ՏԵՂԵԿԱՏՎԱԿԱՆ ՏԵԽՆՈԼՈԳԻԱՆԵՐԻ ԱԿՏԻՎՆԵՐԻ ՌԵԵՍՏՐԻ ՍՏԵՂԾՄԱՆ ԵՎ ԿԱՌԱՎԱՐՄԱՆ ՀԱՄԱԿԱՐԳԻ ՆԵՐԴՐՄԱՆ ԿԱՐԳԸ ՀԱՍՏԱՏԵԼՈՒ ՄԱՍԻՆ

ՆԱԽԱԳԻԾ

ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ԿԱՌԱՎԱՐՈՒԹՅՈՒՆ

ՈՐՈՇՈՒՄ

_____ 2025 թվականի N _____

ՏԵՂԵԿԱՏՎԱԿԱՆ ՏԵԽՆՈԼՈԳԻԱՆԵՐԻ ԱԿՏԻՎՆԵՐԻ ՌԵԵՍՏՐԻ ՍՏԵՂԾՄԱՆ ԵՎ ԿԱՌԱՎԱՐՄԱՆ ՀԱՄԱԿԱՐԳԻ ՆԵՐԴՐՄԱՆ ԿԱՐԳԸ ՀԱՍՏԱՏԵԼՈՒ ՄԱՍԻՆ

Ղեկավարվելով Հայաստանի Հանրապետության Սահմանադրության 146-րդ հոդվածի 4-րդ մասով և հաշվի առնելով Հայաստանի տեղեկատվական համակարգերի կառավարման խորհրդի 2024 թվականի սեպտեմբերի 27-ի թիվ ԽԱ/10-2024 արձանագրային որոշման առաջին կետի պահանջները՝ Հայաստանի Հանրապետության կառավարությունը որոշում է՝

1. Հաստատել տեղեկատվական տեխնոլոգիաների ակտիվների ռեեստրի ստեղծման և կառավարման համակարգի ներդրման կարգը՝ համաձայն հավելվածի։

2. Սույն որոշման հավելվածի 1-ին կետում նշված կազմակերպությունների ղեկավարներին՝

1) տեղեկատվական տեխնոլոգիների ակտիվների կառավարման՝ գույքագրման, նույնականացման, պահպանման և վերահսկման գործընթացներում առաջնորդվել սույն որոշման հավելվածի պահանջներով,

2) սույն որոշման հավելվածով նախատեսված ժամկետներում և կարգով «Հայաստանի տեղեկատվական համակարգերի գործակալություն» Հիմնադրամին ներկայացնել տեղեկատվական տեխնոլոգիաների ակտիվների վերաբերյալ նույն կարգով սահմանված տեղեկատվությունը,

3) սույն որոշման ուժի մեջ մտնելուց հետո ոչ ուշ, քան երեք ամսվա ընթացքում, ավարտել տեղեկատվական տեխնոլոգիաների ակտիվների ռեեստրի ներդրման աշխատանքները։

3. Առաջարկել «Հայաստանի տեղեկատվական համակարգերի գործակալություն» Հիմնադրամին՝

1) Սույն որոշման հավելվածի 1-ին կետում նշված կազմակերպությունների համապատասխան աշխատակիցների համար, ըստ անհրաժեշտության, կազմակերպել վերապատրաստման և իրազեկման միջոցառումներ,

2) ապահովել տեղեկատվական տեխնոլոգիաների ակտիվների գույքագրումն ավտոմատացված եղանակով իրականացնելու համար անհրաժեշտ գործիքակազմի ընտրությունը և մշակել դրանց կիրառման ուղեցույց՝ դրանք սույն որոշման հավելվածի 1-ին կետում նշված կազմակերպություններին տրամադրելու համար։

4. Սույն որոշման հավելվածի 1-ին կետում նշված հանրային հատվածի կազմակերպությունների ղեկավարներին՝ ապահովել իրենց ենթակայության տակ գտնվող պետական ոչ առևտրային կազմակերպություններում և հարյուր տոկոս պետական մասնակցությամբ ընկերություններում սույն որոշմամբ հավելվածի պահանջների կատարումը։

5. Սույն որոշումն ուժի մեջ է մտնում պաշտոնական հրապարակմանը հաջորդող տասներորդ օրը։

Հավելված

ՀՀ կառավարության —--/—-----2025թ.

N —Ն որոշման

ԿԱՐԳ

ՏԵՂԵԿԱՏՎԱԿԱՆ ՏԵԽՆՈԼՈԳԻԱՆԵՐԻ ԱԿՏԻՎՆԵՐԻ ՌԵԵՍՏՐԻ ՍՏԵՂԾՄԱՆ ԵՎ ԿԱՌԱՎԱՐՄԱՆ ՀԱՄԱԿԱՐԳԻ ՆԵՐԴՐՄԱՆ

I. ԸՆԴՀԱՆՈՒՐ ԴՐՈՒՅԹՆԵՐ

1. Սույն կարգով սահմանվում են «Հանրային հատվածի կազմակերպությունների հաշվապահական հաշվառման մասին» ՀՀ օրենքի իմաստով հանրային հատվածի կազմակերպություններում և հարյուր տոկոս պետական մասնակցությամբ ընկերություններում (այսուհետ՝ Կազմակերպություն) տեղեկատվական տեխնոլոգիաների (այսուհետ՝ SS) ակտիվների կառավարման համակարգի ներդրման և գործարկման նվազագույն պահանջները և կարգը։

2. Սույն կարգում կիրառվող հասկացություններն ունեն հետևյալ իմաստը.

1) SS ակտիվ - կազմակերպություններում տվյալների մշակման, պահպանման, փոխանցման կամ պաշտպանության համար օգտագործվող սարքավորումները (օրինակ՝ սերվերներ, աշխատակայաններ, անխափան սնուցման սարքեր, ցանցային սարքավորումներ, տվյալների կրիչներ և այլն), ծրագրային ապահովումներ (օրինակ՝ օպերացիոն համակարգեր, հավելվածներ, տվյալների բազաներ), կայքեր, տվյալներ (օրինակ՝

օգտատերերի տվյալներ, գրանցամատյաններ)։

2) SS ակտիվների ռեեստր (կամ՝ Ռեեստր) - կազմակերպությունում հաշվառված, ձեռք բերված և շահագործվող SS ակտիվների վերաբերյալ տվյալների ամբողջական, ստանդարտացված և վերահսկելի գրառում է, որը պահվում է որևէ թվային ձևաչափով (հարթակ, ծրագրային լուծում, տվյալների շտեմարան)՝ տեղեկատվության համակարգված պահպանման, վերլուծության և թարմացման նպատակով և ապահովում է տվյալ կազմակերպության կառավարման ներքին կարիքների և փաստաթղթերի շրջանառությունը։

3) SS ակտիվների ռեեստրի վարում - կազմակերպությունների SS բոլոր ակտիվների համապարփակ և մանրամասն գույքագրում Ռեեստրում։

4) Կարևոր Ակտիվ – ակտիվ, որի կարևորությունը գնահատվում է գաղտնիության (Confidentiality), ամբողջականության (Integrity) և հասանելիության (Availability) պահանջների վրա հիմնված սանդղակով, որտեղ յուրաքանչյուր չափորոշիչ գնահատվում է 1-ից 3 բալով։ Միավորների գումարը կարող է կազմել 3-ից մինչև 9։ Կարևոր են համարվում այն ակտիվները, որոնք ստացել են 5-ից 7 միավոր ընդհանուր գնահատական։

5) Կրիտիկական Ակտիվ - ակտիվ, որի կարևորությունը գնահատվում է գաղտնիության (Confidentiality), ամբողջականության (Integrity) և հասանելիության (Availability) պահանջների հիման վրա՝ յուրաքանչյուր չափորոշիչի գնահատմամբ 1-ից 3 բալով։ Միավորների գումարը կարող է կազմել 3-ից մինչև 9։ Կրիտիկական են համարվում այն ակտիվները, որոնք ստացել են 8-ից 9 միավորի գնահատում, այսինքն՝ ունեն ամենաբարձր արժեք երկուսից երեք չափորոշիչներով։

6) Ռեեստր վարող - կազմակերպության կողմից նշանակված աշխատակից կամ ստորաբաժանում, որը պատասխանատու է SS ակտիվների ռեեստրի տվյալների հավաքագրման, լրացման, վարման, թարմացման, ճշգրտության և վավերականության ապահովման համար։ Ռեեստր վարողը պարտավոր է տեղեկատվություն ստանալ ակտիվների տնօրինողներից, ներգրավել մասնագիտական թիմեր ըստ անհրաժեշտության, իրականացնել տվյալների ձևաչափային համապատասխանեցում հաստատված պահանջներին և ապահովել պարբերական համագործակցություն «Հայաստանի տեղեկատվական համակարգերի գործակալություն» Հիմնադրամի (այսուհետ՝ Գործակալություն) հետ

II. SS ԱԿՏԻՎՆԵՐԻ ՌԵԵՍՏՐԻ ՁԵՎԱՎՈՐՈՒՄԸ ԵՎ ՎԱՐՈՒՄԸ

3. Ռեեստրը ձևավորվում է տվյալ կազմակերպության ղեկավարի համապատասխան որոշմամբ։ Նույն որոշմամբ սահմանվում են նաև Ռեեստրի վարման համար պատասխանատու ստորաբաժանումները կամ այդ ստորաբաժանման գործառույթները պայմանագրային հիմունքներով իրականացնող իրավաբանական անձին կամ անհատ ձեռնարկատիրոջը (այսուհետ՝ պատասխանատու ստորաբաժանում) և անձինք (այսուհետ՝ Ռեեստր վարող)։ Ռեեստր վարողը պատասխանատու է Ռեեստրում տվյալների լրացման, վարման, վերահսկման, թարմացման ապահովման համար։

4. Ռեեստրում SS ակտիվները ենթակա են գրանցման և թարմացման՝ առնվազն տարեկան երկու անգամ՝ կիսամյակի ավարտից հետո՝ 10 աշխատանքային օրվա ընթացքում, ինչպես նաև՝ յուրաքանչյուր ակտիվի ձեռքբերման, փոփոխման, օտարման դեպքում՝ անհապաղ։

5. Կազմակերպությունները Ռեեստրում գրանցված տվյալների վերաբերյալ հաշվետվություններ են ներկայացնում Գործակալությանը՝ յուրաքանչյուր կիսամյակի ավարտից հետո 10 աշխատանքային օրվա ընթացքում՝ Գործակալության կողմից ներկայացված ձևաչափով, իսկ այդ տվյալներից տեղեկություններ տրամադրվում են տեղեկատվական անվտանգության միջադեպերին արձագանքելու դեպքերում՝ անհապաղ, կամ Գործակալության գրավոր պահանջի հիման վրա՝ վերջինիս սահմանած ձևաչափով։

6. Գործակալությունը, ներկայացված տվյալների հիման վրա, կատարում է մեթոդական վերլուծություն և, անհրաժեշտության դեպքում, ներկայացնում է առաջարկություններ՝ Ռեեստրի վարման գործընթացի բարելավման և կիբեռանվտանգության ռիսկերի կառավարման ուղղությամբ։ Ռեեստրի որակական համապատասխանության ապահովմանն աջակցելու նպատակով Տվյալների թերի կամ ոչ ժամանակին ներկայացման դեպքերում Գործակալությունը կարող է նախաձեռնել լրացուցիչ պարզաբանումների պահանջ կամ վերանայման գործընթաց՝ տվյալների ամբողջականությունն ապահովելու համար։

7. Կազմակերպությունների կողմից SS ակտիվների հավաքագրումը և Ռեեստրում տվյալների լրացումն իրականացվում է ավտոմատացված՝ Գործակալության կողմից առաջարկվող գործիքակազմով։

8. Ռեեստր վարողը պետք է ունենա անհրաժեշտ իրավասություն և հասանելիություն՝ տվյալ ակտիվների վերաբերյալ ամբողջական տեղեկատվություն հավաքագրելու, պարզաբանման համար համապատասխան ստորաբաժանումներին դիմելու, և տվյալների ճշգրտությունն ապահովելու համար։

9. Ռեեստր վարողը սույն կարգի 4-րդ կետով սահմանված ժամկետներում պետք է իրականացնի SS ակտիվների վերաբերյալ տեղեկատվության հավաքագրում և գրանցում Ռեեստրում։

10. Ռեեստրի լրացման գործընթացում, անհրաժեշտության դեպքում, կարող են ներգրավվել մասնագիտական թիմեր՝ կազմակերպության այլ ստորաբաժանումներից։

11. Ռեեստրի տվյալները ստուգվում և հաստատվում են կազմակերպության պատասխանատու ստորաբաժանման ղեկավարի կողմից՝ ապահովելով Ռեեստրում ներառված տեղեկատվության ամբողջականությունը և համապատասխանությունը հաստատված չափորոշիչներին։

12. Ռեեստրում ներառված տվյալների ճշգրտությունը համեմատվում է այլ տեղեկատվական համակարգերում (օրինակ՝ հաշվապահական կամ գնումների համակարգեր) առկա ակտիվների գրառումներին՝ ի հայտ բերելու բացակայող կամ չհաշվառված ակտիվներ։ Չհաշվառված ակտիվներ հայնաբերելու

դեպքում իրականացվում է ակտիվի մուտքագրում Ռեեստր սահմանված ձևաչափով։ Ակտիվի բացակայության դեպքում կազմակերպությունն առաջնորդվում է նյութական և ոչ նյութական ակտիվների գույքագրման համար սահմանված ընթացակարգերով։

13. Կրկնակի կամ սխալ գրանցված ակտիվների հայտնաբերման դեպքում դրանք ենթակա են ճշգրտման կամ հեռացման Ռեեստրից առավելագույնը 2 աշխատանքային օրվա ընթացքում՝ ապահովելով համապատասխան փաստաթղթավորում՝ համաձայն սահմանված կարգի։

14. Կեղծ կամ ոչ լիցենզավորված ծրագրային ապահովման (այդ թվում՝ ժամկետանց, չգրանցված կամ կեղծ լիցենզիաներով) հայտնաբերման դեպքում Ռեեստր վարողը պարտավոր է անհապաղ, բայց ոչ ուշ, քան 24 ժամվա ընթացքում, տեղեկացնել համապատասխան պատասխանատու ստորաբաժանման ղեկավարին՝ տվյալ ակտիվի օգտագործման դադարեցման, համակարգից հեռացման և իրավական հետևանքների գնահատման նպատակով։ Նման դեպքերը պետք է փաստաթղթավորվեն և ներկայացվեն Գործակալությանը՝ հաշվետվության տեսքով։

15. SS ակտիվների տնօրինման, պատասխանատվության կամ գտնվելու վայրի փոփոխության դեպքում տվյալները պետք է անհապաղ թարմացվեն Ռեեստրում։

16. Ռեեստրում ներառված տեղեկատվության ճշգրտության, ամբողջականության, արդիականության և փաստաթղթային ձևակերպման ապահովման պատասխանատվությունը կրում է տվյալ կազմակերպությունը։

17. SS ակտիվները համարվում են գրանցված Ռեեստրում՝ պատասխանատու ստորաբաժանման ղեկավարի կողմից դրանց հաստատման պահից։

18. Ռեեստրում պարտադիր ներառվում է առնվազն 31-րդ կետով սահմանված տեղեկատվությունը։

19. Ռեեստրում յուրաքանչյուր SS ակտիվ պետք է դասակարգվի՝ ըստ տեղեկատվության գաղտնիության (Confidentiality), ամբողջականության (Integrity) և հասանելիության (Availability) պահանջների՝ կիրառելով միջազգային լավագույն փորձը, մասնավորապես՝ ISO/IEC 27005 և հարակից տեղեկատվական անվտանգության ստանդարտների դրույթները։ «ՍիԱյԷյ» (CIA) գնահատումն իրականացվում է համատեղ ձևաչափով՝ ներառելով տվյալ ակտիվի պատասխանատու տեխնիկական և գործառնական ստորաբաժանումների ներկայացուցիչներին՝ ապահովելով գնահատման ամբողջականությունն ու համապատասխանությունը ակտիվի գործնական նշանակությանը։

20. «ՍիԱյԷյ» (CIA) գնահատման համար յուրաքանչյուր չափորոշիչ (Confidentiality, Integrity, Availability) ստանում է թվային արժեք՝ բարձր (High - H)՝ 3 միավոր, միջին (Medium - M)՝ 2 միավոր, ցածր (Low - L)՝ 1 միավոր։ Երեք բաղադրիչների հանրագումարը ձևավորում է ակտիվի անվտանգության գնահատականը. 5-ից 7 միավոր ունեցող ակտիվները դասակարգվում են որպես կարևոր, իսկ 8-ից 9 միավոր ունեցողները՝ կրիտիկական։

III. ՏՏ ԱԿՏԻՎՆԵՐԻ ՌԵԵՍՏՐԻ ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՊԱՀՈՎՈՒՄԸ

21. Ռեեստրի պաշտպանությունը պետք է իրականացվի կազմակերպությունների կողմից՝ հաշվի առնելով տեղեկատվական անվտանգության և տեղեկատվության պահպանման ապահովման ոլորտի գործող օրենսդրության և միջազգային ԻՍՕ/ԻԵԿ 27001 «ՏՏ Անվտանգության ապահովման մեխանիզմներ, Տեղեկատվական անվտանգության կառավարման համակարգեր, Պահանջներ» ստանդարտի պահանջները։

22. Ռեեստրին հասանելիությունը պետք է լինի սահմանափակ։ Մուտքի իրավունքը սահմանվում է կազմակերպության կողմից՝ հիմնվելով ծառայողական պարտականությունների վրա։ Բոլոր մուտքի գործողությունները պետք է գրանցվեն և պարբերաբար վերանայվեն՝ չարտոնված մուտքերի հայտնաբերման և կանխման նպատակով։

23. Ռեեստրին ժամանակավոր հասանելիության տրամադրումը արտակարգ իրավիճակներում թույլատրվում է միայն կազմակերպության ղեկավարի կամ լիազորված պաշտոնատար անձի գրավոր համաձայնությամբ՝ պարտադիր կերպով փաստաթղթավորելով տրամադրման նպատակը, ժամկետը և օգտագործող անձի նույնականացման տվյալները։

24. Ռեեստրի տվյալները պետք է գաղտնագրվեն ինչպես հանգստի վիճակում (at rest), այնպես էլ փոխանցման ընթացքում (in transit)՝ օգտագործելով արդի գաղտնագրման ալգորիթմներ՝ ապահովելով տվյալների պաշտպանությունը չարտոնված հասանելիությունից։

25. Ռեեստրի տեխնիկական խնդիրների կամ տեղեկատվական անվտանգության միջադեպերի դեպքում Ռեեստրի վարողը պարտավոր է տեղեկացնել կազմակերպության տեղեկատվական անվտանգության պատասխանատուին և Գործակալությանը ոչ ուշ, քան միջադեպի հայտնաբերումից հետո 24 ժամվա ընթացքում։

26. Տեղեկատվական անվտանգության միջադեպի արձագանքման բոլոր քայլերը պետք է փաստաթղթագրվեն և պահպանվեն առնվազն երեք տարի՝ հետադարձ վերլուծության և աուդիտային նպատակներով։

27. Ռեեստրի աշխատանքային գրանցամատյանները (օրինակ՝ համակարգային գրառումներ, օգտատերերի մուտքի գործողություններ, սպասարկման գրանցումներ) պետք է պահպանվեն առնվազն մեկ տարի։ Դրանք պետք է հասանելի լինեն միայն Ռեեստրի վարողի, կազմակերպության ղեկավարի, անհրաժեշտ ստորաբաժանման, ինչպես նաև Հայաստանի Հանրապետության օրենսդրությամբ սահմանված՝ համապատասխան վերահսկողություն իրականացնող մարմիններին։ Գրանցամատյանների տվյալների փոփոխումն կամ խմբագրումը խստիվ արգելվում է՝ բացառությամբ տեխնիկական վերականգնման ընթացակարգերի, որոնք պետք է փաստաթղթագրվեն։

28. Ռեեստրի տվյալների պահպանումը ապահովվում է պարբերական պահուստային պատճենմամբ (backup)՝ նվազագույնը ամիսը մեկ անգամ՝

ապահովելով տվյալների վերականգնման հնարավորություն։

29. Պահուստային պատճենները պետք է պահպանվեն անվտանգ և ֆիզիկապես առանձին վայրում՝ ապահովելով տվյալների վերականգնման հնարավորությունը համակարգային խափանումների կամ տվյալների կորստի դեպքում։ Պահուստային պատճենների պահպանման ժամկետը պետք է լինի առնվազն 12 ամիս։

30. Գործակալությունը պետք է իրականացնի Ռեեստրի տեղեկատվական անվտանգության աուդիտներ՝ առնվազն տարեկան մեկ անգամ, գնահատելու համար տվյալ Ռեեստրի համապատասխանությունը ազգային և միջազգային ստանդարտներին և սույն կարգի պահանջներին։ Աուդիտի արդյունքները պետք է փաստաթղթավորվեն՝ և ներկայացվեն համապատասխան մարմիններին՝ անհրաժեշտության դեպքում բարելավման միջոցառումներ իրականացնելու համար։

31. Ռեեստրում ներառվող նվազագույն տեղեկատվությունն է.

1) Օպերացիոն համակարգեր, ծրագրային ապահովումներ, հավելվածներ, կայքեր, տվյալների շտեմարաններ.

- Ակտիվի նույնականացուցիչ (ID) – օրինակ՝ անհատական համարը կամ անունը (SW-0001)
- Ակտիվի անուն – օրինակ՝ Windows 11 կամ [կայք].am
- Գնված/շահագործվող լիցենզիաների քանակ – օրինակ՝ 150/100
- Տնօրինող ստորաբաժանում և պատասխանատու անձ – օրինակ՝ անուն/ազգանուն, SS բաժին
- Օգտագործողներ – օրինակ՝ անուններ/ազգանուններ
- Ադմինիստրատոր – համակարգի ադմինիստրատորի տվյալներ (անուն/ազգանուն)
- Վայր / ակտիվի նույնականացուցիչ – օրինակ՝ գրասենյակի համակարգիչներ, ամպային տիրույթ, լոկալ սերվեր (SV0001)
- Տեսակ/Տարբերակ – օրինակ՝ ծրագրի բանալի, կրիչ կամ բաժանորդագրության տեսակ
- Մատակարար – օրինակ՝ software LLC
- Առանձնահատուկ պահանջներ – օրինակ՝ պահանջվում է VPN հասանելիություն
- Կախվածություններ – օրինակ՝ Active Directory, PostgreSQL
- Սպասարկման ավարտի ժամկետ – օրինակ՝ 01.07.2027
- Պահպանման պայմաններ – օրինակ՝ փակ սերվերային միջավայրում սառեցված հասանելիությամբ, կամ վիրտուալ հոսթինգում
- Պահուստային պատճենման պարբերականություն – օրինակ՝ շաբաթական մեկ անգամ
- Պահուստային պատճենման վայր – օրինակ՝ GitHub, լոկալ սերվեր կամ Azure Backup
- Արխիվացման պահանջներ – օրինակ՝ արխիվացվում է 6 ամիս անց, .tar ֆորմատով՝ յուրաքանչյուր 3 ամիս
- Ոչնչացման եղանակ – օրինակ՝ տվյալների վերագրումով (wipe) կամ ամբողջական ջնջմամբ (shredd հրաման)
- Ոչնչացման ամսաթիվ – օրինակ՝ 01.07.2028

- Ոչնչացման պատճառ – օրինակ՝ «արդիական չէր»
- Ռիսկայնության աստիճան – նշվում են գաղտնիության (C), ամբողջականության (I) և հասանելիության (A) մակարդակները՝ L (ցածր), M (միջին), H (բարձր)
- Ակտիվի կարևորություն – գնահատվում է CIA բաղադրիչների հանրագումարի հիման վրա (H=3, M=2, L=1)
- **Ցանցային սարքավորումներ, սերվերներ (ներառյալ՝ վիրտուալ մեքենաներ), համակարգիչներ**
- Ակտիվի նույնականացուցիչ (ID) – օրինակ՝ անհատական համարը կամ անունը (SV0001 կամ 578547Ա)
- Ակտիվի անուն – օրինակ՝ DB-Server01 կամ PC-4758
- Սերիական նույնականացուցիչ – օրինակ՝ SN: 20230715-001-123
- Տնօրինող ստորաբաժանում և պատասխանատու անձ – օրինակ՝ անուն/ազգանուն, SS բաժին
- Օգտագործողներ – օրինակ՝ անուններ/ազգանուններ
- Ադմինիստրատոր(ներ) – օրինակ՝ համակարգի ադմինիստրատորի տվյալներ (անուն/ազգանուն)
- Վայր – օրինակ՝ տվյալների կենտրոն կամ հասցե
- Տեսակ/Տարբերակ – օրինակ՝ սերվեր, աշխատակայան, վիրտուալ մեքենա
- Օպերացիոն համակարգ - օրինակ՝ windows 2019, Ubuntu 22.04, ESXI 8.2
- Մոդել – օրինակ՝ Dell PowerEdge R740
- Ցանցային տվյալներ (IP, MAC) – օրինակ՝ 192.168.11.20, 00-B0-D0-63-C2-26
- Host name – օրինակ՝ server1
- Rack / Unit ID – օրինակ՝ Rack 45, Unit 36
- Տեխնիկական բնութագրեր – ներառյալ. CPU (մոդել, քանակ, GHz) – օրինակ՝ i5, 5 core, 3.4 GHz, RAM (GB) – օրինակ՝ 16 GB, հիմնական հիշողություն (Storage – տեսակ/ծավալ) – օրինակ՝ SSD, 512 GB
- Շահագործման ժամկետ – օրինակ՝ 10 տարի
- Արտադրողի կողմից աջակցման կարգավիճակ – օրինակ՝ «արդիական է» կամ «արդիական չէ (EOL)»
- Մատակարար – օրինակ՝ computer LLC
- Առանձնահատուկ պահանջներ – օրինակ՝ կրկնօրինակները գաղտնագրված են
- Կախվածություններ – օրինակ՝ արտաքին պահեստային լուծման հասանելիություն, ինտերնետ կապի կայունություն
- Պահեստայնություն – օրինակ՝ առկա է մեկ պահուստային սերվեր՝ համարժեք արտադրողականությամբ
- Կարգաբերումների պահուստային պատճենման պարբերականություն – օրինակ՝ օրական, շաբաթական, ամսական
- Պահուստային պատճենի վայր – օրինակ՝ Backup Server կամ NAS
- Վերականգնման պարբերականություն – օրինակ՝ ամսական՝ թեստային վերականգնում, տարեկան՝ լիակատար վերականգնման փորձարկում
- Օտարման ամսաթիվ – օրինակ՝ 01.07.2028
- Օտարման պատճառ – օրինակ՝ «արդիական չէ»
- Ռիսկայնության աստիճան – նշվում են գաղտնիության (C), ամբողջականության (I) և հասանելիության (A) մակարդակները՝ L (ցածր), M (միջին), H (բարձր)
- Ակտիվի կարևորություն – գնահատվում է CIA բաղադրիչների

հանրագումարի հիման վրա (H=3, M=2, L=1)
- **Օգտատերեր և հաշիվներ (մարդկային ռեսուրսներ)**
- Ակտիվի նույնականացուցիչ (ID) – օրինակ՝ HR0001
- Աշխատողի անուն և ազգանուն
- Պաշտոն / դեր – օրինակ՝ SS բաժնի ինժեներ, հաշվետվությունների վերլուծաբան
- Համակարգեր, որոնց հասանելիություն ունի – օրինակ՝ կենտրոնական երթուղիչ, Zabbix համակարգ
- Հասանելիության օգտանուն (username) – օրինակ՝ a_azganun
- Մուտքի տրամադրման հիմքը – օրինակ՝ պայմանագիր, հրաման, պաշտոնական նամակ
- Մուտքի մակարդակ (Access Level) – օրինակ՝ միայն կարդալու իրավունք, ընթերցում/գրառում, ադմինիստրատոր
- Օգտահաշվի ստեղծման և փակման ամսաթվերը – օրինակ՝ 15.01.2023 – 20.08.2025
- Վերջին մուտքի (Last Login) ամսաթիվը – օրինակ՝ 20.08.2025
- Ռիսկայնության աստիճան – նշվում են գաղտնիության (C), ամբողջականության (I) և հասանելիության (A) մակարդակները՝ L (ցածր), M (միջին), H (բարձր)
- Ակտիվի կարևորություն – գնահատվում է CIA բաղադրիչների հանրագումարի հիման վրա (H=3, M=2, L=1)
- **Թվային և ոչ թվային տվյալներ (պայմանագրեր, համաձայնագրեր, հաշվեհամարներ և այլն)**
- Ակտիվի նույնականացուցիչ (ID) – օրինակ՝ ND0001
- Ակտիվի անուն – օրինակ՝ պայմանագիր, SLA
- Ստեղծման / ստորագրման ամսաթիվ – օրինակ՝ 01.01.2025
- Տնօրինող ստորաբաժանում և պատասխանատու անձ – օրինակ՝ անուն/ազգանուն, SS բաժին
- Հասանելիության պայմաններ – օրինակ՝ թղթային տարբերակում՝ միայն բաժնի ղեկավար և իրավաբան (բանալիով մուտք), թվային տարբերակում՝ Group Policy, Audit log
- Պահպանման վայր – օրինակ՝ contract-db01 սերվեր, տվյալների կենտրոն, հաշվապահական համակարգ, չհրկիզվող պահարան
- Մուտքի հսկողություն – օրինակ՝ արխիվի մատյան (թղթային), Group Policy կամ audit log (թվային)
- Պահուստավորման կարգավորում – օրինակ՝ Backup Server
- Արխիվացման պահանջներ – օրինակ՝ չհրկիզվող պահարան, էլեկտրոնային պահուստավորում
- Ոչնչացման կամ արգելափակման եղանակ – օրինակ՝ փաստաթղթերի ֆիզիկական ոչնչացում, տվյալների անվտանգ ջնջում, համակարգից անջատում
- Ոչնչացման կամ արգելափակման ամսաթիվ – օրինակ՝ 01.01.2026
- Ոչնչացման կամ արգելափակման պատճառ – օրինակ՝ «կենսացիկլի ավարտ», «պահպանման ժամկետի ավարտ»
- Ռիսկայնության աստիճան – նշվում են գաղտնիության (C), ամբողջականության (I) և հասանելիության (A) մակարդակները՝ L (ցածր), M (միջին), H (բարձր)
- Ակտիվի կարևորություն – գնահատվում է CIA բաղադրիչների հանրագումարի հիման վրա (H=3, M=2, L=1)
- **Այլ ակտիվներ**

- Ակտիվի նույնականացուցիչ (ID) – առկայության դեպքում նշվում է ունիկալ համարը կամ սահմանվում է նույնականացուցիչ
- Ակտիվի անուն / կատեգորիա
- Տնօրինող ստորաբաժանում և պատասխանատու անձ – նշվում է ստորաբաժանումը և պատասխանատու պաշտոնյան
- Օգտագործողներ – այն անձինք, որոնք ունեն տվյալ ակտիվի հասանելիություն (դեր/պաշտոն/ստորաբաժանում)
- Ռիսկայնության աստիճան – նշվում են գաղտնիության (C), ամբողջականության (I) և հասանելիության (A) մակարդակները՝ L (ցածր), M (միջին), H (բարձր)
- Ակտիվի կարևորություն – գնահատվում է CIA բաղադրիչների հանրագումարի հիման վրա (H=3, M=2, L=1)