻ ԿԱՌԱՎԱՐՄԱՆ ՀԱՄԱԿԱՐԳ

ՀԱՍՏԱՏՎԱԾ Է

«Ռոսգոսստրախ-Արմենիա» ԱՓԲԸ
Խորհրդի կողմից
04.10.2017թ. Խորհրդի նիստի թիվ 08
արձանագրություն)
Խորհրդի նախագահ _____ Դ. Է. Խաչատուրով

«ՌՈՍԳՈՍՍՏՐԱԽ-ԱՐՄԵՆԻԱ» ԱՓԲԸ ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՔԱՂԱՔԱԿԱՆՈՒԹՅՈՒՆ

Փաստաթղթի կոդ QP630401

Խմբագրություն 01

Փաստաթուղթը խմբագրեց	Ստորաբաժանման անվանումը	Անվտանգության ծառայություն	
	ՏԱ պատասխանատու	Ռաֆայել Գրիգորյան	
Համաձայնեցվեց	Գործադիր տնօրեն	Գագիկ Գրիգորյան	
	Ներքին աուդիտի ղեկավար	Լիանա Բաբաջանյան	
	Մեթոդոլոգիայի և զարգացման գծով գործադիր տնօրենի տեղակալ	Վահագն Աղավելյան	
	Տեղեկատվական տեխնոլոգիաների դեպարտամենտի ղեկավար	Հայկ Սիմոնյան	
	Իրավաբանական դեպարտամենտի ղեկավար	Նարինե Խաչատրյան	
	Որակի կառավարման բաժնի ղեկավար	Մաքրուհի Բալաբանյան	

1. Նպատակ

1.1. «ՌՈՍԳՈՍՍՏՐԱԽ-ԱՐՄԵՆԻԱ» ԱՓԲԸ Տեղեկատվական անվտանգության քաղաքականությունը սահմանում է «ՌՈՍԳՈՍՍՏՐԱԽ-ԱՐՄԵՆԻԱ» ԱՓԲԸ կառուցվածքային և տարածքային ստորաբաժանումների կողմից «ՌՈՍԳՈՍՍՏՐԱԽ-ԱՐՄԵՆԻԱ» ԱՓԲԸ տեղեկատվության, լոկալ և կորպորատիվ ցանցի, սերվերային, ցանցային և համակարգչային տեխնիկայի անվտանգության քաղաքականությունը:

2. Կիրառման ոլորտը

2.1. «ՌՈՍԳՈՍՍՏՐԱԽ-ԱՐՄԵՆԻԱ» ԱՓԲԸ Տեղեկատվական անվտանգության քաղաքականությունը կիրառվում է «ՌՈՍԳՈՍՍՏՐԱԽ-ԱՐՄԵՆԻԱ» ԱՓԲԸ բոլոր աշխատողների կողմից:

3. Տարածման ոլորտը

3.1. «ՌՈՍԳՈՍՍՏՐԱԽ-ԱՐՄԵՆԻԱ» ԱՓԲԸ Տեղեկատվական անվտանգության քաղաքականությունը տարածվում է «ՌՈՍԳՈՍՍՏՐԱԽ-ԱՐՄԵՆԻԱ» ԱՓԲԸ բոլոր աշխատողների վրա:

4. Առնչվող փաստաթղթեր

4.1. ISO 9001:2015 «Որակի կառավարման համակարգեր: Պահանջներ»
4.2. ISO 27001:2013 «Տեղեկատվական անվտանգության կառավարման համակարգեր: Պահանջներ»
4.3. ՀՀ Կենտրոնական Բանկի 09.07.2013թ. No 173-Ն Որոշում

5. Սահմանումներ և հապավումներ

5.1. Ընկերություն՝ «ՌՈՍԳՈՍՍՏՐԱԽ-ԱՐՄԵՆԻԱ» ԱՓԲԸ
5.2. Քաղաքականություն՝ «ՌՈՍԳՈՍՍՏՐԱԽ-ԱՐՄԵՆԻԱ» ԱՓԲԸ ՏԱ անվտանգության քաղաքականություն
5.3. ՏԱԿՀ՝ Տեղեկատվության անվտանգության կառավարման համակարգ
5.4. ՏԱ՝ Տեղեկատվական անվտանգություն
5.5. Տեղեկատվական ակտիվներ՝ տվյալների բազաներ և ֆայլեր, համակարգային փաստաթղթեր, օգտագործողի փաստաթղթեր, ուսումնական նյութեր, բիզնեսի անընդհատության պահպանման պլաններ, անճշտությունների վերացմանն ուղղված միջոցառումների պլաններ, վերը դասակարգված տեղեկատվական ռեսուրսների նույնականացումներ (պատճեններ)
5.6. Ծրագրային ռեսուրսներ՝ օպերացիոն համակարգեր, համակարգչային ծրագրեր, ներքին մշակված ծրագրային ապահովման միջոցներ (insurance softweare)
5.7. Տեղեկատվական ռեսուրսներ՝ հաշվողական տեխնիկա (պրոցեսորներ, մոնիտորներ, փոխադրելի համակարգիչներ), կոմունիկացիոն սարքավորումներ (հեռախոսային կայաններ, երթուղղիչներ (router), ֆաքսեր, մոդեմներ), մագնիսային կրիչներ (երիզներ և սկավառակներ), այլ տեխնիկական սարքավորումներ (հոսանքի աղբյուրներ, օդամղիչներ), լրացուցիչ հարակից ծառայություններ՝ ջեռուցում, լուսավորում և այլն
5.8. Ռեսուրսների դասակարգումն ըստ կարևորության աստիճանի՝ Ընկերությունում սահմանված են տեղեկության հետևյալ դասերը՝ ընդհանուր-հասանելի, ոչ հրապարակային, գաղտնի:
5.9. Ապահովագրական գաղտնիք՝ ապահովագրական գործունեության ընթացքում ապահովադրի, ապահովագրված անձի կամ շահառուի վերաբերյալ ապահովագրողին, վերաապահովագրողին, ապահովագրական միջնորդություն իրականացնող անձին հայտնի դարձած ապահովադրի, ապահովագրված անձի կամ շահառուի առևտրային գաղտնիքը կամ այլ տեղեկություն, որն ապահովադիրը կամ ապահովագրված անձը մտադիր են եղել գաղտնի պահել, և Ընկերությունը, վերաապահովագրական ընկերությունը կամ ապահովագրական միջնորդը տեղյակ է կամ պարտավոր էր տեղյակ լինել այդ մտադրության վերաբերյալ:
5.10.Ընդհանուր-հասանելի տեղեկատվություն՝ զանգվածային լրատվական միջոցներով, հրապարակման, տեղեկատվական հաղորդակցման ցանցերում տեղադրման ենթակա

տեղեկություն: Տեղեկատվությունը որպես «Ընդհանուր-հասանելի» ճանաչվելու որոշումն ընդունում է գործադիր տնօրենը:

5.11.Ոչ հրապարակային տեղեկատվություն՝ Ընկերության ստորաբաժանումների կանոնակարգեր, գործադիր տնօրենի հրամաններ, ցանկացած ներքին գրագրություն (զեկուցագրեր, տեղեկանքներ), Ընկերության Խորհրդի որոշումներ, Ընկերության հաստիքացուցակ, Ընկերության ռազմավարություն, ներքին իրավական ակտեր՝ բացառությամբ գործադիր տնօրենի կողմից «Ընդհանուր-հասանելի» կարգավիճակ ստացած ակտերի:

5.12.Գաղտնի տեղեկատվություն՝ ապահովագրական գաղտնիք պարունակող տեղեկատվություն, հաճախորդների և գործընկերների հետ կնքված պայմանագրեր, բիզնես գործընթացների նկարագրություններ, Ընկերության անվտանգության քաղաքականությունը՝ իր բոլոր բաղկացուցիչ տարրերով, Տեղեկատվական տեխնոլոգիաների անվտանգությանը և ավտոմատացմանը վերաբերվող փաստաթղթեր, ինչպես նաև ապահովագրական գաղտնիք չհանդիսացող, «գաղտնի» գրառմամբ մտից փաստաթղթերը և գործադիր տնօրենի կողմից որպես այդպիսին ճանաչված տեղեկատվությունը:

5.12.1. Ընկերության աշխատողներին խիստ արգելվում է հրապարակել տեղեկատվություն սկսած «Ոչ հրապարակային» դասից: Ամեն դասի համար պետք է սահմանվեն հետևյալ գործողությունները՝ պատճենահանում, պահպանում, փոխանցում փոստով, ֆաքսով, էլեկտրոնային փոստով, փոխանցում բանավոր, ներառյալ բջջային հեռախոսները, ձայնային փոստը, վերացում:

5.13.SS համակարգերի օգտագործողների դասակարգում՝ Ընկերության օգտագործողները դասակարգվում են հետևյալ կերպ՝ Ադմինիստրատորներ, Ղեկավարություն, Աշխատողներ, Ժամանակավոր աշխատողներ (պրակտիկանտներ, հայցորդներ), կապալառուներ:

5.13.1. Ադմինիստրատորների դասին են վերաբերվում նաև SS անվտանգության ադմինիստրատորները:

5.13.2. Վերջիններս լիարժեք հասանելիություն ունեն SS ադմինիստրավորման հետ կապված ռեսուրսների բազաներին:

5.13.3. Ղեկավար դասին են պատկանում Ընկերության գործադիր տնօրենը, նրա տեղակալները և դեպարտամենտի ղեկավարները:

5.13.4. Աշխատողներ խմբին են դասվում Ընկերության մյուս բոլոր աշխատողները:

5.13.5. Ժամանակավոր աշխատողներ դասին են պատկանում պրակտիկանտները, հայցորդները և բոլոր այն անհատները, որոնց Ընկերությունում գտնվելը կրում է ժամանակավոր բնույթ (օրինակ՝ խորհրդատուները, արտաքին սերտիֆիկացման մարմնի աուդիտորները և այլն):

6. Պատասխանատվության կենտրոններ

6.1. Սույն Քաղաքականության մշակման համար պատասխանատու է ՏԱ պատասխանատուն:

6.2. Սույն Քաղաքականության բովանդակության համաձայնեցման համար պատասխանատու է Ընկերության Գործադիր տնօրենը, Մեթոդոլոգիայի և զարգացման գծով գործադիր տնօրենի տեղակալը, Իրավաբանական դեպարտամենտի ղեկավարը, Որակի կառավարման բաժնի ղեկավարը, Ներքին աուդիտի ղեկավարը, Տեղեկատվական տեխնոլոգիաների դեպարտամենտի ղեկավարը:

6.3. Սույն Քաղաքականության հաստատման համար պատասխանատու է Ընկերության Խորհուրդը:

6.4. Սույն Քաղաքականությունն օգտագործողներին տրամադրելու համար պատասխանատու է Որակի կառավարման բաժնի ղեկավարը:

6.5. Սույն Քաղաքականության բնօրինակի պահպանման համար պատասխանատու է Որակի կառավարման բաժնի ղեկավարը:

6.6. Սույն Քաղաքականության մեջ փոփոխություններ կատարելու համար պատասխանատու է ՏԱ պատասխանատուն:

6.7. Օգտագործողների կողմից սույն Քաղաքականության պահանջներին հետևելը ստուգելու համար պատասխանատու են Որակի և ՏԱ ներքին ստուգողները:

7. Փոփոխություններ

7.1. Առաջին խմբագրություն:

8. Հավելվածներ

8.1. Հավելվածներ չկան

9. ԸՆԿԵՐՈՒԹՅԱՆ ՇԱՀԱԳՐԳԻՌ ԿՈՂՄԵՐԸ

9.1. Ընկերությունը, հաշվի առնելով իր ազդեցության կամ հնարավոր ազդեցության ուժն իր կողմից անխափանորեն ծառայություններ մատուցելու կարողություն վրա, որոնք պետք է համապատասխանեն սպառողների պահանջմունքներին, օրենսդրական և իրավական պահանջներին, սահմանել է հետևյալ շահագրգիռ կողմերը և նրանց պահանջները, որոնք էական նշանակություն ունեն Տեղեկատվական անվտանգության կառավարման համակարգի համար.

9.2. Բաժնետերեր

9.2.1. Ապահովել Ընկերության գաղտնի և ոչ հրապարակային տեղեկատվության անվտանգությունը, ամբողջականությունն ու հասանելիությունը՝ համապատասխան կողմերին, ներառյալ հաճախորդների և գործընկերների ոչ հրապարակային, ինչպես նաև Ընկերության համար մրցակցային առավելության նշանակությամբ տեղեկատվությունը:

9.3. Հաճախորդներ

9.3.1. Ապահովել անձնական տվյալների և ապահովագրական ու բժշկական պատմության գաղտնիության ապահովումը և դրանց հասանելիությունը համապատասխան կողմերին՝ ըստ անհրաժեշտության:

9.4. Աշխատողներ

9.4.1. Ապահովել անձնական տվյալների, աշխատավարձի և այլ ոչ հրապարակային տեղեկատվության անվտանգությունը:

9.4.2. Տրամադրել տեղեկատվական անվտանգության ապահովման համար անհրաժեշտ նյութատեխնիկական ռեսուրսներն ու իրազեկվածությունը:

9.5. Պայմանագրի կողմեր

9.5.1. Ապահովել պայմանագրի ոչ հրպարակային տեղեկատվության ապահովումը, ներառյալ մրցակցային առավելության նշանակությամբ տեղեկատվությունը:

9.6. Մատակարարներ

9.6.1. Ապահովել համագործակցության շրջանակներում փոխանակվող ոչ հրպարակային տեղեկատվության ապահովումը, ներառյալ մրցակցային առավելության նշանակությամբ տեղեկատվությունը:

9.7. Հասարակություն

9.7.1. Ապահովել Ընկերության կողմից առաջարկվող ծառայությունների մասին ամբողջական տեղեկատվության հաղորդակցությունը:

9.7.2. Պատշաճ կերպով և ժամանակին հաղորդակցվել հասարակությանը առնչվող տեղեկատվական անվտանգության պատահարների մասին:

9.8. Կառավարություն և Վերահսկող մարմիններ

9.8.1. Ընկերության գործունեության մասին թափանցիկ, ամբողջական և ճշգրիտ հաշվետվությունների ժամանակին ստացում:

10. Նկարագրություն

10.1.Ընդհանուր դրույթներ

10.1.1. Սույն Քաղաքականությունը սահմանում է տեղեկատվության անվտանգության ապահովման շրջանակներում գործունեության նպատակները, խնդիրները, դրանց հասնելու

սկզբունքներն ու միջոցները: Այն ուղղված է Ընկերության կորպորատիվ տվյալների համարժեք պաշտպանվածության և գաղտնիության ապահովմանն ուղղված աշխատանքների իրականացմանը, յուրաքանչյուր շահառու կողմի իրավունքների, պարտականությունների և պատասխանատվությունների հստակ սահմանման միջոցով:

10.1.2. Սույն Քաղաքականությունը ներառում է հետևյալ սկզբունքները՝

10.1.2.1. Տվյալների գաղտնիությունն ապահովվում է հասանելիության կառավարման վերահսկվող և պարտադիր միջոցներով:

10.1.2.2. Ընկերությունում տեղադրվում են միայն արտոնագրված ծրագրային փաթեթներ՝ SS դեպարտամենտի տեխնիկական աջակցման բաժնի աշխատողների կողմից:

10.1.2.3. Բոլոր տեղեկատվական հոսքերը վերահսկվում են և անհրաժեշտության դեպքում սահմանափակվում:

10.1.2.4. Ընկերությունում կիրառվում է գաղտնաբառերի սահմանման և օգտագործման կորպորատիվ քաղաքականություն:

10.1.2.5. Տեղեկատվական համակարգերի հասանելիությունն ու աշխատանքի անընդհատությունն ապահովվում է տվյալների և սարքավորումների կարգավորումների պահուստային կրկնօրինակման միջոցով:

10.1.2.6. Ընկերության աշխատանքների անընդհատությունն ապահովվում է Գործունեության անընդհատության ապահովման ընթացակարգի և պլանի համաձայն, որի արդյունավետությունը պարբերաբար գնահատվում է պլանավորված ուսումնավարժանքներով:

10.1.2.7. Աշխատողների համար պլանավորվում և անցկացվում են իրազեկման և վերապատրաստման ծրագրեր ՏԱ թեմայով:

10.1.2.8. Ընկերության արտաքին շահառուներին (օրինակ՝ կապալառուներին) ծանուցվում է ՏԱ Քաղաքականության և համապատասխան ընթացակարգերի պահանջները՝ պայմանագրային դրույթներով:

10.1.2.9. Վերլուծվում են տեղեկատվության անվտանգության հետ կապված վտանգների հավանականությունն ու դրանց ազդեցության ուժգնությունը, և համապատասխանաբար սահմանվում ու ներդրվում են ՏԱ ռիսկերի նվազեցման միջոցառումները:

10.1.2.10. Արձանագրվում, դասակարգվում և վերլուծվում է տեղեկատվության անվտանգության հետ առնչվող յուրաքանչյուր միջադեպ, որի արդյունքում սահմանվում են ուղղիչ և կանխարգելիչ գործողություններ՝ բացառելու դրա կրկնման հավանականությունը:

10.1.3. Ղեկավարությունը հավանություն է տալիս ՏԱ քաղաքականությանը և տրամադրում է անհրաժեշտ միջոցներ համակարգի ներդրման և շարունակական բարելավման համար:

10.1.4. Ընկերության Տեղեկատվության Անվտանգության Քաղաքականության հիմքում ընկած է ISO 27001:2013 միջազգային ստանդարտը:

10.2. Հակավիրուսային պաշտպանություն

10.2.1. Ընկերության հակավիրուսային պաշտպանության համակարգը բազմամակարդակ և կենտրոնացված համակարգ է, որն ապահովում է հակավիրուսային բազաների ամենօրյա թարմացումը և հակավիրուսային իրավիճակի մոնիթորինգն ու վերահսկումը:

10.2.2. Ադմինիստրավորման և տեխնիկական աջակցման բաժինը պետք է ապահովված լինի ժամանակակից հակավիրուսային համակարգով համակարգչային վիրուսների հայտնաբերման և հեռացման համար: Ընկերության սերվերների և աշխատակայանների վրա պարտադիր տեղադրված են հակավիրուսային ծրագրեր, որոնք ավտոմատ կերպով մշտապես թարմացվում են ամենավերջին հակավիրուսային նորացումներով: Հակավիրուսային ծրագրերը ավտոմատ կերպով ստուգում են համակարգչին միացվող բոլոր արտաքին սարքերը, համակարգչում տեղադրվող և արդեն տեղադրված ծրագրային փաթեթները, բոլոր ցանցային միացումները: Ընկերության

աշխատողները տեղեկացված են վիրուսների կողմից հասցվող վնասների հնարավորության և Ընկերության հակավիրուսային քաղաքականության մասին:

10.2.3. Շահառու կողմերը պետք է տեղեկացվեն Ընկերությունում վիրուսային պատահարների մասին:

10.2.4. Օգտագործողները վիրուսների առկայության կասկածի դեպքում պարտավոր են անհապաղ տեղեկացնել Ադմինիստրավորման և տեխնիկական աջակցման բաժին, որը միջոցներ կձեռնարկի միջադեպի պատճառների հայտնաբերման և հեռացման ուղղությամբ: Գործընթացը պետք է կառավարվի ՏԱ պատահարների կառավարման ընթացակարգերով:

10.3.Տեղեկատվության ֆիզիկական անվտանգություն

10.3.1. «Ոչ հրապարակային» դասակարգվող տեղեկատվությունը ենթակա է չարտոնագրված հասանելիությունից պաշտպանության՝ մուտքի սահմանափակման միջոցով: Տվյալ դասին պատկանող տեղեկատվության հասանելիությունը կարող է իրականացվել լոկալ կամ հեռակա կերպով. հեռակա հասանելիությունն իրականացվում է տրաֆիկի կոդավորման միջոցների կիրառմամբ: «Ոչ հրապարակային» մակարդակի տեղակատվությանը հասանելիություն տրվում է ըստ օգտագործողների կատեգորիաների՝ ադմինիստրատորներ, ղեկավարներ, աշխատողներ: Տվյալ դասին պատկանող տեղեկատվության պատճենահանումը և ցանկացած փոխանցումը սահմանափակվում է Ընկերության տարածքով: Տեղեկատվության ոչնչացումը հնարավոր է միայն դրա սեփականատիրոջ կողմից:

10.3.2. «Գաղտնի» դասակարգվող տեղեկատվությունը ենթակա է չարտոնագրված հասանելիությունից կրիպտոգրաֆիական պաշտպանության և մուտքի պարտադիր արձանագրմամբ: Կորպորատիվ ցանցից հեռակա մուտքն իրականացվում է տրաֆիկի կոդավորման միջոցների կիրառմամբ: Տվյալ դասին պատկանող տեղեկատվության պատճենահանումը և ցանկացած փոխանցումը հնարավոր է միայն Ընկերության տարածքի սահմաններում և միայն լիազորված աշխատողների կողմից: «Գաղտնի» դասակարգվող տեղեկատվության հեռացման իրավունք ունի միայն անվտանգության ադմինիստրատորը SS ադմինիստրատորի հետ միասին (գլխավոր ադմինիստրատորի/օգտագործողի գաղտնաբառը բաժանված է երկուսի միջև) գործադիր տնօրենի թույլատվությամբ:

10.3.3. Անհրաժեշտ է գույքագրել, դասակարգել և մակնշել (պիտակավորել) տեղեկատվական բոլոր ակտիվները (բացառությամբ ընդհանուր հասանելի ակտիվներից)՝ ելնելով Ընկերության հիմնական գործառնությունների պահանջներից:

10.3.4. Յուրաքանչյուր աշխատող պետք է պահպանի իրեն հատկացված տեղեկատվական համակարգերի մուտքի տվյալները, դրանց չտրամադրելով երկրորդ կողմին ինչպես նաև դրանց չպահպանելով ուրիշներին հասանելի վայրում: Աշխատողները պետք է նաև՝

- **10.3.4.1.** դասավորված պահեն աշխատասեղանը,
- **10.3.4.2.** ոչ հրապարակային և գաղտնի ակտիվները պահպանեն փակվող պահարանում,
- **10.3.4.3.** աշխատասեղանը լքելուց անջատեն (hibernate, sleep, lock) համակարգիչը,
- **10.3.4.4.** փաստաթղթերը սեղանին դնեն հակառակ կողմով,
- **10.3.4.5.** համակարգչի էկրանը դարձնեն անհասանելի կողմնակի անձանց:

10.3.5. Աշխատակայաններն ապահովված են անխափան էլեկտրամատակարարման ապահովման սարքավորումներով, որոնք ենթակա են պարբերաբար տեստավորման:

10.3.6. Սերվերները և հատուկ նշանակության համակարգիչներն ու այլ SS տեխնիկաները, որտեղ գործարկված է սերվերային ծրագրային փաթեթներ տեղակայվում են հատուկ կահավորված սերվերային սենյակներում, իսկ սենյակներից դուրս գտնվելու դեպքում՝ հատուկ պաշտպանված պահարաններում:

10.3.7. Տեղեկատվության պահպանման նպատակով կիրառվում են պահուստային կրկնօրինակման և արխիվացման միջոցառումներ:

10.3.8. Իրականցվում է ելքային և մուտքային Ֆաքսմիլային հաղորդագրությունների հաշվառում:

10.4.Հասանելիության կառավարում

10.4.1. Աշխատակայանների և սերվերների վրա վարվում են գործողությունների գրանցամատյաններ, որտեղ գրանցվում են համակարգերի աշխատանքի կարևորագույն իրադարձությունները, ինչպես նաև բոլոր մուտքերը համակարգ: SS ադմինիստրատորների ու անվտանգության պատասխանատուների կողմից իրականացվում է գրանցամատյանների մոնիթորինգ, պարտադիր ուսումնասիրության առարկա են հանդիսանում սխալ կատարված կամ ոչ արտոնյալ մուտքերի փորձերը:

10.4.2. Օգտագործողների առանձին դասերի համար սահմանվում են ֆիզիկական պաշտպանության, մուտքի սահմանափակման, կրիպտոգրաֆիական պաշտպանության, «Backup»-ի, հակավիրուսային պաշտպանության առանձին պահանջներ:

10.5.Լոկալ ցանցի անվտանգություն

10.5.1. Լոկալ ցանցի սարքավորումները՝ ներառյալ ցանցային կոմուտատորներն ու ուղղորդիչները տեղակայվում են առանձնացված սենյակներում կամ հատուկ փակվող պահարաններում, որտեղ ապահովված են անխափան էլեկտրասնուցումը և համապատասխան ջերմային ռեժիմը: Նման տարածքների մուտքն արտոնվում է Գործադիր տնօրենի հրամանով սահմանված անձանց:

10.5.2. Ընկերությունում անցկացված և տեղադրված ցանկացած հոսանքի, հեռախոսի, ցանցային և այլ լարանցում պարտադիր պետք է արտապատկերվեն փաստաթղթային եղանակով և ցանկացած փոփոխության դեպքում թարմացվեն:

10.5.3. Ցանցային լարանցումները պետք է պաշտպանված լինեն անօրինական միացումներից կամ վնասվածքներից: Արգելվում է փակել տեխնիկական անձնակազմի հասանելիությունը ցանցային մալուխներին: Ընկերության բոլոր լարանցումները պետք է փակված լինեն պաշպանիչ տուփերով: Բոլոր տեսակի լարանցումների կենտրոնացման վայրերը պետք է ամփոփվեն արկղերի մեջ, որոնք պետք է կողպվեն և հասանելի լինեն միայն SS դեպարտամենտի անձնակազմի համար:

10.5.4. Էլեկտրոմագնիսական ազդեցություններից զերծ մնալու նպատակով հեռահաղորդակցման լարանցումները պետք է առանձնացված լինեն հոսանքի՝ հատկապես բարձրավոլտ լարանցումներից:

10.5.5. Ցանցի բոլոր չօգտագործվող կետերն ապաակտիվացվում կամ անջատվում են:

10.5.6. Լրացուցիչ պահուստային լարանցումներ հանգույցային կետերի միջև ապահովվում են այնտեղ, որտեղ դա հնարավոր է:

10.5.7. Ոչ լիազորված մուտքի փորձերը հայտնաբերելու և կանխարգելելու նպատակով ցանցում կիրառվում են ներխուժման հայտնաբերման համակարգեր:

10.6.Սերվերների անվտանգություն

10.6.1. Սերվերները և հատուկ համակարգիչները, որոնց վրա տեղակայված է սերվերային ծրագրային փաթեթներ, տեղակայվում են հատուկ սենյակներում, որոնք ապահովված են՝

- **10.6.1.1.** հատուկ ջերմային ռեժիմով
- **10.6.1.2.** մուտքի սահմանապակման համակարգով
- **10.6.1.3.** տեսադիտարկման համակարգով
- **10.6.1.4.** հակահրդեհային համակարգով
- **10.6.1.5.** ահազանգման համակարգով
- **10.6.1.6.** կրկնակի էլեկտրասնուցման գծերով
- **10.6.1.7.** անխափան էլեկտրասնուցման համակարգով
- **10.6.1.8.** խոնավության և ջրի առկայության չափիչ սարքերով:

10.6.2. Սերվերների վրա պարբերաբար իրականացվում է օպերացիոն համակարգերի թարմացում:

10.6.3. Սերվերների ադմինիստրավորումը հիմնականում իրականացվում է հեռակառավարման ծրագրերի միջոցով, որոնց հասանելիությունը տրված է միայն ադմինիստրավորման և տեխնիկական աջակցման բաժնի ադմինիստրատորներին:

10.6.4. Ադմինիստրատորական իրավասությունները տրամադրվում է միայն հատուկ ուսուցում անցած ադմինիստրավորման և տեխնիկական աջակցման բաժնի անձնակազմին:

10.6.5. Admin/Administrator/root/sa անունների օգտագործումը բերվում է նվազագույնի:

10.6.6. Բոլոր սերվերների վրա տեղադրված է ծրագրային փաթեթ, որն ավտոմատ անջատում է սերվերները, սահմանված ժամանակահատվածում պահուստային կամ հիմնական էլեկտրասնուցման համակարգի չվերականգնման դեպքում:

10.7. Կորպորատիվ ցանցի անվտանգություն

10.7.1. Ոչ լարային ցանցի օգտագործման դեպքում կիրառվում են գաղտնագրման միջոցառումներ:

10.7.2. Աշխատակայաններում ոչ լարային սարքավորումների տեղադրումն իրականացվում է միայն ադմինիստրավորման և տեխնիկական աջակցման բաժնի անձնակազմի կողմից: Օգտագործողներին արգելվում է ինքնուրույն տեղադրել սարքավորումներ:

10.7.3. Աշխատակայաններում մոդեմային կապի տեղադրումն իրականացվում է միայն ադմինիստրավորման և տեխնիկական աջակցման բաժնի անձնակազմի կողմից: Օգտագործողներին արգելվում է մոդեմային կապի օգտագործումն առանց SS դեպարտամենտի ղեկավարի թույլտվության:

10.7.4. Չօգտագործվող արձանագրությունները հեռացվում են ուղղորդիչներից, իսկ չօգտագործվող ցանցային միացումներն ավտոմատ անջատվում են:

10.7.5. Արտաքին տեղեկատվական համակարգերի հետ կապը, ինչպես նաև ցանցին հեռակա միացումները, իրականացվում է VPN ցանցերի միջոցով IPSEC կամ SSL արձանագրությունների կիրառմամբ:

10.7.6. Մասնաճյուղային կապի ապահովումն իրականացվում է VPN ցանցի միջոցով IPSEC արձանագրության կիրառմամբ:

10.7.7. Համացանցի և այլ արտաքին տեղեկատվական ռեսուրսների հասանելիությունը տրամադրվում է միայն սահմանափակ թվով անձնակազմի:

10.7.8. Էլեկտրոնային փոստի բոլոր հաղորդագրությունները գրանցվում և պարբերաբար վերահսկվում են:

10.8. Գործունեության անընդհատության ապահովում

10.8.1. Ընկերության գործընթացների անընդհատության ապահովման համար էական նշանակություն ունեցող համակարգերը և սերվերները պետք է ունենան պահուստային սերվերներ, որոնցում պետք է տեղադրված լինի համակարգը և նրանում պահպանվող տեղեկատվության աշխատունակ կրկնօրինակը (հնարավորության դեպքում):

10.8.2. Պահուստային սերվերները պետք է տեղակայված լինեն հիմնական սերվերներից որոշակի հեռավորության վրա՝ հաշվի առնելով արտակարգ իրավիճակների և դրանց ազդեցության գնահատման արդյունքները:

10.8.3. Պետք է սահմանվեն անվտանգության միջոցառումներ, որոնք կապահովեն տվյալների ամբողջականությունը պահուստային կրկնօրինակների վերականգնման ժամանակ:

10.8.4. Ոչ ստանդարտ և արտակարգ իրավիճակներում Ընկերության աշխատանքի անընդհատությունն ապահովելու համար Ընկերությունն առաջնորդվում է արտակարգ իրավիճակներում Ընկերության գործունեության անընդհատության ապահովման և աշխատունակության վերականգնման պլանի համաձայն:

10.8.5. Գլխավոր գրասենյակի տարածքների վնասման դեպքում կառուցված է պահուստային կենտրոն, որտեղ կրկնօրինակված են և պահվում են բոլոր կարևորագույն համակարգերն անընդհատ աշխատունակ վիճակում:

10.8.6. Յուրաքանչյուր ավտոմատացված համակարգի տվյալների շտեմարան և սերվերներում տեղակայված տեղեկատվություն պետք է պարբերաբար կրկնօրինակվեն: Կրկնօրինակները պետք է պահպանվեն ապահով վայրում:

10.8.7. Աշխատողները պետք է վերապատրաստվեն և իրազեկվեն Ընկերության գործունեության անընդհատության ապահովման և աշխատունակության վերականգնման պլանի մասին: Ընկերության գործունեության անընդհատության ապահովման և աշխատունակության վերականգնման պլանի և աշխատողների և համակարգային պատրաստվածության գնահատման համար պետք է պլանավորել և իրականացնել ուսումնավարժանքներ՝ ներառյալ կորպորատիվ ցանցի թափանցելիության թեստեր (penetration test):

10.8.8. Համակարգերի աշխատանքների անընդհատության ապահովման ընթացակարգն ու պլանը պետք է պարբերաբար ստուգվեն SS և ՏԱ պատասխանատուների կողմից:

10.9.Ձայնի փոխանցման անվտանգություն

10.9.1. Հեռախոսակապի համար օգտագործվում են առավել նվազ խոցելի միջոցներ:

10.9.2. Ներքին ԱՀԿ կառավարման ծրագրային ապահովումը և միացումը ԱՀԿ-ին պաշտպանված է գաղտնաբառով:

10.9.3. Հեռախոսազանգերը գրանցվում և ուսումնասիրվում են: