# Տեղեկատվական անվտանգության կառավարման համակարգեր
(թեսթավորման հարցաշար)

| № | Հարցեր | Պատասխաններ |
|---|---|---|
| 1 | 2 | 3 |
| 1 | Ո՞ր ստանդարտի պահանջներին պետք է համապատասխանի տեղակատվական անվտանգության կառավարման համակարգերը | 1. ՀՍՏ ԻՍՕ 27001-2008<br>2. ՀՍՏ ԻՍՕ 14001<br>3. ՀՍՏ ԻՍՕ 9000-2002 |
| 2 | Համաձայն ՀՍՏ ԻՍՕ 27001-2008 ստանդարտի ինչպե՞ս է սահմանվում տեղեկատվական անվտանգությունը | 1. Տեղեկության պաշտպանությունն է վնասակար կոդերից:<br>2. Տեղեկության պաշտպանությունն է բազմազան սպառնալիքներից՝բիզնեսի շարունակականությունը և բիզնես ռիսկերի նվազեցումն ապահովելու, ինչպես նաև ներդրումներից և բիզնես հնարավորություններից ստացվող շահույթն առավելագույնի հասցնելու համար:<br>3. Տեղեկության պաշտպանությունն է գործավարական համակարգերի խափանումներից: |
| 3 | Ի՞նչ է սահմանվում ՀՍՏ ԻՍՕ 27001-2008 ստանդարտով: | 1. ՀՍՏ ԻՍՕ 27001-2008 ստանդարտով սահմանվում է կազմակերպությունում տեղեկատվական անվտանգության ապահովման սկզբունքները:<br>2. ՀՍՏ ԻՍՕ 27001-2008 ստանդարտով սահմանվում է կազմակերպությունում տեղեկատվական անվտանգության կազմակերպման ընթացքը:<br>3. ՀՍՏ ԻՍՕ 27001-2008 ստանդարտով սահմանվում են կազմակերպությունում տեղեկատվական անվտանգության կառավարում իրականացնելու, պահպանելու և բարելավվելու վերաբերյալ ընդհանուր սկզբունքները և ցուցումները |
| 4 | Ըստ ՀՍՏ ԻՍՕ 27001-2008 ստանդարտի տեղեկատվական անվտանգության ներկայացվող պահանջների հիմնական աղբյուրները քանի՞սն են: | 1. 3<br>2. 4<br>3. 7 |
| 5 | Ըստ ՀՍՏ ԻՍՕ 27001-2008 ստանդարտի որո՞նք են տեղեկատվական անվտանգության կառավարման համակարգի ընդհանուր պահանջները: | 1. Կազմակերպությունը պետք է պահպանի և բարելավի փաստաթղթերով ամրագրված ՏԱԿՀ՝ իր ընդհանուր գործունեության և դրա հետ կապված ռիսկերի նկատմամբ:<br>2. Կազմակերպությունը պետք է ստեղծի, ներդնի, գործառնի, հսկի, ընթացաստուգի, վերլուծի, պահպանի և բարելավի փաստաթղթերով ամրագրված ՏԱԿՀ՝ իր ընդհանուր գործունեության նկատմամբ:<br>3. Կազմակերպությունը պետք է ստեղծի, ներդնի, գործառնի, հսկի, ընթացաստուգի, վերլուծի, պահպանի և բարելավի փաստաթղթերով ամրագրված ՏԱԿՀ՝ իր ընդհանուր |

| | | |
|---|---|---|
| | | գործունեության և դրա հետ կապված ռիսկերի նկատմամբ: |
| 6 | Ո՞րն է ՀՍՏ ԻՍՕ 27001-2008 ստանդարտի կիրառման ոլորտը | 1. Սույն ստանդարտը նախատեսված է պետական մարմինների կազմակերպությունների կողմից կիրառման համար:<br>2. Սույն ստանդարտը նախատեսված է բոլոր տեսակի կազմակերպությունների կողմից կիրառման համար:<br>3. Սույն ստանդարտը նախատեսված է առևտրային կազմակերպությունների կողմից կիրառման համար: |
| 7 | Ըստ ՀՍՏ ԻՍՕ 27001-2008 ստանդարտի ինչպիսի՞ն է տեղեկատվական անվտանգության կառավարման համակարգի ստեղծման ընթացքը | 1. Կազմակերպությունը պետք է սահմանի ընդհանուր քաղաքականությանը և նպատակներին համապատասխան ռիսկերի կառավարման և տեղեկատվական անվտանգության բարելավման համար ՏԱԿՀ քաղաքականությունը, նպատակները, գործընթացները, և ընթացակարգերը:<br>2. Կազմակերպությունը պետք է սահմանի տեղեկատվական անվտանգության բարելավման համար ՏԱԿՀ քաղաքականությունը:<br>3. Կազմակերպությունը պետք է սահմանի ընդհանուր քաղաքականությանը և նպատակներին համապատասխան ռիսկերի կառավարման քաղաքականությունը: |
| 8 | Ըստ ՀՍՏ ԻՍՕ 27001-2008 ստանդարտի ինչպիսի՞ն է տեղեկատվական անվտանգության կառավարման համակարգի կատարման (ՏԱԿՀ) ընթացքը | 1. ՏԱԿՀ քաղաքականության , հսկողության միջոցների, գործընթացների և ընթացակարգերի ներդրում<br>2. ՏԱԿՀ քաղաքականության , հսկողության միջոցների, գործընթացների և ընթացակարգերի գործառնություն<br>3. ՏԱԿՀ քաղաքականության , հսկողության միջոցների, գործընթացների և ընթացակարգերի ներդրում և գործառնություն |
| 9 | Ըստ ՀՍՏ ԻՍՕ 27001-2008 ստանդարտի ինչպիսի՞ն է տեղեկատվական անվտանգության կառավարման համակարգի (ՏԱԿՀ) ստուգման ընթացքը | 1. Գործընթացների արդյունավետության գնահատում<br>2. Գործընթացների արդյունավետության գնահատում և ըստ անհրաժեշտության ՏԱԿՀ քաղաքականության, նպատակների և գործնական փորձի հետ համեմատում, ինչպես նաև արդյունքների հայտնում ղեկավարությանը՝վերլուծության համար<br>3. Գործընթացների արդյունավետության գնահատում և արդյունքների հայտնում ղեկավարությանը: |
| 10 | Ըստ ՀՍՏ ԻՍՕ 27001-2008 ստանդարտի ինչպիսի՞ն է տեղեկատվական անվտանգության կառավարման համակարգի (ՏԱԿՀ) գործողության ընթացքը | 1. ՏԱԿՀ ներքին աուդիտի , ղեկավարության կողմից վերլուծության արդյունքների կամ համապատասխան այլ տեղեկատվության |

| | | |
|---|---|---|
| | | հիման վրա ՏԱԿՀ շարունակական բարելավման ապահովման նպատակով ուղղիչ և կանխարգելիչ միջոցառումների ձեռնարկում:<br>2. ՏԱԿՀ ներքին աուդիտի վերլուծության արդյունքների հիման վրա կանխարգելիչ միջոցառումների ձեռնարկում:<br>3. ՏԱԿՀ ղեկավարության կողմից վերլուծության արդյունքների հիման վրա ՏԱԿՀ շարունակական բարելավման ապահովման նպատակով ուղղիչ միջոցառումների ձեռնարկում: |
| 11 | Ըստ ՀՍՏ ԻՍՕ 27001-2008 ստանդարտի ո՞րն է տեղեկատվական անվտանգության քաղաքականության նպատակը: | 1. Ապահովել կազմակերպության աշխատողների մասնակցությունը տեղեկատվական անվտանգության ապահովման հարցերում<br>2. Ապահովել կազմակերպության ղեկավարության մասնակցությունը տեղեկատվական անվտանգության ապահովման հարցերում՝ բիզնեսի պահանջներին , ինչպես նաև օրենդրությանը, այդ թվում ՝ տեխնիկական կանոնակարգերով սահմանված պահանջներին համապատասխան:<br>3. Ապահովել կազմակերպության ղեկավարության միջամտումը տեղեկատվական անվտանգության ապահովման հարցերում |
| 12 | ՀՍՏ ԻՍՕ 27002-2008 ստանդարտը քանի՞ բաժիններից է կազմված: | 1. 10<br>2. 11<br>3. 12 |
| 13 | ՀՍՏ ԻՍՕ 27002-2008 ստանդարտի անվտանգության հիմնական դասերից յուրաքանչյուրը ի՞նչ է նեռառում: | 1. Հսկողության նպատակ<br>2. Մեկ կամ ավելի հսկողության միջոց<br>3. Հսկողության նպատակ և մեկ կամ ավելի հսկողության միջոց |
| 14 | Ի՞նչ գործողություններ է ենթադրում ռիսկերի գնահատումը: | 1. Ռիսկերը գնահատելու միջոցով պետք է կանխվի սպառնացող արտաքին վտանգը:<br>2. Ռիսկերը գնահատելու միջոցով պետք է բացահայտվեն, քանակապես որոշվեն և ըստ առաջնահերթության դասակարգվեն սպառնացող արտաքին վտանգի նշանները :<br>3. Ռիսկերը գնահատելու միջոցով պետք է որոշվի, ինչպես վերացնել արտաքին վտանգի ազդեցության հետևանքների |
| 15 | ինչպե՞ս է սահմանվում տեղեկատվական անվտանգության քաղաքականության հիմնակն դրույթները: | 1. Տեղեկատվական անվտանգության քաղաքականությամբ սահմանվում է ընդհանուր ռազմավարությունը:<br>2. Տեղեկատվական անվտանգության քաղաքականությամբ սահմանվում է տեղակատվական անվտանգության կառավարման նկատմամբ կազմակերպության մոտեցումը<br>3. Տեղեկատվական անվտանգության քաղաքականությունը պետք է արտահայտի ղեկավարության պարտավորությաւնը և |

| | | |
|---|---|---|
| | | սահմանի տեղակատվական անվտանգության կառավարման նկատմամբ կազմակերպության մոտեցումը |
| 16 | Տեղեկատվական անվտանգության պարտականությունների բաշխումը ինչի՞ն պետք է համապատասխանի: | 1. Տեխնիկական կանոնակարգերով սահմանված պահանջներին<br>2. ՀՍՏ ԻՍՕ 27002-2008 ստանդարտին<br>3. Տեղեկատվական անվտանգության քաղաքականու թյունը |
| 17 | Գաղտնիության կամ տեղեկատվության չհրապարակման մասին համաձայնագրերը պետք է համապատասխանեն… | 1. Գործող օրենքներին և կանոնակարգերին այն իրավազորության շրջանակներում, որտեղ դրանք կիրառելի են:<br>2. Տեղեկատվական անվտանգության քաղաքականությանը<br>3. Կազմակերպության քաղաքականությանը |
| 18 | Ե՞րբ պետք է վերանայվեն գաղտնիության կամ տեղեկատվության չհրապարակման մասին համաձայնագրերը | 1. Տարին մեկ անգամ<br>2. 6 անիսը մեկ անգամ<br>3. Պարբերաբար, ինչպես նաև այն դեպքում երբ տեղի են ունեցել այդ պահանջների վրա ազդող փոփոխություն- ներ: |
| 19 | Ի՞նչ է պետք կատարել, նախքան արտաքին կազմակերպությանը կազմակերպության տեղեկատվություն և տեղեկությունների մշակման միջոցներից օգտվելու հնարավորություն տրամադրելը: | 1. Պայմանագիր կնքել<br>2. Ռիսկերը գնահատել<br>3. Ոչինչ չանել |
| 20 | Կազմակերպությունը ինչպե՞ս պետք է ապահովի իր ակտիվների պատշաճ պաշտպանությունը: | 1. Նշանակվում է պատասխանատու անձ:<br>2. Բոլոր ակտիվները համար պետք է ստեղծվի ցուցակ<br>3. Բոլոր ակտիվները պետք է հաշվառվեն և ունենան տնօրինող |
| 21 | Որո՞նք են կազմակերպության ակտիվների տեսակները: | 1. Տեղեկատվությունը, ծրագրային ապահովման միջոցների հետ կապված ակտիվներ, ֆիզիկական ակտիվները:<br>2. Տեղեկատվությունը, ծրագրային ապահովման միջոցների հետ կապված ակտիվներ, ֆիզիկական ակտիվները, մատուցվող ծառայությունները, մարդկային ռեսուրսները, ոչ նյութական ակտիվները:<br>3. Տեղեկատվությունը, մարդկային ռեսուրսները, ոչ նյութական ակտիվները: |
| 22 | Ի՞նչ նպատակով են դասակարգում տեղեկատվությունը: | 1. Տեղեկատվության հետ կապված կարիքները, առաջնահերթությունները և պաշտպանության ակնկալվող աստիճանը սահմանելու համար:<br>2. Տեղեկատվության անվտանգությունը ապահովելու համար:<br>3. Տեղեկատվության անվտանգության աստիճանը որոշելու համար: |
| 23 | Ի՞նչ նպատակով են ստեղծվում պաշտպանվող գոտիները: | 1. Կանխել առանց թույլտվության տեղեկատվությունից օգտվումը:<br>2. Կանխել առանց թույլտվության կազմակերպության տարածք մուտք գործելը և |

| | | |
|---|---|---|
| | | տեղեկատվությունից օգտվելը, վնաս պատճառելը և միջամտելը:<br>3. Անվտանգության |
| 24 | Սարքավորումների անվտանգության ապահովման նպատակը | 1. Կանխել կազմակերպության ակտիվների կորուստը, վնասումը, գողությունը:<br>2. Կանխել կազմակերպության գործունեության ընդհատումը:<br>3. Կանխել կազմակերպության ակտիվների կորուստը, վնասումը, գողությունը, կամ որևէ այլ սպառնալիք և կազմակերպության գործունեության ընդհատումը: |
| 25 | Ի՞նչ պայմանների հետ է կապված սարքավորումների տեղադրումը և պաշտպանումը: | 1. Բնական աղետների կամ վտանգների հետ կապված ռիսկերը նվազեցումը և առանց թույլատվության տեղեկատվությունից օգտվելու հնարավորոիթյունները:<br>2. Հարմարավետության :<br>3. Անվտանգության |
| 26 | Ինչո՞վ է պետք ապահովել կարեվորագույն բիզնես գործունեության օժանդակող սարքավորումները: | 1. Էլեկտրաէներգիայի անխափան մատակարարմամբ:<br>2. Էլեկտրաէներգիայի անխափան սնուցման սարք (UPS)<br>3. Հուսալի հեռահաղորդակցման կապով: |
| 27 | Գործավարական համակարգերում ե՞ որ է պետք կատարել փոփոխություններ: | 1. Համապատասխան հրահանգ ստանալով:<br>2. Կամայական պահին:<br>3. Երբ դրա համար կա հիմնավորված գործնական պատճառ: |
| 28 | Ի՞նչ է պարտականությունների սահմանազատումը: | 1. Աշխատանքային գրաֆիկի սահմանում<br>2. Համակարգի պատահական կամ միտումնավոր չարաշահումների ռիսկերը նվազեցնելու մեթոդ է:<br>3. Աշխատանքի հստակ բաշխման մեթոդ է: |
| 29 | Ո՞րն է շարժական կոդի սահմանումը: | 1. Շարժական կոդը ծրագրային ապահովման միջոց է , որը փոխանցվում է մի համակարգչից մյուսը, ապա գործածվում ինքնաբերաբար և կատարում հատուկ գործառույթ օգտվողի աննշան փոխազդեցությամբ կամ առանց դրա:<br>2. Ինքնաբերաբար գործածվող ծրագրային ապահովման միջոց :<br>3. Օգտվողի հրահանգով աշխատող ելակետային կոդ: |
| 30 | Ո՞րն վնասակար և շարժական կոդերից պաշտպանության նպատակը: | 1. Գործավարական համակարգերի անխափան աշխատանքի ապահովում:<br>2. Տեղեկատվության պաշտպանություն<br>3. Պաշտպանել ծրագրային ապահովման և տեղեկատվության մասիվների ամբողջականությունը: |
| 31 | Ըստ ՀՍՏ ԻՍՕ 27002-2008 որո՞նք են վնասակար կոդերը: | 1. Համակարգչային վիրուսները, ցանցային որդերը, «տրոյական ձիերը» և տրամաբանական ռումբերը:<br>2. Համակարգչային վիրուսները,«տրոյական |

| | | |
|---|---|---|
| | | ծիերը»<br>3. Ցանցային որդերը, «տրոյական ծիերը» և տրամաբանական ռումբերը: |
| 32 | Ո՞րն տեղեկատվության պահեստավորման(back up) նպատակը: | 1. Պահպանել տեղեկատվության ամբողջականությունը:<br>2. Պահպանել տեղեկատվության , ինչպես նաև տեղեկությունների մշակման միջոցների ամբողջականությունն ու մատչելիությունը:<br>3. Պաշտպանել տեղեկատվությունը վնասակար կոդերից: |
| 33 | Ո՞րն կրիչների տնօրինման նպատակը: | 1. Կանխել ակտիվների չթույլատրված հրապարակումը, փևափոխումը հառացումը կամ ոչնչոցումը, ինրպես նաև կազմակերպության բիզնես գործունեության ընդհատումը:<br>2. Կանխել բիզնես գործունեության ընդհատումը:<br>3. Պաշտպանել արտաքին ազդեցությունից: |
| 34 | Ի՞նչ են ներառում դյուրակիր կրիչները՞ | 1. Ժապավեններ, սկավառակներ<br>2. Ժապավեններ, սկավառակներ, մեծ հիշողության սկավառակներ, դյուրակիր կարծրասկավառակները, CD-ները, DVD-ները և տպագիր կրիչները:<br>3. CD-ները, DVD-ները |
| 35 | Գործավարական (օպերացիոն) համակարգից օգտվելու հնարավորության հսկողության նպատակը: | 1. Պաշտպանել ծրագրային ապահովման ամբողջականությունը»<br>2. Առանց թույլտվության տեղեկատվությունից չօգտվել:<br>3. Կանխել գործավարական համակարգերից առանց թույլատվության օգտվելու հնարավորությունը: |
| 36 | Ի՞նչ պետք է ունենան գործավարական (օպերացիոն) համակարգից բոլոր օգտվողները: | 1. Չկրկնվող նույնականացման հատկանիշ(ID):<br>2. Գաղտնաբառ<br>3. Թույլտվություն |
| 37 | Ի՞նչ է համարվում գաղտնաբառը: | 1. Աշխատողին տեղեկատվական համակարգից կամ ծառայությունից օգտվելու հնարավորության միջոց:<br>2. Օգտվողի ինքնության ստուգման միջոց:<br>3. Փոխկապակցման միջոց: |
| 38 | Ի՞նչ են ներառում տեղեկատվական համակարգերը: | 1. Գործավարական համակարգը, օգտվողի կողմից մշակված աշխատածրագրերը:<br>2. Համակարգչի մեջ պարունակվող ամբողջ ինֆորմացիան:<br>3. Գործավարական համակարգը, ենթակառուցվածքը, բիզնես աշխատածրագրերը, պատրաստի արտադրանքը, ծառայությունները և օգտվողի կողմից մշակված աշխատածրագրերը: |

| | | |
|---|---|---|
| 39 | Ինչի՞ն պետք է ենթարկվեն աշխատածրագրերի համար օգտագործվող մուտքային տվյալները: | 1. Վավերականության ստուգման ՝ դրանց ճշգրտությունն ու համապատասխանությունը ապահովելու համար:<br>2. Ստուգման օգտագործողի կողմից:<br>3. Ստուգման՝ գաղտնի ինֆորմացիա պարունակելու նկատմամբ: |
| 40 | Ե՞րբ պետք է արդիականացվեն գործավարական ծրագրերը: | 1. Գոյություն ունի գործավարական համակարգի նոր տարբերակ:<br>2. Ղեկավարության հրահանգով:<br>3. Միայն այն ժամանակ , երբ կա դրա պահանջը: |
| 41 | Ի՞նչ նպատակով է գրվում ելակետային կոդը: | 1. Գործը հեշտացնելու նպատակով:<br>2. Կատարվող ֆայլեր ստեղծելու նպատակով:<br>3. Վերահսկողության նպատակով: |
| 42 | Ի՞նչ է ներառում բիզնեսի շարունակականության կառավարումը: | 1. Ռիսկերի գնահատման ընդհանուր գործընթացը, ռիսկերի որոշման և նվազեցման հսկողության միջոցները, վնասակար միջադեպերի հետևանքների սահմանափակումը և տեղեկատվության մատչելիության ապահովումը:<br>2. Ռիսկերի գնահատման ընդհանուր գործընթաց:<br>3. Վնասակար միջադեպերի հետևանքների սահմանափակումը և տեղեկատվության մատչելիության ապահովումը: |
| 43 | Ո՞րն է բիզնեսի շարունակականության կառավարման տեղեկատվական անվտանգության ապահովման նպատակը: | 1. Հակազդել բիզնեսի ընդհատումներին:<br>2. Պաշտպանել կարևորագույն բիզնես գործընթացները տեղեկատվական համակարգերի խոշոր վթարների հետևանքներից:<br>3. Հակազդել բիզնեսի ընդհատումներին , պաշտպանել կարևորագույն բիզնես գործընթացները տեղեկատվական համակարգերի խոշոր վթարների կամ աղետների հետևանքներից և ապահովել դրանց ժամանակին վերագործարկումը: |
| 44 | Ո՞ր դեպքերը կարող են բիզնես գործընթացների ընդհատման պատճառ հանդիսանալ: | 1. Սարքավորումների ձախողումը, բնական աղետները և ահաբեկչական գործողությունները:<br>2. Սարքավորումների ձախողումը, մարդկային գործոնով պայմանավորված սխալները, գողությունը, հրդեհը, բնական աղետները և ահաբեկչական գործողությունները:<br>3. Մարդկային գործոնով պայմանավորված սխալները: |
| 45 | Ի՞նչ են ներառում մտավոր սեփականության իրավունքները: | 1. Ծրագրային ապահովման միջոցների կամ կամ փաստաթղթի հեղինակային իրավունքները, նախագծման իրավունքները, ապրանքային նշանները, պատենտները և ելակետային կոդի արտոնագրերը:<br>2. Փաստաթղթի հեղինակային իրավունքները<br>3. Ծրագրային ապահովման միջոցների հեղինակային իրավունքները |

| | | |
|---|---|---|
| 46 | Ի՞նչ է ենթադրվում համապատասխանության տեխնիկական ստուգման տակ: | 1. Ծրագրային ապահովման ստուգումը:<br>2. Գործավարական համակարգի զննումը՝սարքերի և ծրագրային ապահովման հսկողության միջոցների ճիշտ կիրառումն ապահովելու համար:<br>3. Համակարգչի տեխնիկական վիճակի զննումը: |
| 47 | Տեղեկատվական համակարգերի աուդիտի միջոցները ինչի՞ց պետք առանձնացված լինեն: | 1. Ոչ մի բանից:<br>2. Պետք է մեկուսացված լինեն բոլոր գործող համակարգերից:<br>3. Մշակման և գործավարական համակարգերից: |
| 48 | Ո՞ւմ վրա է տարածվում Համակարգիչներին ը դրանցից օգտվողների աշխատանքի կազմակերպմանը ու պայմաններին ներկայցվող հիգիենիկ պահանջներ: N2 III – 4.10 – Սանիտարական կանոնները և նորմերը: | 1. Անհատ ձեռնարկատերերի և իրավաբանական անձանց վրա, որոնք բնակչության սպասարկման ոլորտում , հանրային, վարչական և ուսումնա-դաստիարակչական հաստատություններում , օգտագործելով տարբեր տեսակի համակարգիչներ, թվային հաշվիչ սարքեր, իրականացնում են գործունեություն , հիմնարկների վրա:<br>2. Բոլոր պետական հաստատությունների վրա:<br>3. Իրավաբանական անձանց վրա, որոնք բնակչության սպասարկման ոլորտում , հանրային, վարչական և ուսումնադաստիարակչական հաստատությունն-ում , օգտագործելով տարբեր տեսակի համակարգիչներ, թվային հաշվիչ սարքեր, իրականացնում են գործունեություն , հիմնարկների վրա: |
| 49 | Որքա՞ն պիտի լինի հեռավորությունը մոնիտորի էկրանից մինչև համակարգչով աշխատող անձի աչքերը: | 1. Կամայական<br>2. 300-500մմ<br>3. 600-700 մմ, բայց ոչ պակաս քան 500մմ |
| 50 | 50 հաճախականության էլեկտրական դաշտի ֆոնային մակարդակը չպետք է գերազանցի… | 1. 400 վ/մ<br>2. 500 վ/մ<br>3. 600վ/մ |