BSC BUSINESS SUPPORT CENTER

DigiSupport

CIPE CENTER FOR INTERNATIONAL PRIVATE ENTERPRISE

ԲԻԶՆԵՍԻ ԹՎԱՅԻՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՈՒՂԵՑՈՒՅՑ

www.bsc.am

ՆԵՐԱԾՈՒԹՅՈՒՆ

Հարգելի՛ ընթերցող,

Սույն ուղեցույցը կազմվել է «Բի Էս Սի» Բիզնեսի Աջակցման Կենտրոնի (BSC) կողմից Միջազգային Մասնավոր Ձեռնարկատիրության Կենտրոնի (CIPE) աջակցությամբ իրականացվող «Թվային տնտեսության օրակարգի ձևավորում Հայաստանում» ծրագրի շրջանակներում՝ հայաստանյան միկրո, փոքր և միջին ձեռնարկությունների (ՄՓՄՁ-ների) համար:

Ծրագրի շրջանակներում մշակված ուղեցույցներն են՝

- Բիզնեսի թվային փոխակերպման ռազմավարության ուղեցույց
- Բիզնես գործընթացների թվայնացման գործիքներ
- Ձեր բիզնեսը թվային հարթակներում
- Առցանց վաճառքի հարթակներ
- Բիզնեսի թվային անվտանգության ուղեցույց

Վերոնշյալ 5 ուղեցույցները ամբողջությամբ մշակվել են հայերենով, հասանելի են www.bsc.am կայքում և սոցիալական էջերում անվճար օգտագործման համար:

Թվայնացման ծրագրի շրջանակներում իրականացված նախաձեռնություններին կարող եք ծանոթանալ այս հղումով՝ https://bsc.am/hy/digital-economy-in-armenia/

Ուշադրություն. խնդրում ենք հաշվի առնել, որ ուղեցույցում ներկայացված է 2023թ. օգոստոսի դրությամբ տեղեկատվություն, որը, հնարավոր է, ենթարկված լինի հետագա փոփոխությունների:

www.bsc.am

Երևան, 2023թ.

Ուղեցույցը հնարավորություն կտա հասկանալու, թե ինչ նվազագույն քայլեր պետք է իրականացնի ընկերությունը՝ իր վերահսկողության տակ գտնվող տեղեկատվության պահպանման և տեղեկատվական դաշտում անվտանգ գործելու համար:

Անհրաժեշտ է ընդգծել, որ կիբերանվտանգության պահպանմանն ուղղված քայլերը կարող են տարբեր լինել՝ կախված կազմակերպության գործունեության ոլորտից, աշխատակիցների քանակից, վերահսկվող տեղեկատվությունից, սակայն կան նվազագույն պարտադիր քայլեր, որոնք պետք է իրականացնի յուրաքանչյուր կազմակերպություն: Նշված քայլերը արտացոլված են սույն ուղեցույցում:

Ուղեցույցը բաժանված է հիմնական 4 հատվածների

1. Տեղեկատվության քարտեզագրման ձևանմուշ
2. Տեղեկատվական անվտանգության պահպանման հիմնական քայլերի ստուգաթերթիկ
3. Արձագանքման պլանի ձևանմուշ
4. Ոլորտում գործող կառույցների վերաբերյալ տեղեկատվություն

ՏԵՂԵԿԱՏՎՈՒԹՅԱՆ ՔԱՐՏԵԶԱԳՐՈՒՄ

Ընկերության տեղեկատվությունը պաշտպանելու համար համապատասխան միջոցառումներ ձեռնարկելուց առաջ կարևոր է իմանալ, թե ընդհանրապես ինչ տեղեկատվության է տիրապետում ընկերությունը և որքան է կարևոր դրանց անվտանգությունը: Տեղեկատվության քարտեզագրման և կարևորության գնահատման համար կարող եք օգտագործել ստորև ներկայացված ձևանմուշը:

Տեղեկատվություն/ ակտիվ	Գտնվելու վայր	Հասանելիություն	Կարևորություն	Պաշտպանվածություն
Հաճախորդների տվյալներ	Վաճառքի մասնագետի համակարգչի մեջ, Excel ձևաչափով	Վաճառքի մասնագետը, Վաճառքի բաժնի ղեկավարը	Առաջնահերթ կարևոր է	Աշխատակցի համակարգիչը պաշտպանված է գաղտնաբառով

Աղյուսակում նշվածը օրինակ է: Կարող եք աղյուսակը լրացնել Ձեր կազմակերպության օրինակով:

ՏԵՂԵԿԱՏՎՈՒԹՅԱՆ ՊԱՀՊԱՆՄԱՆՆ ՈՒՂՂՎԱԾ ԱՆՀՐԱԺԵՇՏ ՔԱՅԼԵՐ

Կազմակերպության տեղեկատվությունը քարտեզագրելուց հետո անհրաժեշտ է նաև ձեռնարկել համապատասխան քայլեր դա պաշտպանելու համար: Կիբերանվտանգության ապահովման համար պահանջվում է իրականացնել մի շարք քայլեր և ներդնել ռեսուրսներ, որոնց չափը էապես կախված է պահպանվող տեղեկատվության ծավալից, ընկերության գործունեության ոլորտից և մի շարք առանձնահատկություններից:

Այնուամենայնիվ, առանձնացրել ենք մի շարք քայլեր ստորև ներկայացված ստուգաթերթիկում, որոնք պարտադիր են բոլոր ընկերությունների համար:

Ինչպե՞ս օգտագործել ստուգաթերթիկը.

1. Մանրամասնորեն ուսումնասիրե՛ք առաջարկվող պարտադիր քայլերը

2. Ստուգե՛ք, թե նշված քայլերից քանիսն են իրականացվում Ձեր կազմակերպությունում, և նշե՛ք առաջին սյունակում [√]

3. Միջոցնե՛ր ձեռնարկեք՝ իրականացնելու այն քայլերը, որոնք չեն իրականացվում Ձեր կազմակերպության կողմից

✓	Անհրաժեշտ քայլ	Բացատրություն	Գործողություն
☐	Աշխատակազմի գիտելիքների ստուգում	Աշխատակիցներն այն մարդիկ են, որոնց վերահսկողության տակ է կազմակերպությանը պատկանող տեղեկատվությունը, հետևաբար նրանք պետք է ունենան բավարար գիտելիքներ՝ տեղեկատվությունը ապահով պահպանելու համար:	Աշխատակիցների գիտելիքները ստուգելու համար կարելի է պարբերաբար կազմակերպել թեստավորումներ:
☐	Աշխատակազմի վերապատրաստում	Կարևոր է աշխատակիցների համար պարբերաբար վերապատրաստումների կազմակերպումը: Եթե նույնիսկ աշխատակիցներն ունեն բավարար գիտելիքներ, ոլորտում անընդհատ ի հայտ են գալիս նոր գործիքներ, հետևաբար և նոր վտանգներ, որոնց մասին աշխատակիցները պետք է տեղեկացված լինեն:	Վերապատրաստումները կարող են կազմակերպվել ինչպես ներքին տեխնիկական մասնագետի, այնպես էլ արտաքին մասնագետի միջոցով, որը կհանդիսանա դասընթացավար:
☐	Ուղեցույց աշխատակազմի համար	Կարևոր է ունենալ ուղեցույց, որտեղ գրված կլինի կազմակերպության տեղեկատվության ապահով պահպանմանն ուղղված անհրաժեշտ գործողությունների մասին, որին կծանոթանան բոլոր նոր աշխատակիցները աշխատանքը սկսելուց առաջ:	Ուղեցույցը կարող է մշակվել ինչպես ներքին մասնագետների, այնպես էլ արտաքին փորձագետների միջոցով:

DigiSupport

✓	Անհրաժեշտ քայլ	Բացատրություն	Գործողություն
☐	Բազմագործոն նույնականացում (multi-factor authentication)	Բազմագործոն նույնականացումը (MFA) հաշիվ մուտք գործելու բազմաքայլ գործընթաց է, որն օգտվողներից պահանջում է մուտքագրել ավելի շատ տեղեկատվություն, քան պարզապես գաղտնաբառն է: Օրինակ՝ կարող է խնդրել օգտատերերին գաղտնաբառի հետ մուտքագրել իրենց էլ. փոստին ուղարկված ծածկագիրը, պատասխանել գաղտնի հարցի կամ սկանավորել մատնահետքը:	Բազմագործոն նույնականացման միացման գործընթացը տարբեր հարթակներում իրականացվում է տարբեր կերպ:
☐	Հակավիրուսային ծրագիր	Հակավիրուսային ծրագիրը համակարգչային ծրագիր է, որն օգտագործվում է վիրուսային ծրագրերը կանխելու, հայտնաբերելու և հեռացնելու համար:	Կան մի շարք վճարովի և անվճար հակավիրուսային ծրագրեր: Ծրագրի ընտրությունը պետք է կապված լինի կազմակերպության առանձնահատկությունների, առկա համակարգչային ծրագրերի հետ: Հակավիրուսային ծրագիր ներբեռնելուց առաջ առաջարկվում է խորհրդակցել մասնագետի հետ:

✓	Անհրաժեշտ քայլ	Բացատրություն	Գործողություն
☐	Տեղեկատվության հասանելիության սահմանափակում	Ընկերության աշխատակիցները պետք է ունենան հասանելիություն միայն այն տեղեկատվությանը, որն անմիջապես վերաբերում է իրենց աշխատանքին: Մեծ ուշադրություն է անհրաժեշտ դարձնել հաճախորդների անձնական տվյալներին, բանկային հաշիվների տվյալներին և ընկերության ֆինանսական տեղեկատվության պահպանմանը:	Պետք է հստակ սահմանել, թե յուրաքանչյուր աշխատակցի որ տեղեկատվությունն է հասանելի լինելու և որ հարթակով:
☐	Էլ. փոստերի հասանելիության սահմանափակում	Աշխատանքային էլեկտրոնային փոստերը պետք է հասանելի լինեն միայն աշխատանքային համակարգիչներում: Աշխատակիցների անձնական համակարգիչներում ընկերության հարթակների, այդ թվում նաև էլ. փոստերի հասանելիությունը չի խրախուսվում:	Այս նպատակով կարող են իրականացվել 2 հիմնական քայլեր. 1. Բարձրացնել տեղեկացվածության մակարդակը աշխատակիցների շրջանում և սահմանել էլ. փոստից օգտվելու հստակ կանոններ 2. Էլ. փոստեր մուտք գործելու համար միացնել երկքայլ հաստատում՝ այդպիսով մեկ կենտրոնից վերահսկելով ընկերության էլ.

✓	Անհրաժեշտ քայլ	Բացատրություն	Գործողություն
			փոստեր մուտքը այլ համակարգիչներից
☐	Ներքին համակարգչային ցանց	Ներքին համակարգչային ցանցը փոխկապակցված համակարգիչների և այլ սարքերի խումբն է, որը տեղակայված է ընկերությունում: Համակարգիչների ներքին ցանցի ստեղծումը թույլ է տալիս աշխատանքը և տեղեկատվության փոխանցումն ու տարածումը դարձնել առավել անվտանգ:	Համակարգչային ներքին ցանցի անվտանգության ապահովման համար շատ կարևոր է ունենալ կառավարման ընդհանուր կենտրոն, որտեղից կկառավարվեն բոլոր համակարգիչները և դրանց ներքին գաղտնաբառերը:
☐	Անվտանգ գաղտնաբառեր	Ընկերությանը պատկանող բոլոր հարթակների գաղտնաբառերը պետք է լինեն դժվար կռահելի: Խոսքը վերաբերում է ինչպես, օրինակ, սոցցանցերին և էլ. փոստերին, այնպես էլ բանկային հաշիվների, քարտերի և ֆինանսական տեղեկատվության կառավարման հարթակների համար կիրառվող գաղտնաբառերին:	Անվտանգ գաղտնաբառեր ունենալու համար կարող եք դրանցում օգտագործել մի քանի տեսակի սիմվոլներ՝ մեծատառեր, փոքրատառեր, թվեր և այլն:
☐	Անվտանգ Wi-Fi	Wi-Fi ցանցերը խոցելի են կիբերհարձակումների համար, այդ պատճառով անհրաժեշտություն է առաջանում ապահովել ցանցի անվտանգությունը ևս:	Անվտանգ Wi-Fi ունենալու համար դա պետք է պաշտպանել և՛ արտաքին, և՛ ներքին միջոցներով: Առաջնահերթ անհրաժեշտ է ընտրել այնպիսի կապի

✓	Անհրաժեշտ քայլ	Բացատրություն	Գործողություն
			օպերատոր, որը երաշխավորում է անվտանգությունը և ունի ներքին գաղտնաբառեր: Այնուհետև անհրաժեշտ է անվտանգությունը ապահովել նաև ներքին գաղտնաբառերի և անընդհատ մոնիթորինգի միջոցով:
☐	Կարևոր փաստաթղթերի, տեղեկատվության պատճենների առկայություն	Անհրաժեշտ է ունենալ կարևոր փաստաթղթերի պատճեններ կոշտ կրիչներում, որպեսզի ընկերությունը կարևոր տեղեկատվություն չկորցնի տեղեկատվության արտահոսքի, համակարգիչների վարակվելու կամ կիբերհարձակման դեպքում:	Անհրաժեշտ է նախ քարտեզագրել ամբողջ կարևոր տեղեկատվությունը, այնուհետև ընտրել դրանց պատճենների համար ապահով կրիչներ և պատճենել դրանք կրիչներում:
☐	Սոցցանցերի էջերի հասանելիության կարգավորում	Սոցիալական ցանցերի գաղտնաբառերին հասանելիություն պետք է ունենան սահմանափակ թվով աշխատակիցներ, որոնք անմիջապես իրականացնում են հրապարակումներ, գովազդներ կամ կապ են պահպանում հաճախորդների հետ սոցցանցերի միջոցով:	Անհրաժեշտ է քարտեզագրել առկա սոցցանցերի հարթակները, դրանց պատասխանատուներին և հասանելիությունը տալ միայն նրանց:

✓	Անհրաժեշտ քայլ	Բացատրություն	Գործողություն
☐	Ֆինանսական տեղեկատվության անընդհատ մոնիթորինգ	Ընկերության ֆինանսական տեղեկատվությունը ամենահաճախն է հանդիսանում կիբերհանցագործությունների թիրախ և կարիք է առաջանում անընդհատ վերահսկողություն սահմանել դրա վրա:	Բացի նշված քայլերից, անհրաժեշտ է նաև պարբերաբար իրականացնել բանկային հաշիվների քաղվածքների մոնիթորինգ և դրանցում առկա տվյալները համեմատել ընկերության փաստացի գործունեության տվյալների հետ:
☐	Զգուշացում կեղծ մատակարարներից	Հաճախ կիբերհանցագործությունները իրականացվում են «կեղծ» մատակարարների կողմից, որոնք ընկերության հետ որևէ գործարք իրականացնելու պատրվակով փորձում են հասանելիություն ունենալ ընկերությանը պատկանող տեղեկատվությանը՝ հաճախ նաև իրականացնելով ֆինանսական խարդախություններ:	Յուրաքանչյուր կատարվող գործարքից առաջ անհրաժեշտ է մանրամասնորեն ուսումնասիրել մատակարարին և այն տեղեկատվությունը, որը կազմակերպությունը տրամադրում է նրան: Ոչ մի դեպքում չպետք է տրամադրել տեղեկություն գաղտնաբառերի, PIN կոդերի վերաբերյալ:
☐	Բնօրինակ (օրիգինալ) ծրագրերի առկայություն	Կազմակերպությունում անհրաժեշտ է ներդնել միայն օրիգինալ ծրագրեր՝ անմիջապես պաշտոնական աղբյուրից, քանի որ ծրագրերի առկա կրկնօրինակների պարագայում	Անհրաժեշտ է նախ կազմել այն ծրագրերի ցանկը, որոնք անհրաժեշտ են կազմակերպության գործունեության համար, գտնել օրիգինալ ծրագրերի

✓	Անհրաժեշտ քայլ	Բացատրություն	Գործողություն
		հնարավոր են ծրագրային խափանումներ և տեղեկատվության արտահոսք:	կայքերը և ներբեռնել միայն այդ կայքերից:
	Կազմակերպության համակարգիչների և ծրագրերի պարբերաբար թարմացում	Շատ կարևոր է ունենալ առկա ծրագրերի թարմացված տարբերակները: Սա վերաբերում է ինչպես ամպային ծրագրերին, այնպես էլ համակարգիչների տարբեր կոշտ մասերին:	Անհրաժեշտ է իրականացնել անընդհատ մոնիթորինգ և անհրաժեշտ թարմացումներ:

ԱՐՁԱԳԱՆՔՄԱՆ ՊԼԱՆ

Եթե այնուամենայնիվ տեղի է ունեցել կիբերհարձակում կամ տեղեկատվության արտահոսք, ընկերությանն անհրաժեշտ է արագ արձագանքման պլան՝ խնդիրներն անմիջապես շտկելու համար:

Ստորև ներկայացված է արագ արձագանքման պլանի պարզ ձևանմուշ:

Իրավիճակ	Խնդրի լուծման պատասխանատու	Գործողություն, որն անհրաժեշտ է ձեռնարկել խնդիրը վերացնելու համար
Ընկերության էլեկտրոնային փոստերի վրա հաճախակի հարձակումների փորձեր	Ընկերության SS անվտանգության մասնագետ	Բազմագործոն նույնականացման (multi-factor authentication) միացում

Աղյուսակում նշվածը օրինակ է: Կարող եք աղյուսակը լրացնել Ձեր կազմակերպության օրինակով

ՏՎՅԱԼՆԵՐԻ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՊԱՀՊԱՆՈՒՄԸ ՀՀ-ՈՒՄ

ՀՀ-ում գործում է «Անձնական տվյալների պաշտպանության մասին» օրենքը, որն ընդունվել է 2015 թվականին: Օրենքի հիման վրա ստեղծվել է նաև անձնական տվյալների պաշտպանության լիազոր մարմին՝ ՀՀ Արդարադատության նախարարության Անձնական տվյալների պաշտպանության գործակալությունը, որը պարբերաբար իրականացնում է տեղեկացվածության բարձրացման միջոցառումներ՝ այդ թվում նաև սոցցանցերի միջոցով:

Գործակալությունը մշակել է ուղեցույցներ (https://moj.am/page/610) ինչպես համացանցում տվյալների պաշտպանության, այնպես էլ պետական մարմինների կողմից անձնական տվյալների մշակման համար:

Անձնական տվյալների պաշտպանության գործակալության՝ օրենքով նախատեսված լիազորություններից է խորհրդատվություններ տրամադրելը կամ անձնական տվյալներ մշակելու վերաբերյալ լավագույն փորձի մասին տեղեկացնելը:
Գործակալությունն իրականացնում է նաև ուսուցումներ, ուստի կարող եք դիմել գործակալությանը անձնական տվյալների պաշտպանությանը վերաբերող հարցերով (նաև առցանց տիրույթում):

Կիբերանվտանգության ուղղությամբ իրազեկման միջոցառումներ են ձեռնարկվում նաև CyberHub կազմակերպության կողմից, որը վարում է նաև կրթական բլոգ՝ ուղղված գրագիտության բարձրացմանը:

«Բի Էս Սի» Բիզնեսի Աջակցման Կենտրոն ՍՊԸ
ՀՀ, 0002, Երևան, Եկմալյան փողոց 6
+374 10 57 47 78 | +374 77 57 47 78
bsc@bsc.am | www.bsc.am