# Požiadavky na prevádzku ParkSys v režime SaaS

Dodávateľ sa v rámci prevádzky a aplikačnej podpory IT služieb ParkSys zaväzuje poskytovať nasledovné služby:

* Monitoring fungovania služieb ParkSys s jeho integráciou do logovacieho a monitorovacieho systému prevádzky Hlavného mesta, SW Zabbix
* Riešenie incidentov za oblasť ParkSys
* Udržiavanie a nasadzovanie v TEST/PROD prostredí
* Zálohovanie údajov/databáz prostredia ParkSys
* Súčinnosť pri testovaní funkčnosti aplikácií pri nasadzovaní zmien
* Aktualizácia prevádzkovej dokumentácie pri zmene produkčného prostredia
* Realizácia/aktualizácia bezpečnostných nastavení, urgentné nasadzovania hotfixov
* Realizácia/nastavenie prístupových oprávnení do APV a ich infraštruktúry podľa požiadaviek Objednávateľa
* Ku každému výpadku základnej funkčnosti ParkSys (A incident) Dodávateľ vypracuje správu o výpadku s návrhom odstránenia hlavnej príčiny, ktorá zapríčinila nedostupnosť služby.
* Pravidelné monitorovania a nasadzovanie patchov, updaty
* Udržiavanie aktuálnej funkčnosti služby voči aktuálnej legislatíve
* Vypracovať a priebežne aktualizovať kompetenčnú maticu zodpovedných pracovníkov Dodávateľa pri prevádzkovaní služieb a zasielať ju na email poverenému pracovníkovi s odborného IT útvaru Hlavného mesta Bratislava.

Činností súvisiace s riadením prevádzky a aplikačnej podpory:

Dodávateľ sa v rámci prevádzky a podpory zaväzuje zabezpečiť služby riadenia prevádzky a podpory súvisiace s nasledovnými procesmi:

* Monitoring udalostí
* Incident manažment
* Change manažment
* SLM manažment
* Špecifikácia Služieb

## Zoznam a popis služieb IT podpory

Služby prevádzky prostredí sú poskytované na Produkčných a Testovacích (integračných) prostrediach ParkSys v nasledujúcom rozsahu:

### Služby Service Desk

Výkon činností operátorov ServiceDesku HM BA zabezpečuje Objednávateľ na úrovni L1 (základná podpora k používateľom, logovanie tiketov, základná kategorizácia, pridelenie na riešenie, monitoring riešenia u riešiteľov a uzatváranie tiketov v duchu SLA). Dodávateľ zabezpečuje praktický výkon činností riešenia incidentov a požiadaviek na úrovni L2/L3. Všetky požiadavky na Dodávateľa musia byť riadne zaregistrované v jednotnom na to určenom IT nástroji ServiceDesk HM BA. Aby nevznikli pochybnosti, všetka podstatná komunikácia a aktualizácia stavov požiadaviek, incidentov musí byť v tomto jednotnom IT nástroji vedená tak riešiteľmi od Dodávateľa, ako aj zodpovednými pracovníkmi L1 podpory Objednávateľa. V prípade, že Dodávateľ sám diagnostikuje incident v rámci monitoringu služieb ParkSys, je povinný ho do ServiceDesku HM BA neodkladne zaevidovať a prideliť si ho aj sám na riešenie.

### Služby riadenie upozornení (Event management)

Cieľom procesu riadenia upozornení je monitorovanie všetkých na kontinuitu služieb dôležitých upozornení pre potreby riadenia bežnej prevádzky a pre identifikovanie výnimočných stavov služieb/komponent/biznis kritických operácií systému ParkSys a ich eskaláciu riadeným spôsobom. Proces riadenia upozornení poskytuje silný základ pre zabezpečenie dostupnosti služieb, ich zlepšovanie, a celkové oznamovanie upozornení čím redukuje čas výpadkov systému ParkSys, zlepšuje detekciu možných výpadkov, znižuje reakčný čas pri incidentoch, zmenách. Monitoring systému ParkSys je ako nevyhnutný komponent súčasťou služby riadenia upozornení, pretože užitočným spôsobom pomáha detegovať udalosti ktoré nastali, resp. môžu vplyvom zmeny parametrov prostredia nastať. Úlohou riadenia upozornení je teda dať týmto udalostiam z monitoringu väčší význam v podobe evidencie a procesovania upozornení v ServiceDesku HM BA.

Povinnosť Dodávateľa bude monitorovať prevádzkované služby/komponenty/biznis kritické operácie systému parkovania ParkSys (napr. služieb prihlásenia, overenia zákazníka a jeho kategórie v systéme, evidencia obsadenia miesta, zaplatenie, monitoring overenia zaplatenia, nahlásenie nezrovnalosti/porušenie pravidiel v parkovaní, vystavenie pokuty, dostupnosť služieb a iné) Objednávateľa v príslušnom SW monitorovacom nástroji/nástrojoch a v prípade zistenia neštandardných udalostí spojených s kvalitou, resp. blízkym ohrozením kvality a dostupnosti služby/komponentu/biznis kritickej operácie tieto udalosti nahlasovať/zaznamenávať/evidovať v ServiceDesku HM BA a zároveň reagovať na všetky upozornenia z požiadaviek a incidentov evidované v ServiceDesk-u.

Dodávateľ nastaví také sledované prevádzkové parametre služieb/komponent/biznis kritických operácií systému ParkSys (napr. služieb prihlásenia, overenia zákazníka a jeho kategórie v systéme, evidencia obsadenia miesta, zaplatenie, monitoring overenia zaplatenia, nahlásenie nezrovnalosti/porušenie pravidiel v parkovaní, vystavenie pokuty, dostupnosť služieb a iné) Objednávateľa, z ktorých bude zrejme Objednávateľovi v akom stave sa prevádzkované služby/komponenty/biznis kritické operácie nachádzajú, teda ako v priebehu prevádzky reálne pracujú. V prípade výpadku služby/komponenty/biznis kritickej operácie, alebo keď príde k jej výraznej prevádzkovej odchýlke od normálneho stavu (stanovenej v SLA, alebo Objednávateľom v Prevádzkovom poriadku ParkSys), založí monitorovací systém automatizovaným spôsobom ticket v ServiceDesku, ako výstup z neštandardnej udalosti aj s popisom udalosti z log-u, kódom chyby a podobne. Podrobnosti nastavenia monitoringu konkrétnych služieb/komponent/biznis kritických operácií bude súčasťou schváleného Prevádzkového poriadku na úrovni Prevádzkového výboru ParkSys.

V rámci procesu riadenia upozornení evidujeme tieto druhy upozornení:

* **Upozornenia informačnej povahy** – typicky nevyžadujú žiadnu reakciu, nesú v sebe iba informáciu o udalosti z komponentu napr. script dobehol v poriadku, server prešiel z aktívneho módu do pasívneho, backup dobehol korektne.
* **Varovania** – varovania typicky indikujú aktivity ktoré sú mimo normy. Napríklad server beží na 80% záťaži, diskové pole je naplnené na 90%. Tieto hlášky vyžadujú bližšiu pozornosť prevádzky.
* **Odchýlky** – upozornenia o odchýlkach parametrov služby/komponentu indikujú, že sa s ním deje niečo nežiadúce. Táto odchýlka má/môže mať negatívny dopad na dostupnosť služby/komponentu. Napr. server/služba sa vypína, je nedostupná. Tieto hlášky smerujú k incidentom a vyžadujú okamžitú reakciu prevádzky (podľa SLA, priorita, dopad).

Prvotný cieľom bude nastaviť proces riadenia upozornení aj smerom k monitoringu tak, aby boli evidenčne pokryté prioritné varovné hlášky a odchýlky.

V rámci procesu riadenia upozornení budú stanovené rôzne KPI (bude súčasťou Prevádzkového predpisu) a budú reportované dodávateľom:

* Percento upozornení s ktorých sa vytvorili incidenty
* Poradie komponent/služieb ktoré generujú najviac upozornení vo väzbe na odchýlky
* Percento udalosti, ktoré sa zalogovali ako incidenty automatizovaným spôsobom do ServiceDesku HM BA

### Služby riadenie incidentov (Incident management)

Dodávateľ bude vykonávať riadenie incidentov s cieľom vrátiť obnovenie služby systému ParkSys na definovanú úroveň v čo najkratšom čase od evidencie incidentu s minimálnym dopadom na výkon služby. Incident definujeme ako neplánovaný výpadok, prípadne zníženie kvality IT služby.

Vstupom do incident manažmentu na riešenie môže byť akákoľvek identifikovaná/posúdená udalosť, ktorá prichádza z manažmentu udalostí (event management), nahlásená na ServiceDesk dodávateľa telefonicky, emailom, resp. priamo zalogovaná pracovníkom Dodávateľa/Objednávateľa do aplikácie ServiceDesk HM BA.

Medzi hlavné aktivity, ktoré sa vykonávajú pri riešení incidentu sú:

* správna identifikácia incidentu
* zalogovanie incidentu do ServiceDesk aplikácie pri stručnom, pre riešenie riešiteľom postačujúcim popisom,
* určenie kategórie incidentu, v rámci stromu služieb ServiceDesku pri akej službe/module/komponente sa prejavuje
* vyhodnotenie dopadu a urgencie incidentu na fungovanie organizácie a správne určenie priority pre riešenie incidentu. Podľa určenej priority budú nastavené SLA parametre a podmienky pre eskaláciu
* vyhodnotenie vážnosti incidentu. v prípade, ak sa jedná o incident typu „Kritický incident (A)“, ktorý má extrémny dopad na fungovanie služieb/systému, je potrebné postupovať podľa osobitných procesov „Major Incident process“, kde o.i. je potrebné zriadiť osobitný tím, a zabezpečiť promptnú koordináciu tohto incidentu prostredníctvom Incident manažéra Objednávateľa/Dodavateľa. Dodávateľ po vyriešení Kritického (A) incidentu odovzdá Dodávateľovi situačnú správu s navrhovanými preventívnymi opatreniami, aby sa daný incident v budúcnosti neopakoval.
* vyhľadanie riešenia v znalostnej databáze - KED
* diagnostika incidentu
* preskúmanie symptómov a riešenie
* vyriešenie a obnova služby
* ukončenie incidentu
* akceptácia riešenia zo strany zákazníka (Objednávateľ) s možnosťou opätovného otvorenia incidentu
* odozva na riešenie zo strany zákazníka/Objednávateľa (customer feedback)

V rámci incident managementu sa požaduje, aby všetky hlásenia zo strany užívateľov boli registrované do ServiceDesku HM BA, vrátane žiadostí o radu alebo informáciu, nakoľko iba týmto spôsobom je možné získať prehľad o častých otázkach, radách, informáciách, ktoré sa následne využijú napr. pre zavedenie informačných portálov pre užívateľov s FAQ sekciou, taktiež je možné vyhodnotiť znalostnú úroveň užívateľov a zadať podklady pre doškolenie, zmenu UX/IU a v neposlednom rade sa získa komplexná informácia o produktivite pracovníkov ServiceDesku.

V rámci incident managementu požadujeme zaviesť jednoznačnú identifikáciu priority, vytvorením matice, ktorá bude zohľadňovať dopad (rozsah, početnosť, závažnosť) a urgenciu incidentu. Na základe týchto parametrov sa stanoví priorita.

Dodávateľ aktualizuje v súčinnosti s Objednávateľom katalóg IT služieb, podľa ktorého sa nastavia hlavné kategórie v strome ServiceDesk-u Objednávateľa.

### Služby riadenia úrovne služieb (Service Level Management - SLM)

V rámci služby riadenia úrovne služieb sa vytvoria podmienky pre implementáciu nasledujúcich podporných procesov tak na strane Dodávateľa, ako aj na strane Objednávateľa:

* Definovanie katalógu poskytovaných služieb a zabezpečenie jeho aktualizácie vo väzbe služba, produkt, komponent,
* Definovanie evidenčných listov služieb, produktov a komponent vo väzbe na katalóg služieb a ich aktualizácia,
* Zabezpečenie negociácií pri požiadavkách na zmenu parametrov SLA pre službu, produkt a komponent,
* Riadenie životného cyklu služieb, príprava podkladov pre tvorbu SLA, participácia na zavedení, zmena, alebo zrušení služby,
* monitorovanie úrovne poskytovaných služieb a on-line poskytnutie prístupu k údajov z monitoringu Objednávateľovi,
* zber dát o vykonávaných službách (KPI), ktoré sú merateľné podľa hodnôt parametrov SLA
* tvorba a distribúcia SLA reportov
* analýza reportov
* vyhodnocovanie reportov a úrovne poskytovaných služieb
* eskalácia zistených odchýlok SLA
* vykonanie náprav pri zistených odchýlkach

### Služby riadenia prístupov (Access Management)

Služby riadenia prístupu sú známe aj ako správa identít (identity management) a správa oprávnení (rights management). Cieľom procesu riadenia prístupov je zabezpečiť oprávneným používateľom právo na využívanie Služby a neoprávnením používateľom zamedziť prístup k Službe. Samotný proces riadenia prístupov k službám a ich údajom úzko spolupracuje s procesom riadenia informačnej bezpečnosti ako takej. Správa prístupov je zodpovedná za riešenie požiadaviek používateľom na prístup.

Pre potreby riadenia prístupu, bude v ServiceDesku vypublikovaný zoznam rolí s ich popisom a kontaktnou osobou/osobami ktorá je zodpovedná za udelenie súhlasu z nastavením takého prístupu do aplikácie žiadateľovi. Samotný proces zahŕňa aj kontrolu používateľského mena a hesla, kontrolu skupín, rolí s definovanými oprávneniami ako aj samotnú kontrolu prístupu k definovanej skupine.

Úlohou riadenia prístupov je zabezpečiť aby jednotlivci v organizácií mohli používať systémy a dáta v organizácií ktoré ku svojej práci, činnosti skutočne potrebujú. Tento proces prebieha na zásade „najmenšieho oprávnenia“.

Manažment prístupov má pravidelne prehodnocovať role a skupiny (groups), ktoré sa používajú na kontrolu prístupu, aby sa zabezpečilo, že sa udeľujú iba potrebné práva a že medzi rolami a skupinami neexistuje konflikt práv. Preferovaný u Objednávateľa je RBAC (role base access control) model na definovanie segregovanej role, ktorého uplatnenia pomáha zabrániť neželanej koncentrácií oprávnení do aplikácie.

Správa prístupov bude prebiehať tak, aby pomohla Objednávateľovi udržiavať bezpečné aplikačné prostredie, ktoré zabráni neoprávnenému použitiu prístupu, ale aj zabráni narušeniu integrity dát.

Činnosti vykonávané Dodávateľom v procese riadenia prístupov v súčinnosti s Objednávateľom:

* Zber a evidencia požiadaviek na prístup
* Kontrola požiadavky z pohľadu oprávnenej osoby a autorizácie schvaľovateľom
* Samotný manažment nastavenia oprávnení, samotný výkon nastavenia prístupu
* Monitoring stavu identít v organizácií – sledovanie ich zmien a neštandardných udalostí
* Výkon správy prístupov v zmysle ich rušenia a znižovania rozsahu

Každá požiadavka na prístup musí byť:

* riadne vyplnená a zaevidovaná v ServiceDesk-u HM BA.
* vždy schválená vlastníkom role na strane Objednávateľa pre PROD prostredie resp. Projektovým manažérom Objednávateľa, pre prostredia FIX, ak sa jedná o nastavenie počas projektu.
* skontrolovaná gestorom služby/IS u Objednávateľa.
* po nastavení prístupu a jeho overení musí byť tiket v ServiceDesk-u uzavretý.

Obdobne sa pristupuje aj k požiadavke na zmenu resp. zrušenie prístupu. Zoznam (katalóg) gestorov/služieb/IS/rolí musí byť súčasťou ITSM nástroja (ServiceDesk) resp. publikovaný na Intranete Objednávateľa preferovaným spôsobom.

### Služby riadenia zmien (Change Management)

Dodávateľ bude vykonávať služby riadenie zmien s cieľom zabezpečiť potrebnú zmenu v požadovanom čase, účinným a efektívnym spôsobom podľa definovaného pracovného predpisu Objednávateľa. Pre potreby testovania a akceptácie zmien bude Dodávateľ využívať TEST prostredie Objednávateľa.

Objednávateľ je vlastníkom procesu riadenia zmien. v rámci tohto procesu bude vykonávať:

* interný prieskum pre potrebu zmien
* funkčnú špecifikáciu zmeny – požiadavku. Pri jej definovaní bude súčinný analytik APV Dodávateľa.
* Evidenciu a kategorizáciu požiadaviek na zmeny do nástroja ServiceDesk
* riadenia, odsúhlasovanie a monitoring priebehu riadenia zmien v nato zriadených útvaroch Objednávateľa
* Súčinnosť pri posúdení testovacích scenárov a pri samotnom UAT testovaní

Dodávateľ v rámci procesu Riadenia zmien bude v súčinnosti so Objednávateľom vykonávať činnosti v nasledovnom rozsahu:

* Predkladanie návrhov na zlepšenie APV a konzultácie k nim na kontaktných pracovníkov Objednávateľa
* Výkon analýzy a predkladanie návrhov riešenia zmien a ich dopadov
* vytvorenie testovacieho plánu a testovacích scenárov v SW nástroji pre testovanie v SW prostredí Objednávateľa
* plánovanie zavádzania zmien do produktívnej prevádzky, vypracovania a dodanie Release Notes Objednávateľovi
* vykonanie Akceptačných testov za prítomnosti tímu od Objednávateľa
* vyhodnotenie Akceptačných testov a odsúhlasenie zavedenia do produktívnej prevádzky
* Aktualizácia príslušnej technickej dokumentácie APV dotknutej zmenou
* Dodávateľ bude súčinný a vykonávať činnosti pri procese Riadenie zmien v zhode s Postupmi zmenového konania, ktoré v detaile určí Objednávateľ po uzatvorení zmluvy.

### Služby riadenia bezpečnosti IS

Dodávateľ bude v rámci procesu Riadenia bezpečnosti IS v spolupráci z Objednávateľom vykonávať činnosti v zmysle príslušných bezpečnostných smerníc a politík Objednávateľa v nasledovnom rozsahu:

* monitorovanie bezpečnostných incidentov
* hodnotenia zraniteľností
* zálohovanie a archivácia
* riadenie prístupu
* posúdenie zmien konfigurácie
* posúdenie zavádzania nových aplikácií a systémov
* riadenie manažmentu rizík pre oblasť informačnej bezpečnosti
* riadenie kontrolných mechanizmov riadenia informačnej bezpečnosti
* riadenie ochrany proti škodlivému kódu v dohodnutom rozsahu
* riadenie sieťovej bezpečnosti v dohodnutom rozsahu
* riadenie aktualizácie softvéru

### Služby reportingu prevádzkových parametrov IT služieb

Požiadavkou objednávateľa je mať k dispozícií taký reporting, ktorý zabezpečí prehľad o aktuálnom stave jeho:

* IT služieb, biznis kritických operácií Objednávateľa (procesing hlavne správ).
* dôležitých komponent služieb infraštruktúry (aplikačné služby, integrované služby tretích strán, webservice a podobne)

Objednávateĺ požaduje online prístupu k reportom (nie iba na vyžiadanie) formou webového prístupu s možným exportom údajov na ďalšiu analytiku do MS Excel formátu.

Dodávateľ zabezpečí:

Návrh reportov za súčinnosti s Objednávateľom, ktoré budú pokrývať oblasť sledovania stavu služieb, dôležitých komponent a biznis kritických operácií z procesingu správ. Návrh po funkčnej/dátovej stránke odsúhlasí odborný IT útvar Objednávateľa.

* Realizácia reportov – vytvorenie reportov on-demand spustiteľných Objednávateľom za vyššie definované oblasti.
* Publikovanie reportov v preferovanom webovom prostredí s možným exportom údajov do MS Excel
* Zber údajov z log manažmentu/komponent, databázy ServiceDesku resp. ďalších zdrojov.
* Generovanie reportov

### Preberanie nových SW systémov a modulov od tretích strán

Objednávateľ predpokladá v budúcnosti tvorbu ďalších nových modulov, ktoré môžu byť vyvíjané tretími stratami. V prípade, že objednávateľ ide vyvinúť/obstarať SW/služby ktoré majú dopad na služby ParkSys-u od tretej strany musí o tom informovať Dodávateľa. Vzhľadom na povahu a rozsah implementovaného SW, Dodávateľ poskytne plnú súčinnosť pri ich vývoji, testovaní, nasadení, tak aby ho riadne vedel prípadne prevziať do plnej prevádzky, resp. v dohodnutej miere podporovať.

## SLA parametre služieb

SLA (Service Level Agreement – dohoda o úrovni poskytovania služieb) definuje kľúčové parametre kvality, úrovne a rozsahu prevádzkovaných služieb ParkSys.

Nižšie uvádzame požadované základné parametre:

* Prevádzka a podpora bude prebiehať viď Príloha OZ2 - Zoznam biznis požiadaviek
* Minimálna dostupnosť systému ParkSys, parameter viď Príloha OZ2 - Zoznam biznis požiadaviek
* Obdobie vyhodnocovania dostupnosti je mesačné
* Maximálna doba plánovaných odstávok je viď Príloha OZ2 - Zoznam biznis požiadaviek s tým, že odstávky je možné robiť len po odsúhlasení Objednávateľa v časoch kedy používatelia najmenej využívajú systém. Výnimku pre dlhší kumulatívny čas plánovaných mesačných odstávok udeľuje na návrh Dodávateľa vedúci IT útvaru HM BA. Plán plánovaných odstávok musí vypracovať a aktualizovať Dodávateľ, pričom podlieha schváleniu Objednávateľom. Plán odstávok musí byť vypublikovaný na Portáli systému. Neplánované odstávky v prípade kritického incidentu s nasadením hotfix-opravy teda požiadavku vysokej urgencie schvaľuje na návrh Dodávateľa kontaktná osoba Objednávateľa per rollam.
* Garantovaná doba odozvy APV ParkSys na volanie poskytovaných služieb resp. z GUI je d**o** viď Príloha OZ2 - Zoznam biznis požiadaviek(táto podmienka neplatí, ak systém ParkSys je pri jeho volaní priamo závislý od služby tretej strany (napr. platobná brána...), ktorá tento parameter nemusí nespĺňať (napr. má výpadok).
* V prípade nasadzovania urgentných hotfix je z dôvodu zrýchlenia nasadenia opravy na PROD pre neutralizáciu incidentu, Dodávateľom poslaný oznam na prípadne predpokladané krátke výpadky v prevádzke ParkSys Objednávateľovi (výpadky rádovo v sekundách, resp. málo minút).

Incident

Incident je akákoľvek vada, chyba, nedostatok, porucha SW komponentu, alebo IT služby brániaca jeho riadnemu a/alebo bezchybnému používaniu, a/alebo spôsobujúca jeho čiastočnú, alebo úplnú nefunkčnosť, a/alebo spôsobujúca čiastočné a/alebo úplné obmedzenie jeho/jej používania a prevádzkovania.

Pričom vyriešenie incidentu znamená:

* Obnovenie poskytovanej služby za splnení kvalitatívnych metrík služby,
* Poskytnutie náhradného dočasného riešenia – v krajnom prípade len po vyslovenom odsúhlasení objednávateľom, pre obmedzený čas z dôvodu obmedzenia alebo vylúčenia dopadu incidentu, pre ktoré zatiaľ nie je k dispozícii úplné riešenie. Poskytnutie náhradného riešenia sa poskytuje veľmi sporadicky a podlieha odsúhlaseniu Objednávateľom.

Kategorizácia incidentov je definovaná ako kritický incident (A-blocker), Závažný incident (B-major) a Nezávažný incident (C-minor).

*Kritický incident (A-blocker)*

* Sa prejavuje výpadkom fungovania služby, čo znemožňuje jej využívania ako celku resp. spôsobuje zásadné obmedzenie jej funkcionality a rýchlosti pri obsluhe používateľmi počas doby trvania incidentu (napr. registrácia, úhrada za parkovné, identifikácia subjektu, overenie zaplatenia parkovania resp. oprávnenia na parkovanie v zóne/parkovacom mieste, a podobne). Kritický incident sa zväčša opakuje globálne voči všetkým používateľom (výpadok centrálnej služby), alebo integrovaným systémom.
* Ako kritický sa považuje prejav, ktorý je opakovane vyvolateľný, alebo má trvalý charakter, alebo sa prejavuje hromadne.
* Kritickým incidentom, môže byť aj výskyt viacerých závažných a nekritických incidentov, ktorých súčasné pôsobenie znemožňuje využívanie služby, alebo spôsobuje zásadné obmedzenie jej funkcionality a rýchlosti pre občana a integrované inštitúcie.

*Závažný incident (B-major)*

* Sa prejavuje výpadkom fungovania služby (jej funkcií a modulov v rámci dôležitých biznis funkcionalít systému voči používateľom parkovacieho systému) v rozsahu čiastočne obmedzenej funkcionality služby, v dôsledku ktorého je použitie služby zo strany občanov alebo integrovaným inštitúcií závažným spôsobom obmedzené počas doby trvania incidentu.
* Ako závažný sa považuje prejav, ktorý je opakovane vyvolateľný, alebo má trvalý charakter, alebo sa prejavuje hromadne.
* Závažným incidentom, môže byť aj výskyt viacerých nekritických incidentov, ktorých súčasné pôsobenie závažným spôsobom obmedzuje funkcionalít služby pre občana a integrované inštitúcie.

*Nekritický incident (C minor)*

* Incident, ktorý nespôsobí nedostupnosť služby resp. ktorý závažným spôsobom neznižuje funkčný rozsah a rýchlosť poskytovanej služby (napr. drobná funkčná chyba).

### Výpočet parametra D - Dostupnosť služby

D = ((T – SUM V) / T ) \* 100

Vysvetlivky:

D – dostupnosť služby v %

T – počet prevádzkových hodín za sledované obdobie

V – výpadok v hodinách (pre kritický a závažný incident), resp. doba neplánovanej odstávky služby/modulu pre nasadenie hotfix z incidentu na strane Dodávateľa počas sledovaného obdobia sa do vzorca zaokrúhľuje vždy nahor.

### Úroveň spracovania požiadaviek (SLA)

U incidentov definujeme dve základné SLA parametre, ktorými meriame postup ich riešenia a vyriešenia. v prípade problémov definujeme, ako SLA parameter schopnosť identifikovania koreňovej príčiny (známa chyba), jej popis s návrhom riešenia.

*Reakčná doba (RT – response time)*

Je maximálna doba, počas ktorej je dodávateľ, ktorý vykonáva prevádzku služby povinný reagovať na incident od objednávateľa, resp. zaznamenal chybové hlásenie v svojom Monitoringu (monitoring dodávateľa). Čas sa vždy meria od momentu, keď bolo zaznamenané hlásenie v Monitoringu Dodávateľa alebo od momentu zaevidovania incidentu Objednávateľom do ServiceDesku. Hlásenia v monitoringu Dodávateľa, ktoré majú povahu incidentov s dopadom na prevádzkovanú službu objednávateľa musia pracovníci dodávateľa obratom/bezodkladne nahrať ako incident v ServiceDesku HM BA.

*Doba neutralizácie incidentu (FT-fix time)*

Je maximálna doba, do ktorej nahlásený incident musí byť vyriešený a služba obnovená a poskytovaná podľa dohodnutých funkčných a kvalitatívnych parametrov. Čas sa vždy meria od najbližšej hodiny a teda od momentu, keď bolo zaznamenané hlásenie v Monitoringu Dodávateľa alebo od momentu zaevidovania incidentu Objednávateľom do ServiceDesku Objednávateľa. Hlásenia v monitoringu Dodávateľa, ktoré majú povahu incidentov s dopadom na prevádzkovanú službu objednávateľa musia pracovníci obratom/bezodkladne nahrať ako incident v ServiceDesku. Incident môžu zaevidovať aj pracovníci Objednávateľa a presunúť na riešenia na Dodávateľa.

Dodávateľ poskytuje plnenia na nižšie uvedené typy úrovní.

Úroveň riešenia incidentov:

časy na spracovanie incidentov sa počítajú od nahlásenia Incidentu v ServiceDesk-u, resp. zistenia v Monitoringu Dodávateľa/Objednávateľa v časoch podľa viď Príloha OZ2 - Zoznam biznis požiadaviek