**Հ Ա Յ Տ Ա Ր Ա Ր ՈՒ Թ Յ ՈՒ Ն**

**Միգրացիայի և քաղաքացիության ծառայությունում փորձագետ (տեղեկատվական անվտանգության պատսխանատու)**

**ներգրավելու վերաբերյալ**

**1․ Ծրագրով նախատեսված աշխատանքների համառոտ նկարագիրը՝**

1. Մշակել անվտանգության քաղաքականությունները և ընթացակարգերը ըստ անհրաժեշտության։ *Մասնավորապես՝*

ա․ Ընդունելի օգտագործման քաղաքականություն - Acceptable Use Policy

բ․ Ցանցային անվտանգության քաղաքականություն – Network Security Policy

գ․ Տվյալների կառավարման քաղաքականություն – Data Management Policy

դ․ Գաղտնաբառի պահանջների քաղաքականություն -Password Requirements Policy

ե․ Հասանելիության վերահսկման քաղաքականություն - Access Control Policy

զ․ Հեռավար հասանելիության քաղաքականություն – Remote Access Policy

է․ Խախտումների արձագանքման քաղաքականություն - Breach Response Policy

ը․ Միջադեպերի արձագանքման քաղաքականություն – Incident Response Policy

թ․ Աղետից վերականգնման քաղաքականություն - Disaster Recovery Policy

ժ․ Մատակարարների կառավարման քաղաքականություն - Vendor management policy

ի․ Տվյալների կրիչների օգտագործման քաղաքակա նություն - Removable Media Policy

լ․ Անվտանգության իրազեկվածության և վերապատրաստման քաղաքականություն - Security awareness and Training Policy․

1. իրականացնել ՄՔԾ տեղեկատվական համակարգերի կիբերսպառնալիքներից պաշտպանվածության, քաղաքականությունների և ընթացակարգերի պահպանման մշտադիտարկում և աուդիտ․
2. կարգաբերել անվտանգային գործողությունների կենտրոնի (Security Operations Center) աշխատանքների կազմակերպումը՝ ներառյալ անհրաժեշտ տեղեկատվական գործիքները․
3. իրականացնել ՀայՓասս ընկերության կողմից վարվող տեղեկատվական համակարգերի մշտադիտարկում և աուդիտ, ձևավորել անհրաժեշտ միջավայր հավաքագրվող լոգերի պահպանման և վերլուծության համար:
4. գնահատել կիբերանվտանգության ռիսկերը և վերլուծել խոցելիությունը:
5. մշակել առաջին անգամ հիմնական համակարգեր (բնակչության պետական ռեգիստր, կենսաչափական տվյալների համակարգ, փաստաթղթերի շտեմարան) մուտքագրվող տվյալներով նույնականացում կատարելու և նույնականացված տվյալները պահոցում ամրագրելու կարգը․
6. մշակել, ներդնել և պարբերաբար թարմացնել կիբերանվտանգության քաղաքականությունը, չափորոշիչները և ուղեցույցները՝ համապատասխանեցնելով միջազգային չափանիշներին, մասնավորապես՝ ISO/IEC 27001-ին, ISO/IEC 27701-ին և ICAO Doc 9303-ին՝ ապահովելով զգայուն կենսաչափական և անձնական տվյալների համապարփակ պաշտպանությունը․
7. ղեկավարել և համակարգել անվտանգության պարբերական ռիսկերի գնահատումները, ներառյալ խոցելիության պարբերական սկանավորումները, ներթափանցման թեստավորումը և անկախ անվտանգության աուդիտները․
8. կառավարել կիբերանվտանգության միջադեպերը և արձագանքման մեխանիզմները, ներառյալ միջադեպերի բացահայտումը, արձագանքման համակարգումը, արմատային պատճառների վերլուծությունը, մեղմացման պլանավորումը և հաշվետվությունների կազմումը՝ ՊՄԳ պայմանագրի կետերում նշված պայմանագրային պահանջների (օրինակ՝ կետեր 3.3.1, 3.4.3 և 4.4.4) համաձայն․
9. ապահովել համապատասխանությունը ՀՀ ազգային օրենսդրությանը, տվյալների համընդհանուր պաշտպանության կանոնակարգին՝ GDPR-ին, համահունչ գաղտնիության կարգավորմանը և ՊՄԳ պայմանագրում նշված կոնկրետ պայմանագրային պարտավորությունների կատարումը․
10. ապահովել գործընկերների կողմից տվյալների մշակումը և խստորեն պահպանումը ՄՔԾ-ի կողմից վերահսկվող միջավայրերում․
11. հաստատել և վերահսկել կարևորագույն համակարգերի անվտանգության ճարտարապետությունը, ինչպիսիք են կենսաչափական տվյալների պահպանման համակարգերը, փաստաթղթերի տվյալների բազան, X-Road փոխգործելիության հարթակը և այլ ինտեգրված կառավարական հարթակներ՝ համաձայն պայմանագրային տեխնիկական պահանջների (ՊՄԳ պայմանգրի 3-րդ հավելված)․
12. սահմանել և պահպանել մանրամասն անվտանգության փաստաթղթեր, համապարփակ աուդիտի գրառումներ, համապատասխանության մոնիթորինգի համակարգեր և անվտանգության գրանցամատյաններ՝ համաձայն պայմանագրային և կարգավորող հաշվետվությունների պահանջների համապատասխան․
13. կանոնավոր կերպով անցկացնել անվտանգության վերաբերյալ վերապատրաստումներ և իրազեկման ծրագրեր՝ բարձրացնելով անձնակազմի իրազեկվածությունը կիբերանվտանգության սպառնալիքների, պատասխանատվությունների և լավագույն փորձի վերաբերյալ․
14. համագործակցել գործընկերների հետ՝ կիբերանվտանգության շրջանակները, տվյալների կառավարման պրակտիկան և համակարգերի տեղակայումները վերանայելու և հաստատելու համար՝ ապահովելով պայմանագրային պարտավորությունների խիստ պահպանումը, հսկողություն իրականացնելու միջոցով:

**2․ Փորձագետ ներգրավելու ժամկետն է՝ մինչև մեկ տարի:**

**3․   Փորձագետի աշխատավարձը կազմում է՝** **691.000** **(վեց հարյուր իննսունմեկ հազար)** ՀՀ դրամ (ներառյալ հարկերը)։

**4․ Փորձագետին ներկայացվող պահանջներն են՝**

1. համակարգչային գիտություն և (կամ) տեղեկատվական տեխնոլոգիաներ և (կամ) տեղեկատվական անվտանգություն և (կամ) կիբերնետիկա և (կամ) մաթեմատիկա կամ ֆիզիկա մասնագիտությամբ բարձրագույն կրթություն․
2. տեղեկատվական տեխնոլոգիաների, կիբերանվտանգության կառավարման

ոլորտներում առնվազն 5 տարվա մասնագիտական ​​​​փորձ․

1. ISO/IEC 27001 և ISO/IEC 27701 ստանդարտների ներդրման փորձի առկայություն, կենսաչափական տվյալների կառավարման ICAO Doc 9303 ստանդարտների իմացություն։
2. Կիբերանվտանգության շրջանակների և գործիքների խորը տեխնիկական գիտելիքների՝ ներառյալ firewall-ների, կոդավորման տեխնոլոգիաների, ներխուժման հայտնաբերման/կանխարգելման համակարգերի, անվտանգության տեղեկատվության և իրադարձությունների կառավարման (SIEM) լուծումների և խոցելիության սկանավորման ծրագրակազմի իմացություն․
3. իրադարձությունների արձագանքման թիմերը կառավարելու, կիբերանվտանգության ռիսկերի գնահատելու, խոցելիության կառավարման և ներթափանցման թեստավորման գործունեությունը կառավարելու կարողություն․
4. հաղորդակցման հմտություններ՝ բարդ անվտանգության հասկացությունները հստակ ձևակերպելու կարողությամբ՝ ինչպես տեխնիկական թիմերի, այնպես էլ ղեկավարության և արտաքին շահագրգիռ կողմերին հստակ ձևակերպելու ունակությամբ․
5. CISSP, CISM, ISO 27001 գլխավոր աուդիտորի կամ համարժեք հավաստագրերի առկայությունը խիստ նախընտրելի են․
6. հայերեն, անգլերեն և ռուսերեն լեզուների գերազանց իմացություն (գրավոր և բանավոր)։

**5․ Դիմումների ընդունման վերջնաժամկետն է 2025թ. սեպտեմբերի 24-ը ներառյալ:**

**6․ Աշխատավայրը`** **ՀՀ ք. Երևան, Դավթաշեն, 4-րդ թաղ․, 17/10։**

**7․ Չի թույլատրվում հավակնորդի հետ պայմանագիր կնքել, եթե տվյալ անձը պաշտոնից ազատվել կամ տվյալ անձի ծառայությունը վերջին մեկ տարվա ընթացքում դադարեցվել է կարագապահական տույժ կիրառելու, օրենքով սահմանված փորձաշրջանը չանցնելու, օրենքի խախտմամբ պաշտոնի նշանակվելու, «Հանրային ծառայության մասին» ՀՀ օրենքով սահմանված անհամատեղելիության պահանջները չպահպանելու, Հայաստանի Հանրապետության քաղաքացիությունը դադարեցնելու, ուժի մեջ մտած՝ նրա նկատմամբ կայացված մեղադրական դատավճռի դեպքերում, բացառությամբ այն դեպքերի, երբ նշանակվել է տուգանք, ինչպես նաև երկու տարի անընդմեջ իր մեղքով վերապատրաստման անհատական ծրագրով հաստատված կրեդիտները չստանալու դեպքում։**

**8․ Ընտրություն կատարելու եղանակը`**

Դիմում ներկայացրած քաղաքացիների փաստաթղթերի և ինքնակենսագրականների ուսումնասիրություն և (կամ) հարցազրույց։

**9․ Դիմող քաղաքացիները պետք է ներկայացնեն հետևյալ փաստաթղթերը.**

* դիմում Նախարարության գլխավոր քարտուղարի անունով **(դիմումի ձևը կցվում է)**,
* հայտարարություն **(ձևը** **կցվում է**) ՀՀ կառավարության 02.08.2018թ. N 878-Ն որոշմամբ հաստատված կարգի 13-րդ կետով նախատեսված սահմանափակումների բացակայության մասին․
* տվյալ պաշտոնը զբաղեցնելու համար մասնագիտական գիտելիքների և աշխատանքային ունակությունների տիրապետման տեսանկյունից ներկայացվող պահանջների բավարարումը հավաստող փաստաթղթերի` դիպլոմի/ների), վկայական/ների), աշխատանքային գրքույկի (վերջինիս բացակայության դեպքում անհրաժեշտ է ներկայացնել տեղեկանք/ներ համապատասխան մարմնից/ներից) պատճենները բնօրինակների հետ միասին, հայերեն ինքնակենսագրական (CV)․
* արական սեռի անձինք` նաև զինվորական գրքույկի կամ դրան փոխարինող ժամանակավոր զորակոչային տեղամասից կցագրման վկայականի պատճենները` բնօրինակի հետ միասին, կամ համապատասխան տեղեկանք․
* մեկ գունավոր լուսանկար 3X4 սմ չափի․
* անձնագրի կամ նույնականացման քարտի պատճենը։

**10․ Քաղաքացին փաստաթղթերը ներկայացնում է անձամբ կամ էլեկտրոնային փոստի միջոցով։**

**11․ Փաստաթղթերն (անձամբ ներկայացնելու դեպքում) ընդունվում են ամեն օր` ժամը 09։30-12։30-ը (բացի շաբաթ և կիրակի օրերից)։**

 Լրացուցիչ տեղեկությունների համար դիմել ՀՀ ներքին գործերի նախարարություն (ք. Երևան, Նալբանդյան 130, 3-րդ հարկ, 310 սենյակ, հեռ.` 010-59-64-81, էլեկտրոնային փոստի հասցեն` hrmd@mia.gov.am):