## Správa privilegovaných účtov - Opis predmetu zákazky

**Predmetom obstarávania je:**

* analýza prostredia infraštruktúry verejného obstarávateľa v rozsahu potrebnom pre vypracovanie detailného návrhu riešenia
* vypracovanie detailného návrhu riešenia;
* dodanie systému pre riadenie a správu privilegovaných účtov (ďalej len „systém SPÚ“) s využitím na trhu bežne dostupného SW produktu zameraného na problematiku Privileged Access managementu (PAM), vrátane potrebných licencií spolu s ich maintenance/ subskripcií SW produktu a všetkých jeho potrebných modulov, v trvaní 5 rokov vrátanie času potrebného na implementáciu;
* implementácia systému SPÚ, vrátane SW licencií/subskripcií;
* poskytovanie servisných služieb uchádzačom v dĺžke 5 rokov od ukončenia implementácie.

Systém SPÚ bude implementovaný a prevádzkovaný v infraštruktúre verejného obstarávateľa (on premise). Komponenty potrebné pre zabezpečenie analytickej funkcionality a vyhodnocovania môžu byť realizované aj v cloude, pre tieto komponenty platia rovnaké požiadavky na dostupnosť ako u ostatných komponentov systému SPÚ.

Dodaný systém SPÚ musí pokryť hlavne:

* centralizovanú správu privilegovaných účtov a ich používateľov a riadenie celého ich životného cyklu,
* riadenie prístupov používateľov ku jednotlivým komponentom ICT ako sú zariadenia, operačné systémy, služby IT, ... (ďalej len „koncové systémy“),
* centralizovanú správu tzv. secrets, tzn. technologických účtov, ktoré využívajú koncové systémy pre prístup k iným koncovým systémom a riadenie celého ich životného cyklu,
* bezpečné uloženie hesiel, kľúčov a informácií o účtoch v chránenom úložisku (vault),
* bezpečné a auditované zdieľanie privilegovaných účtov používateľmi,
* analýza a poskytovanie rizikových bezpečnostných udalostí, odhaľovanie pokusov o zneužitie privilegovaných prístupov.

Pojem privilegovaný účet označuje účet v koncovom systéme, ktorý má vysoké oprávnenia, t. j. účty typu/role root v Linux/UNIX systémoch, účty typu/role Administrátor vo Windows systémoch a pod., resp. každý účet, ktorý má vyššie oprávnenia než bežné používateľské a ktorý slúži k výkonu správy akejkoľvek časti koncového systému. Privilegovaný účet môže byť zdieľaný.

Pojem používateľ označuje fyzickú osobu, ktorá používa privilegované účty. Ide hlavne o pracovníkov prevádzky, dodávateľov, alebo vývojárov.

Pojem technologický účet označuje systémové účty používané koncovými systémami (obvykle pre prístup k iným koncovým systémom), ktoré nie sú viazané na fyzickú osobu.

Pojem privilegovaný prístup označuje konfiguračné spojenie používateľa s privilegovaným/ /technologickým účtom a koncovým systémom v systéme SPÚ.

Detailné požiadavky na systém SPÚ sú uvedené v prílohe PNOZ – Funkcionálne a bezpečnostné požiadavky na systém SPÚ.

Pri implementácii a prevádzke systému SPÚ musia byť okrem požiadaviek uvedených v tomto opise predmetu zákazky dodržané aj štandardy (architektonické, bezpečnostné, technologické, projektové), ktoré sú uvedené v prílohe PNOZ – Funkcionálne a bezpečnostné požiadavky na systém SPÚ. Rovnako záväzné sú pre nastavenia systému SPÚ aj iné interné predpisy verejného obstarávateľa (napr. bezpečnostné politiky hesiel a pod.), ktoré majú nevýznamný dopad na tvorbu cenovej ponuky a ktoré budú uchádzačovi poskytnuté vo fáze tvorby detailného návrhu riešenia (ďalej len „DNR“).

## 2. Určenie rozsahu nasadenia

Tu uvedené údaje slúžia pre určenie potrebného množstva SW produktov, ich licencií či subskripcií, ktoré uchádzač dodá a tiež pre určenie rozsahu implementačných prác.

Celkový počet interných používateľov systému SPÚ bude maximálne 70, z tohto počtu bude počas realizácie projektu zapojených 55, ostatné budú podľa potreby verejného obstarávateľa dodávané počas bežnej prevádzky na objednávku, v rozsahu podľa požiadaviek verejného obstarávateľa uvedených v objednávke.

Celkový počet externých používateľov (nie zamestnancov verejného obstarávateľa, pracovníci zmluvnej dodávateľskej podpory) systému SPÚ bude maximálne 150, z tohto počtu bude počas realizácie projektu zapojených 115, ostatné budú podľa potreby verejného obstarávateľa dodávané počas bežnej prevádzky na objednávku, v rozsahu podľa požiadaviek verejného obstarávateľa uvedených v objednávke.

Všetky konkrétne množstvá uvedené v kapitolách 2.1 a 2.2 sú maximálne a nimi je daný rozsah dodávky SW produktu. Zoznamy v kapitolách 2.3 až 2.5 slúžia pre zorientovanie sa v zložitosti infraštruktúry verejného obstarávateľa a nemusia byť úplné.

### 2.1 Zoznam fyzických zariadení, ku ktorým sa pristupuje prostredníctvom privilegovaných účtov

Fyzické servery:

Celkový počet fyzických serverov je 85. Technológie zahrňujú vendorov HP, Dell, Supermicro. Lenovo. Spôsob prístupu: WebGUI cez protokoly http/https, terminálový klient cez protokol SSH.

Sieťové zariadenia:

Celkový počet sieťových zariadení je 490. Technológie zahrňujú vendorov HP, Cisco, Fortinet, f5, IBM, Brocade, Infoblox, Barracuda, Forcepoint, SkyHigh, ADVA, Mitel. Spôsob prístupu: WebGUI cez protokoly http/https, terminálový klient cez protokol SSH.

Diskové polia:

Celkový počet diskových polí je 4. Technológie zahrňujú vendorov HP a Dell. Spôsob prístupu: WebGUI cez protokoly http/https a terminálový klient cez protokol SSH.

Desktopy:

Celkový počet desktop zariadení je 1600 (500 PC a 1100 notebookov).

### 2.2 Zoznam OS, ku ktorým sa pristupuje prostredníctvom privilegovaných účtov

Celkový počet Windows serverov je 280.

Celkový počet Linux serverov je 170.

Celkový počet VMware ESXi je 45 ks.

Celkový počet VMware virtuálnych appliance (Photon OS/Ubuntu) je 10 ks.

Celkový počet proprietárnych OS na sieťových zariadeniach je 490. Technológie zahrňujú vendorov HP, Cisco, Fortinet, f5, IBM, Brocade, Infoblox, Barracuda, Forcepoint, SkyHigh, ADVA, Mitel.

Celkový počet Windows Desktop (Windows 10 a 11) je 1600. Z toho približne 500 je trvalo dostupných PC a 1100 je notebookov, ktoré sa pripájajú podľa potreby.

### 2.3 Zoznam technologických služieb IT, ku ktorým sa pristupuje prostredníctvom privilegovaných účtov

LogRhythm

Flowmon

NetMon

Tenable SC

Sandbox – Trellix

DB Oracle

Oracle APEX

DB MS SQL

MS SSAS

DB MS SSIS

DB MS ReportServer

PowerBI ReportServer

Red Hat SSO

Red Hat JBoss

Tomcat

SpringBoot

VMware vCenter

VMware Horizon + AppVolume

NetBackup

Veeam M365 Bkp

MS Active Directory

MS Entra

MS IIS

FortiClient EMS server (cloud)

HP Proactive Insights

Lotus Notes

Zoznam uvedených technologických služieb nemusí byť úplný a môže byť počas prípravy DNR doplnený o ďalšie technologické služby.

### 2.4 Zoznam zákazníckych služieb IT, ku ktorým sa pristupuje prostredníctvom privilegovaných účtov

Celkový počet zákazníckych služieb je cca 220. Nižšie uvádzame tie, ktoré nevyužívajú autentifikačné mechanizmy niektorej z technologických služieb uvedených v bode 2.3. Zoznam nemusí byť úplný a môže byť počas prípravy DNR doplnený.

CA Service Desk Manager:

* CA Web Screen Painter
* CMDB Visualizer Admin Console
* CA SAP Bussiness Objects,
* CA SAP Bussiness Intelligence,
* CA SAP Universe Designe Tool
* TIBCO Jaspersoft

TRAP – Php / custom Webklient JavaFX (klient)

SIPS – custom Webklient JavaFX (klient)

EBS – Grails / Groovy / custom Webklient JavaFX (klient)

Excalibur

Swift Alliance Access

MDM – Ivanti MobilIron

IBFO – Wall Street Suite

FINU – SAP suite

EBOS - custom klient pre Windows

Personalistika a mzdy - custom klient pre Windows

Dispečér - custom klient pre Windows

Microsoft Endpoint Configuration Manager - custom klient pre Windows

SEPA Engine - Oracle SQL Developer

### 2.5 Rozhrania a protokoly

RDP

SSH

Https

ftps

sftp

SQL over TCP (TCP port 1433)

RPC Port-mapper (initial connection to WMI to locate provider system) (TCP port 135)

SSKS 7770 (license a admin tool)

jdbc (OCI/thin)

Oracle Net Stack

WMI

WS-Management (WinRM)

Zoznam rozhraní nemusí byť konečný, môže byť počas prípravy DNR rozšírený.

## Požiadavky na implementáciu systému SPÚ

Od úspešného uchádzača verejný obstarávateľ požaduje naimplementovanie produkčného aj testovacieho prostredia systému SPÚ v infraštruktúre NBS.

Pre produkčné prostredie dodá uchádzač dva kusy HW appliance, ktoré budú implementované v hlavnom a záložnom technologickom pracovisku (HTP, ZTP) verejného obstarávateľa a na ktorých bude prevádzkovaná minimálne služba vault a tiež sa na ňu budú ukladať nahrávky a ich metadáta realizované systémom SPÚ. HW appliance musia byť osaditeľné do štandardného 19 palcového racku a ich výška nepresiahne 2U. Konfigurácia HW appliance musí byť navrhnutá tak, aby splňovala požiadavky na dostupnosť služby a výkon potrebný pre požadovaný rozsah nasadenia. Súčasťou dodávky bude aj HW podpora pre HW appliance s parametrami podpory určenými uchádzačom tak, aby bolo pri poruche HW možné dodržať požadované SLA pre systém SPÚ. V prípade, že súčasťou HW appliance nie je operačný systém, musí byť aj tento samostatnou súčasťou dodávky. Ostatné komponenty systému SPÚ môžu byť prevádzkované na HW appliance, alebo budú realizované vo forme virtuálnych appliance vo virtuálnej VMware infraštruktúre verejného obstarávateľa. Virtuálne servery pre tento účel poskytne uchádzačovi verejný obstarávateľ. V prípade, že súčasťou virtuálnej appliance nie je operačný systém, musí byť aj tento samostatnou súčasťou dodávky.

Produkčné prostredie systému SPÚ bude implementované v režime vysokej dostupnosti (HA), model hot/standby, synchrónny mód. Primárne uzly budú appliance umiestnené na HTP, standby appliance budú umiestnené na ZTP, failover vrátane presmerovania používateľov automatizovaný. Pre účely disaster recovery vault-u poskytne verejný obstarávateľ virtuálny server v ďalšom nezávislom pracovisku verejného obstarávateľa, pričom tento vault bude prevádzkovaný v režime cold standby so synchronizáciou vykonávanou jeden krát denne. Tento virtuálny server bude možné využiť aj na účely automatizácie failover procesu ak to bude potrebné. Uchádzač dodá aj proces s popisom. Pre automatické presmerovanie používateľov je tiež možné využiť službu f5 appliance (loadbalancing, failover) verejného obstarávateľa.

Správu všetkých appliance pre systém SPÚ bude aj počas bežnej prevádzky zabezpečovať uchádzač v plnom rozsahu. Konfiguráciu úložiska na HW appliance navrhne uchádzač tak, aby zabezpečil retenciu nahrávok v dĺžke jedného roka. Konfiguráciu všetkých appliance navrhne uchádzač tak, aby naplnil výkonnostné požiadavky a požiadavky na SLA verejného obstarávateľa.

Testovacie prostredie musí mať plnohodnotnú funkcionalitu, ale bez potreby plnenia požiadaviek na výkon, dostupnosť (nie je požadované HA) a rozsah produkčného prostredia, t. j. pri minimalistických HW a SW licenčných nákladoch. Pre účely prevádzky testovacieho prostredia poskytne verejný obstarávateľ výpočtové prostriedky vo vlastnej virtuálnej infraštruktúre. Prostredie bude prevádzkované trvale počas prevádzky Produkčného prostredia a bude slúžiť pre potreby školení a testovania pri nasadzovaní nových funkcionalít, úpravách či updatovaní systému SPÚ.

Súčasťou implementácie systému SPÚ bude:

* Analýza prostredia infraštruktúry verejného obstarávateľa v rozsahu potrebnom pre vytvorenie DNR.
* Vytvorenie detailného návrhu riešenia (v texte aj „DNR“) dodávaného systému, zapracovanie pripomienok verejného obstarávateľa do DNR.
* Dodávka SW licencií a ich maintenance/ subskripcií pre požadovaný počet používateľov/ účtov/ koncových systémov a implementované funkcionality.
* Analýza koncových systémov, ktorej výstupom bude vytvorenie dokumentu/ zadania pre budúcu implementáciu secrets managementu (implementácia secrets managementu nie je predmetom tohto obstarávania; verejný obstarávateľ požadujem od uchádzača ponúknúť taký SW produkt, ktorý umožní implementáciu secrets managemetu) s využitím SW produktu, ktorý je súčasťou ponuky, maximálne množstvo koncových systémov, ktoré je potrebné zanalyzovať je 220. Počas analýzy je potrebné najmä posúdiť možnosť integrácie koncových systémov do secrets managementu bez závažných úprav na strane koncového systému a v prípade, že možná je, tak s využitím akej technológie. Výstup analýzy by mal obsahovať zoznam systémov, ktoré nie je možné integrovať so zdôvodnením prečo to nie je možné, zoznam systémov u ktorých integrácia možná je a akou technológiou a tiež zoznam všetkých technologických účtov, ktoré sú využívané v koncových systémoch.
* Nasadenie systému SPÚ v požadovanom rozsahu a v rozsahu požadovaných funkcionalít, v súlade s DNR, najmä však:
* vytvorenie katalógu roly pre používateľov
* vytvorenie zoznamu privilegovaných účtov
* vytvorenie prístupovej matice, ktorá mapuje katalóg roly so zoznamom privilegovaných účtov a zadefinovanie úrovne prístupov na koncové systémy pre jednotlivé roly, príp. jednotlivých používateľov
* vytvorenie používateľov, účtov, roly a koncových systémov
* vytvorenie privilegovaných prístupov
* vytvorenie základných reportov a dashboardov
* zrealizovanie integrácií systému SPÚ na iné služby IT verejného obstarávateľa
* vytvorenie a popísanie procesov súvisiacich so systémom SPÚ
* dodanie dokumentácie k systému SPÚ
* Testovanie systému SPÚ a príprava na akceptáciu diela
* Školenie pre používateľov systému SPÚ – separátne, pre každú z definovaných roly v systéme SPÚ – v rozsahu potrebnom k vykonávaniu bežných prevádzkových úkonov jednotlivých roly
* Projektový manažment na strane dodávateľa počas celej doby trvania projektu

Súčasťou implementácie nie je:

* Implementácia centralizovanej správy secrets (secrets management), jej realizácia bude vykonaná samostatným projektom neskôr, SW produkt ju ale musí umožňovať.

**Požiadavky na reporty a dashboardy**

1. Uchádzač zrealizuje maximálne 3 custom reporty a 1 dashboard podľa požiadaviek verejného obstarávateľa, ktoré budú zo strany verejného obstarávateľa špecifikované po zrealizovaní školení.

**Požiadavky na integráciu s inými službami IT verejného obstarávateľa**

1. so skenerom zraniteľností - systém SPÚ musí umožniť využitie účtov spravovaných v systéme SPÚ na skenovanie zraniteľností integrovaných systémov (Windows, SSH, Oracle credentials a pod.),
2. s  Monitoringom bezpečnosti IT (systém slúžiaci na zber a vyhodnocovanie auditných a bezpečnostných udalostí v informačných systémoch a infraštruktúrach IS) – logovanie auditných záznamov o využívaní privilegovaných účtov, prístupu k heslám,
3. s Monitoringom infraštruktúry IT (centrálny systém Zabbix pre operačný monitoring infraštruktúry IT a informačných systémov),
4. so systémom pre multifaktorovú autentifikáciu (MFA) verejného obstarávateľa v prípade, že bude požadovaná obstarávateľom v čase vytvárania DNR.

**Požiadavky na procesy**

1. Popísať proces pre riadenie účtov, používateľov a roly a popísať autorizačné pravidlá.
2. Popísať proces životného cyklu privilegovaných prístupov.
3. Popísať schvaľovacie procesy súvisiace so životným cyklom privilegovaných prístupov.
4. Popísať prevádzkový proces  k správe privilegovaných prístupov pre správcov systému SPÚ.
5. Popísať break glass proces pre disaster recovery prístup ku cold vault-u.

**Požiadavky na dokumentáciu k systému SPÚ**

Dokumentáciu systému SPU je nutné vypracovať v súlade s internými požiadavkami verejného obstarávateľa (verejný obstarávateľ má preddefinované vzorové formuláre), ku kľúčovým dokumentom patria najmä:

1. Detailný návrh riešenia (DNR)
2. Používateľská dokumentácia
3. Technická dokumentácia
4. Inštalačná dokumentácia
5. Administrátorská dokumentácia
6. Dokumentácia pre školenia

# 4. Servisné služby

### 4.1 Prevádzková doba systému SPU

Systém SPÚ bude prevádzkovaný nepretržite 24 hodín denne.

### 4.2 Členenie servisných služieb

Servisné služby členíme na:

* Služby podpory a údržby, ktoré sú zahrnuté v pravidelných paušálnych poplatkoch, fakturovaných štvrťročne,
* Implementačné a konzultačné služby, ktoré sa realizujú na objednávku v množstve vyjadrenom v osobohodinách, maximálne množstvo hodín implementačných a konzultačných služieb počas trvania servisnej zmluvy nepresiahne 3000 hodín,
* Rozširovanie systému SPÚ.

### 4.3 Podpora, údržba a implementačné služby - popis

Popis jednotlivých služieb je uvedený v nasledovnej tabuľke:

|  |  |  |
| --- | --- | --- |
| **ID** | **Oblasť (proces)** | **Služba** |
| P-1 | Podpora | Poskytovanie poradenstva (telefonicky, elektronickou poštou, prostredníctvom IS Service Desk) súvisiacich s problematikou bežnej prevádzky dodaného systému a jeho častí ako aj s chybovými hláseniami systému, funkcionality dodaného systému, administrácie dodaného systému |
| P-2 | Podpora | Sledovanie a vyhodnocovanie aktualizácií softvéru, poskytovanie informácií objednávateľovi o nových verziách a opravách programového vybavenia dodaného informačného systému a použitých softvérov tretích strán spolu s odporúčaním na ich aplikovanie, vrátane predkladania návrhov na zlepšenie výkonnosti a možností rozvoja |
| P-3 | Podpora | Poskytovanie poradenstva (prostredníctvom IS Service Desk) súvisiacich s postupmi pri zmenách konfigurácie dodaného systému |
| P-4 | Podpora | Sledovanie operačného stavu a výkonnosti dodaného systému s využitím natívnych nástrojov dodaného systému a operačného monitoringu objednávateľa, do ktorého bude poskytovateľovi zriadený potrebný prístup (proaktívny monitoring) |
| P-5 | Podpora | Nahlasovanie akéhokoľvek **bezpečnostného zistenia** ihneď po jeho identifikácii **Pozri bod 1.2 a,** |
| P-6 | Podpora | Súčinnosť pri výskyte **bezpečnostného incidentu** **pozri body 1.2 b, c, d , e, f,**  |
| P-7 | Podpora | Súčinnosť pri výskyte **bezpečnostnej hrozby****pozri body 1.2 b. c. f,** |
| P-8 | Podpora | Súčinnosť pri výskyte **podozrivej udalosti****pozri body 1.2 b, c, f,** |
| P-9 | Podpora | Posudzovanie návrhov objednávateľa na malé zmeny nastavenia a konfigurácie dodaného systému ako aj konzultácie v rozsahu do 8 osobohodín / 1 požiadavka na zmenu |
| U-1 | Údržba | Riešenie a odstránenie prevádzkových aj bezpečnostných incidentov klasifikovaných. ako: **„Zásadný incident**“ a obnova riadnej prevádzky buď výkonom činností na mieste, po vzájomnej dohode objednávateľa a poskytovateľa zabezpečeným vzdialeným prístupom |
| U-2 | Údržba | Riešenie a odstránenie prevádzkových aj bezpečnostných incidentov klasifikovaných ako: **„Závažný incident**“ a obnova riadnej prevádzky buď výkonom činností na mieste, po vzájomnej dohode objednávateľa a poskytovateľa zabezpečeným vzdialeným prístupom |
| U-3 | Údržba | Riešenie a odstránenie prevádzkových aj bezpečnostných incidentov klasifikovaných ako: **„Nepodstatný incident“** buď výkonom činností na mieste, po vzájomnej dohode objednávateľa a poskytovateľa zabezpečeným vzdialeným prístupom |
| U-4 | Údržba | Nasadzovanie opravných balíčkov (patch) a aktualizácií do všetkých komponentov dodaného systému, nasadzovanie odsúhlasuje poverený pracovník objednávateľa |
| U-5 | Údržba | Zaznamenávanie prevádzkových a bezpečnostných incidentov identifikovaných poskytovateľom ihneď po identifikovaní, do ticketovacieho nástroja verejného obstarávateľa v prípade, že incident ešte nebol identifikovaný a zaznamenaný pracovníkmi objednávateľa. |
| K-1 | Konzultácia | Konzultácie priamo na pracovisku objednávateľa alebo online |
| S-1 | Skolenie | Školenie k dodanému systému, prípadne jeho ľubovoľnej časti podľa požiadaviek uvedených v objednávke (školenie sa vykoná v priestoroch objednávateľa, pokiaľ sa objednávateľ s poskytovateľom nedohodnú inak) |
| I-1 | Implementácia | Vykonať predbežnú analýzu a vypracovať písomnú ponuku na funkčnú analýzu požiadavky a na návrh riešenia |
| I-2 | Implementácia | Vykonať funkčnú analýzu požiadavky a vypracovať návrh riešenia  |
| I-3 | Implementácia | Realizácia požiadavky, aktualizácia sprievodnej dokumentácie dodaného systému |

|  |
| --- |
| **Popis kategórie incidentov** |
| **Závažnosť/typ incidentu** | **Popis naliehavosti incidentu** |
| Zásadný prevádzkový incident | Do tejto klasifikácie spadajú všetky neplánované výpadky prevádzky IS oznámené poskytovateľovi objednávateľom, u ktorých sa riešením incidentu zistí, že je spôsobený vážnou chybou alebo nedostatkom IS a táto chyba a/alebo nedostatok zabraňuje jeho riadnemu používaniu v prevádzke nasledovne:1. Aplikačné funkcie systému nie sú funkčné ako celok, alebo ide o takú chybu alebo nedostatok IS, ktorý neumožní úspešne realizovať bankové procesy v NBS podporované IS alebo
2. Aplikačné funkcie IS, prostredníctvom ktorých sa realizujú časovo závislé bankové procesy súvisiace najmä s hotovostnými, majetkovými prevodmi a účtovnými procedúrami, nie sú úplne funkčné, alebo
3. Aplikačné funkcie IS, ktoré majú priamy dopad na riadny chod NBS, nie sú funkčné.
 |
| Závažný prevádzkový incident | Do tejto klasifikácie spadajú všetky neplánované výpadky prevádzky IS oznámené poskytovateľovi objednávateľom, u ktorých sa riešením incidentu zistí, že je spôsobený chybou alebo nedostatkom IS a táto chyba a/alebo nedostatok zabraňuje jeho plnohodnotné používanie v prevádzke nasledovne:1. Aplikačné funkcie IS neumožňujú vykonanie činnosti a/alebo vytvorenie výstupov, ktoré NBS potrebuje na splnenie svojich záväzkov voči externým subjektom,
2. Aplikačné funkcie IS, prostredníctvom ktorých sa realizujú časovo závislé bankové procesy súvisiace najmä s hotovostnými, majetkovými prevodmi a účtovnými procedúrami, nie sú čiastočne funkčné.
 |
| Nepodstatný prevádzkový incident | Do tejto klasifikácie spadajú všetky neplánované výpadky prevádzky IS oznámené poskytovateľovi objednávateľom, ktoré nie sú klasifikované ako závažné alebo zásadné incidenty. Incidenty tejto klasifikácie síce obmedzujú používanie systému ale v zásade neobmedzujú základné funkcie a prevádzku tohto IS. |

* 1. **Bezpečnostnými zisteniami** sú podľa stupňa významu (utriedené od najvyššieho po najnižší):
	2. **bezpečnostný incident,**
	3. **bezpečnostná hrozba,**
	4. **podozrivá udalosť.**

Uvedené pojmy súbližšiedefinované v Prílohe č. 5: Slovník pojmov Servisnej zmluvy.

* 1. Nahlasovanie a poskytovanie súčinnosti zo strany Poskytovateľa pri riešení bezpečnostných zistení:
		1. Poskytovateľ sa zaväzuje nahlásiť akékoľvek bezpečnostné zistenie ihneď po jeho identifikácii,
		2. Poskytovateľ sa zaväzuje poskytnúť súčinnosť pri identifikácií a analýze bezpečnostného zistenia  v rozsahu potrebnom na jeho detailnú identifikáciu, zistenie času vzniku a trvania, rozsahu a príčiny,
		3. Poskytovateľ sa zaväzuje poskytnúť súčinnosť pri návrhu opatrení a termínov na odstránenie bezpečnostného zistenia, a takisto identifikovať prípadné dopady navrhnutých opatrení na funkčnosť a prevádzku systému,
		4. Poskytovateľ sa zaväzuje poskytnúť súčinnosť pri kontrole a identifikácii zmien v IT infraštruktúre a IS objednávateľa po narušení bezpečnosti **(platí len pre bezpečnostné incidenty)**,
		5. Poskytovateľ sa zaväzuje poskytnúť súčinnosť pri odstránení následkov vyplývajúcich z narušenia bezpečnosti **(platí len pre bezpečnostné incidenty)**,
		6. Poskytovateľ sa zaväzuje poskytnúť súčinnosť pri návrhu a realizácii opatrení na zamedzenie opakovania bezpečnostného zistenia v termíne na základe vzájomnej dohody.

### 4.4 Podpora, údržba a implementačné služby – úroveň služieb

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Dostupnosť služby** | **Frekvencia vykonávania / Lehota na reakciu** | **Lehota na vykonanie služby** |
| P-1 | 5x9 (7.00-16.00)pracovné dni | podľa potreby | do 48 hodín od prijatia žiadosti |
| P-2 | 5x9 (7.00-16.00)pracovné dni | priebežne, minimálne raz mesačne vo forme reportu zaslaného formou emailu | - |
| P-3 | 5x9 (7.00-16.00)pracovné dni | podľa potreby | do 48 hodín od prijatia žiadosti |
| P-4 | 5x9 (7.00-16.00)pracovné dni | priebežne | - |
| P-5 | 5x9 (7.00-16.00)pracovné dni | Ihneď | - |
| P-6 | 5x9 (7.00-16.00)pracovné dni | v potrebnom rozsahu | do 48 hodín od prijatia žiadosti |
| P-7 | 5x9 (7.00-16.00)pracovné dni | v potrebnom rozsahu | do 48 hodín od prijatia žiadosti |
| P-8 | 5x9 (7.00-16.00)pracovné dni | v potrebnom rozsahu | do 48 hodín od prijatia žiadosti |
| P-9 | 5x9 (7.00-16.00)pracovné dni | v potrebnom rozsahu | do 48 hodín od prijatia žiadosti |
| U-1 | 5x16 (6.00-22.00**)**pracovné dni | do 2 hodín od prijatia žiadosti | do 8 hodín od prijatia žiadosti |
| U-2 | 5x16 (6.00-22.0**0**)pracovné dni | do 4 hodín od prijatia žiadosti | do 24 hodín od prijatia žiadosti |
| U-3 | 5x9 (7.00-16.00)pracovné dni | do 8 hodín od prijatia žiadosti | do 72 hodín od prijatia žiadosti |
| U-4 | 5x9 (7.00-16.00)pracovné dni | do 8 hodín od odsúhlasenia | do 72 hodín od odsúhlasenia ak nie je dohodnuté inak |
| U-5 | 5x9 (7.00-16.00)pracovné dni | ihneď po identifikovaní | - |
| K-1 | 5x9 (7.00-16.00)pracovné dni | do 4 hodín od prijatia žiadosti | podľa objednávky |
| S-1 | 5x9 (7.00-16.00)pracovné dni | do 4 hodín od prijatia žiadosti | podľa objednávky |
| I-1 | 5x9 (7.00-16.00)pracovné dni | do 8 hodín od prijatia žiadosti | do 72 hodín od prijatia žiadosti ak nie je s obstarávateľom dohodnuté inak |
| I-2 | 5x9 (7.00-16.00)pracovné dni | do 8 hodín od prijatia žiadosti | do 72 hodín od prijatia žiadosti ak nie je s obstarávateľom dohodnuté inak |
| I-3 | 5x9 (7.00-16.00)pracovné dni | do 24 hodín od prijatia žiadosti | podľa objednávky |
|  |  |  |  |

Pri poskytovaní služby Údržba je Lehota služby záväzná aj v prípade, ak by pri jednotlivých činnostiach služby Údržba požadovaných objednávateľom počas Dostupnosti služby malo jej dodržanie prekročiť hornú hranicu stanovenej pracovnej doby.

### 4.5 Rozsah systému SPÚ

Uchádzač dodá počas trvania zmluvy maximálne nasledovný rozsah/počet systému SPÚ:

* 15 interných používateľov,
* 35 externých používateľov.

# Prístup k realizácii projektu

Verejný obstarávateľ požaduje od uchádzača, aby bol projekt riadený na základe metodiky, ktorú určuje pracovný predpis NBS č. 20/2020 o projektovom riadení. Projektové témy, ktoré nie sú priamo upravené vyššie uvedenou metodikou budú realizované v súlade s PRINCE2 metodikou.

Predpis č. 20/2020 o projektovom riadení je samostatnou prílohou súťažných podkladov.

Obstarávateľ požaduje, aby uchádzač v rámci ponuky vypracoval projektový plán a v priebehu projektu aktualizoval plán projektu pre realizáciu jednotlivých projektových výstupov.

Uchádzač navrhne projektový plán, ktorý zabezpečí dodanie manažérskych a špecializovaných produktov podľa jednotlivých etáp s cieľom naplnenia zadania projektu a ktorý bude reflektovať projektové závislosti, riziká a kapacity.

Verejný obstarávateľ požaduje, aby uchádzač v priebehu projektu vypracoval aj plány jednotlivých etáp projektu.

Verejný obstarávateľ požaduje, aby uchádzač v jednotlivých plánoch uviedol požiadavky na súčinnosť objednávateľa pre dané výstupy a iné externé závislosti (napr. z iných projektov), vrátane kalkulácie požadovaných kapacít na strane objednávateľa podľa pozícií.

Projektový plán a etapové plány požaduje objednávateľ vypracovať vo formáte MS Project.

Verejný obstarávateľ požaduje, aby uchádzač pri príprave časového harmonogramu počítal so schvaľovacím procesom na strane verejného obstarávateľa:

* 15 pracovných dní v prípade schválenia dokumentácie (v závislosti od rozsahu);
* 20 pracovných dní v prípade schválenia ostatných výstupov (v závislosti od rozsahu).

##

## Projektové aktivity a výstupy – sumárny prehľad

Objednávateľ požaduje, aby poskytovateľ v rámci plnenia predmetu dodávky dodal práce a služby, manažérske a špecializované produkty, dokumentáciu a zmluvné dodávky podľa jednotlivých etáp projektu (štruktúra reflektuje Pracovný predpis o projektovom riadení v Národnej banke Slovenska) a zároveň reflektuje základné usmernenia a pravidlá ECB a ESCB. Uvedené produkty budú dodané v slovenskom jazyku. Odklon od nižšie uvedeného zoznamu projektových výstupov je možný po vzájomnej dohode oboch strán.

### Zmluvné dodávky

Zmluvné dodávky projektu predstavujú:

1. dodávaná služba realizovaná v zmysle požiadaviek na riešenie,
2. projektová dokumentácia,
3. sprievodná dokumentácia dodávaného systému,
4. dokumentácia týkajúca sa integračných rozhraní,
5. zmluvne stanovené práce a služby
6. prínosy systému budú prezentované dodávateľom úvodom projektu pre zainteresované strany projektu (riadiaca rada, projektový tím).

### Riadená projektová dokumentácia (manažérske produkty)

Rozsah manažérskych produktov je stanovený internou projektovou metodikou a obsahuje najmä nasledovné produkty dodávané v súlade s harmonogramom jednotlivých fáz a etáp projektu:

* Projektový iniciálny dokument (PID) vrátane komunikačnej stratégie
* Organizačné zabezpečenie projektu (súčasť PID)
* Stratégia testovania
1. Projektové plány
	* + Detailný Plán projektu
		+ Plán etapy migrácie údajov
		+ Plán školení personálu
		+ Plán testovania dodávaného riešenia
		+ Plán testovania systému na migráciu údajov
		+ Plán testovania integračných rozhraní, plán testovania z pohľadu systémovej integrácie
		+ Plán skúšobnej prevádzky
		+ Detailný roll-out plán riešenia
2. Správy o stave realizácie projektu
	* + Správa o stave realizácie projektu
		+ Správa o testovaní dodávaného systému
		+ Správa o skúšobnej prevádzke
		+ Správa o ukončení projektu
		+ Správa o získaných poznatkoch (Lessons learned)
3. Prijímacie protokoly spracované pri dodaní systému
	* + Protokoly o funkčnom testovaní (priebežne počas testovania)
		+ Protokoly o integračnom testovaní
		+ Protokoly o migračnom testovaní
		+ Akceptačný protokol testovania
		+ Akceptačný protokol integračných rozhraní
		+ Akceptačný protokol migračného testovania
		+ Akceptačný protokol nasadenia do skúšobnej prevádzky
		+ Akceptačný protokol nasadenia do bežnej prevádzky
		+ Protokol o splnení a dokončení predmetu zmluvy
4. Katalógy riadenia jednotlivých oblastí projektu
* Katalóg rizík,
* Katalóg požiadaviek,
* Katalóg nedostatkov,
* Katalóg otvorených otázok
* Katalóg zmenových požiadaviek
1. Ostatné manažérske produkty
	* + Zoznam úloh, zodpovedností a termínov plnenia (t.j.To-Do list)
		+ Príprava prezentácií na projektové stretnutia
		+ Zápisy z projektových stretnutí
		+ Správa o stave projektu na týždňovej báze
		+ Prehľad plnenia plánu vo formáte MS Project (súčasť Správy o stave projektu)
		+ Správa o stave a riadení projektových rizík na mesačnej báze

### Sprievodná dokumentácia (špecializované produkty)

Rozsah špecializovaných produktov je daný samotným zadaním a projektu a obsahuje najmä nasledovné výstupy:

* 1. Vývojová dokumentácia dodávaného systému
		+ Rozdielová analýza
		+ Detailný návrh riešenia (DNR)
		+ Detailný návrh riešenia a funkčný prototyp systému pre migráciu
		+ Prístup k testovaniu (súčasť Testovacej stratégie)
		+ Migračná stratégia
		+ Integračná dokumentácia

Detailný návrh riešenia bude v súlade politikami a usmerneniami NBS, ESCB, zákonmi a predpismi.

* 1. Ostatná projektová dokumentácia
		+ Prevádzkový poriadok dodávaného systému
		+ Zoznam licencií
		+ Informácie, podklady a vysvetlenia
	2. Používateľská dokumentácia dodávaného systému
		+ Používateľská príručka dodávaného systému
		+ Príručka správy a prevádzky dodávaného systému
		+ Integračný manuál
	3. Inštalačná dokumentácia
		+ Inštalačná a konfiguračná príručka dodávaného systému
		+ Inštalačná a konfiguračná príručka systému na migráciu údajov
		+ Príručka migrácie údajov
	4. Technická dokumentácia
	5. Prevádzková dokumentácia

Spôsob výkonu požadovaných činností

* + Pre pracovníkov uchádzača bude zriadený vzdialený prístup s využitím VPN verejného obstarávateľa v rozsahu, aby mohli vykonávať požadované činnosti.
	+ Všetky činnosti, u ktorých je to požadované verejným obstarávateľom budú realizované na pracovisku verejného obstarávateľa (on-premise).
	+ Prístup k systému SPÚ bude možný výhradne s využitím VPN verejného obstarávateľa, alebo z pracoviska verejného obstarávateľa.

# Iné požiadavky verejného obstarávateľa na predmet zákazky:

Verejný obstarávateľ požaduje, aby uchádzač v ponuke predložil potvrdenie od výrobcu ponúkaného softvéru, že:

1. ponúkaný softvér pochádza od autorizovaného distribútora z oficiálnej distribučnej siete výrobcu na území Európskeho hospodárskeho priestoru a
2. ponúkaný softvér je určený pre trh Európskeho hospodárskeho priestoru a
3. ponúkaný softvér nemá ohlásený dátum ukončenia životnosti (End of Life) alebo predaja (End of Sale).