ԹՎԱՅԻՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ

ԽՈՐՀՐԴԱՏՎԱԿԱՆ ՔԱՂԱՔԱԿԱՆՈՒԹՅՈՒՆ

ՈՉ ԱՌԵՎՏՐԱՅԻՆ ԿԱԶՄԱԿԵՐՊՈՒԹՅՈՒՆՆԵՐԻ ՀԱՄԱՐ

Այս քաղաքականության մշակմանն աջակցել է Բազմակողմանի տեղեկատվության ինստիտուտը:

ք.Գյումրի 2022թ.

Բովանդակություն

Հիմնախնդիր

Հայաստանում գործող շահույթ չհետապնդող կառույցների մեծամասնության շրջանում թվային անվտանգությունը չի համարվում առաջնահերթություն՝ գործունեության իրականացման ապահովության, թվային ակտիվների պաշտպանության ուղղությամբ ինստիտուցիոնալ հիմքերի ներդրման, անձնական տվյալների պաշտպանության, գաղտնիության քաղաքականության ապահովման համատեքստում:

Չնայած այն բանին, որ երկրում գործող ակտիվ կազմակերպությունները թիրախավորվում են և՛ արտաքին, և՛ ներքին ուժերի կողմից, մի կողմից ադրբեջանական, թուրքական և այլ երկրների կառավարությունների ու հաքերային խմբերի, մյուս կողմից, իշխանությունների և քաղաքական այլ խմբերի կողմից՝ մարդու իրավունքների և ժողովրդավարության համատեքստում ակտիվ գործունեություն ծավալելու հիմքով, այդուհանդերձ թվային միջավայրում գործունեության նկատմամբ կարևորությունը չի գնահատվում ըստ արժանվույն: Այս խնդիրը պայմանավորված է նաև համապատասխան ռեսուրսների և փորձագիտական աջակցության պակասով:

Թվային անվտանգության նկատմամբ նման իրավիճակը հաճախ բերում է մի շարք ռիսկերի՝ թվային ակտիվների կորստի, թվայնացված և ֆիզիկական տվյալների կորստի, անձնական տվյալների և գաղտնի տվյալների արտահոսքի, ֆիզիկական և թվային հարձակումների, կազմակերպության գործունեության խաթարման, կազմակերպության նկատմամբ անվստահության առաջացման և այլն:

Նպատակ

Այս քաղաքականության նպատակն է նպաստել Հայաստանում գործող շահույթ չհետապնդող կառույցների թվային անվտանգությանը և ֆիզիկական պաշտպանվածությանը: Այն խթանում է կազմակերպության թվային ակտիվների պաշտպանության նպատակով ինստիտուցիոնալ հիմքերի ներդրմանն ու կիրառմանը՝ որպես կազմակերպության առօրյա գործունեության մաս:

Քաղաքականությունում ներկայացված խորհրդատվական բնույթի առաջարկները միտված են պաշտպանելու կազմակերպության թե՛ թվային ակտիվները, թե՛ ֆիզիկական անվտանգությունը, ինչպես նաև մեղմացնելու/չեզոքացնելու հնարավոր ռիսկերը, որոնք կարող են հանդիսանալ թվային տվյալների կորստի և/կամ արտահոսքի պատճառ:

Խնդիրներ

Այս քաղաքականության խնդիրները նպատակաուղղված են լուծելու կազմակերպությունների թվային ակտիվների անվտանգությունը, թվային անվտանգության ապահովումը ֆիզիկական համատեքստում, հնարավոր ռիսկերի չեզոքացումը ու կանխարգելումը: Խորհրդատվական բնույթի քաղաքականության խնդիրն է աջակցել կազմակերպություններում թվային ակտիվների պաշտպանության ինստիտուցիոնալ հիմքերի ներդրմանը և դրանց կանոնակարգմանը, ինչպես առօրյա գործունեության, այնպես էլ ճգնաժամային ու ֆորս մաժորային իրավիճակներում և անհաղթահարելի ուժի պայմաններում:

Ստորև ներկայացված են սույն քաղաքականության խնդիրները՝

- Ներկայացնել խորհրդատվական բնույթի առաջարկներ ուղղված թվային ակտիվների անվտանգությանը:
- Ներկայացնել խորհրդատվական բնույթի առաջարկներ ուղղված ֆիզիկական տվյալների անվտանգությանը:
- Ներկայացնել խորհրդատվական բնույթի առաջարկներ ուղղված ֆիզիկական անվտանգությանը:
- Ներկայացնել խորհրդատվական բնույթի առաջարկներ ուղղված թվային և ֆիզիկական ակտիվների պաշտպանության ինստիտուցիոնալ հիմքերի ներդրմանը:
- Ներկայացնել խորհրդատվական բնույթի առաջարկներ ուղղված կազմակերպության աշխատակիցների, շահառուների և գործընկեր կառույցների շրջանում թվային անվտանգության կրթության խթանմանը և փորձի փոխանակմանը:
- Ներկայացնել խորհրդատվական բնույթի առաջարկներ ուղղված թվային և ֆիզիկական ակտիվների պաշտպանությանը՝ ճգնաժամային ու ֆորս մաժորային իրավիճակների համատեքստում:

Քաղաքականություններ

Շարժվելով այս քաղաքականության խորհրդատվական բնույթի առաջարկներով կազմակերպությունը կարևորում է թվային և ֆիզիկական ակտիվների անվտանգությանն ու պաշտպանությանն ուղղված հնարավոր բոլոր գործողությունները:

Ընդունելով այս քաղաքականությունը, կազմակերպությունը ձեռնարկում է քայլեր ուղղված միջոցների ստեղծմանը և զարգացմանը, որոնք կնպաստեն խորհրդատվական

առաջարկների իրագործմանը, դրանց ինստիտուցիոնալացմանն ու մշտական կիրառմանը՝ որպես առօրյա գործունեության մաս։

Առաջնորդվելով այս քաղաքականության խորհրդատվական բնույթի առաջարկներով, կազմակերպությունը կիսում է իր փորձը և կարողությունները աշխատակիցների, շահառուների և գործընկեր կառույցների շրջանում՝ նպաստելով գործելաոճի համանման մշակույթի ձևավորմանը, զարգացմանն ու պահպանմանը։

Ստորև ներկայացված են քաղաքականության խորհրդատվական բնույթի առաջարկները։

ՄԱՍ 1. Թվային ակտիվների անվտանգություն

Թվային ակտիվների գույքագրում

Թվային ակտիվները կազմակերպությունում առկա այն տեխնիկական և ցանցային միջոցներն են, որոնք հանդիսանում են տեղեկատվության մշակման՝ ստացման, խմբագրման, ուղարկման, պահպանման և ոչնչացման գործիքներ, օրինակ՝ Wi-Fi երթուղիչներ, տպիչ սարքեր, համակարգիչներ, դյուրակիր համակարգիչներ, բջջային հեռախոսներ, արտաքին կրիչներ, արտաքին կոշտ սկավառակներ, խտասկավառակներ, հիշողության միկրո քարտեր, կենտրոնական պահոցներ, տեսախցիկներ, կորպորատիվ և անձնական էլեկտրոնային փոստեր, սոցիալական մեդիայի օգտահաշիվներ, էջեր, խմբեր, ալիքներ, մեսենջերներ, հեռահաղորդակցության այլ ծառայություններ, ամպային ծառայություններ, տվյալների շտեմարաններ, աշխատանքային առցանց այլ հարթակներ և գործիքներ։

Թվային ակտիվների գույքագրման նպատակով կազմակերպությունը կատարում է հետևյալ քայլերը՝

1. Կազմակերպությունը տարեկան պարբերականությամբ իրականացնում է կազմակերպությունում առկա թվային ակտիվների գույքագրում։
2. Կազմակերպությունն իր հիմնական աշխատակիցներից որևէ մեկին նշանակում է թվային ակտիվների պատասխանատու-վերահսկող անձ, ով տարվա կտրվածքով պարբերաբար ստուգում է գույքագրված ակտիվների առկայությունը, դրանց ամբողջականությունը, մաշվածությունը և անվտանգությանը սպառնացող ռիսկերը։
3. Թվային ակտիվների գույքագրումը կազմակերպությունում իրականացվում է աշխատակիցների մասնակցությամբ։ Յուրաքանչյուր աշխատակից նշանակվում է իր գործունեության ընթացքում կիրառվող թվային ակտիվի պատասխանատու։
4. Թվային ակտիվների կորստի պարագայում, դրա համար պատասխանատու անձը տեղեկացնում է կազմակերպության համապատասխան աշխատակցին կամ ղեկավարին։

Համակարգիչների պաշտպանություն

Աշխատանքային համակարգիչների և դյուրակիր համակարգիչների պաշտպանությունն ու անվտանգությունն ապահովելու նպատակով կազմակերպությունը ներդնում է հնարավոր ջանքերն ու ռեսուրսները դրա համար անհրաժեշտ քայլերն ամբողջությամբ և ժամանակին իրականացնելու համար։

Համակարգիչների պաշտպանությանն ու տվյալների անվտանգության ապահովման նպատակով կազմակերպությունն իրականացնում է հետևյալ քայլերը՝

Կանոնավոր կերպով ստուգում, համոզվում և արձանագրում է, որ.

1. Աշխատանքային և դյուրակիր համակարգիչներին հասանելիություն ունեն միայն կազմակերպության աշխատակիցները, իսկ շահառուների համար նախատեսված սարքավորումներին՝ շահառուները։
2. Աշխատանքային և դյուրակիր համակարգիչները պաշտպանված են ապահով և հուսալի գաղտնաբառերով (առնվազն ութ նիշ՝ լատինական տառեր, թվեր, այլ նիշեր) և դրանք հասանելի չեն երրորդ անձանց։ Գաղտնաբառերի կորստի դեպքում պահպանված են հուշումներ կամ կազմակերպության պատասխանատու անձի և/կամ ղեկավարը դրանք փոխելու, վերստեղծելու տեխնիկական հնարավորություն ունեն։
3. Եթե միևնույն համակարգչից օգտվում են և՛ աշխատակիցները, և՛ շահառուները, ապա դրանք բաժանված են օգտատերերի, որոնցից յուրաքանչյուրն ունի իր գաղտնաբառը։
4. Համակարգչի հիմնական օգտագործողն ունի ադմինիստրատորի անունից գործողություններ իրականացնելու թույլտվություն, եթե կազմակերպությունը չունի համապատասխան տեխնիկական աշխատակից։ Տեխնիկական աշխատակցի առկայության պայմաններում ադմինիստրատորի անունից գործողություններ իրականացնելու թույլտվությունը պատկանում է միայն պատասխանատու անձին։
5. Համակարգիչներում ներդրված ծրագրային ապահովումները, այդ թվում համակարգչի օպերացիոն համակարգը լիցենզավորված է, իր մեջ ներառում է անհրաժեշտ բոլոր թարմացումները։
6. Համակարգիչներում միացված է ավտոմատ թարմացումը և նախաձեռնված են անվտանգության ապահովմանն ուղղված բոլոր գործողությունները։ Համակարգչի օպերացիոն համակարգը ավտոմատ թարմանում է։ Վերջին թարմացումը համապատասխանում է օպերացիոն համակարգը թողարկողի կողմից կատարած փոփոխություններին։
7. Համակարգիչներում առկա չեն «կոտրված» ծրագրային ապահովումներ, թողարկողի վերաբերյալ տեղեկատվություն չպարունակող ծրագրային ապահովումներ, խաղային, վնասակար և համակարգչի աշխատանքին խոչընդոտող, ինչպես նաև աշխատանքային բնականոն գործունեությունն իրականացնելու համար նախատեսված ծրագրային ապահովումներից բացի այլ ծրագրային ապահովումներ։

8. Համակարգիչներում առկա են հակավիրուսային ծրագրեր, որոնք ստուգում են համակարգչում, էլեկտրոնային փոստերում, ամպային ծառայություններում առկա ֆայլերը, դրանցում առկա հնարավոր վիրուսները: Հակավիրուսային ծրագրերը միացված են և ավտոմատ կերպով իրականացնում են ամբողջական՝ արագ և խորը սկանավորում: Հակավիրուսային ծրագրերը ֆայլերի ներբեռնման ընթացքում իրականացնում են սկանավորում և նախապես ծանուցում են դրանց վտանգավորության վերաբերյալ, եթե այդպիսի ռիսկեր հայտնաբերվել են:
9. Եթե կա երրորդ անձանց կողմից գրասենյակ ներթափանցելու վտանգ, համակարգիչներում ակտիվացված է տվյալների ամբողջական գաղտնագրումը, որի գաղտնաբառը հասանելի չէ երրորդ անձանց: Գաղտնաբառի կորստի դեպքում պահպանված են հուշումներ կամ դրանց կրկնօրինակներն առկա են կազմակերպության պատասխանատու անձի և/կամ ղեկավարի մոտ և/կամ ապահով այլ վայրում:
10. Կազմակերպությունը համակարգիչներն ամրագրում է աշխատակիցներին և կազմակերպության գործունեության այլ կանոնակարգերով աշխատակիցներին նշանակում է պատասխանատու անձ դրանց պահպանման և անվնաս շահագործման համար:
11. Աշխատանքային համակարգիչները միացված են հոսանքի պահոցների, որոնք կարգավորում են համակարգիչներ մտնող հոսանքի տատանումները և հոսանքազրկումների ժամանակ կարող են շարունակել իրենց աշխատանքն անխափան՝ առանց տվյալների կորստի և տեխնիկական խնդիրների:

Շարժական սարքերի պաշտպանություն

Շարժական սարքերի համատեքստում կազմակերպությունը դիտարկում է դյուրակիր համակարգիչները, բջջային հեռախոսները, պլանշետները, արտաքին հիշողության սարքերը: Շարժական սարքերի պաշտպանությունն իրականացնելու նպատակով կազմակերպությունը ձեռնարկում է հետևյալ քայլերը՝

Կանոնավոր կերպով ստուգում, համոզվում և արձանագրում է, որ.

1. Աշխատանքային բջջային հեռախոսներին, սմարթֆոններին, պլանշետներին հասանելիություն ունեն միայն կազմակերպության աշխատակիցները, իսկ շահառուների համար նախատեսված սարքավորումներին՝ շահառուները:
2. Աշխատանքային բջջային հեռախոսները, սմարթֆոնները, պլանշետները, արտաքին հիշողության սարքերը պաշտպանված են ապահով և հուսալի գաղտնաբառերով (առնվազն ութ նիշ՝ լատինական տառեր, թվեր, այլ նիշեր) և դրանք հասանելի չեն երրորդ անձանց: Գաղտնաբառերի կորստի դեպքում պահպանված են հուշումներ կամ կազմակերպության պատասխանատու անձը և/կամ ղեկավարը տեխնիկական հնարավորություն ունեն փոխելու, վերստեղծելու գաղտնաբառը:

3. Բջջային հեռախոսներում և պալնշետներում կիրառվում են միայն դրանց թողարկողի կողմից ստեղծված ինտերնետ-խանութների հավելվածները և ծրագրային ապահովումները:
4. Բջջային հեռախոսներում և պալնշետներում բացառված են այնպիսի ծրագրային ապահովումներն ու հավելվածները, որոնք առնչություն չունեն դրանց շահագործման նպատակների հետ: Առկա չեն երրորդ կողմից ստեղծված հավելվածներ և ծրագրային ապահովումներ:
5. Բջջային հեռախոսներում և պալնշետներում միացված է ավտոմատ թարմացումը և նախաձեռնված են անվտանգության ապահովմանն ուղղված բոլոր գործողությունները: Բջջային հեռախոսների և պալնշետների օպերացիոն համակարգերն ավտոմատ թարմանում են: Վերջին թարմացումները համապատասխանում են օպերացիոն համակարգերը թողարկողի կողմից կատարած փոփոխություններին:
6. Կազմակերպությունը բջջային հեռախոսները և պալնշետները ամրագրում է աշխատակիցներին և կազմակերպության գործունեության այլ կանոնակարգերով աշխատակիցներին նշանակում է պատասխանատու անձ դրանց պահպանման և անվնաս շահագործման համար:

Հաշիվների պաշտպանություն

Հաշիվների համատեքստում կազմակերպությունը դիտարկում է հեռահաղորդակցության և տեղեկատվության մշակման՝ ստացման, խմբագրման, ուղարկման, պահպանման և ոչնչացման հետևյալ հնարավոր գործիքները.

- Վեբ-կայք
- Կորպորատիվ էլեկտրոնային փոստեր
- Անձնական էլեկտրոնային փոստեր
- Ամպային ծառայություններ
- Սոցիալական մեդիայի օգտահաշիվներ
- Սոցիալական մեդիայի էջեր, խմբեր, ալիքներ
- Հեռահաղորդակցության համար կիրառվող մեսենջերներ

Շարժվելով խորհրդատվական քաղաքականությամբ, կազմակերպությունը ձեռնարկում է հնարավոր բոլոր քայլերը հաշիվների պաշտպանության համար: Իրականացնելու նպատակով կազմակերպությունը ձեռնարկում է հետևյալ քայլերը՝

Կանոնավոր կերպով ստուգում, համոզվում և արձանագրում է, որ.

1. Բոլոր հաշիվներն ունեն ապահով և հուսալի գաղտնաբառեր, որոնց հասանելիություն ունեն միայն աշխատակիցները կամ դրանց համար պատասխանատու անձը:
2. Բոլոր հաշիվներում, որոնք ֆունկցիոնալ առումով ունեն հնարավորություն, ակտիվացված է երկփուլային նույնականացման գործիքը՝ բացի հիմնական

գաղտնաբառի մուտքագրումից, անհրաժեշտ է մուտքագրել նաև երկրորդ՝ մեկանգամյա, ավտոմատ գեներացվող գաղտնաբառ, որը կարող է ծանուցվել ինչպես SMS-ի, այնպես էլ երրորդ կողմի հավելվածի միջոցով, օրինակ՝ Google Authenticator:

3. Բոլոր հաշիվների վերականգնման համար ճշտորեն լրացված են պահուստային հեռախոսահամարները և էլեկտրոնային փոստի հասցեները:
4. Կիրառվում են առավել ապահով և անվտանգ փոստային ծառայություններ, որոնք բացառում են հաշիվների կոտրումը պայմանավորված իրենց թերություններով կամ ցածր պաշտպանվածությամբ:
5. Կիրառվում են այնպիսի փոստային ծառայություններ, որոնք ապահովում են ամպային ծառայությունների լայն հնարավորություն և համակարգչում առկա տվյալների համաժամանակյա պահպանման և պահուստավորման հնարավորություն:
6. Ամպային ծառայություններում պահպանվող տվյալների հասանելիությունը հանրային չէ և մուտքի թույլտվություն տրված են միայն կազմակերպության աշխատակիցներին և կազմակերպությունից դուրս վստահելի և անվտանգ էլեկտրոնային փոստեր ունեցող անձանց:
7. Հաշիվներ մուտք չեն արվում այլ՝ ոչ աշխատանքային սարքավորումներից կամ աշխատանքային սարքավորումներից, որոնք նախատեսված են նաև շահառուների համար: Այլ պարագայում, բոլոր հաշիվներից կանոնավոր կերպով իրականացվում է ելք:
8. Շահառուների համար նախատեսված սարքավորումների դիտարկիչներում չեն պահպանվում հաշիվների գաղտնաբառեր և դրանց հասանելիություն ունեն միայն աշխատակիցները կամ դրանց համար պատասխանատու անձը:
9. Տարեկան առնվազն մեկ անգամ փոփոխվում են հաշիվների մուտքի տվյալները և դրանց մասին տեղեկատվությունը պահպանվում է ապահով վայրում:
10. Բոլոր սարքավորումները, որոնցում ակտիվ են հաշիվները, պաշտպանված են ապահով և հուսալի գաղտնաբառերով: Սարքավորումների գաղտնաբառերը չեն կրկնում միմյանց և չունեն ընդհանուր տրամաբանական հաջորդականություն կամ տարբերություն, որը հնարավոր կլինի հեշտորեն գուշակել:
11. Բոլոր հաշիվների գաղտնաբառերը չեն կրկնում միմյանց և չունեն ընդհանուր տրամաբանական հաջորդականություն կամ տարբերություն, որը հնարավոր կլինի հեշտորեն գուշակել:
12. Եթե աշխատակիցների անձնական հաշիվները փոխկապակցված են էջերի, խմբերի, ալիքների կառավարման հետ, ապա աշխատակիցների անձնական սարքավորումները նույնպես պահպանում են սույն քաղաքականությամբ առաջարկվող կանոնները:
13. Էջերի, խմբերի, ալիքների կառավարման համար նշանակված են մեկից ավելի ադմինիստրատորներ և մեկ օգտահաշվի բլոկավորման պարագայում, մյուս օգտատերը կկարողանա կառավարել դրանք, նշանակել նոր ադմինիստրատորներ, խմբագիրներ և այլն:

14. Հաշիվների կառավարմամբ զբաղվող պատասխանատու անձը տիրապետում է դրանց կիրառման ընդհանուր դրույթներին և գաղտնիության քաղաքականությանը, ծանոթանում է դրանց փոփոխությունների վերաբերյալ ծանուցումներին և տեղեկացնում մյուս աշխատակիցներին։
15. Հաշիվների կառավարման ընթացքում պաշտպանվում են շրջանառվող բովանդակությունների հեղինակային իրավունքները։ Բացառվում են անհանդուրժողականության և ատելության խոսքի դրսևորումները, մարդու հիմնարար իրավունքներին և ազատություններին, տեղական և միջազգային օրենսդրությանն ու պարտավորություններին հակասող գործողությունները, կեղծ տեղեկատվության շրջանառումը և այլ գործողություններ, որոնք կարող են հակասել ընդհանուր պայմաններին և դրույթներին՝ հանգեցնելով հաշիվների, էջերի, խմբերի և ալիքների ժամանակավոր սառեցմանը կամ արգելափակմանը։
16. Կազմակերպությունը պարբերաբար ստուգում է հաշիվների մուտքի պատմությանը և իրականացված գործողություններին՝ համոզվելով, որ դրանք կատարվել են աշխատակիցների կողմից՝ ծանոթ են մուտքի վայրերը, մուտք իրականացնող սարքավորումները։
17. Հեռահաղորդակցության և տեխնոլոգիական այլ գործիքներից օգտվելիս իրականացվում է պատշաճ գրանցում և մուտքը չի իրականացվում գործող հաշիվների տվյալներով։

Համացանց և ներքին ցանցեր, թրաֆիկի պաշտպանություն

Կազմակերպությունը ձեռնարկում է քայլ ուղղված համացանցի ազատ և անվտանգ օգտագործմանը, ներքին ցանցերի անխափան աշխատանքին, դրանց անվտանգությանը և թրաֆիկի պաշտպանությանը։ Կազմակերպությունը կարևորում է տվյալների շրջանառման անվտանգությունն ու այդ ուղղությամբ իրականացնում է հետևյալ քայլերը՝

Կանոնավոր կերպով ստուգում, համոզվում և արձանագրում է, որ.

1. Wi-Fi երթուղիչն աշխատում է անխափան։
2. Wi-Fi երթուղիչի կարգավորումների կառավարման մուտքի համար դրված է ապահով և հուսալի մուտքանուն և գաղտնաբառ։
3. Wi-Fi երթուղիչին միանալու համար դրված է ապահով և հուսալի գաղտնաբառ, որին հասանելիություն ունեն միայն աշխատակիցները։
4. Wi-Fi երթուղիչը բաժանված է ենթացանցերի՝ շահառուների, հյուրերի համար և աշխատակիցների համար։ Յուրաքանչյուր ենթացանց ունի ապահով և հուսալի գաղտնաբառ և դրանք հասանելի չեն երրորդ կողմին։
5. Տարեկան մեկ անգամ և ըստ անհրաժեշտության իրականացվում է Wi-Fi երթուղիչի գաղտնաբառի փոփոխություն՝ անցանկալի միացումներից և ինտերնետ կապի խափանումներից խուսափելու համար։
6. Աշխատանքային և դյուրակիր համակարգիչները, տպիչ սարքերը, Wi-Fi երթուղիչները միացված են ընդհանուր ներքին ցանցին և կենտրոնական պահոցին։

Ներքին ցանցն անվտանգ է և պաշտպանված, բացառված են տեխնիկական խոտանները, որոնք կարող են հանգեցնել տվյալների կորստի և տեսանելի չեն երրորդ կողմին:

7. Ներքին ցանցի կարգավորումների կառվարաման համար կիրառվում է բարդ գաղտնաբառ, որին հասանելիություն ունեն միայն ղեկավար կազմը և դրա համար պատասխանատու տեխնիկական աշխատակիցը:
8. Կենտրոնական պահոցն աշխատում է անխափան և կանոնավոր կերպով իրականացնում է տվյալների համաժամանակյա պահպանում և պահուսատվորում:
9. Անվտանգ որոնումների և համացանցային ծառայություններից օգտվելու համար աշխատակիցների կողմից կիրառվում է VPN (Virtual Private Network): Հիմնականում կիրառվում է ինտերնետ հասանելիության սահմանափակումների, գաղտնիության խիստ ռեժիմի պահպանման դեպքերում:
10. Կազմակերպության աշխատակիցները բացառում են անձնական, ֆինանսական, բանկային և այլ տվյալների մուտքագրումը այնպիսի վեբ էջերում, որոնք գաղտնագրված չեն https-ով:
11. Կազմակերպության սարքերը չեն միացվում հանրային Wi-Fi-ների և այդպիսով վտանգի տակ չեն դրվում դրանցում առկա թվային տվյալները:

Արտաքին հիշողության սարքերի պաշտպանություն

Կազմակերպությունն արտաքին հիշողության սարքերի համատեքստում դիտարկում է արտաքին կրիչները, արտաքին կոշտ սկավառակները, խտասկավառակները, հիշողության միկրո քարտերը և այլն:

Կազմակերպությունը կարևորում է տվյալների շրջանառման, պահպանման, մշակման անվտանգությունն ու այդ ուղղությամբ իրականացնում է հետևյալ քայլերը՝

Կանոնավոր կերպով ստուգում է, համոզվում է և արձանագրում է, որ.

1. Արտաքին հիշողության սարքերն անվնաս են և դրանցում պարունակվող տեղեկատվության կորստի ռիսկերը գնահատման ենթակա չեն:
2. Արտաքին հիշողության սարքերը գտնվում են կազմակերպության աշխատակիցների պատասխանատվության ներքո, հասանելի չեն երրորդ անձանց:
3. Արտաքին հիշողության սարքերը պաշտպանված են ապահով և հուսալի գաղտնաբառերով, որոնց տիրապետում են միայն աշխատակիցները:
4. Արտաքին հիշողության սարքերի գաղտնաբառերը պարբերաբար փոփոխվում են: Գաղտնաբառերը պահպանվում են ապահով վայրում, դրանց կորստի դեպքում կան բավարար հուշումներ:
5. Արտաքին հիշողության սարքերը պարբերաբար ֆորմատավորվում են:
6. Արտաքին հիշողության սարքերը յուրաքանչյուր անգամ կիրառելիս սկանավորվում են հակավիրուսային ծրագրերի կողմից:

7. Արտաքին հիշողության սարքերը միացումը և անջատումը համակարգիչներին իրականացվում է ըստ տեխնիկական ցուցումների և այդ գործողություններն իրականացվում են խնամքով:
8. Արտաքին հիշողության սարքերը չեն ենթարկվել ֆիզիկական ներգործության, պահպանվում են ապահով, չոր, մագնիսական ներգործությունից և ճառագայթումից պաշտպանված վայրում և, պաշտպանված են դրանց համար նախատեսված միջոցներով:

Աշխատանք տվյալների հետ և թվային տվյալների պաշտպանություն

Թվային տվյալների համատեքստում կազմակերպությունը դիտարկում է ցանկացած փաստաթուղթ, մեդիա ֆայլ, տվյալ, բովանդակություն, որը կարող է պարունակել տեղեկատվություն կազմակերպության, կազմակերպության գործունեության, շահառուների, գործընկերների մասին: Դրանք կարող են լինել անձնական տվյալներ, ծրագրային փաստաթղթեր: Փաստաթղթաշրջանառության և էլեկտրոնային հաղորդակցության ընթացքում շրջանառվող բովանդակությունները համարվում են թվային տվյալներ:

Կազմակերպությունը գիտակցում է տվյալների հետ աշխատանքի կարևորությունը, գնահատում է դրանց զգայունությունը և ճանաչում է դրանց անվտանգ պահպանման իր պատասխանատվությունը, որը կազմակերպության այլ կանոնակարգերով և Հայաստանում գործող օրենքներով տարածվում է աշխատակիցների և կազմակերպության վրա:

Կազմակերպությունը ստանձնում է կազմակերպության, կազմակերպության աշխատակիցների, շահառուների, գործընկերների տվյալների մշակման ամբողջականության, օրինաչափության և համաչափության սկզբունքների պահպանումը, այդ թվում դրանց գաղտնիության պահպանման պատասխանատվությունը կազմակերպության այլ կանոնակարգերով և Հայաստանում գործող օրենքներով, որը բացառում է տվյալների կորուստը, արտահոսքը և փոխանցումը երրորդ անձանց:

Կազմակերպությունը տվյալների մշակման (ցանկացած գործողություն տվյալների հետ՝ ստեղծում, հավաքագրում, խմբագրում, ապաանձնավորում, նույնականացում, պահպանում, ոչնչացում և այլն) գործընթացում առաջնորդվում է «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի, Հայաստանի կողմից ստանձնած միջազգային պարտավորությունների, այլ օրենքների և ենթաօրենսդրական ակտերի կետերով և ստանձնում է իրավական ողջ պատասխանատվությունը, ինչպես նաև կարևորում է անձնական տվյալների մշակման էթիկական նորմերը՝ գիտակցելով և գնահատելով մշակման գործընթացի հնարավոր հետևանքները և ռիսկերը:

Թվային տվյալների պաշտպանության ուղղությամբ կազմակերպությունը ձեռնարկում է հետևյալ քայլերը՝

Կանոնավոր կերպով ստուգում, համոզվում և արձանագրում է, որ.

1. Թվային տվյալների մշակումն իրականացվում է անվտանգ և ապահով միջոցներով:
2. Թվային տվյալները հասանելի չեն երրորդ անձանց կամ հասանելի են այն չափով, որքանով անհրաժեշտ է դրանց հասանելիությունը և չի հակասում տեղական օրենսդրությանը:
3. Թվային տվյալների նկատմամբ հասանելիությունը սահմանափակված է՝ ըստ աշխատակիցների լիազորությունների և պատասխանատվության տիրույթի:
4. Թվային տվյալները հուսալիորեն պահպանվում են համակարգիչներում, բջջային հեռախոսներում, պլանշետներում, կենտրոնական պահոցում, արտաքին հիշողության սարքերում:
5. Իրականացվում է թվային տվյալների ավտոմատ համաժամանակյա թարմացում կամ դրա անհնարինության պարագայում այն իրականացվում է ձեռքով՝ թվային տվյալների կրկնօրինակման և պատճենման միջոցով:
6. Թվային տվյալներն արխիվացվում են ըստ կազմակերպության այլ կանոնակարգերով սահմանված ժամանակացույցի, դրա բացակայության դեպքում՝ օրենքով սահմանված կարգով:
7. Թվային տվյալները ոչնչացվում են պատշաճ կերպով, եթե դրանց պահպանման համար նախատեսված առավելագույն ժամանակը լրացել է և դրանց պահպանման անհրաժեշտությունը բացակայում է:
8. Կազմակերպությունը լքող աշխատակիցները հանձնում են իրենց տիրապետության և պատասխանատվության տակ գտնվող թվային, ֆիզիկական տվյալները, թվային ակտիվներն ամբողջությամբ, իրենց մոտ չեն պահպանում տվյալների կրկնօրինակներ, պատճեններ, ծանուցվում են տվյալների արտահոսքի պարագայում հնարավոր հետևանքների և իրավական պատասխանատվության կանչվելու վերաբերյալ:
9. Թվային տվյալների մշակման գործընթացում ներգրավվում է նվազագույն քանակի անձ, որքան անհրաժեշտ է դրանց մշակման համար:
10. Անձնական տվյալների մշակումն իրականացվում է անձնական տվյալների սուբյեկտի համաձայնության պարագայում:
11. Անձնական տվյալների փոխանցում երրորդ անձին, առանց անձնական տվյալների սուբյեկտի համաձայնության, բացառվում է:

ՄԱՍ 2. Թվային անվտանգությունը ֆիզիկական համատեքստում

Ֆիզիկական տվյալների գույքագրում և պաշտպանություն

Ֆիզիկական տվյալների համատեքստում կազմակերպությունը դիտարկում է թվային տվյալների տպագիր պատճենները: Թվային տվյալների տպագիր պատճենները կարող են լինել ֆինանսական, ծրագրային փաստաթղթեր, անձնական տվյալներ, պայմանագրեր, գրանցման թերթիկներ, ցուցակներ, համաձայնագրեր, որոշումներ և այլն:

Ֆիզիկական տվյալների գույքագրման նպատակով կազմակերպությունը կատարում է հետևյալ քայլերը՝

1. Այն թվային տվյալները, որոնք ենթադրում են նաև ֆիզիկական գոյություն, պետք է լինեն տպագրված և արխիվավորված համաձայն կազմակերպության կանոնակարգերի: Դրանց բացակայության պայմաններում ֆիզիկական տվյալները պահպանվում են՝ առանձին թղթապանակներով՝ կա՛մ ըստ նախագծերի, կա՛մ ըստ տարեթվերի, կա՛մ այլ տրամաբանական բաժանման, որի միջոցով հեշտորեն հնարավոր կլինի գտնել դրանք և իրականացնել մշակման աշխատանքներ:
2. Յուրաքանչյուր թղթապանակ պետք է պարունակի փաստաթուղթ, որտեղ թվարկված կլինի տվյալ թղթապանակում առկա ֆիզիկական տվյալների ցանկը:
3. Կազմակերպությունը տարեկան պարբերականությամբ իրականացնում է կազմակերպությունում առկա ֆիզիկական տվյալների գույքագրում:
4. Կազմակերպությունն իր հիմնական աշխատակիցներից որևէ մեկին (կամ դրանց համար պատասխանատու անձին) նշանակում է ֆիզիկական տվյալների պատասխանատու-վերահսկող անձ, ով տարվա կտրվածքով պարբերաբար ստուգում է գույքագրված տվյալների առկայությունը, դրանց ամբողջականությունը, մաշվածությունը և անվտանգությանը սպառնացող ռիսկերը:
5. Ֆիզիկական տվյալների գույքագրումը կազմակերպությունում իրականացվում է աշխատակիցների մասնակցությամբ: Յուրաքանչյուր աշխատակից նշանակվում է իր գործունեության ընթացքում կիրառվող ֆիզիկական տվյալների պատասխանատու:
6. Թվային ակտիվների կորստի պարագայում, դրա համար պատասխանատու անձը տեղեկացնում է կազմակերպության համապատասխան աշխատակցին կամ ղեկավարին:
7. Ֆիզիկական տվյալների արխիվացումն իրականացվում է ըստ կազմակերպության այլ կանոնակարգերով սահմանված ժամանակացույցի, դրա բացակայության դեպքում՝ օրենքով սահմանված կարգով:
8. Ֆիզիկական տվյալների ոչնչացումն իրականացվում է ըստ կազմակերպության այլ կանոնակարգերով սահմանված ժամանակացույցի, դրա բացակայության դեպքում՝ օրենքով սահմանված կարգով:
9. Բացառված են ֆիզիկական տվյալների հասանելիությունը երրորդ անձանց:
10. Ֆիզիկական տվյալները պահպանվում են դրանց համար հատկացված վայրում (ոչ խոնավ, ոչ հրավտանգ վայրեր):

Տարածքի ֆիզիկական պաշտպանվածություն

Թվային ակտիվների և ֆիզիկական տվյալների պաշտպանության համատեքստում կազմակերպությունը կարևորում է նաև իր գործունեության վայրի ֆիզիկական անվտանգությունը: Տարածքի ֆիզիկական պաշտպանվածության նպատակով կազմակերպությունը ձեռնարկում է հետևյալ քայլերը՝

Համոզվում է, որ

1. Տարածքն ապահովված է անվտանգության և տեսահսկման համակարգով: Տեսահսկման համակարգը կապակցված է ներքին ցանցին և կենտրոնական պահոցին, ինչը թույլ է տալիս նշված ժամանակահատվածում իրականացնել տեսագրությունների պահպանում և ապահովում է տեսահսկման հասանելիությունն այլ վայրերից:
2. Անվտանգության և տեսահսկման համակարգն աշխատում է անխափան և համաժամանակյա:
3. Տեսահսկման համար տեղադրված են անհրաժեշտ քանակի տեսախցիկներ: Դրանք տեղադրված են ճիշտ վայրերում: Տեսախցիկները գտնվում են բավարար բարձրության վրա և ֆիքսում են առավելագույն տարածք: Հնարավորության դեպքում դրանք ինքնաշխատ են և խելացի՝ զգայուն են շարժումների և միջավայրում փոփոխությունների նկատմամբ և իրականացնում են նկարահանումը նշված պարագաներում՝ իրականացնելով ծանուցում արձանագրված փոփոխությունների վերաբերյալ:
4. Անվտանգության և տեսահսկման համակարգը տարեկան մեկ անգամ անցնում է տեխնիկական ստուգում և սպասարկում:
5. Տեսահսկման համակարգը պաշտպանված է ապահով և հուսալի գաղտնաբառով, որին հասանելիություն ունեն միայն դրա համար պատասխանատու անձինք:
6. Տարածքի մուտքի հասանելիություն ունեն միայն աշխատակիցները և տարածքի պահպանման համար պատասխանատու այլ անձինք:
7. Տարածքի դուռը ապահով է և հնարավոր չէ հեշտորեն կոտրել: Անհրաժեշտության դեպքում այն փոխարինված է երկաթյա դռնով:
8. Եթե տարածքը գտնվում է առանձնատանը կամ շենքի ցածր հարկերում, ապա իրականացված է վանդակաճաղերի մոնտաժ բոլոր պատուհաններին:
9. Տեղադրված են տագնապային ահազանգերը: Տագնապային ահազանգի վերաբերյալ ստացվում է ծանուցում բջջային հեռախոսին և նման իրավիճակների դեպքում պատասխանատու անձանց և ստորաբաժանումներին:
10. Կազմակերպությունում առկա են և տեսանելի վայրում փակցված են արտակարգ իրավիճակների տարհանման պլանները:
11. Կազմակերպությունում առկա են հակահրդեհային անվտանգության բոլոր միջոցները և աշխատակիցները տիրապետում են դրանցից օգտվելու կանոններին:

ՄԱՍ 3. Թվային անվտանգության ինստիտուցիոնալ ապահովում

Կազմակերպությունը կարևորում է թվային անվտանգության ինստիտուցիոնալ ապահովումը: Թվային անվտանգության ապահովումն ինստիտուցիոնալ հիմքերի վրա դնելու նպատակով կազմակերպությունը կիրառում է Թվային անվտանգության խորհրդատվական քաղաքականությունը՝ որպես կազմակերպության թվային անվտանգության ներքին քաղաքականություն՝ լրամշակելով այն ըստ կարիքների և առաջնահերթությունների:

Կազմակերպությունը պարբերաբար անդրադառնում է թվային անվտանգության հիմնահարցերին, տարեկան կտրվածքով և այլ ժամանակաչափերով իրականացնում է թվային անվտանգության խորհրդատվական քաղաքականությամբ կամ այլ քաղաքականություններով և կանոնակարգերով սահմանված գործընթացները՝ դրանցում ներգրավելով իր աշխատակիցներին։

Կազմակերպությունը փաստաթղթավորում է թվային անվտանգությանն ուղղված իր կանոնակարգերն ու մոտեցումները՝ դարձնելով դրանք աշխատանքի և ամենօրյա գործունեության մաս։

Կազմակերպությունն իր նախագծերում և ֆինանսական առաջարկներում դիտարկում է թվային անվտանգության զարգացմանը, դրա պահպանմանն ուղղված անհրաժեշտ ռեսուրսների հայցումը՝ հիմնավորելով թվային անվտանգության նշանակալիությունն ու կարևորությունը կազմակերպության գործունեության հիմքում։

Կազմակերպությունը գեներացնում է միջոցներ և ռեսուրսներ, որոնք կարող են խթանել թվային անվտանգությանը։ Կազմակերպությունն իր գործունեության մեջ նշանակալի տեղ է հատկացնում թվային անվտանգությանը և դրան ուղղված ռեսուրսների հայցումը, դրա համար հատկացված ժամանակն ու միջոցները հիմնավորում է իր ստանձնած պարտավորություններով և Թվային անվտանգության խորհրդատվական քաղաքականությամբ կամ համանման այլ քաղաքականությամբ ու կանոնակարգերով, որոնցով առաջնորդվում է։

ՄԱՍ 4. Մարդկային ռեսուրսներ, շարունակական կրթություն և փորձի փոխանակում

Կազմակերպությունը կարևորում է իր աշխատակիցների շրջանում թվային գրագիտության խթանումը՝ որպես Թվային անվտանգության խորհրդատվական քաղաքականությամբ սահմանված կետերի պահպանման երաշխիք։

Կազմակերպությունը մշտապես իրականացնում է թվային անվտանգությանն ուղղված փորձի փոխանակում իր կրտսեր և ավագ աշխատակիցների միջև՝ ապահովելով նաև թվային անվտանգությանն ուղղված փորձառության ինստիտուցիոնալիզացումը։

Կազմակերպությունն իր նոր աշխատակիցներին ծանոթացնում է Թվային անվտանգության խորհրդատվական քաղաքականության հետ և աշխատանքային ու ծառայությունների մատուցման պայմանագրերով ամրագրում դրանց նկատմամբ պատասխանատվությունը։

Կազմակերպությունը՝ կազմակերպությունը լքող աշխատակիցներին ծանուցում է թվային և ֆիզիկական տվյալների գաղտնիության պահպանման պարտավորություններինն։ Կազմակերպությունը լքող աշխատակիցն իր գործունեության ընթացքում հավաքագրված և մշակված, ինչպես նաև իր տիրապետության տակ գտնվող տեղեկատվությունն ամբողջությամբ փոխանցում է իրեն փոխարինող աշխատակցին և/կամ կազմակերպության ղեկավարին։

Կազմակերպությունը ծառայություններ ձեռք բերելիս և պայմանագրեր կնքելիս հատուկ կետ է սահմանում անձնական տվյալների պաշտպանության, շրջանառվող տեղեկատվության գաղտնիության և դրանց արտահոսքի պարագայում հնարավոր հետևանքների ու պատասխանատվության վերաբերյալ:

Կազմակերպությունն իր աշխատակիցների համար կազմակերպում է վերապատրաստումներ, որոնք իրականացվում են կազմակերպության տեխնիկական աշխատակցի կամ հրավիրյալ մասնագետի կողմից: Կազմակերպությունն աշխատակիցների փորձի փոխանակման և վերապատրաստման նպատակով կանոնավոր կերպով իրականացնում է միջոցների հայթայթում և ռեսուրսների գեներացում:

Կազմակերպությունը կարևորում է տեխնոլոգիաների զարգացմանը զուգընթաց նոր գիտելիքների ձեռքբերումը, դրանց տարածումն աշխատակիցների շրջանում:

Կազմակերպությունը նպաստում է նաև իր գործընկեր կառույցների և շահառուների թվային անվտանգության իրազեկվածությանը՝ հիմք ընդունելով նաև այն հանգամանքը, որ տվյալների շրջանառումը տեղի է ունենում ոչ միայն կազմակերպության ներսում, այլև արտաքին հաղորդակցության գործընթացում և դրանց նկատմամբ վերահսկողությունն ու անվտանգության ապահովումը պետք է լինի երկուստեք:

ՄԱՍ 5. Ճգնաժամեր, Ֆորս մաժորային իրավիճակներ և անհաղթահարելի ուժ

Կազմակերպությունն իրավունքի դաշտում անհաղթահարելի ուժ կամ ֆորս մաժոր դիտարկում է արտակարգ իրադարձությունները, որոնք կախված չեն մարդկանց կամքից, գործում են օբյեկտիվորեն, չեն կարող կանխատեսվել կամ կարող են կանխատեսվել, բայց չեն կարող կանխվել և վերացվել:

Ֆորս մաժորը պայմանագրային համատեքստում պայմանագրի կողմերին ազատում է պարտավորությունը լրիվ կամ մասնակի չկատարելու համար պատասխանատվությունից, եթե պարտավորության չկատարումն այնպիսի հանգամանքների կամ իրադարձությունների հետևանք է, որոնք կողմերը չէին կարող կանխել կամ կանխատեսել: Այդպիսի հանգամանքներ կարող են լինել պատերազմները, գործադուլները, արտակարգ կամ ռազմական դրություն հայտարարելը, համաճարակները, բնական աղետները (երկրաշարժ, ջրհեղեղ, հրաբխի ժայթքում և այլն), որոնք անհնարին են դարձնում պայմանագրի կողմերի կամ նրանցից մեկի կողմից պայմանագրով ստանձնած պարտավորությունների կատարումը: Կազմակերպությունը ինքնուրույն է գնահատում ֆորս մաժորային իրավիճակներում պարտավորությունների կատարման մասնաբաժինը:

Կազմակերպությունը կարևորում է ճգնաժամային և ֆորս մաժորային իրավիճակներում իր աշխատակիցների գործողությունները թվային ակտիվների, թվային և ֆիզիկական տվյալների պաշտպանության համատեքստում:

Կազմակերպությունն ինքնուրույն է որոշում իր աշխատակիցների գործողությունները ճգնաժամային և ֆոսր մաժորային իրավիճակներում թվային ակտիվների, թվային և ֆիզիկական տվյալների պաշտպանության համատեքստում: Կազմակերպությունն այդ ամենը համաձայնեցնում է իր աշխատակիցների և Խորհրդի հետ:

Կազմակերպությունը շարունակում է կարևորել թվային և ֆիզիկական տվյալների պաշտպանությունը և անձնական տվյալների զգայունությունը ճգնաժամային և ֆորս մաժորային իրավիճակներում նույն չափով, որքանով դրանք կարևորվում են առօրյա գործունեության ընթացքում:

Կազմակերպությունն իրականացնում է թվային ակտիվների տեղափոխում՝ աշխատակիցների միջոցով: Յուրաքանչյուր աշխատակից իր հետ վերցնում է այն թվային ակտիվները, որոնք հնարավոր է տեղափոխել և որոնք գտնվում են տվյալ աշխատակցի պատասխանատվության ներքո:

Հեռավար՝ ոչ գրասենյակային աշխատանքի դեպքում ևս աշխատակիցների կողմից պահպանվում են սույն Թվային անվտանգության խորհրդատավական քաղաքականության առաջարկները կամ կազմակերպության այլ կանոնակարգերով և քաղաքականություններով սահմանված կետերը:

Կազմակերպությունը կարող է ճգնաժամային և ֆորս մաժորային իրավիճակներում իրականացնել ֆիզիկական տվյալների անհապաղ արխիվացում կամ ոչնչացում:

Կազմակերպությունը կարող է ճգնաժամային և ֆորս մաժորային իրավիճակներում իրականացնել թվային տվյալների անհապաղ արխիվացում կամ ոչնչացում:

Թվային և ֆիզիկական տվյալների ոչնչացման վերաբերյալ որոշումը կայացնում է կազմակերպության ղեկավարը կամ դրա համար պատասխանատու անձը՝ այդ մասին պատշաճ կերպով ծանուցելով աշխատակիցներին՝ ներկայացնելով տեխնիկական ուղեցույց տվյալների ոչնչացման քայլերի վերաբերյալ:

Կազմակերպության թվային ֆիզիկական ակտիվների (համակարգիչներ, բջջային հեռախոսներ, տպիչ սարքեր, պլանշետներ և այլն) ոչնչացումը ստանձնում է ղեկավարությունը:

Հակապանդում

Թվային անվտանգության խորհրդատվական բնույթի քաղաքականությունը մշակվել է Բոլորը հանուն հավասար իրավունքների հիմնադրամի (ԲՀՀԻ հիմնադրամ) կողմից «Աջակցություն քաղաքացիական հասարակությանը՝ հանուն բարեփոխումների վրա ներգործության» ծրագրի շրջանակում:

Նյութի բովանդակության համար պատասխանատու է միայն ստեղծողը: Քաղաքականությունում արտահայտված տեսակետները/ բովանդակությունը կարող են չհամընկնել Շվեդիայի կառավարության տեսակետների հետ:

«Աջակցություն քաղաքացիական հասարակությանը՝ հանուն բարեփոխումների վրա ներգործության» ծրագիրն իրականացվում է Եվրասիա համագործակցություն հիմնադրամի կողմից Շվեդիայի կառավարության աջակցությամբ:

Web: www.allrights.am

Email: info@allrights.am

ք.Գյումրի 2022թ.