PIETEIKUMS DALĪBAI TIRGUS IZPĒTĒ

***„Informācijas drošības pārvaldnieka pakalpojumi”***

|  |  |
| --- | --- |
| **Pasūtītājs:**  **Latvijas Valsts prezidenta kanceleja**  Pils laukums 3,  Rīga, LV-1900  Latvija | **Piegādātājs:**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  (piegādātāja nosaukums un adrese) |

Ar šo SIA \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ apstiprina, ka piekrīt tirgus izpētes noteikumu prasībām, apliecina, ka pakalpojuma sniegšanā iesaistītie speciālisti atbilst prasībām un piedāvā veikt preču piegādi/pakalpojuma izpildi saskaņā ar tirgus izpētes noteikumu prasībām (tehnisko specifikāciju, finanšu piedāvājumu).

1. Apstiprinām, ka pievienotie dokumenti veido šo piedāvājumu.
2. SIA \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_reģistrēts likumā noteiktajos gadījumos un likumā noteiktajā kārtībā.
3. Pakalpojuma sniegšanā tiks iesaistīti šādi darbinieki:
   1. Vārds, uzvārds, p.k.

|  |  |
| --- | --- |
| Pretendenta nosaukums: |  |
| Reģistrācijas datums: |  |
| Reģistrācijas Nr.: |  |
| Juridiskā adrese: |  |
| Kontaktpersona (Vārds, Uzvārds, amats): |  |
| Tālrunis: |  |
| E-pasts: |  |
| Banka: |  |
| Kods: |  |
| Konta Nr.: |  |

Datums

Paraksts/ Paraksta atšifrējums

**TEHNISKĀ SPECIFIKĀCIJA**

***„Informācijas drošības pārvaldnieka pakalpojumi”***

# 

# Informācija par Pasūtītāju:

## Pasūtītājs: Latvijas Valsts prezidenta kanceleja (turpmāk – Pasūtītājs), reģ.nr. 90000038578, Pils laukums 3, Rīga, LV-1900.

## Kontaktpersona: Jānis Mūsiņš, Informācijas tehnoloģiju nodaļas vadītājs, tālr.: 67092152, e-pasts: [janis.musins@president.lv](mailto:janis.musins@president.lv).

# Tirgus izpētes priekšmets:

## Tirgus izpētes priekšmets: Latvijas Valsts prezidenta kancelejas (turpmāk – Kanceleja) informācijas drošības pārvaldnieka funkcijas pastāvīga nodrošināšana Latvijas Republikas normatīvo dokumentu (piemēram, bet ne tikai – Informācijas tehnoloģiju drošības likums un Ministru kabineta 2015. gada 28. jūlija noteikumi Nr. 442 “Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām” (turpmāk – MK noteikumi Nr. 442), Ministru kabineta 2011. gada 1. februāra noteikumi Nr. 100 „[Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība](http://likumi.lv/doc.php?id=225776)” (turpmāk – MK noteikumi Nr. 100), Ministru kabineta 2010. gada 1. jūnija noteikumi Nr. 496 “Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība” (turpmāk – MK noteikumi Nr.496)) prasībām un atbilstoši piemērojamajām IT nozares labās prakses (piemēram, ISO/IEC 27002:2013) vadlīnijām.

## Tirgus izpētes CPV kodi: 72220000-3 “Sistēmu un tehnisko konsultāciju pakalpojumi, 7222230-0 “Informācijas tehnoloģijas pakalpojumi”.

# Piedāvājumu iesniegšana:

## Piedāvājumu jāiesniedz (parakstītu ar drošu elektronisko parakstu vai izdrukātu, parakstītu un ieskenētu) nosūtot līdz 2019.gada 05.jūlija plkst. 17:00 uz e-pastu: [info@president.lv](mailto:info@president.lv)

# Pakalpojuma sniegšanas vieta klātienē: Pils laukums 3, Rīga.

# Izpildes termiņš: 12 mēneši (vai sasniegta līguma summa 9999 EUR).

# Iepirkuma priekšmeta apjoms:

## Līdz 9999 EUR līguma darbības laikā, neskaitot pievienotās vērtības nodokli.

# Esošā situācija informācijas drošības pārvaldības jomā:

## atbilstoši normatīvo aktu prasībām ir izstrādāti un apstiprināti Kancelejas iekšējie noteikumi:

### Informācijas drošības politika;

### Iekšējie informācijas sistēmu drošības noteikumi;

### Informācijas sistēmu lietošanas noteikumi;

### Informācijas drošības risku vadības noteikumi;

### Informācijas sistēmu darbības atjaunošanas plāns;

### Informācijas drošības incidentu apstrādes noteikumi;

## veikta informācijas risku analīze un sagatavots risku pārvaldības plāns 2019. gadam;

## definētas informācijas sistēmu konfidencialitātes, integritātes un pieejamības drošības klases saskaņā ar MK noteikumu Nr. 442 7.1. punktu un apstiprināta Kancelejas informācijas sistēmu klasifikācija;

## darbojas ielaušanās noteikšanas/novēršanas sistēmas uz Ugunsmūra (Palo Alto iekārta) (IDS (Intrusion Detection System) un IPS (Intrusion Prevention System)), kas nodrošina visas ienākošo/ izejošo datu plūsmas monitoringu, atpazīto aizdomīgo darbību bloķēšanu un informatīvus paziņojumus pie noteiktām aizdomīgām darbībām, kas tiek identificētas datu plūsmā.

# Darba uzdevums:

## nodrošināt Kancelejas informācijas drošības pārvaldības sistēmas darbību atbilstoši Eiropas Savienības un Latvijas Republikas normatīvo aktu prasībām (piemēram, bet ne tikai - MK noteikumi Nr. 442), kā arī piemērojamajām IT nozares labās prakses vadlīnijām (ISO/IEC 27002:2013);

## izstrādāt, uzturēt (pārskatīt, aktualizēt, pilnveidot) ar informācijas drošības pārvaldību un drošības nodrošināšanu saistītos Kancelejas iekšējos normatīvos aktus, nodrošināt to ieviešanu, kā arī nodrošināt tajos noteikto prasību izpildes kontroli;

## regulāri organizēt un uzraudzīt informācijas drošības pasākumu īstenošanu vismaz šādā apjomā:

### informācijas drošības incidentu pārvaldība un risku analīze;

### informācijas sistēmu un telekomunikāciju tīklu drošības auditi;

### drošības audita laikā konstatēto ievainojamību un nepilnību novērtēšana, prioritizēšana un novēršana;

### informācijas resursu klasifikācija;

### preventīvu un uzraudzības rīku izmantošana un uzturēšana;

## nodrošināt pieejas tiesību pārvaldības procesa uzraudzību attiecībā uz Kancelejas pārziņā esošajām informācijas sistēmām, kā arī sadarbībā ar atbildīgajiem par lietotāju kontu pārvaldību, informācijas un tehnisko resursu turētājiem veikt ikgadēju lietotāju tiesību atbilstības pārbaudi;

## pārraudzīt un analizēt informācijas tehnoloģiju iekārtu pierakstus, organizēt konstatēto nepilnību novēršanu;

## piedalīties Kancelejas informācijas un komunikāciju tehnoloģiju stratēģiskās plānošanas pasākumu norisē, attiecībā uz jautājumiem, kuri skar drošības pārvaldības attīstības pasākumu definēšanu un to ieviešanas nosacījumu noteikšanu, attiecībā uz fiziskās un loģiskās drošības pasākumiem;

## sadarbībā ar Kancelejas Informācijas tehnoloģiju nodaļu plānot, koordinēt un uzraudzīt drošības risinājumu ieviešanu, papildināšanu, uzlabošanu;

## piedalīties esošo Kancelejas informācijas sistēmu izmaiņu, kā arī jaunu informācijas sistēmu plānošanas un iegādes procesos, Kancelejas veikto iepirkumu procedūru nolikumu sagatavošanā attiecībā uz drošības pārvaldības prasību definēšanu, kā arī nodrošināt noteikto drošības prasību izpildes un ievērošanas uzraudzību jaunu informācijas sistēmu vai esošo informācijas sistēmu izmaiņu ieviešanas procesā;

## piedalīties pretendentu piedāvājumu izvērtēšanā un atzinumu sagatavošanā par to atbilstību Kancelejas izvirzītajām prasībām drošības pārvaldības jautājumos;

## piedalīties Kancelejas Informācijas tehnoloģiju pārvaldības ietvaros noslēdzamo līgumu sagatavošanā attiecībā uz Kancelejas informācijas drošības aizsardzību;

## nodrošināt konsultāciju un ieteikumu sniegšanu attiecībā uz Kancelejas iekšējā tīkla uzbūves attīstību un tā darbības pārvaldību;

## nodrošināt konsultāciju un ieteikumu sniegšanu par informācijas sistēmu nepārtrauktas darbības nodrošināšanu un iespējamajiem risinājumiem tās uzlabošanai;

## piedalīties informācijas sistēmu darbības atjaunošanas nodrošināšanā ārkārtas situāciju rašanās gadījumā;

## izstrādāt ieteikumus efektīvākai datu plūsmas uzraudzībai un ziņošanai par iespējamo incidentu, kā arī plānot, koordinēt un uzraudzīt attiecīgo līdzekļu ieviešanu un darbību;

## izvērtēt nepieciešamību ieviest jaunus drošības risinājumus un esošo risinājumu papildināšanas/ uzlabošanas darbus, piemēram, bet ne tikai:

### sistēmu un infrastruktūras auditācijas pierakstu glabāšana/ apkopošana un to analīze vienuviet (Splunk, Graylog, Syslog, vai analoga risinājuma);

### aizdomīgo DNS pieprasījumu identificēšana (reižu skaits, TTL neliels/ netipisks vārds u.tml.);

### datu zuduma novēršanas sistēmas (*Data Loss Prevention*) konfigurācijas nosacījumu definēšana;

### dokumentu piekļuves noteikšana (piem., *Rights Management Services (RMS)*) u.tml.;

### automātisku ievainojamību skenēšana un ziņošana, ja tiek atklāta ievainojamība (Qualys Vulnerability management, Rapid7 Insight VM vai līdzīgu);

## nodrošināt konsultāciju un ieteikumu sniegšanu citos ar informācijas un informācijas sistēmu drošību saistītos jautājumos pēc Kancelejas atbildīgo darbinieku pieprasījuma;

## sadarbojoties ar Kancelejas personas datu aizsardzības speciālistu, veikt šādus uzdevumus:

### piedalīties personas datu drošības stratēģijas izstrādē un īstenošanā;

### sniegt  konsultatīvu  un  organizatorisku  atbalstu  drošības  risku identificēšanā,  analīzē  un  pasākumu  ieviešanā  risku  mazināšanai  un novēršanai personas datu aizsardzībā (ciktāl tas saistīts ar informācijas un informācijas sistēmu drošības jautājumiem);

### sniegt  priekšlikumus  Kancelejas  drošības  pasākumu  pilnveidošanai personu datu aizsardzības jomā.

## nodrošināt darbinieku regulāru apmācību informācijas drošības aizsardzības jomā, t.sk., jauno darbinieku apmācības;

## plānot, koordinēt un uzraudzīt sociālās inženierijas testus darbiniekiem, piemēram, organizējot viltotu e-pastu ar lūgumu atvērt e-pasta pielikumu, saiti vai citu resursu, nosūtīšanu, pēc kā apkopotos rezultātus iesniegt Kancelejas vadībai;

## Sagatavot un Kancelejas atbildīgajai kontaktpersonai iesniegt:

### atskaiti par iepriekšējā mēnesī izpildītajiem darbiem, saskaņā ar kuru Kancelejai tiek piestādīts rēķins par attiecīgajā periodā sniegtajiem pakalpojumiem;

### informāciju par plānotajiem nākamā ceturkšņa pasākumiem Kancelejas informācijas drošības uzlabošanas jomā.

# Prasības pretendentiem:

## Pretendents pēdējo trīs gadu laikā - 2016., 2017. vai 2018. gadā - ir nodrošinājis informācijas sistēmu drošības pārvaldības pakalpojuma sniegšanu valsts un/ vai pašvaldības institūcijām vai to kapitālsabiedrībām;

## Pretendentam vai pretendenta pakalpojuma sniegšanā iesaistītajam personālam ir vismaz 3 (trīs) gadu pierādāma pieredze informācijas un komunikācijas tehnoloģiju drošības jomā.

## Līdzvērtīgu piedāvājumu gadījumā priekšrocība tiks dota pretendentam (vai pretendenta pakalpojuma sniegšanā iesaistītajam personālam), kuram ir:

### augstākā izglītība informācijas tehnoloģiju, eksakto zinātņu, biznesa vadības, finanšu, ekonomikas vai tiesību jomā;;

### pierādāma kompetence informācijas drošības pārvaldības jomā, ko apliecina CISA, CISM, CISSP, ISO/IEC 27001 vadošā auditora/ auditora vai ekvivalents sertifikāts (iesniedzama sertifikāta kopija);;

### pierādāma kompetence informācijas un komunikācijas tehnoloģiju pārvaldības jomā, ko apliecina TIL vai ISO20000 Lead auditor sertifikāts vai ekvivalents sertifikāts (iesniedzama sertifikāta kopija);

### risku pārvaldības speciālists ar starptautiski atzītu sertifikāciju risku vadībā, piemēram: M\_o\_R, ISO 31000, CRISC vai ekvivalenta (iesniedzama sertifikāta kopija).;

## pretendenta un tā darbinieku atbilstība Ministru kabineta noteikumu Nr.100 6.punkta un Ministru kabineta noteikumu Nr. 496 27. punkta prasībām (pretendenta amatpersonas un darbinieki tiks pakļauti MK noteikumos minētajām drošības pārbaudēm pirms līguma slēgšanas).

# Piedāvājumā jāapraksta vismaz: pakalpojuma sniegšanā iesaistīto speciālistu atbilstība kvalifikācijas prasībām un pieredze.

# Papildnosacījumi:

## pakalpojuma sniegšana ietver pakalpojuma sniedzēju ekspertu darbu Kancelejas telpās un citu organizāciju telpās, ja tas ir saistīts ar Kancelejas interešu pārstāvību iepriekš minēto sniedzamo pakalpojumu ietvaros;

## pakalpojumu sniegšanas laikā Pakalpojuma sniedzējam ir jānodrošina atbalsta sniegšana Kancelejai drošības incidentu rašanās gadījumā, ievērojot šādus pakalpojumu sniegšanas laikus:

### jebkurā diennakts laikā jebkurā dienā ne vēlāk kā 2 (divu) stundu laikā no brīža, kad par incidentu paziņots informācijas drošības pārvaldnieka pakalpojumu sniedzējam, ja incidenta rezultātā ir pilnībā apturēta Kancelejas mājaslapas [www.president.lv](http://www.president.lv) darbība;

### ne vēlā kā līdz Kancelejā noteiktās darba dienas beigām (darba laikā no plkst. 8.30 līdz plkst. 17.00) no incidenta pieteikšanas brīža, ja tā rezultātā ir apturēta citu Kancelejas informācijas sistēmu darbība;

## konsultāciju sniegšana Pakalpojuma sniedzējam ir jānodrošina ne vēlāk kā 2 (divu) darba dienu laikā no pieteikuma saņemšanas brīža;

## ja objektīvu iemeslu dēļ Pakalpojuma sniedzējs nevar nodrošināt 11.2.1. un 11.2.2. punktā minēto pieteikumu novēršanas laiku ievērošanu, par konkrētā gadījuma novēršanu individuāli vienojas ar līgumā noteikto Kancelejas kontaktpersonu, norādot konkrētus iemeslus, kas kavē attiecīgā pasākuma veikšanu un laiku, kad attiecīgais pieteikums tiks novērsts.

TIRGUS IZPĒTES

**“*„Informācijas drošības pārvaldnieka pakalpojumi”***

**Finanšu piedāvājuma forma**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nr.p.k.** | **Pakalpojuma nosaukums** | **Iepirkuma priekšmeta apjoms (mēneši)** | **Piedāvājuma cena par vienu vienību, *euro* bez PVN** | **Summa, *euro* bez PVN** |
| 1. | Informācijas drošības pārvaldnieka pakalpojumi | **12** |  |  |
|  | | | **Summa kopā bez PVN** |  |
| **PVN 21%** |  |
| **Summa kopā ar PVN** |  |

Datums

Paraksts/ Paraksta atšifrējums

TIRGUS IZPĒTES

**“*„Informācijas drošības pārvaldnieka pakalpojumi”***

**Pretendenta kvalifikācijas apliecinājumu formas**

1. **Pretendenta sniegto līdzīgo pakalpojumu apliecinājuma forma**

|  |  |  |
| --- | --- | --- |
| **Nr.** | **Pakalpojuma saņēmēja nosaukums** | **Pakalpojuma saņēmēja kontaktpersona\*** |
| 1. |  |  |
| 2. | … |  |

1. **Pretendenta vai tā projektā iesaistītā personāla pieredzes informācijas drošības jomā apliecinājuma forma**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nr.** | **Uzņēmums/ projekts, kurā iegūta pieredze informācijas drošības** | **Pieredzes gūšanas periods (no, līdz)** | | **Pieredzi apliecināt pilnvarotas personas kontaktinfor-mācija\*** |
| **No**  **(mēn/gads)** | **Līdz**  **(mēn./gads)** |
| 1. |  |  |  |  |
| 2. | .. |  |  |  |

1. **Pretendenta vai tā darbinieku kompetenci apliecinošo sertifikātu uzskaitījums**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nr.** | **Izglītības iestāde** | **Sertifikācija** | **Izsniegšanas datums** | **Kvalifikāciju apliecinošie dokumenti** |
| 1. |  |  |  |  |
| 2. |  |  |  |  |

Datums

Paraksts/ Paraksta atšifrējums