DataCentrum **Cintorínska 5, 814 88 B r a t i s l a v a**

Úloha č.: ***407***

Identifikačný list úlohy na rok 2022

1. Názov úlohy:

Informačný systém účtovníctva fondov (ISUF)

2. Predmet riešenia:

- prevádzka ISUF,
- používanie a podpora ISUF,
- riadenie prístupov,
- bezpečnostný projekt,
- zálohovanie,
- riadenie SLA (systém riadenia úrovne poskytovania služieb),
- auditné zistenia,
- zabezpečenie nákupu SSL certifikátov.

3. Identifikácia vstupov úlohy:

- detailné riešenie úlohy ISUF (samostatný dokument),
- platná legislatíva EÚ a SR,
- závery vyplývajúce zo zistení vykonaných auditov.

4. Návrh a postup riešenia v nadväznosti na schválený projektový zámer:

- zabezpečenie prevádzkovania a spravovanie produkčného, vývojového, školiaceho a testovacieho systému ISUF:
  - zabezpečenie technickej podpory existujúcich aplikačných systémov, podpora prevádzky infraštruktúry, dostupnosť infraštruktúry 24/7,
  - vykonávanie aktualizácie (patchovanie)operačných systémov serverov ISUF na základe pravidiel prehodnocovania potreby patchovania,
  - aktualizácia procesu riadenia konfigurácie informačných aktivít ISUF,
  - riešenie problémov s dostupnosťou IS v integrovanom prostredí cez SAP PI,
  - monitorovanie prevádzky ISUF, riešenie incidentov pomocou CMP pre systém ISUF,
  - administrácia databázy konfiguračných položiek,
  - aktualizácia rolí a zodpovedností subjektov zastrešujúcich prevádzku systému ISUF;
- poskytovanie služieb užívateľom súvisiacich s používaním aplikácie ISUF:
  - štandardné riešenie a zabezpečenie aplikačnej, technickej a technologickej podpory používateľom prostredníctvom CPU v súlade s pracovným postupom CPU,
- koordinácia prác v procese zabezpečenia pripájania nových koncových užívateľov do KTI pre potreby ISUF:
  - centralizácia požiadaviek na pripojenie nových koncových bodov do KTI pre potreby ISUF,
  - analýza možností pripojenia koncového bodu do KTI,
  - spolupráca s útvarom CPU pri realizácii pripojenia koncového bodu do KTI,
  - vypracovanie procesu riadenia vzdialených prístupov do systému ISUF,
  - zabezpečenie 2 vzdialených prístupov pre dodávateľa systému ISUF,
- zabezpečenie prístupov pre používateľov systému ISUF:
  - centralizácia žiadostí o prístup do ISUF, zakladanie a archivácia žiadostí o prístup,
  - vytvorenie prístupov pre užívateľov systému podľa požiadavky,
  - pravidelná kontrola a blokovanie prístupu pre neaktívnych užívateľov,
  - zrušenie prístupu pre neaktívnych užívateľov systému ISUF,
  - sledovanie a vyhodnocovanie logov o aktivitách koncových používateľov,
  - doplnenie aktívnych prvkov pre riadenie privilegovaných prístupových práv a riadenie privilegovaných prístupových práv,

- riadenie Bezpečnostného projektu ISUF:
  - aktualizácia Bezpečnostného projektu ISUF v súlade s aktuálne platnou legislatívou (GDPR, zákonom o kybernetickej bezpečnosti),
  - dodržiavanie Bezpečnostnej politiky a bezpečnostných pravidiel aj tretími stranami,
- Analýza rizík:
  - realizácia opatrení z Analýzy rizík,
  - zabezpečenie kontinuálneho procesu monitorovania a hodnotenia rizík ISUF,
  - vykonať aktualizáciu analýzy rizík s dôrazom na zabezpečenie povinností vyplývajúcich z nariadenia EÚ o ochrane osobných údajov (GDPR) a zákona o kybernetickej bezpečnosti,
- úlohy a testy vyplývajúce z BP ISUF:
  - riešenie úloh vyplývajúcich z BP ISUF alebo implementácia BP do systému ISUF,
  - vykonanie a otestovanie úplnej obnovy systému ISUF zo zálohy a vypracovanie záznamov z testovania,
  - vykonanie penetračných testov,
- záložné pracovisko a záložný systém ISUF:
  - zabezpečenie a udržiavanie záložného pracoviska, prevádzka záložného systému ISUF,
  - zabezpečenie technickej podpory záložného systému a on-line zálohovania,
  - spolupráca s útvarom bezpečnosti pri zabezpečení záložného systému ISUF
- riadenie SLA vo vzťahu k MF SR:
  - zabezpečenie systému riadenia úrovne poskytovaných služieb,
  - aktualizácia katalógu IT služieb,
  - vykonávanie pravidelného monitoringu a vyhodnocovanie úrovne poskytovaných služieb,
- riadenie poskytovaných služieb tretími stranami:
  - vykonávanie pravidelného monitoringu a vyhodnocovanie úrovne poskytovaných služieb tretími stranami,
  - zaviazanie externých subjektov dodržiavať pracovný postup DataCentra č. 38 *Likvidácia pamäťových médií,*
- auditné zistenia:
  - náprava nedostatkov a plnenie opatrení vyplývajúcich zo zistení z auditov vo vzťahu k poskytovaným službám pre MF SR,
  - informovanie o zisteniach súvisiacich s inými auditmi vo vzťahu k poskytovaným službám v rámci ISUF.

5. Výstupy z riešenia:

- reporty, správy, analýzy, informácie, dokumentácie a evidencie súvisiace s vykonávaním jednotlivých aktivít a zabezpečovaním úloh vyplývajúcich z dokumentu *Detailné riešenie úlohy ISUF,*
- odpočty plnenia opatrení zo zistenia vykonaných auditov.

6. Termíny plnenia:

Rok 2022 – priebežne.

7. Odberateľ - užívateľ výsledkov:

- Platobný orgán / Certifikačný orgán MF SR,
- všetci užívatelia ISUF.

8. Kapacita potrebná na riešenie v čl. / hodinách:

762

9. Riziká riešenia úlohy:

- nedostatok odborných kapacít pre riešenie jednotlivých častí úlohy,
- poruchy, prípadne zlyhanie komunikačných alebo technologických prvkov.

10. Hodnotiace kritériá:

- dostupnosť služieb systému ISUF (produktívny 99 %),
- aktualizovaná konfiguračná analýza,
- zabezpečená dostupnosť IS v prostredí SAP PI,
- úspešnosť úrovne vyriešených hlásení (97 % hlásení/požiadaviek na službu) registrovaných v CPU s prioritou 1 postúpených na druhú úroveň podpory v priemere do 1 hod. a vyriešených do 24 hod.,
- aktualizované role a zodpovednosti subjektov v rámci DC a tretích strán,
- zabezpečenie pripojenia koncových bodov pre potreby ISUF,
- vypracovanie procesu riadenia vzdialených prístupov a vytvorenie 2 vzdialených prístupov do systému ISUF,
- vytvorenie prístupov pre používateľov do systému ISUF do 2 pracovných dní podľa požiadavky,
- vykonávanie riadenia privilegovaných prístupových práv,
- vykonanie aktualizácie BP ISUF,
- vykonanie testu úplnej obnovy systému ISUF zo zálohy,
- vykonanie penetračných testov systému ISUF,
- funkčný záložný systém,
- aktualizovaný katalóg služieb,
- prijatie opatrení zameraných na nápravu nedostatkov vyplývajúcich zo zistení auditov,
- vypracovanie reportov, odpočtov plnenia úloh,
- zabezpečený súlad bezpečnostnej politiky a analýzy rizík s nariadením EÚ o ochrane osobných údajov (GDPR) a zákona o kybernetickej bezpečnosti.