

ՀԱՍՏԱՏՎԱԾ Է
«ՌԵՍՈ» ԱՊԱՀՈՎԱԳՐԱԿԱՆ
ՓԱԿ ԲԱԺՆԵՏԻՐԱԿԱՆ ԸՆԿԵՐՈՒԹՅԱՆ
Խորհրդի որոշմամբ

ստ 27.10.2016թ.

«ՌԵՍՈ» Ապահովագրական ՓԲԸ խորհրդի նախագահ՝

Գ. Զաքարյան



«ՌԵՍՈ» ԱՊԱՀՈՎԱԳՐԱԿԱՆ ՓԲԸ
ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՔԱՂԱՔԱԿԱՆՈՒԹՅԱՆ
ՔԱՂՎԱԾՔ

ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԿԱՌԱՎԱՐՄԱՆ ՀԱՄԱԿԱՐԳԸ

1. ՏԱԿՀ-ը հանդիսանում է Ընկերության կառավարման ընդհանուր համակարգի անբաժանելի մաս:
2. ՏԱԿՀ-ը գործունեությունը հիմնված է ռիսկերի վերլուծության և գնահատման վրա:
3. ՏԱԿՀ-ը կոչված է ապահովելու, վերլուծելու, պարբերաբար վերանայելու և հետևողականորեն բարելավելու տեղեկատվական անվտանգության ապահովման գործընթացը:
4. ՏԱԿՀ-ի բաղկացուցիչ մասերն են՝
 - կազմակերպչական համապատասխան կառուցվածքը՝ տեղեկատվական անվտանգության ապահովման ոլորտում դերերի և պատասխանատվությունների բաժանում,
 - քաղաքականություններ և կանոնակարգեր՝ մշակված ՀՀ Կենտրոնական բանկի իրավական ակտերի, միջազգային լավագույն փորձի և համապատասխան ստանդարտների պահանջների հիման վրա,
 - ռիսկերի կառավարման գործընթացը,
 - տեղեկատվական միջադեպերի կառավարման գործընթացը,
 - տեղեկատվական անվտանգության պլանավորման, մոնիտորինգի, վերանայման և բարելավման գործընթացները՝ փաստաթղթավորված համաձայն գրանցումների և փաստաթղթերի կառավարման ստանդարտների պահանջների:

ՏԱԿՀ ՇՐՋԱՆԱԿԸ

1. Ընկերությունում ՏԱԿՀ-ն տարածվում է ապահովագրական գործունեության վրա, որը իրականացվում է Հայաստանի Հանրապետությունում, ք. Երևան, 0014, Կոմիտասի պող. , 62 շ. , 93-93/1 հասցեում, և ապահովում է հաճախորդների և կոմերցիոն տեղեկատվության անվտանգությունը, պահպանումը և ամբողջականությունը:

ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՔԱՂԱՔԱԿԱՆՈՒԹՅԱՆ ՆՊԱՏԱԿԸ

1. ՏԱ քաղաքականության հիմնական նպատակն է սահմանել Ընկերության ներսում տեղեկատվական տեխնոլոգիաների կիրառման, հսկման, գործելու և զարգացման հիմնական ուղղությունները:
2. ՏԱ քաղաքականությունը մեթոդաբանական հիմք է հանդիսանում Ընկերությունում տեղեկատվական անվտանգության ապահովման նպատակով մշակվող այլ փաստաթղթերի (կարգերի, որոշումների, ընթացակարգերի, պայմանագրերի և այլն) համար:
3. ՏԱ ապահովման նպատակով կազմվող փաստաթղթերը մշակվում են՝ հաշվի առնելով հետևյալ հիմնադրությունները.
 - տեղեկատվության գաղտնիություն՝ տեղեկատվության պաշտպանությունը չթույլատրված ընթերցումից, արտահոսքից, հրապարակումից և չարտոնագրված տրամադրումից,

Հանրամատչելի

- տեղեկատվության ամբողջականության՝ տեղեկատվության հուսալիության, չարտոնագրված փոփոխումների ապահովագրության, ամբողջականության և մշակման մեթոդների ապահովություն,
 - տեղեկատվության հասանելիության՝ արտոնագրված/նույնականացված օգտագործողներին անհրաժեշտ տեղեկատվության և դրա հետ կապված ակտիվների հասանելիության ապահովում,
 - պատասխանատվության բաժանում/դերերի բաժանում,
 - հսկողություն:
4. Տեղեկատվական անվտանգության քաղաքականության նպատակն է.
- ապահովել Ընկերության կողմից մշակվող, պահպանվող, ներկայացվող, ստացվող և փոխանցվող տեղեկատվության անվտանգությունը,
 - ապահովել Ընկերության կողմից կիրառվող տեխնիկաձրագրային և ցանցային համակարգերի անվտանգությունը,
 - կազմակերպել ֆիզիկական անվտանգությունը,
 - ապահովել Ընկերության բիզնես գործընթացների անընդհատությունը,
 - Ընկերության ՏԱԿՀ-ը համապատասխանեցնել ԻՍՕ/ԻԷԿ 27001:2005 և ԻՍՕ/ԻԷԿ 27001:2013 «Տեղեկատվական տեխնոլոգիաներ. Անվտանգության ապահովման մեխանիզմներ. Տեղեկատվական Անվտանգության Կառավարման Համակարգեր. Պահանջներ» ստանդարտի պահանջներին,
 - պատշաճ կերպով ապահովել ՀՀ Կենտրոնական Բանկի կողմից ընդունված նորմատիվ ակտերով սահմանված պահանջները,
 - ապահովել ՀՀ օրենսդրության և միջազգային իրավական ակտերի պահանջների կատարումը Ընկերության կողմից: