ՊԵՏՈՒԹՅԱՆ ԿԱՐԻՔՆԵՐԻ ՀԱՄԱՐ ՀԱԿԱՎԻՐՈՒՍԱՅԻՆ ՀԱՄԱԿԱՐԳՉԱՅԻՆ ԾՐԱԳՐԱՅԻՆ ՓԱԹԵԹՆԵՐԻ ՄԱՏՈՒՑՄԱՆ ՊԵՏԱԿԱՆ ԳՆՄԱՆ ՊԱՅՄԱՆԱԳԻՐ N ԳՀԾՁԲ-ԱԻՆ-20/58

«17» 04 2020թ.

ք. Երևան

Արտակարգ իրավիճակների նախարարությունը, ի դեմս գլխավոր քարտուղար Վ. Օհանյանի, որը գործում է նախարարության կանոնադրության հիման վրա (այսուհետ՝ Պատվիրատու), մի կողմից, և «Էյչ Գրուպ» ՍՊԸ-ն, ի դեմս տնօրեն Կ. Հարությունյանի, որը գործում է ընկերության կանոնադրության հիման վրա (այսուհետ՝ Կատարող), մյուս կողմից, կնքեցին սույն պայմանագիրը հետևյալի մասին:

1. ՊԱՅՄԱՆԱԳՐԻ ԱՌԱՐԿԱՆ

1.1 Պատվիրատուն հանձնարարում է, իսկ Կատարողը ստանձնում է հակավիրուսային համակարգչային ծրագրային փաթեթների ի մատուցման պարտավորությունը (այսուհետ՝ ծառայություն)՝ համաձայն սույն պայմանագրի (այսուհետ՝ պայմանագիր) անբաժանելի մասը կազմող N 1 հավելվածով սահմանված Տեխնիկական բնութագիր-գնման ժամանակացույցի պահանջների:

1.2 Ծառայությունը մատուցվում է պայմանագրի N 1 հավելվածով սահմանված Տեխնիկական բնութագիր-գնման ժամանակացույցին համապատասխան և սահմանված ժամկետներով:

2. ԿՈՂՄԵՐԻ ԻՐԱՎՈՒՆՔՆԵՐԸ ԵՎ ՊԱՐՏԱԿԱՆՈՒԹՅՈՒՆՆԵՐԸ

2.1 Պատվիրատուն իրավունք ունի՝

2.1.1 Ցանկացած ժամանակ ստուգել Կատարողի կողմից մատուցվող ծառայության ընթացքը և որակը՝ առանց միջամտելու Կատարողի գործունեությանը.

2.1.2 Եթե մատուցվել է պայմանագրի N 1 հավելվածում նշված Տեխնիկական բնութագիր-գնման ժամանակացույցին չհամապատասխանող ծառայություն.

ա) Չընդունել ծառայությունը՝ իր հայեցողությամբ սահմանելով անպատշաճ որակի ծառայությունը պայմանագրին համապատասխանող ծառայությամբ անհատույց փոխարինման ողջամիտ ժամկետ և պահանջել Կատարողից վճարելու պայմանագրի 5.2 կետով նախատեսված տուգանքը, ինչպես նաև 5.3 կետով նախատեսված տույժը.

բ) Հրաժարվել պայմանագիրը կատարելուց և պահանջել վերադարձնելու ծառայության համար վճարված գումարը և պահանջել Կատարողից վճարելու պայմանագրի 5.2 կետով նախատեսված տուգանքը.

2.1.3 Միակողմանի լուծել պայմանագիրը, եթե Կատարողն էականորեն խախտել է պայմանագիրը: Կատարողի կողմից պայմանագիրը խախտելն էական է համարվում, եթե՝

ա) մատուցված ծառայությունը չի համապատասխանում պայմանագրի N 1 հավելվածով սահմանված պահանջներին,

բ) խախտվել է ծառայության մատուցման ժամկետը:

2.2 Պատվիրատուն պարտավոր է՝

2.2.1 Քննարկել և ընդունել Տեխնիկական բնութագիր-գնման ժամանակացույցին համապատասխան մատուցված ծառայության արդյունքը, իսկ ծառայության արդյունքում թերություններ հայտնաբերելու դեպքերում՝ այդ մասին անհապաղ գրավոր հայտնել Կատարողին:

2.2.2 Ծառայության արդյունքն ընդունելու դեպքում Կատարողին վճարել վերջինիս վճարման ենթակա գումարները, իսկ ժամկետի խախտման դեպքում՝ նաև պայմանագրի 5.5 կետով նախատեսված տույժը:

2.3 Կատարողն իրավունք ունի՝

2.3.1 Պատվիրատուից պահանջել վճարելու իրեն վճարման ենթակա գումարները, իսկ Պատվիրատուի կողմից պայմանագրի 4.2 կետում նշված ժամկետի խախտման դեպքում նաև պայմանագրի 5.5 կետով նախատեսված տույժը:

2.4 Կատարողը պարտավոր է՝

2.4.1 Պայմանագրի N 1 հավելվածով սահմանված պայմաններով ապահովել ծառայության մատուցումը՝ ղեկավարվելով գործող օրենսդրությամբ:

2.4.2 Պայմանագրով նախատեսված դեպքերում վճարել պայմանագրի 5.2 և 5.3 կետերով նախատեսված տույժը և տուգանքը:

2.4.3 Որակավորման և պայմանագրի կատարման ապահովման գործողության ընթացքում լուծարման կամ սնանկացման գործընթաց սկսելու դեպքում դրա մասին նախապես գրավոր տեղեկացնել Պատվիրատուին:

3. ԾԱՌԱՅՈՒԹՅԱՆ ՀԱՆՁՆՄԱՆ ԵՎ ԸՆԴՈՒՆՄԱՆ ԿԱՐԳԸ

3.1 Մատուցված ծառայությունն ընդունվում է Պատվիրատուի և Կատարողի միջև հանձնման-ընդունման արձանագրության ստորագրմամբ: Ծառայությունը Պատվիրատուին հանձնելու փաստը ֆիքսվում է Պատվիրատուի և Կատարողի միջև երկկողմ հաստատված փաստաթղթով՝ նշելով փաստաթղթի կազմման ամսաթիվը:

Մինչև պայմանագրով ծառայության մատուցման համար նախատեսված օրը ներառյալ Կատարողը Պատվիրատուին է տրամադրում իր կողմից ստորագրված՝ ծառայությունը Պատվիրատուին հանձնելու փաստը ֆիքսող փաստաթուղթը (հավելված N 3.1), իսկ էլեկտրոնային գնումների armeps համակարգի միջոցով (գործողության իրականացման ձեռնարկը տեղադրված է www.procurement.am հասցեով գործող կայքի «Էլեկտրոնային գնումներ» բաժնում)՝ նաև հանձնման-ընդունման արձանագրությունը (հավելված N 3): Ընդ որում Կատարողը հանձնման-ընդունման արձանագրությունը չի կնքում, հաստատում է էլեկտրոնային ստորագրությամբ՝ լրացնելով միայն այն սյունակները, որոնք վերաբերում են իր տվյալներին (լրացման կարգը տեղադրված է www.procurement.am հասցեով գործող կայքի «Օրենսդրություն» բաժնի «Ֆինանսների նախարարի հրամաններ» ենթաբաժնում):

3.2 Եթե մատուցված ծառայությունը համապատասխանում է պայմանագրի պայմաններին, Պատվիրատուն պայմանագրի 3.1 կետում նշված փաստաթղթերը ստանալու օրվան հաջորդող աշխատանքային օրվանից հաշված աշխատանքային օրվա ընթացքում ստորագրում և էլեկտրոնային գնումների armeps համակարգի միջոցով Կատարողին է տրամադրում իր կողմից ստորագրված հանձնման-ընդունման արձանագրությունը և դրա ստորագրման համար հիմք հանդիսացած դրական եզրակացությունը:

3.3 Եթե մատուցված ծառայությունը կամ դրա մի մասը չի համապատասխանում պայմանագրի պայմաններին, ապա Պատվիրատուն չի ստորագրում հանձնման-ընդունման արձանագրությունը և պայմանագրի 3.2 կետում նշված ժամկետում էլեկտրոնային գնումների armeps համակարգի միջոցով Կատարողին հետ է վերադարձնում հանձնման-ընդունման արձանագրությունը և դրա չստորագրման համար հիմք հանդիսացած բացասական եզրակացությունը: Սույն կետի կիրառման դեպքում Պատվիրատուն ձեռնարկում է նման իրավիճակի համար պայմանագրով նախատեսված միջոցները և Կատարողի նկատմամբ կիրառում է պայմանագրով նախատեսված պատասխանատվության միջոցներ:

3.4 Եթե պայմանագրի 3.2 կետով սահմանված ժամկետում Պատվիրատուն չի ընդունում մատուցված ծառայությունը կամ չի մերժում դրա ընդունումը, ապա մատուցված ծառայությունը համարվում է ընդունված և պայմանագրի 3.2 կետով սահմանված վերջնաժամկետին հաջորդող աշխատանքային օրը Պատվիրատուն էլեկտրոնային գնումների համակարգի միջոցով Կատարողին է տրամադրում իր կողմից ստորագրված հանձնման-ընդունման արձանագրությունը:

4. ՊԱՅՄԱՆԱԳՐԻ ԳԻՆԸ

4.1. Սույն պայմանագրով Կատարողի մատուցման ենթակա ծառայության գինը կազմում է 1416000 (մեկ միլիոն չորս հարյուր տասնվեց հազար) ՀՀ դրամ, ներառյալ ԱԱՀ-ն:

Գինը ներառում է Կատարողի կողմից իրականացվող բոլոր ծախսերը՝ այդ թվում հարկերը, տուրքերը և ՀՀ օրենդրությամբ սահմանված այլ վճարները:

Ծառայության մատուցման գինը կայուն է և Կատարողն իրավունք չունի պահանջել ավելացնելու, իսկ Պատվիրատուն նվազեցնելու այդ գինը:

4.2 Պատվիրատուն իրեն մատուցած ծառայության դիմաց վճարում է ՀՀ դրամով անկանխիկ՝ դրամական միջոցները Կատարողի հաշվարկային հաշվին փոխանցելու միջոցով: Դրամական միջոցների փոխանցումը կատարվում է հանձման-ընդունման արձանագրության հիման վրա՝ պայմանագրի վճարման ժամանակացույցով (հավելված N 2) նախատեսված չափերով և ամիսներին: Եթե արձանագրությունը կազմվում է տվյալ ամսվա 20-ից հետո և այդ ամսում վճարման ժամանակացույցով նախատեսված են ֆինանսական միջոցներ, ապա վճարումն իրականացվում է մինչև 30 աշխատանքային օրվա ընթացքում, բայց ոչ ուշ, քան մինչև տվյալ տարվա դեկտեմբերի 30-ը:

5. ԿՈՂՄԵՐԻ ՊԱՏԱՍԽԱՆԱՏՎՈՒԹՅՈՒՆԸ

5.1 Կատարողը պատասխանատվություն է կրում ծառայության մատուցման՝ պայմանագրի պահանջների պահպանման համար:

5.2 Պայմանագրի N 1 հավելվածում նշված տեխնիկական բնութագրին չհամապատասխանող ծառայություն մատուցելու յուրաքանչյուր դեպքում Կատարողից գանձվում է տուգանք՝ պայմանագրի 4.1 կետում նախատեսված գումարի 0,5 (զրո ամբողջ հինգ տասնորդական) տոկոսի չափով:[22] Ընդ որում տուգանքը հաշվարկվում է նաև ծառայությունը սույն պայմանագրով սահմանված ժամկետում մատուցելու, սակայն պատվիրատուի կողմից այդ ընդունվելու դեպքում:

---

[19] *Եթե Կատարողի կողմից գնային առաջարկը ներկայացվել է առանց ԱԱՀ-ի, ապա պայմանագիրը կնքելիս «ներառյալ ԱԱՀ-ն» բառերը անվում են:*

5.3 Պայմանագրով նախատեսված ծառայության մատուցման ժամկետը խախտելու դեպքում Կատարողից յուրաքանչյուր ուշացված աշխատանքային օրվա համար գանձվում է տույժ՝ մատուցման ենթակա, սակայն չմատուցված ծառայության գնի 0,05 (զրո ամբողջ հինգ հարյուրերորդական) տոկոսի չափով:

5.4 Պայմանագրի 5.2 և 5.3 կետերով նախատեսված տուգանքը և տույժը հաշվարկվում և հաշվանցվում են ծառայություն մատուցելու արդյունքում Կատարողին վճարման ենթակա գումարների հետ:

5.5 Պատվիրատուի կողմից պայմանագրի 4.2 կետով նախատեսված ժամկետի խախտման դեպքում Պատվիրատուի նկատմամբ յուրաքանչյուր ուշացված աշխատանքային օրվա համար հաշվարկվում է տույժ՝ վճարման ենթակա, սակայն չվճարված գումարի 0,05 (զրո ամբողջ հինգ հարյուրերորդական) տոկոսի չափով:

5.6 Պայմանագրով չնախատեսված դեպքերում կողմերն իրենց պարտավորությունները չկատարելու կամ ոչ պատշաճ կատարելու համար պատասխանատվության են ենթարկվում ՀՀ օրենսդրությամբ սահմանված կարգով:

5.7 Տույժերի և (կամ) տուգանքի վճարումը Կողմերին չի ազատում իրենց պայմանագրային պարտավորությունները լրիվ կատարելուց:

6. ԱՆՀԱՂԹԱՀԱՐԵԼԻ ՈՒԺԻ ԱԶԴԵՑՈՒԹՅՈՒՆ (ՖՈՐՍ-ՄԱԺՈՐ)

Սույն պայմանագրով և սույն պայմանագրի հիման վրա կնքված համաձայնագրերով պարտավորություններն ամբողջությամբ կամ մասնակիորեն չկատարելու համար կողմերն ազատվում են պատասխանատվությունից, եթե դա եղել է անհաղթահարելի ուժի ազդեցության հետևանքով, որը ծագել է սույն պայմանագիրը կնքելուց հետո, և որը կողմերը չէին կարող կանխատեսել կամ կանխարգելել: Այդպիսի իրավիճակներ են երկրաշարժը, ջրհեղեղը, հրդեհը, պատերազմը, ռազմական և արտակարգ դրություն հայտարարելը, քաղաքական հուզումները, գործադուլները, հաղորդակցության միջոցների աշխատանքի դադարեցումը, պետական մարմինների ակտերը և այլն, որոնք անհնարին են դարձնում սույն պայմանագրով պարտավորությունների կատարումը: Եթե արտակարգ ուժի ազդեցությունը շարունակվում է 3 (երեք) ամսից ավելի, ապա կողմերից յուրաքանչյուրն իրավունք ունի լուծել պայմանագիրը՝ այդ մասին նախապես տեղյակ պահելով մյուս կողմին:

7. ԱՅԼ ՊԱՅՄԱՆՆԵՐ

7.1 Պայմանագիրն ուժի մեջ է մտնում կողմերի ստորագրման պահից և գործում է մինչև կողմերի պայմանագրով ստանձնած պարտավորությունների ողջ ծավալով կատարումը:

Պայմանագրով նախատեսված կողմերի իրավունքների և պարտականությունների կատարման պայման է հանդիսանում պայմանագիրը ՀՀ ֆինանսների նախարարության կողմից հաշվառված լինելու հանգամանքը:

7.2 Պայմանագրից ծագած կողմի վճարային պարտավորությունը չի կարող դադարել այլ պայմանագրից ծագած՝ հակընդդեմ պարտավորության հաշվանցով, առանց կողմերի գրավոր և կնիքով հաստատված համաձայնության: Պայմանագրից ծագած պահանջի իրավունքը չի կարող փոխանցվել այլ անձի, առանց պարտապան կողմի գրավոր համաձայնության:

7.3 Այն դեպքում, երբ օրենքով նախատեսված կարգով օրենքի պահանջների կատարման նկատմամբ հսկողության կամ վերահսկողության կամ բողոքների քննության արդյունքում արձանագրվում է, որ գնման գործընթացում, մինչև պայմանագրի կնքումը, Կատարողը ներկայացրել է կեղծ փաստաթղթեր (տեղեկություններ և տվյալներ), կամ վերջինիս ընտրված մասնակից ճանաչելու մասին որոշումը չի համապատասխանում Հայաստանի Հանրապետության օրենսդրությանը, ապա այդ հիմքերն ի հայտ գալուց հետո Պատվիրատուն միակողմանիորեն լուծում է պայմանագիրը, եթե արձանագրված խախտումները մինչև պայմանագրի կնքումը հայտնի լինելու դեպքում գնումների մասին Հայաստանի Հանրապետության օրենսդրության համաձայն հիմք կհանդիսանային պայմանագիրը չկնքելու համար: Ընդ որում, Պատվիրատուն չի կրում պայմանագրի միակողմանի լուծման հետևանքով Կատարողի համար առաջացող վնասների կամ բաց թողնված օգուտի ռիսկը, իսկ վերջինս պարտավոր է Հայաստանի Հանրապետության օրենքով սահմանված կարգով փոխհատուցել իր մեղքով Պատվիրատուի կրած վնասներն այն ծավալով, որի մասով պայմանագիրը լուծվել է:

7.4 Պայմանագրի հետ կապված վեճերը ենթակա են քննության Հայաստանի Հանրապետության դատարաններում:

7.5 Պայմանագրում փոփոխություններ և լրացումներ կարող են կատարվել միայն Կողմերի փոխադարձ համաձայնությամբ՝ համաձայնագիր կնքելու միջոցով, որը կհանդիսանա պայմանագրի անբաժանելի մասը:

Արգելվում է պայմանագրում, իսկ եթե պայմանագրի գինը գործոնային է, ապա նաև այդ պայմանագրին կից հաջորդող յուրաքանչյուր տարիներին կնքված համաձայնագրում կատարել այնպիսի փոփոխություններ, որոնք հանգեցնում են գնվող ծառայության ծավալների կամ ձեռք բերվող ծառայության միավորի գնի կամ պայմանագրի գնի արհեստական փոփոխման:

Պայմանագրի կողմերից անկախ գործոնների ազդեցությամբ պայմանագրի փոփոխման յուրաքանչյուր դեպք սահմանում է Հայաստանի Հանրապետության կառավարությունը:

7.6 Ծառայության մատուցման ժամկետը կարող է երկարաձգվել մինչև պայմանագրով այդ ժամկետը լրանալը՝ Կատարողի առաջարկության առկայության դեպքում՝ պայմանով, որ Պատվիրատուի մոտ չի վերացել ծառայության օգտագործման պահանջը, իսկ Կատարողի առաջարկությունը ներկայացվել է ոչ ուշ, քան պայմանագրով ի սկզբանե ծառայությունների մատուցման համար սահմանված ժամկետը լրանալուց առնվազն 5 օրացուցային օր առաջ: Ընդ որում սույն կետով սահմանված դեպքում ծառայության մատուցման ժամկետը կարող է երկարաձգվել մեկ անգամ մինչև 30 օրացուցային օրով, բայց ոչ ավել քան պայմանագրով սահմանված ժամկետն է:

7.7 Պայմանագրի պատշաճ կատարման պայմաններում կողմերի (Կատարող կամ Պատվիրատու) օգուտները (խնայողություններ) կամ կրած վնասները տվյալ կողմի օգուտը կամ կրած վնասն են:

Պայմանագրի կողմերի՝ երրորդ անձանց նկատմամբ պարտավորությունները՝ ներառյալ պայմանագրի կատարման շրջանակում Կատարողի կնքած այլ գործարքները և դրանցից բխող պարտավորությունները, դուրս են պայմանագրի կարգավորման դաշտից և չեն կարող ազդել պայմանագրի կատարման արդյունքն ընդունելու վրա: Այդ գործարքների և դրանցից բխող պարտավորությունների կատարման հետ կապված հարաբերությունները կարգավորվում են այդ գործարքների հետ կապված հարաբերությունները կարգավորող նորմերով, և դրանց համար պատասխանատու է Կատարողը:

7.8 Պայմանագիրը չի կարող փոփոխվել կողմերի պարտավորությունների մասնակի չկատարման հետևանքով կամ ամբողջությամբ լուծվել կողմերի փոխադարձ համաձայնությամբ՝ բացառությամբ՝ Հայաստանի Հանրապետության օրենսդրությամբ սահմանված կարգով ծառայության մատուցման համար անհրաժեշտ ֆինանսական հատկացումների նվազեցման դեպքերի: Ընդ որում, պայմանագրի կողմերի՝ պարտավորությունների մասնակի չկատարման կամ ամբողջությամբ լուծման կողմերի փոխադարձ համաձայնությունն անհրաժեշտ է ձեռք բերել նախքան Հայաստանի Հանրապետության օրենսդրությամբ սահմանված կարգով ծառայության մատուցման համար անհրաժեշտ ֆինանսական հատկացումների նվազեցումը:

7.9 Կատարողի կողմից ստանձնած պարտավորությունները չկատարելու կամ ոչ պատշաճ կատարելու հիմքով պայմանագիրն ամբողջությամբ կամ մասնակի միակողմանի լուծելու մասին ծանուցումը Պատվիրատուն հրապարակում է www.procurement.am հասցեով գործող ինտերնետային կայքի «Պայմանագրերը միակողմանի լուծելու մասին ծանուցումներ» բաժնում՝ նշելով հրապարակման ամսաթիվը: Կատարողը, պայմանագիրը միակողմանի լուծելու վերաբերյալ, համարվում է պատշաճ ծանուցված՝ ծանուցումը, սույն կետով սահմանված հրապարակվելուն հաջորդող օրվանից: Պայմանագիրն ամբողջությամբ կամ մասնակի միակողմանի լուծելու մասին ծանուցումը տեղեկագրում հրապարակվելու օրը Պատվիրատուն այն ուղարկվում է նաև Կատարողի էլեկտրոնային փոստին:

7.10 Սույն պայմանագրի կապակցությամբ ծագած վեճերը լուծվում են բանակցությունների միջոցով: Համաձայնություն ձեռք չբերելու դեպքում վեճերը լուծվում են ՀՀ դատարաններում:

7.11 Սույն պայմանագիրը կազմված է ____ էջից, կնքվում է երկու օրինակից, որոնք ունեն հավասարազոր իրավաբանական ուժ: Սույն պայմանագրի N 1, N 1.1, N 2, N 3 և N 3.1 հավելվածները հանդիսանում են պայմանագրի անբաժանելի մասը, յուրաքանչյուր կողմին տրվում է պայմանագրի մեկ օրինակ:

7.12 Սույն պայմանագրի նկատմամբ կիրառվում է Հայաստանի Հանրապետության իրավունքը:

8. ԿՈՂՄԵՐԻ ՀԱՍՑԵՆԵՐԸ, ԲԱՆԿԱՅԻՆ ՎԱՎԵՐԱՊԱՅՄԱՆՆԵՐԸ ԵՎ ՍՏՈՐԱԳՐՈՒԹՅՈՒՆՆԵՐԸ

ՊԱՏՎԻՐԱՏՈՒ	ԿԱՏԱՐՈՂ
Արտակարգ իրավիճակների նախարարություն	<<Էյչ Գրուպ>> ՍՊԸ
Դավիթաշեն 4-րդ թաղ., Ա.Միկոյան 109/8	ՀՀ, ք.Երևան, Բաշինջաղյան 1 փ, 13/30
ՖՆ գործառնական վարչություն	<<Արմսվիսբանկ>> ՓԲԸ
Հ/Հ 900011019313	Հ/Հ 2500010488760100
ՀՎՀՀ 00153247	ՀՎՀՀ 01254973
Վ. Օհանյան	Կ. Հարությունյան
(ստորագրություն)	(ստորագրություն)
Կ.Տ.	Կ.Տ.

Հավելված N 1
«17» 04 2020 թ. կնքված
ԳՀԾՁԲ-ԱԻՆ-20/58 ծածկագրով պայմանագրի

ՏԵԽՆԻԿԱԿԱՆ ԲՆՈՒԹԱԳԻՐ - ԳՆՄԱՆ ԺԱՄԱՆԱԿԱՑՈՒՅՑ

ՀՀ դրամ

Ծառայության							
հրավերով նախատեսված չափաբաժնի համարը	գնումների պլանով նախատեսված միջանցիկ ծածկագիրը՝ ըստ ԳՄԱ դասակարգման (CPV)	տեխնիկական բնութագիրը	չափման միավորը	ընդհանուր գինը/ՀՀ դրամ	ընդհանուր քանակը	մատուցման	
						հասցեն	ժամկետը
1	72211195/1	ՀՀ ԱԻՆ պատկանող աշխատանքային համակարգիչների անվտանգ աշխատանքը ապահովելու նպատակով արտոնագրված հակավիրուսային և ցանցային անվտանգության (ֆիլտր) ծրագրի կամ ծրագրային փաթեթի ժամկետի երկարաձգում, որը նախատեսված է վիրուսների, անցանկալի ծրագրային կոդերի, լրտեսական ծրագրերի, ինչպես նաև ցանցային գրոհների հայտնաբերման, կանխարգելման, հակազդման և որոշ դեպքերում վնասված ֆայլերի վերականգնման համար: 230 հատ համակարգչի հակավիրուսի երկարաձգման փաթեթի ձեռքբերում:	դրամ	1416000	1 /230 համակարգիչ/	ՀՀ քաղաք Երևան Դավթաշեն 4,Ա.Միկոյան 109/8	Պայմանագիրն ուժի մեջ մտնելուց հետո մինչև 25.12.2021թ

ծառայության մատուցման վերջնաժամկետը չի կարող ավել լինել, քան տվյալ տարվա դեկտեմբերի 25-ը:

րագրային փաթեթների ակտիվացումը պետք է կատարվի 2021թ. հունվարին, իսկ գործողության ամկետը՝ մինչև 2022 թվականի հունվար/մեկ տարի/

Հակավիրուսային ծրագրի տեխնիկական բնութագրիչները

Ընդհանուր պահանջներ

ակավիրուսային միջոցները պետք է ներառեն.

Հակավիրուսային ծրագրային պաշտպանություն Windows կայանների համար
Հակավիրուսային ծրագրային պաշտպանություն MacoS կայանների համար
Հակավիրուսային ծրագրային պաշտպանություն Linux կայանների համար
Հակավիրուսային ծրագրային պաշտպանություն Windows ֆայլային սերվերների համար
Հակավիրուսային ծրագրային պաշտպանություն Linux ֆայլային սերվերների համար
Հակավիրուսային ծրագրային պաշտպանություն շարժական սարքերի համար (սմարթֆոններ և լանշետներ)
ենտրոնացված ղեկավարման, մոնիթորինգի և թարմացման ծրագրային միջոց
Ձնասաբեր հարձակումների և ծրագրերի սիգնատուրաների թարմացվող բազա
Հուսերեն լեզվով շահագործման ուղեցույց

ոլոր հակավիրուսների ծրագրային ինտերֆեյսերը, ներառյալ ղեկավարման միջոցինը, պետք է լինեն ուսերեն և անգլերեն լեզուներով:

Բոլոր հակավիրուսային միջոցները, ներառյալ ղեկավարման միջոցը, պետք է ունենան կոնտեքստային տեղեկատվական համակարգ՝ ռուսերեն և անգլերեն լեզուներով:

Wind•ws աշխատանքային կայանների համար հակավիրուսային ծրագրային միջոցների պահանջներ
Wind•ws աշխատանքային կայանների համար հակավիրուսային ծրագրային միջոցները պետք է գործեն հետևյալ համակարգերով աշխատող կայանների վրա.

- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows 10

Windows կայանների համար նախատեսված հակավիրուսային ծրագրային միջոցները պետք է ապահովեն հետևյալ գործառույթները.

- Հակավիրուսային սքանավորում ռեալ ժամանակում, ինչպես նաև օբյեկտի կոնտեքստային մենյուից
- Նախատեսված գրաֆիկով հակավիրուսային սքանավորում
- Միացվող սարքավորումների հակավիրուսային սքանավորում
- Էվրիստիկ վերլուծության հնարավորություն, որը թույլ կտա ճանաչել և արգելափակել նախկինում անհայտ վնասաբեր ծրագրերը
- Ակտիվ վարակվածության գործողությունների չեզոքացում
- Համակարգում ծրագրի վարքագծի և նրա կողմից ստեղծված գործողությունների վերլուծություն՝ նրա վնասակար ակտիվությունը և չարտոնված գործողությունները չեզոքացնելու համար
- Ընդհանուր կատալոգներին և ֆայլերին դիմումների վերլուծություն՝ ցանցում հասանելի պաշտպանվող ռեսուրսների գաղտնագրման փորձերը կանխելու համար
- Վնասակար ծրագրերի գործողությունների արգելափակում, որոնք օգտագործում են ծրագրի խոցելիությունը, այդ թվում համակարգային գործընթացների հիշողության պաշտպանություն:
- բուժման ժամանակ վնասակար ծրագրի կատարած գործողությունների հետընթացի հնարավորություն, այդ թվում վնասակար ծրագրի կողմից գաղտնագրված ֆայլերի վերականգնում
- արտոնությունների սահմանափակման հնարավորություն (գրանցում ռեեստրում, ֆայլերի, կատալոգների և այլ գործընթացների մատչում, առաջադրանքների պլանավորման դիմում, սարքավորումներին մատչելիության, օբյեկների մատչման և այլն) գործընթացների և ծրագրերի համար: Վստահության մակարդակի որոշմամբ ծրագրերի դինամիկ թարմացվող և կարգավորվող ցուցակներ:
- ամպային պաշտպանություն նոր վտանգներից, որը ծրագրին թույլ է տալիս ռեալ ժամանակում դիմել արտադրողի ռեսուրսներին՝ գործարկվող ծրագրի կամ ֆայլի մասին տեղեկություն ստանալու համար:
- RAR, ARJ, ZIP, CAB, LHA, JAR, ICE ֆորմատով արխիվային ֆայլերի հակավիրուսային ստուգում և բուժում, այդ թվում գաղտնաբառով պաշտպանված:
- Հետևյալ պրոտոկոլներով աշխատող էլեկտրոնային փոստի մուտքային և ելքային հաղորդագրությունների պաշտպանություն վնասակար ծրագրերից. IMAP, SMTP, POP3, MAPI, NNTP
- փոստային կցված ֆայլերի ֆիլտր՝ տրված ֆայլերի տիպը անվանափոխելու կամ հեռացնելու հնարավորությամբ
- HTTP, FTP պրոտոկոլներով համակարգչի վրա բեռնվող թրաֆիկի ստուգում, այդ թվում էվրիստիկ վերլուծության միջոցով՝ հուսալի ռեսուրսների կարգավորման և արգելափակման ու վիճակագրության հնարավորությամբ:
- Web էջերից ներբեռնվող բաներների և pop-up պատուհանների արգելափակում:

- Ֆիշինգային և անհուսալի կայքերի ճանաչում և արգելափակում
- Ներքին ցանցային էկրանի առկայություն, որը թույլ է տալիս ստեղծել ցանցային փաթեթների կանոններ և ցանցային կանոններ ծրագրերի համար՝ ցանցային սեգմենտները դասակարգելու հնարավորությամբ
- Ներխուժումների հայտնաբերման և կանխարգելման համակարգի (IDS/IPS) և ցանկացած ցանցում, այդ թվում անլար, առավել հանրահայտ ծրագրերի ակտիվության ցանցային կանոնների օգտագործմամբ ցանցային գրոհներից պաշտպանություն
- ցանցային կամուրջների միջոցով կայացած ցանցային միացումների վերահսկում՝ մի քանի ցանցային կապերի միաժամանակյա միացման արգելափակման հնարավորությամբ
- բաղադրիչի առկայություն, որը թույլ է տալիս ստեղծել հատուկ կանոններ, որոնք արգելում կամ թույլ են տալիս ծրագրերի տեղադրում և/կամ գործարկումներ բոլորի կամ օգտվողների որոշակի խմբերի համար (Active Directory կամ լոկալ օգտագործողներ/խմբեր): Բաղադրիչը պետք է վերահսկի հայտերը ինչպես ծրագրի տեղակայման, մետատվյալների, վկայականի կամ մատնահետքի և MD5 կամ SHA256 ստուգման գումարի այնպես էլ ծրագրակազմի արտադրողի կողմից տրամադրված նախապես որոշված կատեգորիաների կողմից: Բաղադրիչը պետք է աշխատի սև կամ սպիտակ ցուցակի ռեժիմում, ինչպես նաեւ վիճակագրության հավաքման կամ արգելափակման ռեժիմում
- Օգտվողի՝ արտաքին մուտքային/ելքային սարքերի հետ աշխատանքի վերահսկում, սարքի տիպի և/կամ օգտագործվող կապուղու տիպին համապատասխան, ինչպես նաև հնարավորություն ստեղծելու վստահելի սարքերի ցուցակ ըստ դրանց իդենտիֆիկատորի, Active Direct•ry համապատասխան օգտվողներին արտաքին սարքերի հետ աշխատելու համապատասխան առավելություն տալով:
- իրադարձությունների մատյանում շարժական կրիչների վրա ֆայլեր գրելու և/կամ ջնջելու մասին գրանցելու հնարավորություն
- օգտվողի կողմից ինտերնետի հետ աշխատելու վերահսկում, այդ թվում՝ որոշակի բովանդակության ռեսուրսների հասանելիության բացահայտ ցուցադրման կամ թույլտվության, արտադրողի կողմից նախկինում ստեղծված և դինամիկ թարմացվող կատեգորիաների, ինչպես նաեւ տեղեկատվության տեսակի (աուդիո, վիդեո եւ այլն): Ծրագրային ապահովումը պետք է թույլ տա մուտքագրել վերահսկողության ժամանակային պարամետրեր, ինչպես նաև հանձնել այն միայն կոնկրետ օգտագործողներին Active Directory- ից
- BadUSB տիպի հարձակումներից պաշտպանության մեխանիզմի առկայություն
- Համակարգչի վրա տեղադրված ծրագրերում խոցելիություն հայտնաբերելու համար հատուկ մոդուլի գործարկում, որը կկարողանա ստեղծել հայտնաբերված խոցելիությունների մասին հաշվետվություն
- Պաշտպանություն ծրագրային ծառայության չարտոնված հեռահար կառավարումից, ինչպես նաև ծրագրի պարամետրերի մատչման պաշտպանություն գաղտնաբառի միջոցով՝ վնասակար ծրագրերից, ներխուժումներից և արտոնություն չունեցող օգտվողներից
- Հակավիրուսային պաշտպանության միայն ընտրված մոդուլների տեղադրման հնարավորություն
- Վերոնշյալ բոլոր մոդուլների կենտրոնացված ղեկավարում միասնական ղեկավարման համակարգի միջոցով
- Առաջադրանքների թողարկում ժամանակացույցով և/կամ անմիջապես համակարգի վերաթողարկումից հետո
- Ֆայլային տարածության սքանավորման ընթացքում համակարգչի ռեսուրսների ճկուն կառավարում՝ օգտվողներին հարմարավետ աշխատանքով ապահովելու համար
- Սքանավորման ընթացքի արագացում՝ շնորհիվ այն օբյեկտների սքանավորման բացառման, որոնց դրությունը նախորդ սքանավորման համեմատ փոփոխության չի ենթարկվել

- Հակավիրուսային ծրագրի ամբողջականության ստուգման հնարավորություն
- Հակավիրուսային ստուգումից բացառելու հնարավորություն ըստ ֆայլի ծավալի, դոմենի/կատալոգի դիմակի կամ ֆայլի մոտ վստահելի թվային ստորագրության առկայության
- Հակավիրուսային ծրագրում պաշտպանված պահուստարանի առկայություն՝ ջնջված վարակված ֆայլերի համար՝ դրանք վերականգնելու հնարավորությամբ
- պաշտպանված պահուստարանի առկայություն՝ հակավիրուսի աշխատանքի հաշվետվությունների համար
- հակավիրուսի գրաֆիկական ինտերֆեյսի միացման և անջատման հնարավորություն, ինչպես նաև նվազագույն հնարավորություններով պարզեցված գրաֆիկական ինտերֆեյսի առկայություն

Mac աշխատանքային կայանների համար հակավիրուսային ծրագրային միջոցների պահանջներ
Mac աշխատանքային կայանների համար հակավիրուսային ծրագրային միջոցները պետք է գործեն հետևյալ համակարգերով աշխատող կայանների վրա.

- macoS High Sierra 10.13
- macoS Sierra 10.12
- Mac oS X 10.11 (El Capitan)
- Mac oS X 10.10 (Y•semite)
- Mac oS X 10.9 (Mavericks)

Mac կայանների համար նախատեսված հակավիրուսային ծրագրային միջոցները պետք է ապահովեն հետևյալ գործառույթները.

- Ռեզիդենտ հակավիրուսային մոնիթորինգ
- Ամպային պաշտպանություն նոր վտանգներից, որը ծրագրին թույլ է տալիս ռեալ ժամանակում դիմել արտադրողի ռեսուրսներին՝ գործարկվող ծրագրի կամ ֆայլի մասին տեղեկություն ստանալու համար:
- Հակավիրուսային բազաների թարմացում ըստ ժամանակացույցի
- Վարակված ֆայլերը ջնջելուց առաջ ռեզերվային պատճենում՝ դրանց հետագա վերականգնման համար
- Էվրիստիկ վերլուծության հնարավորություն, որը թույլ կտա ճանաչել և արգելափակել նախկինում անհայտ վնասաբեր ծրագրերը
- Ներխուժումների հայտնաբերման և կանխարգելման համակարգի (IDS/IPS) և ցանկացած ցանցում, այդ թվում անլար, առավել հանրահայտ ծրագրերի ակտիվության ցանցային կանոնների օգտագործմամբ ցանցային գրոհներից պաշտպանություն
- Ֆիշինգային և վնասակար կայքերի արգելափակում հակավիրուսի արտադրողի ամպային ծառայությունների բազաներում առկա տեղեկությունների հիմքով
- Safari, Google Chrome և Firefox բրաուզերներով փոխանցվող ինֆորմացիայի պաշտպանություն (HTTP և HTTPS թրաֆիկ)
- Սքանավորման ընթացքի արագացում՝ շնորհիվ այն օբյեկտների սքանավորման բացառման, որոնց դրությունը նախորդ սքանավորման համեմատ փոփոխության չի ենթարկվել

Linux աշխատանքային կայանների համար հակավիրուսային ծրագրային միջոցների պահանջներ
Linux աշխատանքային կայանների համար հակավիրուսային ծրագրային միջոցները պետք է գործեն հետևյալ համակարգերով աշխատող կայանների վրա.

- Ubuntu 14.04.5, 16.04.4, 17.10.1 LTS
- Red Hat Enterprise Linux 6.9, 7.4
- CentoS-6.9, 7.4
- Debian GNU / Linux 8.10, 9.4
- oracleLinux 7.4

- SUSE Linux Enterprise Server 12 SP3
- openSUSE 42.3

inux կայանների համար նախատեսված հակավիրուսային ծրագրային միջոցները պետք է ապահովեն ետևյալ գործառույթները

- Ռեզիդենտ հակավիրուսային մոնիթորինգ
- Ամպային պաշտպանություն նոր վտանգներից, որը ծրագրին թույլ է տալիս ռեալ ժամանակում դիմել արտադրողի ռեսուրսներին՝ գործարկվող ծրագրի կամ ֆայլի մասին տեղեկություն ստանալու համար:
- SMB / NFS հասանելի ռեսուրսների ստուգում
- Էվրիստիկ վերլուծության հնարավորություն, որը թույլ կտա ճանաչել և արգելափակել նախկինում անհայտ վնասաբեր ծրագրերը
- Օգտվողի կամ ադմինիստրատորի հրամանով հակավիրուսային սքանավորում ըստ ժամանակացույցի
- zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj. արխիվներում ֆայլերի հակավիրուսային ստուգում
- տեքստային ֆորմատով էլեկտրոնային փոստի ստուգում (Plain text)
- Ֆայլերի ստուգման օպտիմիզացիայի մեխանիզմի առկայություն (բացառումներ, վստահելի պռոցեսներ, ստուգման ժամանակի լիմիտավորում, ստուգվող ֆայլի ծավալի լիմիտ, ստուգված և վերջին ստուգումից հետո չփոփոխված ֆայլերի մասին տեղեկության քեշավորում)
- SMB/NFS պրոտոկոլներով ցանցային մատչումով լոկալ կատալոգներում գտնվող ֆայլերի պաշտպանություն հեռահար կոդավորումից
- Կասկածելի և վնասված օբյեկտների տեղափոխում կարանտին
- Microsoft outlook-ի հավելվածների փոստային բազաների ստուգում
- SAMBA-ի մակարդակում ֆայլային գործընթացների ստուգման հնարավորություն
- Օպերացիոն համակարգի ցանցային էկրանի ղեկավարում՝ նախնական կանոնների վերականգնման հնարավորությունով
- Առաջադրանքների թողարկում ժամանակացույցով և/կամ անմիջապես համակարգի վերաթողարկումից հետո
- HTML և CSV ֆորմատներով հաշվետվությունների արտահանման և պահպանման հնրավորություն
- Ֆայլային տարածության սքանավորման ընթացքում համակարգչի ռեսուրսների ճկուն կառավարում՝ օգտվողներին հարմարավետ աշխատանքով ապահովելու համար
- Բուժումից և հեռացումից առաջ վարակված օբյեկտի կրկնօրինակի ռեզերվային պահուստարանում պահպանելու հնարավորություն՝ ցանկության դեպքում վերականգնման հնարավորությամբ, եթե տվյալ ֆայլը պարունակում է կարևոր տեղեկություն
- առանց root իրավունքի առկայության գրաֆիկական ինտերֆեյսով ղեկավարելու հնարավորություն
- Վերոնշյալ բոլոր մոդուլների կենտրոնացված ղեկավարում միասնական ղեկավարման համակարգի միջոցով

Windws ֆայլային սերվերների համար հակավիրուսային ծրագրային միջոցների պահանջներ

Windows ֆայլային սերվերների համար հակավիրուսային ծրագրային միջոցները պետք է գործեն հետևյալ համակարգերով աշխատող կայանների վրա.

- Windows Server 2003, 2003 R2
- Windows Server 2008, 2008 R2
- Windows Server 2012, 2012 R2
- Windows Server 2016

Windows ֆայլային սերվերների համար նախատեսված հակավիրուսային ծրագրային միջոցները պետք է ապահովեն հետևյալ գործառույթները

- Հակավիրուսային սքանավորում ինչպես ռեալ ժամանակում, այնպես էլ դիմումով տարբեր ֆունկցիաներ կատարող սերվերների վրա. Դոմենների կոնտրոլերների և հավելվածների սերվերներ, ֆայլային սերվերներ
- Օգտվողի կամ ադմինիստրատորի հրամանով և ժամանակացույցով հակավիրուսային սքանավորում
- Առաջադրանքների թողարկում ժամանակացույցով և/կամ անմիջապես համակարգի վերաթողարկումից հետո
- Ամպային պաշտպանություն նոր վտանգներից, որը ծրագրին թույլ է տալիս ռեալ ժամանակում դիմել արտադրողի ռեսուրսներին՝ գործարկվող ծրագրի կամ ֆայլի մասին տեղեկություն ստանալու համար:
- RAR, ARJ, ZIP, CAB արխիվներում ֆայլերի հակավիրուսային ստուգում, այդ թվում գաղտնաբառով պաշտպանված
- Ֆայլերի, ֆայլային համակարգերի այլընտրանքային հոսքերի (NTFS-streams), բեռնման գրանցման, լոկալ և արտաքին սկավառակների բեռնման սեկտորի պաշտպանություն
- պաշտպանված սերվերի վրա Microsoft Windows Script Technologies (կամ Active Scripting) կողմից ստեղծված VBScript- ի եւ JScript սցենարների կատարման փորձերի շարունակական հետեւում: Սկրիպտների ծրագրային կոդերի ստուգում եւ ավտոմատ կերպով արգելում դրանցից առավել վտանգավոր համարվողները: Հանրային թղթապանակներին եւ ֆայլերին դիմումների վերլուծություն, ցանցում հասանելի պաշտպանված ռեսուրսների գաղտնագրման փորձերի բացահայտում
- Microsoft Windows կոնտեյների ստուգման հնարավորություն
- ներխուժման հայտնաբերման եւ կանխարգելման համակարգի (IDS / IPS) միջոցով պաշտպանություն ցանցային հարձակումներից, որոնք օգտագործում են եւ ցանցի գործունեության ամենատարածված կանոնները ծրագրերի համար և որոնք գործում են ցանկացած համակարգչային ցանցում, ներառյալ անլար ցանցերը
- Ռիսկերի մեղմացման տեխնիկան օգտագործելով գործընթացների հիշողության մեջ խոցելիության շահագործման դեմ պաշտպանական մեխանիզմներ
- Սքանավորման ընթացքի արագացում՝ շնորհիվ այն օբյեկտների սքանավորման բացառման, որոնց դրությունը նախորդ սքանավորման համեմատ փոփոխության չի ենթարկվել
- Առանձին գործընթացի միջոցով սեփական մոդուլների ստուգում՝ հնարավոր խախտումների կամ վնասվածության համար
- Սերվերի կարևորագույն տարածքների ստուգման կարգավորում առանձին գործընթացով
- սերվերային ռեսուրսների բաշխում հակավիրուսային և այլ ծրագրերի միջև, կախված խնդիրների առաջնայնությունից. ֆոնային հակավիրուսային սկանավորումը շարունակելու ունակություն.
- Կարեւոր իրադարձությունների մասին ադմինիստրատորներին տեղեկացնելու մի քանի ուղիների առկայություն (էլ. Փոստ, ձայնային ծանուցում, բացվող պատուհան, իրադարձությունների գրառում)
- ծառայությունների և հավելվածների պարամետրերին դերաբաշխված թույլտվություն, վնասակար ծրագրերից, չարամիտ օգտվողներից կամ անվերահսկելի օգտագործողներից պաշտպանության և հակավիրուսային կառավարումը արգելելու կամ թույլատրելու համար
- Հակավիրուսի աշխատանքային պռոցեսների քանակի ձեռքով առաջադրելու հնարավորություն
- Գրաֆիկական ինտերֆեյսը անջատելու կարողություն
- Լոկալ և հեռահար ղեկավարման պանելի առկայություն՝
- Հրամանների տողից հակավիրուսի պարամետրերի ղեկավարում

- Վերոնշյալ բոլոր մոդուլների կենտրոնացված ղեկավարում միասնական ղեկավարման համակարգի միջոցով
- Օպերացիոն համակարգի ցանցային էկրանի ղեկավարում՝ նախնական կանոնների վերականգնման հնարավորությունով

Linux ֆայլային սերվերների համար հակավիրուսային ծրագրային միջոցների պահանջներ

Linux ֆայլային սերվերների համար հակավիրուսային ծրագրային միջոցները պետք է գործեն հետևյալ համակարգերով աշխատող կայանների վրա.

- Ubuntu 14.04.5, 16.04.4, 17.10.1, 18.04. LTS
- Red Hat® Enterprise Linux® 6.9, 7.4
- CentoS-6.9, 7.4
- Debian GNU/Linux 8.10, 9.4
- oracleLinux 7.4.
- SUSE® Linux Enterprise Server 12 SP3.
- openSUSE® 42.3.

Linux ֆայլային սերվերների համար նախատեսված հակավիրուսային ծրագրային միջոցները պետք է ապահովեն հետևյալ գործառույթները

- Ռեզիդենտ հակավիրուսային մոնիթորինգ
- Ամպային պաշտպանություն նոր վտանգներից, որը ծրագրին թույլ է տալիս ռեալ ժամանակում դիմել արտադրողի ռեսուրսներին՝ գործարկվող ծրագրի կամ ֆայլի մասին տեղեկություն ստանալու համար:
- SMB / NFS հասանելի ռեսուրսների ստուգում
- Էվրիստիկ վերլուծության հնարավորություն, որը թույլ կտա ճանաչել և արգելափակել նախկինում անհայտ վնասաբեր ծրագրերը
- Օգտվողի կամ ադմինիստրատորի հրամանով հակավիրուսային սքանավորում ըստ ժամանակացույցի
- zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj. արխիվներում ֆայլերի հակավիրուսային ստուգում
- տեքստային ֆորմատով էլեկտրոնային փոստի ստուգում (Plain text)
- Ֆայլերի ստուգման օպտիմիզացիայի մեխանիզմի առկայություն (բացառումներ, վստահելի պռոցեսներ, ստուգման ժամանակի լիմիտավորում, ստուգվող ֆայլի ծավալի լիմիտ, ստուգված և վերջին ստուգումից հետո չփոփոխված ֆայլերի մասին տեղեկության քեշավորում)
- SMB/NFS պրոտոկոլներով ցանցային մատչումով լոկալ կատալոգներում գտնվող ֆայլերի պաշտպանություն հեռահար կոդավորումից
- Կասկածելի և վնասված օբյեկտների տեղափոխում կարանտին
- Microsoft outlook-ի հավելվածների փոստային բազաների ստուգում
- SAMBA-ի մակարդակում ֆայլային գործընթացների ստուգման հնարավորություն
- Օպերացիոն համակարգի ցանցային էկրանի ղեկավարում՝ նախնական կանոնների վերականգնման հնարավորությունով
- Առաջադրանքների թողարկում ժամանակացույցով և/կամ անմիջապես համակարգի վերաթողարկումից հետո
- HTML և CSV ֆորմատներով հաշվետվությունների արտահանման և պահպանման հնրավորություն
- Ֆայլային տարածության սքանավորման ընթացքում համակարգչի ռեսուրսների ճկուն կառավարում՝ օգտվողներին հարմարավետ աշխատանքով ապահովելու համար

- Բուժումից և հեռացումից առաջ վարակված օբյեկտի կրկնօրինակի ռեզերվային պահուստարանում պահպանելու հնարավորություն՝ ցանկության դեպքում վերականգնման հնարավորությամբ, եթե տվյալ ֆայլը պարունակում է կարևոր տեղեկություն
- առանց root իրավունքի առկայության գրաֆիկական ինտերֆեյսով ղեկավարելու հնարավորություն
- Վերոնշյալ բոլոր մոդուլների կենտրոնացված ղեկավարում միասնական ղեկավարման համակարգի միջոցով

Կենտրոնացված ղեկավարման, մոնիթորինգի և թարմացման ծրագրային միջոցների պահանջներ
Կենտրոնացված ղեկավարման, մոնիթորինգի և թարմացման ծրագրային միջոցները պետք է գործեն հետևյալ համակարգերով աշխատող կայանների վրա.

- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows 10
- Windows Server 2008, 2008 R2
- Windows Server 2012, 2012 R2
- Windows Server 2016;

Կենտրոնացված ղեկավարման, մոնիթորինգի և թարմացման ծրագրային միջոցները պետք է գործեն տվյալների բազաների կառավարման համակարգի հետևյալ տարբերակների հետ

- Microsoft SQL
- MySQL

Կենտրոնացված ղեկավարման, մոնիթորինգի և թարմացման ծրագրային միջոցները պետք է ապահովեն հետևյալ գործառույթները

- Միասնական դիստրիբուտիվից հակավիրուսային պաշտպանության կառավարման համակարգի տեղադրում
- Պաշտպանվող հանգույցների քանակից կախված տեղադրման ընտրություն
- Active Directory-ից տեղեկության կարդացման հնարավորություն՝ կազմակերպության համակարգիչների գրանցումների և օգտվողների մասին տվյալներ ստանալու նպատակով
- Ցանցում IP հասցեի, հոսթի անվանման, դոմենի անվանման, ենթացանցի դիմակի միջոցով համակարգիչների փնտրման և հայտնաբերման հնարավորություն
- Ցանցում նոր համակարգիչների հայտնվելու դեպքում դրանց գրանցումները ըստ ղեկավարման խմբերի ավտոմատ դասավորում
- Ղեկավարման կենտրոնի միջոցով անհամատեղելի հավելվածների կենտրոնացված հեռացում (ձեռքով և ավտոմատ կերպով)
- Կանոնների և խնդիրների փոփոխությունների պատմության պահպանություն, հնարավորություն նախորդ տարբերակներին վերադառնալու
- Հակավիրուսային ագենտի տարատեսակ տեղադրման մեթոդների առկայություն. Հեռահար տեղադրման համար – RPC, GPo, ղեկավարման համակարգի միջոցով, լոկալ տեղադրման համար – տեղադրման ինքնուրույն փաթեթի ստեղծման հնարավորություն
- Անվտանգության կանոններում հատուկ թրիգերների նշման հնարավորություն, որոնք կվերաբաշխեն հակավիրուսային ծրագրի կարգավորումները ըստ օգտատերերի, ընթացիկ IP հասցեի, համակարգչի ցանցում կամ անվտանգության խմբում գտնվելու: Պետք է լինի հնարավորություն այդ թրիգերների խմբավորման համար:
- Օգտվողի համակարգչի օպերացիոն համակարգում և դրանում տեղադրված ծրագրերում խոցելիությունների ավտոմատ փնտրում և վերացում
- Մինչև օգտվող համակարգիչների վրա ներբեռնված թարմացումների տարածումը դրանց թեստավորում. Օգտվողի աշխատատեղ թարմացումների տրամադրում անմիջապես դրանց ստացումից հետո

- Ցանցում վիրտուալ մեքենաների ճանաչում և դրանց միջև ծանրաբեռնվածության բաշխում այն դեպքում, երբ դրանք գտնվում են նույն ֆիզիկական սերվերի վրա
- Ադմինիստրատորների և օպերատորների դերերի կարգավորման հնարավորությամբ բազմամակարդակ համակարգի ստեղծում, ինչպես նաև հաշվետվությունների տրամադրում յուրաքանչյուր մակարդակում
- Կենտրոնացված ղեկավարման համակարգի օգտվողների նախակարգաբերված դերերի առկայություն: Օգտվողների գրանցումների համար պետք է իրականացվի կոնկրետ նշված իրավասություններով դերերի խմբերի ստեղծում:
- Կամայական մակարդակի ադմինիստրավորման սերվերների հիերարխիայի ստեղծում և հնարավորություն վերևի մակարդակից դրանց կենտրոնացված ղեկավարման:
- Ղեկավարման սերվերների համար multi-tenancy աջակցություն
- Ծրագրային միջոցների և հակավիրուսային բազաների թարմացման հնարավորություն տարատեսակ աղբյուրներից, ինչպես կապուղիներով այնպես էլ մեքենայական կրիչներից
- Տեղակայված ծրագրակազմի և սարքավորումների գույքագրում օգտվողների համակարգիչների վրա
- Պլանավորված գործառույթների մասին SMS հաղորդագրությունների ուղարկման հնարավորություն
- Ղեկավարման համակարգի և ցանցի ծանրաբեռնվածությունը կանխելու համար կազմակերպության ցանկացած համակարգիչ որպես թարմացումների տարածման աղբյուր գրանցելու հնարավորություն
- Ղեկավարման համակարգի ծանրաբեռնվածությունը կանխելու համար կազմակերպության ցանկացած համակարգիչ որպես հակավիրուսային ագենտների՝ նշված օգտատերերին, կառավարման կենտրոնացված համակարգին ուղարկելու աղբյուր գրանցելու հնարավորություն
- Հակավիրուսային պաշտպանության, լիցենզավորման ինչպես նաև գույքագրման մասին գրաֆիկական հաշվետվություններ կազմում
- Համակարգի մասին նախապես կարգաբերված ստանդարտ հաշվետվությունների առկայություն
- Հաշվետվությունների արտահանում PDF և XML ֆորմատներով
- Ամբողջ ցանցում ռեզերվային պահուստարանների և կարանտինների կենտրոնացված ղեկավարում, որոնց վրա տեղադրված է հակավիրուսային ԾԱ
- Կառավարման սերվերում նույնականացման համար ներքին հաշիվների ստեղծում:
- Կառավարման համակարգում ներկառուցված միջոցներով կառավարման համակարգի ռեզերվային պատճենում
- Windows Failover Clustering աջակցում
- Windows Certificate Authority ծառայության հետ ինտեգրացիայի աջակցում
- Հավելվածը կառավարելու web կոնսոլի առկայություն

Հակավիրուսային բազաների թարմացման պահանջներ

Թարմացվող հակավիրուսային տվյալների բազաները պետք է ապահովեն հետեյալ ֆունկցիոնալությունը.

• Կանոնավոր թարմացում առնվազն 24 անգամ օրացուցային օրվա ընթացքում:

• Թարմացման ուղիների բազմազանություն, ներառյալ կապի ուղիներով եւ արտաքին էլեկտրոնային սարքերով:

• Էլեկտրոնային թվային ստորագրության միջոցով թարմացումների ամբողջականությունն ու ինքնության ստուգում:

Շահագործման փաստաթղթերի պահանջներ

Բոլոր հակավիրուսային պաշտպանության ծրագրային արտադրանքների, այդ թվում՝ կառավարման գործիքների գործառնական փաստաթղթերը պետք է ներառեն պետական ստանդարտների պահանջներին համապատասխան պատրաստված փաստաթղթեր, ռուսերենով լեզվով, այդ թվում՝

• Օգտագործման ուղեցույց (administrator).

Հակավիրուսային արտադրանքի հետ տրամադրվող փաստաթղթերը պետք է մանրամասն նկարագրեն համապատասխան հակավիրուսային պաշտպանության տեղադրման, կազմակերպման և շահագործման գործընթացը:

Տեխնիկական աջակցման պահանջներ

Հակավիրուսային ծրագրային ապահովման տեխնիկական աջակցությունը պետք է

- Տրամադրվի ռուսերեն լեզվով, հակավիրուսային արտադրանք արտադրողի, նրա գործընկերների սերտիֆիկացված մասնագետների կողմից՝ Ռուսաստանի Դաշնության տարածքում՝ հեռախոսով, էլեկտրոնային փոստով և ինտերնետով:

Արտադրողի կայքը պետք է լինի ռուսերենով, ունենա հատուկ բաժին, որը նվիրված է արտադրանքի տեխնիկական աջակցությանը, գիտելիքների բազայի, ինչպես նաև ֆորում ծրագրային արտադրանքի օգտագործողների համար:

ՊԱՏՎԻՐԱՏՈՒ

Արտակարգ իրավիճակների նախարարություն
Դավիթաշեն 4-րդ թաղ., Ա.Միկոյան 109/8
ՖՆ գործառնական վարչություն
Հ/Հ 900011019313
ՀՎՀՀ 00153247

Վ. Օհանյան
(ստորագրություն)
Կ.Տ.

ԿԱՏԱՐՈՂ

<<Էյչ Գրուպ>> ՍՊԸ
ՀՀ, ք.Երևան, Բաշինջաղյան 1 փ, 13/30
<<Արմսվիսբանկ>> ՓԲԸ
Հ/Հ 2500010488760100
ՀՎՀՀ 01254973

Կ. Հարությունյան
(ստորագրություն)
Կ.Տ.

Հավելված N 2
«17» 04 2020թ. կնքված
ԳՀԾՁԲ-ԱԻՆ-20/58 ծածկագրով պայմանագրի

ՎՃԱՐՄԱՆ ԺԱՄԱՆԱԿԱՑՈՒՅՑ*

ՀՀ դրամ

Ծառայության														
հրավերով նախատեսված չափաբաժնի համարը	գնումների պլանով նախատեսված միջանցիկ ծածկագիրը՝ ըստ ԳՄԱ դասակարգման (CPV)	անվանումը	դիմաց վճարումները նախատեսվում է իրականացնել 2020թ-ին՝ ըստ ամիսների, այդ թվում											
			հունվար	փետրվար	մարտ	ապրիլ	մայիս	հունիս	հուլիս	օգոստոս	սեպտեմբեր	հոկտեմբեր	նոյեմբեր	դեկտեմբեր	Ընդամենը
1	72211195/1	հակավիրուսային համակարգչային ծրագրային փաթեթներ	,	,	,	,	,	,	,	,	,	,	,	1416000	1416000

* *Վճարման ենթակա գումարները ներկայացվում են ամողական կարգով:*

ՊԱՏՎԻՐԱՏՈՒ
Արտակարգ իրավիճակների նախարարություն
Դավիթաշեն 4-րդ թաղ., Ա.Միկոյան 109/8
ՖՆ գործառնական վարչություն
Հ/Հ 900011019313
ՀՎՀՀ 00153247

Վ. Օհանյան
(ստորագրություն)
Կ.Տ.

ԿԱՏԱՐՈՂ
<<Էյչ Գրուպ>> ՍՊԸ
ՀՀ, ք.Երևան, Բաշինջաղյան 1 փ, 13/30
<<Արմսվիսբանկ>> ՓԲԸ
Հ/Հ 25000104887601000
ՀՎՀՀ 01254973

Կ. Հարությունյան
(ստորագրություն)
Կ.Տ.

Հավելված 3
« 17 » 04 2020թ. կնքված
ԳՀՇՁԲ-ԱԻՆ-20/58 ծածկագրով պայմանագրի

Պայմանագրի կողմ	Պատվիրատու
_____	_____
_____	_____
գտնվելու վայրը _____	գտնվելու վայրը _____
հհ _____	հհ_____
հվհհ _____	հվհհ_____

ԱՐՁԱՆԱԳՐՈՒԹՅՈՒՆ N
ՊԱՅՄԱՆԱԳՐԻ ԿԱՄ ԴՐԱ ՄԻ ՄԱՍԻ ԿԱՏԱՐՄԱՆ ԱՐԴՅՈՒՆՔՆԵՐԻ ՀԱՆՁՆՄԱՆ-ԸՆԴՈՒՆՄԱՆ

« » « » 20 թ.

Պայմանագրի /այսուհետ՝ Պայմանագիր/ անվանումը՝

_____

Պայմանագրի կնքման ամսաթիվը՝ «____» «_____» 20 թ.
Պայմանագրի համարը՝ _____
Պատվիրատուն և Պայմանագրի կողմը՝ հիմք ընդունելով պայմանագրի կատարման վերաբերյալ « » « » 20 թ. դուրս գրված N ___ հաշիվ ապրանքագիրը, կազմեցին սույն արձանագրությունը հետևյալի մասին.
Պայմանագրի շրջանակներում Պայմանագրի կողմը մատուցել է հետևյալ ծառայությունները՝

N	Մատուցված ծառայությունների							
	անվանումը	տեխնիկական բնութագրի համառոտ շարադրանքը	քանակական ցուցանիշը		կատարման ժամկետը		Վճարման ենթակա գումարը /հազար դրամ/	Վճարման ժամկետը /ըստ վճարման ժամանակացույցի/
			ըստ պայմանագրով հաստատված գնման ժամանակացույցի	փաստացի	ըստ պայմանագրով հաստատված գնման ժամանակացույցի	փաստացի		

Սույն արձանագրության երկկողմ հաստատման համար հիմք հանդիսացած հաշիվ ապրանքագիրը և դրական եզրակացությունը հանդիսանում են սույն արձանագրության բաղկացուցիչ մասը և կցվում են:

Ծառայությունը հանձնեց	Ծառայությունն ընդունեց
_____	_____
ստորագրություն	ստորագրություն
_____	_____
ազգանուն, անուն	ազգանուն, անուն
Կ.Տ.	Կ.Տ.

Հավելված 3.1
«17» 04 2020թ. կնքված
ԳՀԾՁՔ-ԱԻՆ-20/58 ծածկագրով պայմանագրի

ԱԿՏ N

պայմանագրի արդյունքը Պատվիրատուին հանձնելու փաստը ֆիքսելու վերաբերյալ

Սույնով արձանագրվում է, որ _____-ի (այսուհետ՝ Պատվիրատու) և _____-ի
Պատվիրատուի անունը Կատարողի անունը

(այսուհետ՝ Կատարող) միջև 20 թ. _____ -ին կնքված N _____
պայմանագրի կնքման ամսաթիվը պայմանագրի համարը

գնման պայմանագրի շրջանակներում Կատարողը 20 թ. _____-ին հանձնման-ընդունման նպատակով Պատվիրատուին հանձնեց ստորև նշված ծառայությունները.

Ծառայության		
անվանումը	չափման միավորը	քանակը (փաստացի)

Սույն ակտը կազմված է 2 օրինակից, յուրաքանչյուր կողմին տրամադրվում է մեկական օրինակ:

ԿՈՂՄԵՐԸ

Հանձնեց

_____
ազգանուն, անուն

_____
ստորագրություն

Ընդունեց
հայտը նախագծած ներկայացուցիչ՝

_____
ազգանուն, անուն

_____
ստորագրություն