B.1 OPIS PREDMETU ZÁKAZKY

Predmetom zákazky je dodanie riešenia zabezpečujúceho aplikáciu a zosúladenie spracovania dát v rámci elektronického testovania realizovaného prostredníctvom systému e-Test s požiadavkami Všeobecného nariadenia o ochrane osobných údajov 2016/679 tzv. GDPR, ktoré zahŕňa analýzu, inštaláciu riešenia, jeho integráciu, customizáciu, nasadenie do prevádzky a poskytnutie súvisiacich služieb, ako aj tvorbu reportov a dodanie príslušnej dokumentácie, zaškolenie a poskytovanie prevádzkovej a aplikačnej podpory.

1. Špecifikácia požiadavky

1.1 Funkčné požiadavky

1.1.1 Všeobecný popis požadovaného riešenia

Riešenie (ďalej aj „dielo“) dodané ako samostatný (sub)systém (modul) musí zabezpečiť aplikáciu príslušných ustanovení čl. 28 nariadenia EÚ č. 679/2016 (Naradenie GDPR) a zákona č. 18/2018 Z. z. pri spracovaní dát v rámci elektronických testovaní realizovaných prostredníctvom systému e-Test, resp. súlad spracovania osobných údajov v súvislosti s elektronickým testovaním s vyššie uvedenými legislatívnymi predpismi a z nich vyplývajúcimi požiadavkami.
Požadované riešenie musí pokryť nasledovné oblasti:
- automatické odhlásenie z portálu elektronického testovania pri nečinnosti T minút,
- automatické uzamknutie účtu v prípade N neplatných pokusov o prihlásenie,
- potreba sprísniť požiadavky a pravidlá pre heslové politiky,
- potreba na individuálne účty pre prevádzkovateľov a administrátorov,
- rozšírené šifrovanie citlivých údajov a ochrana šifrovacích kľúčov.

Riešenie musí okrem vyššie uvedeného pokryť nasledovné oblasti:
- centrálny zber logov a bezpečnostných udalostí,
- korelácia bezpečnostných udalostí,
- generovanie výstrah,
- reportovanie bezpečnostných udalostí.

Kľúčovými požiadavkami pre nové funkcionality sú:
- Zber logov zo zdrojov.
- Ochrana údajov, blokovanie aktivít.
- Monitorovanie zmien údajov.
- Korelácia udalostí.
- Reporting.
- Poskytnutie informácie na prešetrenie incidentov.
- Bezpečné uchovanie logov.
- Generovanie upozornení.

1.2 Licencie a implementácia

Riešenie musí zahrňovať dodávku **kompletných licencií vrátane licenčného maintenance v trvaní min. 12 mesiacov a údržbu riešenia po dobu 24 mesiacov** odo dňa nasadenia diela do testovacej prevádzky**.**
Dodávka riešenia musí zahŕňať implementačné a servisné služby pre danú technológiu minimálne v nasledujúcom rozsahu:
- Technické inštalácie a implementácie všetkých SW, ktoré budú súčasťou riešenia.
- Napojenie riešenia na zdroje logov na úroveň aplikácie.
- Vytvorenie korelačných pravidiel a reportov na základe spoločne definovaných use-cases bezpečnostného monitoringu (úspešný uchádzač poskytne svoje best-practice use cases v nevyhnutnom rozsahu).
- Napojenie a integrácia do aktuálneho prostredia verejného obstarávateľa.

Licenčný maintenance zahrňuje min.:
- poskytnutie záruky/záručnej aplikačnej podporu na SW komponenty v trvaní podľa výrobcom stanovenej záručnej doby,
- nárok na inštaláciu nových verzií jednotlivých SW počas obdobia, pre ktoré je zaplatená podpora SW komponentov a to v súlade s licenčnými podmienkami výrobcu SW,
- prístup k správam o úpravách a údržbe (patches) SW komponentov a to v súlade s licenčnými podmienkami výrobcu SW.

1.3 Podrobné požiadavky na ochranu dát

1.3.1 Všeobecné požiadavky

Požiadavky na monitorovanie bezpečnosti:	
1	Riešenie musí podporovať aspoň tieto protokoly: Syslog, FTP, SFTP/SCP, SNMP, ODBC/JDBC, CP-LEA, log file protocol
2	Riešenie bude založené na bez-agentovom zbere logov (zber bez nutnosti inštalovať agenta na cieľovom systéme)
3	Počet zdrojov pre zber protokolov nesmie byť licencovaný alebo zahrnutý v ponuke neobmedzenej licencie
4	Riešenie musí umožňovať archiváciu auditných logov
5	Centrálny manažment všetkých komponentov a administratívnych funkcií vo webovom používateľskom rozhraní musí byť prístupné prostredníctvom protokolu HTTPS
6	Riešenie musí umožniť používateľom riešenia definovať prístup k jednotlivým zariadeniam, ich skupinám alebo sieťovým segmentom
7	Riešenie musí automaticky identifikovať zdroje logov
8	Riešenie musí podporovať šifrovanú komunikáciu medzi zdrojom logov a navrhovaným riešením
9	Je požadovaná integrácia s adresárovým systémom (LDAP, Active Directory) pre potreby overenie používateľa
10	Log management – riešenie musí umožňovať agregáciu udalostí podľa typov, analýzu, hodnotenia, zavedenia nového zdroja udalosti, nastavenia pravidiel zhromažďovania údajov a archívu udalostí
11	Je požadovaná podpora zberu sieťových tokov (NetFlow, IPFIX, sFlow, J-flow, Packeer, Flowlog file) z prvkov infraštruktúry (switche, routery, sieťové sondy, atď)
12	Riešenie musí umožňovať automatické aktualizácie
13	Riešenie musí poskytnúť automatický proces zálohovania
14	Riešenie musí poskytovať internú kontrolu stavu zariadenia (health-check) a upozorniť používateľa, ak sa vyskytol problém
15	Riešenie musí poskytovať analytické a korelačné funkcie bez dodatočných zásahov a činností (out-of-the-box)
16	Riešenie musí byť dodané ako all-in-one appliance s možnosťou rozšírenia na distribuovanú architektúru s možnosťou využitia existujúcej licencie
17	Riešenie musí byť škálovateľné, napr. pridanie nových zariadení, lokácií, aplikácií atď.
18	Riešenie musí umožňovať rozšírenie výberu o používateľské položky z obsahu logov, ktoré môžu byť použité pre vyhľadávanie a korelácie
19	Riešenie musí zabezpečovať integritu zhromaždených údajov
20	Ukladané musia byť raw data aj normalizované informácie. Údaje musia byť uložené v komprimovanom formáte.
21	Riešenie musí umožňovať spätnú analýzu logov (napr.: s novými pravidlami alebo pri nahrávaní údajov zo súboru) v dvoch variantoch: a) s časom, kedy systém zaznamenal udalosť; b) s časom, kedy bola udalosť vygenerovaná na zdrojovom zariadení
22	Riešenie musí umožňovať agregovvanie udalosti z logov aj položiek, ktoré nie sú štandardne zahrnuté v riešení
23	Riešenie musí umožňovať rozčlenenie vyhľadávaných údajov (Drilldown); vyhľadávacie rozhranie systému správy logov musí ponúkať možnosť rozčlenenia vyhľadaných údajov až na datailnú úroveň, ako je IP adresa, typ udalosti, protokol, port atď.
24	Požadovaný spôsob zadávania vyhľadávania: vyhľadávacie rozhranie na správu logov musí poskytovať podporu ako pre dotazy zadávané pomocou Boolovskej logiky, ako aj regulárne výrazy
25	Riešenie musí poskytovať alerty na detekované anomálie, zmeny chovania siete a zmeny v generovaní logov a udalostí
26	Riešenie musí umožňovať kombinované vyhľadávanie v indexovaných a neindexovaných údajoch v systéme pre správu logov s použitím regulárnych výrazov a fulltextové vyhľadávanie v neštruktúrovanom texte.
27	Korelačný modul musí už po inštalácii (out-of-the-box) poskytnúť metódy korelačných pravidiel, ktoré automatizujú detekciu incidentov a súvisiace workflow procesy

28	Korelácia medzi zariadeniami musí už po inštalácii (out-of-the-box), umožňovať: detekcia chýb autentifikácie, chovanie perimetra, výskyt červov bez potreby špecifikovať typy sledovaných zariadení
29	Riešenie musí poskytnúť alerting, vychádzajúci z detekovaných bezpečnostných hrozieb od monitorovaných zariadení
30	Riešenie musí poskytnúť alerting založený na základe vypozorovaných anomáliách a zmenách v správaní siete (analýza sieťových tokov). Riešenie musí poskytnúť NBAD (Network Behavior Anomaly Detection) funkcionalitu.
31	Riešenie musí poskytnúť alergting porušenia bezpečnostných pravidiel, založený na stanovenej bezpečnostnej politike (napr. IM prevádzka je zakázaná)
32	Riešenie musí umožňovať vykonanie akcií v závislosti od prijatého logu, napr. Odoslanie e-mailu, notifikáciu alebo spustenie vopred definovaného skriptu
33	Riešenie musí umožňovať prácu s IP reputačnou databázou (botnet kanály, atď). IP reputačné informácie musia byť zahrnuté v cene riešenia
34	Riešenie musí generovať alert pri výpadku logov z konkrétneho zariadenia
35	Riešenie musí umožňovať vstavaný mechanizmus klasifikácie systémov podľa typu (napr. poštový server vs. databázový server)
36	Riešenie musí vyhodnotiť chýbajúce sekvencie (napr. služba prestala fungovať)
37	Riešenie musí mať možnosť monitorovať históriu útokov (typov udalostí) na kritické komponenty a históriu útoku jednotlivých užívateľov
38	Riešenie musí mať schopnosť korelovať udalosti DHCP, VPN a Active Directory a sledovať priebeh relácie používateľa v rámci inštitúcie (Presná identifikácia používateľa)
39	Riešenie musí umožňovať korelovať údaje o udalostiach so statickými a dynamickými zoznamami označujúcich položky, ktoré majú alebo by nemali byť povolené v sieti (t. j. zoznam nezabezpečených protokolov)
40	Riešenie musí poskytnúť rozhranie pre reporting, prostredníctvom ktorého bude možné vytvárať nové zostavy bez nutnosti pripravovať SQL dotazy pomocou grafického editora
41	Riešenie musí poskytovať nezmenenú funkciu reportingu aj pri zmene alebo výmene niektorých technológií, ako je firewall alebo IDS
42	Riešenie musí byť rozšíriteľné o podporu zberu a analýzy sledovanej sieťovej prevádzky až po aplikačný vrstvu modelu ISO/OSI
43	Riešenie musí byť rozšíriteľné o nástroje na zachytenie sieťovej prevádzky (full packet caputure a pre forenznú analýzu ako rozšírenie.
44	Riešenie musí poskytnúť webové užívateľské rozhranie pre správu, analýzu, reportovanie, atď. Rozhranie by nemalo obsahovať pluginy alebo byť založené na technológiách Java, Flash alebo hrubého klienta
45	Riešenie musí poskytovať natívnu podporu pre vysokú dostupnosť (HA) bez rozširujúcich komponentov/softvéru tretích strán
46	HA musí byť možné pripojiť v ktorejkoľvek fáze, bez preinštalovania celého riešenia
47	Riešenie musí poskytovať automatické aktualizácie riešenia bez pomoci profesionálnych služieb predajcu
48	Riešenie nesmie spôsobovať nefunkčnosť vlastných signatúr atp.
49	Riešenie musí poskytnúť možnosť rozšírenia a zhromažďovania informácií payloadu paketov v sieťovej komunikácii
50	Riešenie musí byť schopné udržať databázu zariadení konzistentnú aj v týchto prípadoch, nakoľko niektoré zariadenia v sieti často menia svoju IP adresu.
51	Riešenie musí zaznamenávať aktivitu používateľa v čase a to aj v prípade, ak táto informácia nie je okamžite zahrnuté do všetkých udalostí
52	Riešenie musí ponúkať prístup k dátam prostredníctvom otvoreného REST API pre integráciu s inými systémami a to minimálne pre: práca s udalosťami, flows, assety, incidenty, konfiguračnými a lookup tabuľkami
53	Riešenie musí byť navrhnuté tak, aby bolo schopné pracovať s internými prekrývajúcimi sa rozsahmi adries, spolu so sieťovými tokmi, udalosťami a zariadeniami v sieti.
54	Riešenie musí byť schopné agregovať záznamy sieťovej prevádzky z oboch strán dátového toku do jedného záznamu popisujúceho obojsmernú komunikáciu

55	Riešenie musí viesť logy aj flows v normalizovanom formáte aj vo formáte „RAW“
56	Riešenie nebude licenčne obmedzené počtom používaných korelačných pravidiel
57	Riešenie nebude licenčne obmedzené počtom generovaných reportov
58	Riešenie musí byť schopné konsolidovať výsledky z niekoľkých riešení, ako sú vulnerability skenery, risk management nástroje a externé vstupy bezpečnostných informácií z rôznych zdrojov
59	Riešenie musí zahŕňať funkcionalitu pre výmenu štandardizovaných informácií informačno-bezpečnostného charakteru, ako je STIX alebo TAXII
60	Riešenie musí ponúkať bezpečnostné informácie, ako je IP Reputation feed, botnety, zdroje malwaru, atp, ktoré sú pravidelne aktualizované a sú korelované v reálnom čase so všetkými udalosťami
61	Riešenie musí ponúkať grafickú vizualizáciu typu a závažnosti incidentov v priebehu času
62	Riešenie musí pracovať s identifikátormi fyzickej osoby (napr.: e-mail, užívateľské meno, ID, telefón, vstupná karta) a spojiť ich s konkrétnou osobou
63	Riešenie musí poskytovať funkcionalitu pre behaviorálnu analýzu užívateľov a musí byť integrovaný priamo s riešením
64	Behaviorálna analýza užívateľov musí používať strojové učenie (machine learning)
65	Riešenie musí byť schopné spojiť dva alebo viac incidentov s rovnakým indexom (napr.: používateľ, adresa IP, vlastný atribút) v jeden celok, aby sa poskytol komplexný pohľad na incident
66	Riešenie musí umožňovať stiahnutie rozšírení alebo pravidiel, so zabezpečením validácie
67	Riešenie musí byť schopné filtrovať prichádzajúce udalosti podľa štandardizovaných atribútov, vrátane používateľských, bez vplyvu na licenciu, teda nesmie negatívne ovplyvniť počet EPS
68	Riešenie musí ponúkať intuitívny grafický editor pre parsovanie a mapovanie udalostí zo zariadení, ktoré nie sú podporované out-of-box
69	Riešenie musí umožňovať zobrazenie hodnoty z look up tabuľky spolu s normalizovaným zobrazením konkrétnej udalosti (napr.: doplnenie informácie, ak je používateľské meno systémovým kontom alebo že daný systém je produkčný/testovací)
70	Riešenie musí umožňovať použitie Geolokalizačných databáz.
71	Riešenie musí byť schopné minimalizovať stratu prichádzajúcich udalostí pri propagovaní zmien alebo patchovaní systému
72	Riešenie musí byť schopné pracovať v prostredí s prekrývajúcimi sa internými IP rozsahmi
73	Riešenie musí byť schopné kategorizovať jednotlivé logy do logických celkov pre ľahšiu prácu s nimi, napríklad: systém, politiky, autentifikácia, malware atď.

Požiadavky na ochranu údajov:	
74	Riešenie podporuje monitorovanie všetkých relácií (vzdialená alebo lokálna).
75	Riešenie identifikuje: časovú pečiatku každej operácie, celý príkaz operácie, meno používateľa, odkazovaný objekt.
76	Riešenie poskytuje nepretržité monitorovanie používania a toku citlivých údajov.
77	Riešenie musí analyzovať údaje v reálnom čase.
78	Riešenie umožňuje aktívne blokovanie podľa: IP adresa zdroja a cieľa, mena používateľa, databázy, tabuľky, stĺpca alebo názov súboru, typu databázy.
79	Riešenie musí korelovať udalosti podľa nastavených prahových hodnôt.
80	Riešenie musí byť schopné učiť sa odhaliť anomálie, aby identifikovalo: nezvyčajné alebo nové aktivity, nezvyčajné alebo nové chyby, noví používatelia, nové typy objektov požadovaných používateľom, zmena správania v štruktúre SQL, zmena správania prístupovom čase k údajom.
81	Riešenie musí umožňovať odosielanie alarmov, udalostí, ktoré identifikuje, pomocou: e-mailu, syslog udalosti (konfigurovateľné pre integráciu so systémami SIEM), programovateľné rozhranie API.
82	Riešenie musí umožňovať prístup ku kontrolovaným údajom kontrolovať RBAC a to na dvoch vrstvách: prístup k systémovým funkciám, prístup k uloženým údajom.

83	Analýza SQL prúdu musí pokrývať prichádzajúce a odchádzajúce prenosy a generované chyby.
84	Riešenie musí byť schopné blokovať činnosti nad údajmi v databázach podľa definovaných pravidiel.
85	Riešenie musí podporovať sady pravidiel pre požiadavky PCI-DSS, SOX a GDPR.
86	Riešenie musí umožňovať vytvorenie vlastných klasifikačných pravidiel podľa: regulárnych výrazov, porovnávania so slovníkom, programovateľných rozhraní API.
87	Riešenie musí umožňovať vytváranie reportov v tabuľkovej a grafickej forme.
88	Riešenie musí umožňovať vytváranie automatizovaných reportov podľa naplánovaného rozsahu.
89	Systém by mal umožniť definovať postup vytvárania a distribúcie automatických výstrah a správ
90	Riešenie musí uchovávať archivované údaje v šifrovanej podobe.
91	Riešenie musí byť schopné monitorovať konfiguračné nastavenia a identifikovať zmeny na: databázovej úrovni (SQL, skripty), úrovni operačného systému (skripty, premenné prostredia, registre).
92	Riešenie musí umožňovať šifrovanie súborov údajov a diskových oddielov.

1.3.2 Kapacitné požiadavky

01	Schopnosť uchovávať lokálne údaje bezpečnostných monitorovacích prvkov aspoň 3 mesiace pre spracovanie v reálnom čase
02	Licencia max. Events Per Seconds (EPS): 500 EPS
03	Licencia max. Flows Per Minute (FPM): 10 000 FPM
04	Schopnosť kontrolovať a monitorovať databázy pre spracovanie v reálnom čase
05	Schopnosť šifrovať databázu v reálnom čase
06	Licencia pre databázu min. 2ks

1.4 Zaškolenie a podpora

Súčasťou predmetu zákazky je aj zaškolenie administrátorov pre zabezpečenie administrácie funkcionality v rámci daného riešenia. Zaškolenie bude v rozsahu najmenej 8 hodín pre 3 – 6 zamestnancov verejného obstarávateľa a bude vykonané v slovenskom jazyku v priestoroch verejného obstarávateľa.
Zároveň úspešný uchádzač zabezpečí formou konzultačných hodín odbornú technickú podporu pre dodané riešenie v rozsahu 2 hod. mesačne. Odborná technická pomoc sa použije na poskytovanie pokročilej technickej asistencie pri plánovaných zmenách v prevádzkových nastaveniach a funkčnosti riešenia a technická asistencia vo forme projekčných postupov pre plánované upgrady, na základe požiadavky verejného obstarávateľa.
Súčasťou predmetu zákazky je aj poskytnutie záruky na kvalitu a funkčnosť diela s prevzatím zodpovednosti za vady a nedostatky, ktoré sa na diele vyskytnú do uplynutia záručnej doby, t. j. 24 mesiacov odo dňa nasadenia diela do testovacej prevádzky, pričom úspešný uchádzač tieto vady a nedostatky musí odstrániť v závislosti od ich charakteru a následkov (v prípade „mimoriadnych“ období okamžite po ich nahlásení); pod riadnym odovzdaním diela sa rozumie jeho nasadenie do ostrej prevádzky potvrdené podpisom preberacieho protokolu zo strany verejného obstarávateľa;

1.5 Dokumentácia

Súčasťou predmetu zákazky je aj kompletná dokumentácia (technická a používateľská) v slovenskom jazyku v elektronickej forme. Akékoľvek zmeny v dokumentácii (Pridanie nových funkcií, opráv, zmien) bude vždy okamžite poskytnuté úspešným uchádzačom v elektronickej verzii dokumentácie počas trvania služby podpory.
V prípade, ak súčasťou implementácie bude vytvorenie vlastných parserov pre nepodporované zdroje logov, definícií pre nové korelácie, alerty a reporty, požaduje verejný obstarávateľ, aby bola k nim vytvorená a dodaná podrobná dokumentácia.

K dodanému riešeniu musí byť dodaná príslušná dokumentácia zahrňujúca najmä:

a. zdrojové kódy s popisom (t. j. komentované zdrojové kódy) v strojovo čitateľnej podobe v elektronickej forme na CD/DVD/USB nosiči,

b. technickú dokumentáciu v slovenskom jazyku v elektronickej forme na CD/DVD/USB nosiči, ktorá bude obsahovať:
   i. postup skompilovania riešenia,
   ii. dátový model riešenia,
   iii. popis architektúry,
   iv. väzby na iné systémy (vrátane centrálneho systému na elektronické testovanie – eTest),
   v. popis tokov dát;
c. prevádzkovú dokumentáciu v slovenskom jazyku v elektronickej forme na CD/DVD/USB nosiči, ktorá bude obsahovať:
   i. inštalačný postup riešenia,
   ii. konfiguráciu systémového SW serverov a pracovných staníc,
   iii. chybové stavy a postup ich riešenia,
   iv. popis mechanizmu riadenia prístupu užívateľov a komunikujúcich systémov,
   v. popis dávkových procedúr, nastavenie a postupnosť ich spúšťania,
   vi. popis procedúr pre zálohovanie a obnovu dát,
   vii. popis použitých a navrhovaných technických číselníkov, ich naplnenie pri inicializácii (ak sa uplatňuje),
   viii. popis systému žurnálovania,
   ix. popis recovery procedúry,
d. užívateľskú dokumentáciu v slovenskom jazyku v elektronickej forme na CD/DVD/USB nosiči, ktorá bude obsahovať:
   i. popis riešenia (aplikačného programového vybavenia) a jeho funkcií,
   ii. postupy a úkony potrebné pre riadne používanie riešenia,
   iii. chybové a neštandardné stavy a dostupné spôsoby ich riešenia,
e. metadáta v softvérovom prostriedku na správu údajov v elektronickej forme na CD/DVD/USB nosiči.

Zdrojový kód, ktorý je vytvorený počas zhotovovania riešenia ako autorského diela, bude otvorený v súlade s licenčnými podmienkami verejnej softvérovej licencie Európskej únie podľa osobitného predpisu[1] a to v rozsahu, v akom zverejnenie tohto kódu nemôže byť zneužité na činnosť smerujúcu k narušeniu alebo k zničeniu dodaného riešenia.
Zdrojový kód musí byť spustiteľný v prostredí verejného obstarávateľa a musí byť v podobe, ktorá zaručuje možnosť overenia, že je kompletný a v správnej verzii, tzn. umožňujúcej kompiláciu, inštaláciu, spustenie a overenie funkcionality, a to vrátane podrobnej dokumentácie zdrojového kódu takejto časti dodaného riešenia. Zdrojový kód bude verejnému obstarávateľovi odovzdaný na neprepisovateľnom technickom nosiči dát s viditeľne označeným názvom „zdrojový kód“ a označením časti a verzie dodaného riešenia, ktorej sa týka. O odovzdaní a prevzatí technického nosiča dát bude spísaný a podpísaný písomný preberací protokol.
Vyššie uvedené požiadavky sa primerane použijú aj pre akékoľvek opravy, zmeny, doplnenia, upgrade alebo update zdrojového kódu jednotlivého čiastkového plnenia tvoriaceho dodané riešenie, ku ktorým dôjde pri plnení alebo v rámci záručných opráv (ďalej len „zmena zdrojového kódu“). Dokumentácia zmeny zdrojového kódu musí obsahovať podrobný popis a komentár každého zásahu do zdrojového kódu.
Dokumentovaný zdrojový kód alebo zdokumentovaná zmena zdrojového kódu bude verejnému obstarávateľovi odovzdaná najneskôr v deň odovzdania a prevzatia príslušného plnenia – časti dodaného riešenia. V prípade predčasného ukončenia zmluvy je úspešný uchádzač povinný odovzdať verejnému obstarávateľovi aktuálne dokumentované zdrojové kódy a koncepčné prípravné materiály všetkých súčastí dodávaného riešenia tak, aby bol verejný obstarávateľ držiteľom zdrojového kódu minimálne k v danej chvíli aktuálnej verzii dodaného riešenia.
Verejný obstarávateľ môže zdrojový kód alebo jeho zmeny neobmedzene používať, rozširovať a upravovať zdrojový kód bez súhlasu zhotoviteľa, zdieľať s ostatnými subjektmi verejnej správy či ich dodávateľmi alebo ho uverejniť.

1.6 Aktualizácie

Vzhľadom na to, že všetky IT systémy prechádzajú kontinuálnym vývojom, požaduje verejný obstarávateľ, aby nasadenie riešenia malo možnosť kontinuálnych upgradov, aktualizácií, doplňovania a rozširovania

[1] Vykonávacie rozhodnutie Komisie (EÚ) 2017/863 z 18. mája 2017, ktorým sa aktualizuje verejná open source softvérová licencia Európskej únie (EUPL) v záujme ďalšej podpory zdieľania a opätovného používania softvéru vyvinutého verejnými správami (Ú. v. EÚ L 128, 19.5.2017).

jeho možností po dobu 24 mesiacov odo dňa nasadenia riešenia do testovacej prevádzky, ktoré sú zahrnuté v cene riešenia.

1.7 Požiadavky na realizáciu predmetu zákazky

Verejný obstarávateľ má v úmysle používať systém e-Test v stave akom je a vyžaduje od úspešného uchádzača, aby predmet zákazky (dielo) dodal ako samostatný (separátny) subsystém/modul.
Úspešný uchádzač sa zaväzuje realizovať predmet zákazky a akékoľvek požiadavky na realizáciu predmetu zákazky v súlade s ust. § 89 ods. 3 zákona č. 185/2015 Z. z. Autorský zákon v znení neskorších predpisov. resp. spôsobom neporušujúcim autorské práva nositeľa autorských práv systému e-Test (t. j. napr. formou nadstavby, parametrizácie a pod ...).
Úspešný uchádzač sa zaväzuje, že svojím konaním pri poskytovaní plnení podľa zmluvy, ktorá bude výsledkom tohto verejného obstarávania, nebude zasahovať do autorských práv nositeľa autorských práv systému e-Test.

1.8 Testovacia prevádzka, akceptačné kritériá

Nasadením do testovacej prevádzky sa zahájí akceptačný proces. Dĺžka trvania akceptačného procesu je max. 22 pracovných dní.
Verejný obstarávateľ sa zaväzuje zabezpečiť všetku nevyhnutnú súčinnosť tak, aby bola testovacia prevádzka a akceptačný proces úspešne ukončený v tu uvedenej lehote. Ak podmienky poskytnutia nevyhnutnej súčinnosti nie sú výslovne uvedené v tejto špecifikácii ani v zmluve o dielo alebo poskytnutie nevyhnutnej súčinnosti nevyplýva z povahy takejto súčinnosti, je úspešný uchádzač povinný na poskytnutie nevyhnutnej súčinnosti vyzvať verejného obstarávateľa a poskytnúť mu primeranú lehotu na poskytnutie nevyhnutnej súčinnosti. Úspešný uchádzač nebude v omeškaní s plnením svojich záväzkov, ak takýto záväzok nemôže riadne a včas splniť pre neposkytnutie nevyhnutnej súčinnosti zo strany verejného obstarávateľa.
Akceptačný proces zahŕňa overenie dodaného diela porovnaním jeho skutočných vlastností s ich špecifikáciou stanovenou v tomto dokumente.
Akceptačný proces zahŕňa akceptačné testy, ktoré budú prebiehať na základe špecifikácie akceptačných testov vypracovaných a odsúhlasených úspešným dodávateľom. Úspešný uchádzač je povinný poskytnúť návrh špecifikácie akceptačných testov, vrátane testovacích scenárov, najneskôr do 5 pracovných dní pred dohodnutým dňom nasadenia diela do testovacej prevádzky, resp. začatím nového/opakovaného akceptačného testovania po zapracovaní opráv. Verejný obstarávateľ má právo vyjadrovať sa a požadovať zapracovanie svojich odôvodnených pripomienok k špecifikácii akceptačných testov a ďalším parametrom akceptačného testovania (akceptačné scenáre a pod.).
Úspešný uchádzač je povinný všetky požiadavky verejného obstarávateľa splniť bez zbytočného odkladu a predložiť neodkladne plnenie k čiastkovému opakovanému akceptačnému testovaniu. Akceptačný proces sa bude opakovať, kým príslušné zapracovanie pripomienok verejného obstarávateľa nesplní požadované akceptačné kritériá a to v lehote podľa prvého odseku tejto kapitoly.
Úspešný uchádzač garantuje v rámci testovacej prevádzky:

- priamy kontakt na pracovníka (Single Point of Contact) v pracovnej dobe za účelom nahlasovania a riešenia vád zistených počas testovacej prevádzky a/alebo akceptačného testovania,
- reakčnú dobu pre všetky kategórie vád zistených počas testovacej prevádzky a/alebo akceptačného testovania max. 2 hod. od nahlásenia na SPOC,
- dobu vyriešenia kritických vád (výpadok celého systému, nedochádza k logovaniu udalostí zo žiadneho zdroja, výpadok dlhší ako 30 minút) zistených počas testovacej prevádzky a/alebo akceptačného testovania max. 24 hodín od nahlásenia na SPOC,
- dobu vyriešenia iných ako kritických vád (výpadok čiastkového komponentu, ktorý nemá vplyv na funkčnosť systému ako celku) zistených počas testovacej prevádzky a/alebo akceptačného testovania max. 72 hodín od nahlásenia na SPOC,
- dostupnosť potrebného počtu pracovníkov v pracovnej dobe (v pohotovosti) pre zásahy súvisiace s odstránením vád zistených počas akceptačného testovania,
- nepretržité riešenie vád v poradí podľa dohody medzi SPOC a zástupcom verejného obstarávateľa,
- pravidelné pracovné stretnutia medzi zástupcami úspešného uchádzača a verejného obstarávateľa min. raz týždenne.

**Pozn.: Pracovnou dobou sa pre účely tejto kapitoly rozumejú pracovné dni od 9:00 do 17:00.*

Ak nebude v rámci testovacej prevádzky preukázaná plná funkčnosť diela a/alebo odstránené všetky vady zistené počas akceptačného testovania, resp. z dôvodov neposkytnutia nevyhnutnej súčinnosti zo strany verejného obstarávateľa, môže byť lehota na ukončenie akceptačného procesu výnimočne predĺžená

o ďalších max. 22 pracovných dní.

1.9 Požiadavky na prevádzkovú a aplikačnú podporu

Riešenie bude prevádzkované v Dátovom centre Ministerstva školstva, vedy, výskumu a športu Slovenskej republiky. Verejný obstarávateľ sa zaväzuje zabezpečiť príslušnú súčinnosť s Dátovým centrom Ministerstva školstva.

Úspešný uchádzač poskytne k dodanému riešeniu:

a. záručnú aplikačnú podporu v trvaní 90 dní odo dňa nasadenia diela do testovacej prevádzky (ZAP),
b. štandardnú prevádzkovú podporu a údržbu v trvaní 24 mesiacov odo dňa nasadenia diela do testovacej prevádzky (SLA).

Služby štandardnej prevádzkovej podpory a záručnej aplikačnej podpory zahŕňajú:

- Hotline (neobmedzený počet nahlasovateľov vád zo strany verejného obstarávateľa) pre SLA, resp. priamy kontakt na pracovníka (Single Point Of Contact - SPOC) pre ZAP,
  - Upgrade riešenia až 1x za 12 mesiacov (SLA)
  - Dostupnosť 5x8 (9:00 – 17:00),
- Pravidelné pracovné stretnutia minimálne raz mesačne v rámci ZAP,
- Ad-hoc pracovné stretnutia podľa potreby pre ZAP,
  - Proaktívny monitoring aplikácie a proaktívne riešenie problémov, incidentov a vád rámci pracovnej doby

V prípade „kritickej vady“ (výpadok celého systému, nedochádza k logovaniu udalostí zo žiadneho zdroja, výpadok dlhší ako 30 minút) vyžaduje verejný obstarávateľ reakčnú dobu 2 hod., dobu vyriešenia bezodkladne, max. Však do 48 hod. pre ZAP.
V prípade „inej ako kritickej vady“ (výpadok čiastkového komponentu, ktorý nemá vplyv na funkčnosť systému ako celku) vyžaduje verejný obstarávateľ reakčnú dobu max. 2 hod., dobu vyriešenia bezodkladne, max. však do 96 hod. pre ZAP.
Ak z objektívnych dôvodov nezávislých od vôle úspešného uchádzača nie je možné odstrániť vady v lehotách uvedených v tejto kapitole, vykoná sa odstránenie vady v primeranej lehote na základe dohody medzi verejným obstarávateľom a úspešným uchádzačom.
V prípade, ak nebude úspešný uchádzač schopný odstrániť vady v lehotách uvedených v tejto kapitole, je verejný obstarávateľ oprávnený zabezpečiť odstránenie vady treťou osobou na náklady úspešného uchádzača.
Trvanie ZAP a SLA sa predĺži o čas potrebný na odstránenie vád; ZAP a SLA neplynie po dobu, po ktorú verejný obstarávateľ nemôže užívať predmet plnenia pre jeho vady, za ktoré zodpovedá úspešný uchádzač.
Úspešný uchádzač je povinný trvale udržiavať v pohotovosti v pracovnej dobe (pracovné dni od 9:00 do 17:00) potrebný počet pracovníkov pre zásahy v rámci prevádzkovej a aplikačnej podpory.

2. Opis súčasného stavu

Za účelom zabezpečenia elektronického testovania sa využíva systém elektronického testovania e-Test, ktorý bol vytvorený v rámci realizácie projektu spolufinancovaného z prostriedkov ESF s názvom „Zvyšovanie kvality vzdelávania na základných a stredných školách s využitím elektronického testovania“, a ktorého bol Národný ústav certifikovaných meraní vzdelávania (NÚCEM) riešiteľom. Systém obsahuje rozsiahly súbor úloh a testov zo všeobecnovzdelávacích predmetov, gramotností a pod. Elektronizácia hodnotiacich procesov v systéme e-Test vytvára predpoklady pre efektívne a objektívne hodnotenie úrovne vedomostí žiakov z príslušného vyučovacieho predmetu, výsledky testov sa okrem individuálneho hodnotenia používajú aj ako podklad pre zjednocovanie požiadaviek na kvalitu vyučovania všetkých typov škôl a analýzu stavu a potrieb zvyšovania úrovne vzdelávania na Slovensku.
Použitím systému e-Test bolo zavedené elektronické testovanie v troch úrovniach, a to: národné certifikačné testovania (Maturita on-line a Testovanie 9 on-line a Testovanie 5 online), školské testovania a učiteľské testovania, vrátane rozsiahlej databázy úloh a testov pre tieto testovania.
NÚCEM naďalej prevádzkuje a aktívne využíva systém e-Test pri realizácii elektronickej formy testovaní na základných a stredných školách, čo zahŕňa zabezpečenie prevádzky, administráciu a monitoring elektronického testovacieho systému e-Test, zostavovanie špecifických elektronických testov z existujúcej banky úloh a vytváranie nových úloh, zabezpečovanie školských e-testovaní a certifikačných e-testovaní (E-Maturita, E-Testovanie 9 a E-Testovanie 5), metodickú podporu školám pri realizácii e-testovaní (školských, certifikačných a učiteľských), vyhodnotenie a štatistické spracovanie výsledkov e-testovaní

a reportovanie školám. Do školských testovaní sa ročne zapojí takmer 800 škôl. Elektronické testovania ročne absolvuje v rámci celej SR vyše 50 000 žiakov. Systém e-Test je v plnej prevádzke prístupný aj pre učiteľov na učiteľské testovania, v rámci ktorých si učitelia môžu vytvárať vlastné učiteľské testy z úloh, ktoré sú v databáze systému. Zároveň NÚCEM priebežne dopĺňa databázu úloh o ďalšie úlohy z vyučovacích, cudzích jazykov, matematiky, prírodovednej gramotnosti, čitateľskej gramotnosti a matematiky.
V dôsledku legislatívnej zmeny v oblasti ochrany osobných údajov (čl. 28 nariadenia EÚ č. 679/2016 a zákon č 18/2018 Z.z.) je nevyhnutné tieto aplikovať aj v procesoch súvisiacich s elektronickým testovaním formou nového subsystém, ktorý bude zabezpečovať spracovanie osobných údajov užívateľov v súlade s kritériami bezpečnosti v zmysle vyššie uvedených legislatívnych úprav.

Za účelom poskytnutia komplexných informácii vo vzťahu k plneniu predmetu zákazky verejný obstarávateľ uvádza nižšie popis systému e-Test využívaného na zabezpečenie elektronického testovania.
Systém e-Test je súbor aplikačného a neaplikačného softvéru na elektronické testovanie a tvorbu katalógu úloh a testov.
Systém je nositeľom obsahu (dát samotných) a metód prístupu k nasledovným dátam:

- Databáza a archív úloh a testov NÚCEM (pre certifikačné a školské testovania)
- Kalendár testovaní
- Databáza a archív výsledkov kandidátov
- Databáza a archív výkazov, reportov, štatistík
- Databáza riadenia prístupov a adresár používateľov
- Auditné záznamy

Samotný systém sa skladá zo samostatných aplikačných modulov, ktoré spolu komunikujú:

- Portál (portál pre zamestnancov NÚCEM, portál pre žiakov, učiteľov, autorov úloh a testov)
- Centrum výkazov a štatistík
- Správa používateľov a riadenie prístupov
- Šifrovací modul
- Licenčný server
- Hlavný konsolidačný portál
- Archív

Prístup do jednotlivých modulov je riešený prostredníctvom rolí a oprávnení, ktoré sa nastavujú na systémovej úrovni.

Stručný popis jednotlivých modulov:

Portál
Portál je informačný portál, ktorý umožňuje prístup k informáciám o elektronickom testovaní oprávneným používateľom (zamestnancom NÚCEM, žiakom, učiteľom, riaditeľom škôl, prípadne autorom úloh a testov, atď.). Obsahuje všetky informácie o elektronickom testovaní, manuály, najdôležitejšie termíny, kontakty a organizačné pokyny. Umožňuje prístup k špecifickým a jedinečným dátam – výsledkom školy, prehľadom, grafickým výstupom, porovnaniam s inými školami a pod. Súčasťou portálu je testovacia aplikácia pre online testovanie. Portál obsahuje aj monitorovací a administratívny modul.

Tvorba úloh a testov
Systém e-Test umožňuje zaškoleným pracovníkom NÚCEM vytvárať databázu úloh a testov, ktorá obsahuje úlohy a testy pre vybrané všeobecnovzdelávacie predmety. Systém e-Test umožňuje centrálny vývoj úloh - to znamená, že všetci používatelia - autori, posudzovatelia, recenzenti atď. pracujú na jednej centrálnej databáze úloh. Prístupy používateľov do aplikácie a k dátam sú jednoznačne dané rolami a oprávneniami. Podľa oprávnení môžu vytvoriť, upraviť a vyradiť úlohy a testy, organizovať úlohy a testy do súborov (databázu úloh), prehľadávať ich, riadiť kvalitu testov a úloh, posudzovať a schvaľovať, štatisticky vyhodnocovať a parametrizovať kvalitu úloh a testov, či hodnotiť správnosť odpovedí certifikačných a školských testov, vrátane adaptívnych.

Nástroj na testovanie a hodnotenie
Systém e-Test umožňuje vykonávanie testovania samotné kandidátov. Systém obsahuje nástroj, v ktorom sa prezentujú testovacie položky, nástroj na automatické hodnotenie odpovedí a/alebo distribúciu hodnotiteľom. Proces testovania je daný svojou postupnosťou – vynútený štart, testovanie (zodpovedanie

úloh), vedomé ukončenie testu. Hodnotiteľ vstupuje do procesu pri školských a celonárodných testovaniach.

Centrum výkazov a štatistík
Centrum výkazov a štatistík je analytický a reportovací nástroj na vytváranie, úpravy a publikovanie tlačových zostáv, výsledkov testovania, exportov, štatistík, grafov a tabuliek oprávneným používateľom priamo do portálu. Výsledky z testovaní sa archivujú v elektronickej podobe podľa archivačného poriadku.

Správa používateľov a riadenie prístupov
Správa používateľov a riadenie prístupov je modul na správu identít a účtov, správu prístupov. Modul umožňuje registráciu a správu používateľa, samoobsluhu správy hesiel, priradenie a správu profilu používateľa, priradenie a správu (kontrolu, zmenu, riadenie) prístupov, prihlásenie používateľa a overenie identity, správu adresára – organizačných jednotiek a používateľov, hľadanie v adresári.

Šifrovací modul
Šifrovací modul je modul, ktorý zabezpečuje šifrovanie tam, kde je potrebné zabezpečiť ochranu a bezpečnosť citlivých údajov. Banka úloh s certifikačnými úlohami a testami je mimoriadne chránená šifrovacím modulom a je prístupná len úzkemu okruhu oprávnených používateľov.

Licenčný server
Licenčný server slúži na evidenciu licencií o systéme e-Test.

Hlavný konsolidačný portál
Hlavný konsolidačný portál poskytuje rozhranie na import a aktualizáciu číselníkov, zoznamov a registrov z registrov rezortu školstva alebo z registrov školských informačných systémov pre oprávnených používateľov vo forme importovaného súboru v predpísanej štruktúre, alebo pre oprávnené externé systémy vo forme zabezpečených webových služieb.

Archív
Archív je archivačný modul, ktorý slúži na odľahčenie produkčného systému od starých dát a zachovanie udržateľnej prevádzky aplikácie a na dlhodobé uchovanie dát. Dáta pochádzajúce zo systému e-Test sa archivujú v elektronickej podobe podľa archivačného poriadku.

Bezpečnosť systému e-Test
Vzhľadom na charakter systému je časť informácií o bezpečnosti systému dôverná.
Systém e-Test dodržiava bezpečnostné štandardy na všetkých úrovniach:

- súlad s bezpečnostným projektom systému e-Test,
- súlad so štandardmi pre informačné systémy verejnej správy,
- zabezpečené prístupy do jednotlivých prostredí a na jednotlivé servery,
- zabezpečené prístupy do jednotlivých aplikačných modulov,
- šifrovanie a ochrana citlivých dát pomocou šifrovacích hardvérových kľúčov pridelených oprávneným používateľom a šifrovacieho modulu umiestneného v dátovom centre Ministerstva školstva, vedy, výskumu a športu SR (DC MŠVVaŠ SR),
- zabezpečená komunikácia medzi jednotlivými časťami systému ako aj komunikácia s tretími stranami (vzájomná autentifikácia použitím certifikátov),
- logy a auditné záznamy.

Systém e-Test je prevádzkovaný vo virtualizovanom prostredí DC MŠVVaŠ SR. Virtualizačnú platformu a systémovú správu až po úroveň operačných systémov na jednotlivých serveroch spravujú pracovníci DC MŠVVaŠ SR. Aplikačná prevádzka systému e-Test je zabezpečovaná internými pracovníkmi NÚCEM. Pravidelné prevádzkové činnosti zabezpečujúce riadny chod systému e-Test a aplikačnú podporu systému e-Test vykonáva externý dodávateľ rozšírenej aplikačnej podpory na základe SLA.