**PRIESKUM TRHU pre účely URČENIA PREDPOKLADANEJ HODNOTY ZÁKAZKY**

**VÝZVA NA PREDLOŽENIE INDIKATÍVNEJ PONUKY**

podľa § 6 ods. 1 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení

niektorých zákonov v znení neskorších predpisov

**1. Identifikácia verejného obstarávateľa :**

Názov: Úrad geodézie, kartografie a katastra Slovenskej republiky

Sídlo: Chlumeckého 2, 812 20 Bratislava

IČO: 00166260

Štatutárny orgán: Ing. Ján Mrva - predseda

Internetová adresa organizácie (URL): http://www.skgeodesy.sk/sk/ugkk/

Kontaktná osoba: Mgr. Martin Nociar

Telefón +421 2 2081 6063

e-mail: martin.nociar@skgeodesy.sk

Profil VO: http://www.uvo.gov.sk/vyhladavanie-profilov/zakazky/676

Profil zákazky: https://eo.eks.sk/ElektronickaTabula/Sukromna/1799

**2. Názov predmetu zákazky**

*Prieskum trhu (PHZ) – „Návrh organizačných a technických opatrení riadenia informačnej bezpečnosti v súlade s požiadavkami zaistenia kybernetickej bezpečnosti a ochrany osobných údajov v zmysle európskej a národnej legislatívy.“*

**3. Druh zákazky:**

Tovary Služby Práce

**4. Kód CPV:**

**72310000-1 Spracovanie údajov**

**79417000-0 Bezpečnostné poradenstvo**

**71241000-9 Štúdia realizovateľnosti, poradenská služba, analýza**

**72220000-3 Systémové a technické poradenstvo**

**72316000-3 Analýza údajov**

**72222300-0 Služby informačných technológií**

**5. Stručný opis predmetu zákazky:**

Predmetom zákazky je vypracovanie a aktualizácia riadiacej, prevádzkovej dokumentácie a návrh a realizáciu opatrení pre potreby ÚGKK podľa slovenských a európskych legislatívnych požiadaviek, predovšetkým:

Požiadavky kladené na informačné technológie verejnej správy v zmysle Zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „Zákon o ITVS“)

Požiadavky zaistenia kybernetickej bezpečnosti v zmysle Zákona č. 69/2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „Zákon o KB“) a nadväzujúcich vyhlášok Národného bezpečnostného úradu, najmä vyhlášky č. 362/2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „Vyhláška o BO KB“).Bližšia špecifikácia predmetu obstarávania je uvedená v prílohe č. 1 tejto výzvy.

**6. Hlavné miesto poskytovania služieb: Úrad geodézie, kartografie a katastra Slovenskej**

**republiky, Chlumeckého 2, 812 20 Bratislava, Slovenská republika**

**7. Spôsob určenia ceny:**

Do indikatívnej cenovej kalkulácie požaduje verejný obstarávateľ zahrnúť všetky náklady

spojené s poskytnutím predmetu zákazky (napr. palivový poplatok, telekomunikačný

poplatok, mýtny poplatok a pod.).

Indikatívna cena za predmet zákazky musí byť pre účely predpokladanej hodnoty zákazky

stanovená v zmysle zákona č. 18/1996 Z. z. o cenách v znení neskorších predpisov. Indikatívna cena musí byť v súlade s § 2 citovaného zákona o cenách založená na cene obchodného alebo sprostredkovateľského výkonu, ekonomicky oprávnených nákladoch a primeranom zisku. Indikatívna cena musí byť vyjadrená v eurách v súlade so zákonom č. 659/2007 Z. z. o zavedení meny euro v Slovenskej republike a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a Vyhlášok č. 97/ 2008 Z . z. a 75/2008 Z. z. Návrh indikatívnej ceny musí obsahovať všetky náklady spojené s plnením predmetu zákazky.

Pri tvorbe ceny je potrebné zohľadniť aj:

- primeranosť jej stanovenia na základe jemu vzniknutých nákladov a primeranosť zisku,

- lehoty dodania,

- spôsob zadávania zákazky na realizáciu predmetu zákazky.

Ak je uchádzač platcom dane z pridanej hodnoty (ďalej len “DPH”), navrhovanú cenu uvedie:

- Navrhovaná celková cena bez DPH,

- Sadzba DPH v % a vyčíslená hodnota DPH,

- Navrhovaná celková cena vrátane DPH.

Ak uchádzač nie je platcom DPH, na skutočnosť, že nie je platcom DPH, upozorní označením

„Nie som platcom DPH“. Verejný obstarávateľ požaduje v indikatívnej ponuke uviesť aj odhadovanú prácnosť realizácie predmetu zákazky v človekohodinách.

**Cenovú ponuku zasielajte vo forme vyplnenej tabuľky „Príloha č. 2 – Indikatívna cenová**

**ponuka“.**

**8. Lehota na predkladanie ponuky**

Lehota na predkladanie ponúk je do: 08.12.2020 do 12:00 hod.

**9. Spôsob predloženia indikatívnej cenovej ponuky**

Elektronicky prostredníctvom systému EO EKS, a to zaslaním správy v profile zákazky

uvedenom v bode 2. tejto výzvy.

**10. Ďalšie súvisiace informácie:**

10.1 Podmienky financovania:

Verejný obstarávateľ uhradí cenu za predmet zákazky na

základe predloženej faktúry/faktúr zhotoviteľa. Splatnosť faktúr je 30 kalendárnych dní odo dňa doručenia. Verejný obstarávateľ neposkytuje zálohové/preddavkové platby.

10.2 Predloženie ponuky je indikatívne a do budúcna nekonštatuje konflikt záujmov a nebráni hospodárskemu subjektu zúčastniť sa zadávania zákazky na vyššie uvedený predmet zákazky po jeho vyhlásení.

**Príloha č. 1**

# Názov zákazky

Návrh organizačných a technických opatrení riadenia informačnej bezpečnosti v súlade s požiadavkami zaistenia kybernetickej bezpečnosti a ochrany osobných údajov v zmysle európskej a národnej legislatívy.

# Zadanie

Predmetom zákazky je vypracovanie a aktualizácia riadiacej, prevádzkovej dokumentácie a návrh a realizáciu opatrení pre potreby ÚGKK podľa slovenských a európskych legislatívnych požiadaviek, predovšetkým:

Požiadavky kladené na informačné technológie verejnej správy v zmysle Zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „Zákon o ITVS“)

Požiadavky zaistenia kybernetickej bezpečnosti v zmysle Zákona č. 69/2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „Zákon o KB“) a nadväzujúcich vyhlášok Národného bezpečnostného úradu, najmä vyhlášky č. 362/2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „Vyhláška o BO KB“).

# Požadovaná riadiaca dokumentácia v oblasti informačnej bezpečnosti.

## Vypracovanie/aktualizácia bezpečnostnej dokumentácie

Bezpečnostná dokumentácia musí byť vypracovaná s ohľadom na prevádzkovanú infraštruktúru IKT, aplikačnú a bezpečnostnú architektúru a implementované bezpečnostné opatrenia, organizačné usporiadanie, pracovné roly, zodpovednosti a rozdelenie právomocí v rámci riadenia operačných rizík rezortu ÚGKK.

### Identifikácia legislatívnych a normatívnych požiadaviek:

Dokumentácia musí obsahovať komplexné posúdenie všetkých legislatívnych a normatívnych požiadaviek kladených na ÚGKK ako prevádzkovateľa základných služieb, ako prevádzkovateľa informačných technológií verejnej správy a ako organizáciu spracúvajúcu osobné údaje svojich zamestnancov, klientov a prípadných tretích osôb. Dokument musí určiť všetky relevantné požiadavky, mapovať ich plnenie v prostredí ÚGKK a stanoviť pravidlá priebežnej kontroly ich dodržiavania.

### Návrh bezpečnostných politík informačnej / kybernetickej bezpečnosti

## Bezpečnostné politiky musia obsahovať základné zásady a ciele v nasledovných oblastiach riadenia IB/KB:

## Organizácia bezpečnosti

## Riadenie bezpečnostných rizík

## Riadenie informačných aktív

## Riadenie dodávateľských vzťahov

## Riadenie vývoja a údržby v oblasti informačno-komunikačných technológií

## Riadenie a prevádzka informačno-komunikačných technológií

1. Riadenie súladu a kontinuity procesov a činností

### Klasifikácia informácií a kategorizácia sietí a informačných systémov

Výstup musí obsahovať zoznam vybraných komponentov sietí a informačných systémov, ktorý identifikuje jednotlivé siete a informačné systémy a ich podporných systémov a podsystémov. Zoznam môže byť v textovej, tabuľkovej alebo grafickej forme a aktíva musia byť klasifikované v súlade s klasifikačnou schémou podľa prílohy č. 2. Vyhlášky o BO KB. Osobitne musia byť ohodnotené osobné údaje spracúvané v jednotlivých informačných systémoch. Zoznam vychádza z **Prílohy č. 1** tohto opisu.

## Vymedzenie rozsahu a spôsobu plnenia opatrení

Predmetom zákazky je vypracovanie a dodanie súborov požadovanej dokumentácie v nasledovnom členení:

1. Organizácia informačnej bezpečnosti, riadenie aktív a rizík
2. Personálna bezpečnosť a riadenie dodávateľov.
3. Riadenie technických zraniteľností, bezpečnosti sietí a informačných systémov, správa riadenie prístupov k informačným systémom, využitie kryptografických mechanizmov
4. Bezpečnostné incidenty, riadenie, monitoring, testovanie a bezpečnostné audity
5. Fyzická bezpečnosť

### Organizácia informačnej bezpečnosti

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

* menovanie a určenie zodpovedností a právomocí manažéra informačnej a kybernetickej bezpečnosti,
* aplikovanie princípu najnižších privilégií, podľa ktorej sú každému používateľovi obmedzené privilégiá v maximálnom rozsahu potrebnom na splnenie pridelených úloh,
* oddelenie zodpovedností a právomocí používateľov,
* aplikovanie zásady nezávislého hodnotenia, merania a preskúmavania efektivity a účinnosti prijatých opatrení na ošetrenie rizík,
* zásady jasného vymedzenia právomoci, povinnosti a zodpovednosti používateľov.

### Riadenie aktív, hrozieb a rizík

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

* inventarizácia všetkých aktív, od ktorých závisí poskytovanie služieb ÚGKK, ,
* identifikácia zodpovedných osôb za inventarizáciu aktív,
* identifikácia vlastníkov aktív,
* identifikácia zraniteľností a hrozieb,
* analýza rizík s ohľadom na identifikované aktíva,
* určenie vlastníkov rizík,
* návrh organizačných a technických bezpečnostných opatrení v závislosti od identifikovaných rizík,
* identifikácia implementovaných bezpečnostných opatrení,
* identifikácia bezpečnostných opatrení, ktoré nebudú implementované spolu s odôvodnením,
* analýza funkčného dopadu,
* návrh postupov pre pravidelné preskúmavanie identifikovaných rizík a v závislosti od toho aktualizácie prijatých bezpečnostných opatrení.

### Personálna bezpečnosť

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

* postupy pri zaradení alebo presune osoby do niektorej z bezpečnostných rolí,
* postupy pri skončení pracovnoprávneho vzťahu alebo iného obdobného pracovného alebo zmluvného vzťahu,
* budovanie bezpečnostného povedomia a plán vzdelávania zamestnancov ÚGKK,
* hodnotenie účinnosti vzdelávania zamestnancov ÚGKK a dodávateľov zastávajúcich niektorú z bezpečnostných rolí,
* kontrola dodržiavania a riešenie prípadov porušenia definovaných bezpečnostných politík, vrátane disciplinárneho postupu pri ich porušení.

### Riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

* popis spôsobu riadenia dodávateľských služieb, akvizície, vývoja a údržby informačných systémov,
* analýzu rizík dodávateľských služieb, akvizície, vývoja a údržby informačných systémov,
* návrh kontrolných a auditných postupov pre overenie dodržiavania bezpečnostných požiadaviek dodávateľmi služieb,
* definovanie obsahu zmluvy s treťou stranou, vývoj a akvizícia siete a informačného systému základnej služby s ohľadom na:
	+ zaistenie kompatibility s existujúcimi sieťami a informačnými systémami a
	+ zachovanie úrovne bezpečnosti ustanovenej v bezpečnostnej stratégii.

### Riadenie technických zraniteľností systémov a zariadení

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

* metódy a nástroje na identifikáciu a ošetrovanie existujúcich zraniteľností SW a HW a využívanie publikovaných informácií (výrobcovia, bezpečnostné organizácie, ...) viď príloha č.1 kapitola 6

### Riadenie bezpečnosti sietí a informačných systémov

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

* Pravidlá pre segmentáciu sietí a riadenie komunikácie medzi segmentami, blokovanie neautorizovaných portov a návrh segmentácie a komunikačných pravidiel s ohľadom na prevádzkované systémy a technológie v ÚGKK,
* Podmienky pre umiestnenie špecifikovaných služieb do vyhradených segmentov siete,
* Postupy pre bezpečnostnú konfiguráciu serverov,
* ochranu prepojenia medzi internými a externými sieťami, vytváranie black-listov,
* zaistenie bezpečného mobilného a vzdialeného prístupu do interných sietí,
* evidenciu a monitorovanie bezpečnosti všetkých vstupno-výstupných bodov na hranici siete, ochranu pred prienikom a únikom dát,
* ochranu pred škodlivým kódom na zariadeniach, ktoré sa pripájajú do internej siete z externého prostredia,
* zmluvné zaručenie bezpečnosti pripojenia dodávateľov vrátane preukázania plnenia.

### Riadenie bezpečnosti prevádzky siete a informačného systému

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

* riadenie zmien,
* riadenie záplat a aktualizácií,
* riadenie kapacít,
* pravidelné zálohovanie a testovanie obnovy informácií zo záloh,
* ochranu pred škodlivým kódom,
* inštaláciu softvéru a zariadení v sieťach a informačných systémoch,
* zaznamenávanie a vyhodnocovanie prevádzkových a bezpečnostných záznamov.

### Riadenie prístupov

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

* zásady riadenia prístupu k informáciám,
* identifikáciu a autentizáciu používateľov,
* práva a povinnosti používateľov a rolí zodpovedných za riadenie prístupu používateľov,
* riadenie prístupu k sieťam, operačnému systému a jeho službám, prístup k aplikáciám,
* riadenie vzdialeného prístupu,
* monitorovanie prístupov, vedenie prevádzkových záznamov o prístupe do siete a informačného systému,
* vykonávanie pravidelných kontrol prístupových účtov a prístupových oprávnení.

### Používanie kryptografických opatrení

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

* používanie dostatočne odolných kryptografických prostriedkov na zaistenie dôvernosti, integrity, dostupnosti a hodnovernosti údajov v rámci sietí a informačných systémov,
* pravidlá kryptografickej ochrany údajov pri ich prenose alebo uložení v rámci sietí a informačných systémov,
* riadenie a ochranu kryptografických kľúčov a certifikátov počas ich celého životného cyklu,
* využívanie kryptografie pri dvojfaktorovej autentifikácii používateľov,
* vykonávanie kontroly a auditu v tejto oblasti.

### Riešenie bezpečnostných incidentov

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

* detekciu, evidenciu a riešenie bezpečnostných incidentov,
* určenie právomocí a zodpovedností používateľov a zodpovedných rolí,
* postupy hlásenia bezpečnostných incidentov s dosahom na spracúvanie osobných údajov voči orgánu dohľadu a voči dotknutým osobám,
* pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálneho systému včasného varovania.

### Monitorovanie, testovanie bezpečnosti a bezpečnostné audity

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

* bezpečnostný dohľad nad činnosťou sietí, informačných systémov a ich používateľov,
* vytváranie a zaznamenávanie prevádzkových záznamov o
	+ manipulácii s osobnými, chránenými a prísne chránenými informáciami a údajmi alebo s nimi spojenými informačnými aktívami,
	+ iniciácii, akceptácii alebo odmietnutí pripojenia do siete alebo informačného systému,
	+ zmene prístupových práv používateľov,
	+ zmene pravidiel bezpečnostných prvkov,
	+ varovných alebo chybových hláseniach systémov,
	+ podozrivých alebo škodlivých aktivitách a ďalších informáciách nevyhnutných na posúdenie závažnosti kybernetického bezpečnostného incidentu v spojení s kritickosťou danej služby alebo zariadenia,
* ochranu a uchovávanie prevádzkových záznamov,
* určenie zodpovedných rolí za monitorovanie a vyhodnocovanie prevádzkových záznamov, nahlásenie podozrivej aktivity,
* vykonávanie auditu kybernetickej bezpečnosti.

### Riadenie kontinuity procesov

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

* požiadavky na zabezpečenie kontinuity riadenia informačnej a kybernetickej bezpečnosti pri vzniku bezpečnostného incidentu,
* vypracovanie stratégie a krízových plánov na zabezpečenie dostupnosti siete a informačného systému,
* vykonanie analýzy dopadov bezpečnostného incidentu na prevádzkované služby,
* určenie adekvátnych zdrojov na zabezpečenie riadenia kontinuity činností,
* určenie komunikačného plánu spolu s kontaktnými údajmi, určeniami rolí a zodpovednosti,
* určenie cieľovej doby a cieľového bodu obnovy,
* testovanie a vyhodnocovanie procesu riadenia kontinuity činností a realizácie opatrení na zvýšenie odolnosti sietí a informačných systémov základnej služby,
* určenie plánov havarijnej obnovy a postupov zálohovania na obnovu siete a informačného systému,
* pravidelné preverenie záloh, testovanie obnovy záloh a precvičovanie zavedených krízových plánov.

### Fyzická bezpečnosť a bezpečnosť prostredia

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

* technické a organizačné opatrenia na zaistenie fyzickej ochrany siete a informačného systému alebo aspoň ich najdôležitejších komponentov pred nepriaznivými prírodnými
* vplyvmi a vplyvmi prostredia, možnými dôsledkami havárií a fyzickým prístupom nepovolaných osôb,
* požiadavky na bezpečné uloženie fyzických záznamov obsahujúcich citlivé a osobné údaje a podmienky ich archivácie,
* ochranu prevádzkového priestoru v závislosti na kritickosti komponentov,
* kontrolu dodržiavania pravidiel na prácu v zabezpečenom priestore,
* zabezpečenie vhodného prevádzkového prostredia a dodávky podporných služieb,
* požiadavky na kapacity v bezpečne vzdialenom záložnom zabezpečenom priestore,
* zaistenie súladu prevádzky s vnútornými predpismi a zmluvnými záväzkami, zásadu „čistého stola“ a „čistej obrazovky“,
* kontrolu dodržiavania pravidiel,
* životný cyklus a ochranu technických komponentov sietí a informačných systémov a všetkých typov relevantných záloh.

## Analýza rizík

Očakávaným výstupom je dokument, ktorý musí obsahovať posúdenie bezpečnostných rizík vyplývajúcich z hrozieb pôsobiacich na aktíva v správe ÚGKK.

# Osobitné požiadavky

## Posúdenie prevádzkovaných základných služieb

Výstup musí pokrývať identifikáciu a posúdenie prevádzkovaných základných služieb so zvážením súvisiacej infraštruktúry IKT, aplikačnej a bezpečnostnej architektúry a spoločenskej zodpovednosti ÚGKK.

## Návrh bezpečnostnej stratégie kybernetickej bezpečnosti

Bezpečnostná stratégia kybernetickej bezpečnosti musí vychádzať z výsledkov analýzy rizík kybernetickej bezpečnosti a musí obsahovať formuláciu cieľov kybernetickej bezpečnosti a základné princípy na dosiahnutie týchto cieľov, určenie právomocí a zodpovedností za riadenie kybernetickej bezpečnosti, rizík kybernetickej bezpečnosti a aktualizáciu bezpečnostnej dokumentácie.

## Popis existujúceho stavu

V rámci analýzy je potrebné vychádzať z dokumentu prílohy č.1 tohto opisu. V kapitole 6, 7 a 9 je definovaná analýza aktuálneho stavu v rámci ÚGKK a riadených organizácií GKÚ a VÚGK.

V rámci navrhovania technických opatrení ÚGKK preferuje využitie existujúcich systémov monitoringu Zabbix, CA Spectrum, spracovania logov - Splunk log management, systémy pre file sharing – Microsoft SharePoint. Požadujeme aby sa poskytovateľ primárne orientoval na využitie existujúcich systémov a ich prípadné rozšírenie novými modulmi.

V rámci riešenia bude vítaná iniciatíva dodávateľa na konsolidáciu existujúcich supportných systémov a návrh optimalizácie ich vyžitia nielen v oblasti KB. V prípade ak z analýz vystane odporúčanie na implementáciu iného podporného systému, ktorý realizuje špecifický typ činnosti ÚGKK sa nebráni takejto implementácii.

## Súvisiace aktivity

Bezpečnostné opatrenia navrhnuté v rámci tohto obstarania musia byť implementované v rámci existujúceho a súvisiacich obstarávaní a preto je dôležité osobitne špecifikovať technické požiadavky v nasledovných oblastiach:

* WAN siete – požiadavky na nastavenia FW, sledovania perimetra siete, pripojenie vzdialených pobočiek, parametre IPSEC
* VPN prístupy – zabezpečenie a odporúčané spôsoby pripojenia do privátnej siete, obmedzenia prístupov a protokolov
* LAN siete - požiadavky potrebné implementovať v rámci sietí LAN
* Servery – požiadavky potrebné implementovať na úrovni Operačných systémov a aplikácií
* Klientske PC – odporúčania na zabezpečenie pracovných staníc
* WIFI – odporúčania na zabezpečenia wifi sietí s dôrazom na rozdelenie pre Guest siete a privátne siete

## Implementačné aktivity

Existujúce systémy monitorovania a spracovania logov – Zabbix, CA Spectrum, Splunk.

Na základe vzniknutej dokumentácie a popisov existujúceho stavu je požadované od dodávateľa zabezpečiť implementáciu monitoringu a logovania do existujúcich alebo novo špecifikovaných systémov slúžiacich na zber a vyhodnocovanie bezpečnostných udalostí na úrovni sietí, firewalov, serverov, klientskych staníc a ďalších identifikovaných zdrojov udalostí v rámci infraštruktúry ÚGKK.

V rámci implementácie požadujeme návrh rozdelenia rolí, systémov projektov v systémoch monitoringu, stanovenia úrovní tresholdov v rámci delenia hrozieb a manuály na spracovanie incidentov v existujúcich alebo novo implementovaných systémoch

Pre využitie v budúcich projektoch požadujeme od dodávateľa vypracovať implementačný manuál a postup ako pridávať ďalšie potrebné zdroje do systémov monitoringu a logovania udalostí. Implementačný manuál bude k dispozícii pre všetky cieľové existujúce alebo novo implementované podporné systémy.

Príloha č.1 k opisu predmetu zákazky

Dokument – Štúdia\_zabezpečenia\_KB.pdf od spoločnosti Synergon a.s z 5.9.2019. vzhľadom na citlivé informácie obsiahnuté v dokumente tento nie je verejne prístupný. Dokument bude k dispozícii záujemcom v rámci VO na základe podpisu NDA.

Príloha č. 2

( zvlášť dokument )