

## **SMERNICE INFORMATIKE UKC LJUBLJANA**

## Kazalo vsebine:

1.	Smernice upravljanja informacijske varnosti .....	3
2.	Smernice programske opreme .....	3
3.	Smernice za infrastrukturo.....	7
4.	Neprekinjeno poslovanje in obvladovanje tveganj vezano na informacijske sisteme .....	8
5.	Lokacija podatkov .....	9
6.	Rok hrambe .....	9
7.	Pogodba o zagotavljanju nivoja storitev (SLA - Service level agreement) .....	9
8.	Zagotovitev delovanja informacijskega sistema .....	13
9.	Ukrepanje in rezultati .....	14
10.	Poročilo o delovanju platforme in odpravi napak .....	14
11.	Preverjanje skladnosti izvajalca s smernicami .....	14

## 1. Smernice upravljanja informacijske varnosti

- Izvajalec mora zagotoviti skladnost z zahtevami Informacijske varnostne politike, ki je skladna z zahtevami ISO/IEC 27001.
- Izvajalec mora imeti uveden sistem za upravljanje incidentov po ITIL oziroma upravlja incidente znotraj naročnikovega sistema za upravljanje incidentov.
- Naročnik redno izvaja analize tveganj in prilagaja varnostne ukrepe.
- Implementirane morajo biti politike za varnostno uničenje podatkov in strojne opreme, anonimizacijo in psevdonimizacijo osebnih podatkov, kjer je to potrebno zaradi zahtev ZVOP.
- Izvajalec mora zagotavljati mora skladnost z vsemi relevantnimi zakoni in predpisi o kibernetiki varnosti.
- Izvajalec mora redno izvajati varnostno oceno, naročnik pa preverjanja izvajalca 1x letno na način kot ga predpiše naročnik.
- Naročnik si pridružuje pravico do naročila zunanjega izvajalca, ki bo varnostno preveril sistem. Izvajalec je zavezan, da bo sodeloval in odpravil vse zaznane ranljivosti. Odpravljanje visokih in srednjih ranljivosti se morajo sproti odpravljati v skladu z SLA.
- Za vsa poročila in vprašalnike, ki jih izvajalec pripravlja pri izvajanju posamezne pogodbe, naročnik lahko predpiše tehnični in vsebinski format katerega se mora izvajalec držati.
- Naročnik mora zagotoviti, da so vsi varnostni dogodki ustrezno evidentirani in obravnavani.
- Naročnik mora zagotavljati ustrezno fizično in informacijska varnost podatkovnih centrov.
- Naročnik redno ocenjuje izvajalce in izboljšuje varnostno politiko.
- Izvajalec mora omogočati revizije skladnosti s strani UKC Ljubljana.
- Izpolnjene morajo biti varnostne in skladnostne smernice, ki se nanašajo na zakon o informacijski varnosti ali v skladu z dobro prakso v IKT industriji.
- Lastništvo podatkov: vsi vneseni podatki so last naročnika. Izvajalec je dolžan izvoziti podatke in ustrezno dokumentirati njihovo strukturo in relacije.

## 2. Smernice programske opreme

- Izvajalec mora poskrbeti, da imajo vsi uporabniki edinstvena uporabniška imena.
- Izvajalec mora poskrbeti, da aplikacija ločuje navadne in privilegirane uporabniške račune.
- Izvajalec mora zagotoviti, da nobeno uporabniško ime in/ali geslo ni vpisano neposredno v programsko kodo (hard-coded).
- Aplikacija mora omogočati dodeljevanje dostopa na podlagi vlog (role-based access control).
- Izvajalec mora zagotoviti delovanje aplikacije brez privilegiranih pravic.
- Aplikacija mora omogočati implementirano stroge politike gesel. Uporabniška gesla morajo imeti najmanj 10 znakov in morajo biti ustrezne kompleksnosti (vsebovati vsaj eno malo črko, eno veliko

črko in vsaj eno številko). Gesla je potrebno menjati minimalno vsakih 12 mesecev; 24 zaporednih gesel je neponovljivih; Geslo se zaklene za petnajst minut po petih nepravilnih poizkusih vnosa. Priporočamo uporabo AD uporabniških računov (SSO).

Privilegirana uporabniška gesla zahtevajo višji nivo kompleksnost. Upoštevati:

- Sodobne NIST smernice (<https://pages.nist.gov/800-63-4/sp800-63b.html>)
  - <https://www.schneier.com/blog/archives/2024/09/nist-recommends-some-common-sense-password-rules.html>).
  - Za administratorje pa je OBVEZEN »Phishing Resistant MFA« (<https://www.sans.org/blog/what-is-phishing-resistant-mfa/>)
- Za vse privilegirane aktivnosti mora sistem zahtevati vsaj dvo-faktorsko avtentikacijo (2FA) še bolj več-faktorsko avtentikacijo (MFA).
  - Aplikacija mora imeti uvedene mehanizme za spremljanje in evidentiranje dostopa uporabnikov do sistema.
  - Aplikacija mora biti razvita skladno s standardi, dobrimi praksami in smernicami ter zagotavljati visoko raven zaupnosti, celovitosti in razpoložljivosti podatkov.
  - Vsi podatki morajo biti šifrirani med prenosom. Posebne vrste osebnih podatkov morajo biti šifrirane tudi ob hranjenju.
  - Izvajalec mora zagotavljati vse popravke in posodobitve, da zagotavljajo, zaščito pred znanimi in zaznanimi ranljivostmi (varnostne konfiguracije in programsko opremo).
  - Izvajalec mora sodelovati pri preiskavah incidentov ter omogočiti forenzično zaščito podatkov.
  - Izvajalec je dolžan poročati naročniku o varnostnih incidentih, ki bi lahko vplivali na delovanje UKCL. Ravno tako mora kot ključni dobavitelj kritičnemu subjektu zagotavljati skladnost z Zakonom o informacijski varnosti, vključno s poročanjem pristojnemu organu.
  - Izvajalec mora zagotoviti ustrezno upravljanje sprememb ter sledenje varnostnim popravkom in posodobitvam programske opreme. Največ 2 meseca po odkritju nekritične ranljivosti in 14 dni za kritične.
  - Izvajalec mora redno izvajati varnostnega preverjanja aplikacije in revizije svojega razvojnega sistema, ki vključuje vdorno testiranje in varnostno preverjanje in ga izvaja zunanje neodvisna strokovna organizacija. Izvajalec je dolžan odpraviti vsa priporočila z kritično in resno oznako prioriteto. Naročnik pa ima pravico zahtevati poročilo.
  - Izvajalec mora zagotoviti delovanje aplikacij in sistema tudi v primeru uporabe rešitev za preprečevanje izgub podatkov (DLP).
  - Razvita programska oprema mora biti testirana skladno z najnovejšimi OWASP priporočili. OWASP testiranje (Open Web Application Security Project) je skupina vizualizacij in postopkov za testiranje varnosti spletnih aplikacij in web servisov, ki jih je razvil odprtokodni skupni tok OWASP. Cilj temelji na uporabi različnih testnih metodologij za katalogizacijo in verifikacijo varnosti aplikacije.

- Izvajalec izdelava načrt obnove sistema in ga redno testira in posodablja (Standard Operating Procedures). Izvedba preizkusa preklopa skupaj z vsemi deležniki (UKCL, Skrbniki infrastrukture, Skrbniki aplikacije). Izvajalec mora v načrtu obnove sistema upoštevati sekundarno in druge lokacije, če jih naročnik predvidi. Omogočiti mora prisotnost naročnika pri izvajanju testiranja obnove in okrevanja o katastrofi.
- Obvezna uporaba glavnih uveljavljenih standardov v zdravstvu (Health standardov), kot je npr. HL7, IHE, FHIR, openEHR,...
- Aplikacija mora, na uporabniškem nivoju, delovati na sodobnih in podprtih verzijah operacijskih sistemov Microsoft Windows, oziroma sodobnih in podprtih verzijah vsaj 4 najpogostejših spletnih brskalnikov.
- Informacijski sistem za svoje delovanje ne sme zahtevati administratorskih pravic na računalnikih uporabnikov.
- Smernice za implementacijo novih servisov so:

- *Modularna mikroservisna arhitektura*

Servisi morajo biti razviti na način, ki omogoča neodvisnost, enostavno nalaganje, skalabilnost in medsebojno povezljivost.

Modularen pristop omogoča organsko rast sistema in enostavno dodajanje novih funkcionalnosti. Prav tako omogoča izolirano zamenjavo oz. nadgradnjo posameznih modulov z minimalnim vplivom na delovanje celotnega sistema.

- *Standardni protokoli za komunikacijo med posameznimi moduli*

Medsebojna komunikacija med servisi mora potekati preko standardnih in uveljavljenih protokolov kot so REST HTTP in GRPC, AMQP, SOAP. Komunikacija servisov naj bo zasnovana kot (oz. odvisno od vsebine procesa naj omogoča) »event driven« (dogodkovni) pristop. Preostali servisi se lahko naročijo na določene dogodke sistema in na osnovi tega vodijo svoj proces naprej.

- *Uporaba podatkovnega vodila (Service bus) za integracijo in obveščanje o dogodkih med posameznimi servisi*

Z uporabo podatkovnih vodil, kot so RabbitMQ, Kafka in podobni »event driven« prisotno zmanjšamo odvisnost (direktne integracije) med posameznimi servisi, omogočimo hitrejši tok informacij (PUSH pristop) in razbremenimo sistem. Prav tako omogočimo dostop do informacij vsem udeležencem, ki jih potrebujejo brez potrebe po še eni dodatni integraciji med dvema servisoma.

- *Uporaba kontejnerjev kot načina za razvoj in nalaganje (deployment) servisov*

Nalaganje servisov v okviru kontejnerjev omogoča konsistentnost obnašanja aplikacije čez različna okolja. Kontejnerji bolj učinkovito uporabljajo resurse kot običajne virtualne mašine omogočajo ob doseganju enak izolacije procesov.

- *Monitoriranje servisov/telemetrija(Observability)*

Servisi morajo podpirati standardne mehanizme obveščanja o svojem trenutnem statusu. Standardni protokoli kot je OpenTelemetry omogočajo zajem podatkov o logih, metrikah in sledeh (tracing) preko katerih lahko nadziramo delovanje sistema kot celote, odzivnost, prepustnost sistema, ugotavljamo ozka grla in morebitne napake.

Vsak servis mora imeti implementiran način za preverjanje zdravstvenega stanja (Health check), ki pomeni ali je sistem operativen ali ne. Z avtomatskimi mehanizmi nezdrave servise odstranimo iz delovanja in jih nadomestimo z zdravimi.

- Smernice za novega spletnega klienta (vmesnika) so:

- *Odziven design (Responsive design)*

Prikaz spletne aplikacije se mora avtomatično prilagoditi različnim formatom zaslonov oz. povečevanju manjšanju okna kjer se vsebina izrisuje, npr. to lahko pomeni zlaganje elementov enega pod drugim v primeru oženja po horizontali oz. skrivanje določenih elementov.

- *Uporaba sodobnih JavaScript ogrodij za razvoj spletnih aplikacij*

Sodobna odprtokodna in razširjena orodja, ki se danes uporabljajo in omogočajo izgradnjo dinamičnih, interaktivnih spletnih aplikacij so React, Vue.js., Angular in drugi.

- *Napredne spletne aplikacije (Progressive Web App - PWA)*

Aplikacija mora po potrebi omogočati offline način delovanja, komunikacijo v realnem času npr. signalR in podpirati native-app like uporabniško izkušnjo. Npr. namestitev kot samostojna (offline ali online) aplikacija na mobilni napravi.

- *Upravljanje stanja (State management) znotraj spletnih aplikacij*

Uporaba orodij/knjižnic kot so Redux, Vuex, Pinia za upravljanje stanja znotraj spletnih aplikacij omogoča dinamično uporabniško interakcijo in konsistentnost prikaza podatkov skozi različne dele aplikacije.

- *Uporaba sodobnih standardov in priporočil za zagotavljanje varnosti*

Uporaba HTTPS. Definiranje Content Security Policies (definira kaj so viri skript in ostalih resursov, ki se izvajajo v spletni aplikaciji), ki preprečuje določene tipe napadov kot so podtikanje skript. Uporaba sodobnih standardnih načinov za avtentikacijo kot je OAuth2/OpenID. Uporaba glavnih uveljavljenih standardov v zdravstvu (Health standardov), kot je npr. HL7, IHE, FHIR,...

- *Upoštevati smernice glede piškotkov*

Pridobitev soglasja: Pred uporabo piškotkov morate pridobiti soglasje uporabnikov, razen za nujno potrebne piškotke. Uporabnike morate jasno obvestiti o namenu uporabe piškotkov in pridobiti njihovo izrecno privolitev.

Jasna opredelitev piškotkov: Preden uporabniki podajo soglasje, morate natančno opredeliti vse piškotke, ki jih uporabljate, ter njihov namen.

Dokumentacija soglasij: Vsa pridobljena soglasja morate dokumentirati in shraniti.

Možnost zavrnitve in upravljanja: Uporabnikom morate omogočiti, da lahko zavrnejo določene vrste piškotkov (npr. oglaševalske piškotke) in da lahko kadarkoli spremenijo svoje nastavitve glede piškotkov.

Obvestilo o piškotkih: Na spletni strani morate imeti vidno obvestilo o uporabi piškotkov, ki vključuje informacije o vrstah piškotkov, njihovem namenu in trajanju.

Skladnost z zakonodajo: Uporaba piškotkov mora biti skladna z zakonodajo, kot je Splošna uredba o varstvu podatkov (GDPR) in Zakon o elektronskih komunikacijah (ZEKom-2).

### 3. Smernice za infrastrukturo

- Aplikacija mora zagotavljati revizijske sledi dostopa do osebnih podatkov.
- Izvajalec mora zagotavljati vse popravke in posodobitve, da zagotavljajo, zaščito pred znanimi in zaznanimi ranljivostmi (varnostne konfiguracije in programsko opremo).
- Izvajalec mora sodelovati pri preiskavah incidentov ter omogočiti forenzično zaščito podatkov.
- Izvajalec je dolžan poročati naročniku o varnostnih incidentih, ki bi lahko vplivali na delovanje UKCL. Ravno tako mora kot ključni dobavitelj kritičnemu subjektu zagotavljati skladnost z Zakonom o informacijski varnosti, vključno s poročanjem pristojnemu organu.
- Izvajalec mora zagotoviti delovanje implementirane rešitve za požarnim zidom in vpeljanimi varnostnimi rešitvami.
- Implementiran mora biti nadzor in beleženje vseh varnostnih dogodkov in dostopov. Sistemi morajo omogočati pošiljanje zapisov v centralni sistem za upravljanje dnevniških zapisov in dogodkov (SIEM) v eni od standardnih normaliziranih oblik.
- Zagotavljajo ustrezno varnostno kopiranje podatkov in redno preverjanje obnovljivosti teh kopij.
- Izvajalec postavi vse kritične sisteme v načinu visoke razpoložljivosti.
- Naročnik ima in vzdržuje načrt za odzivanje na kibernetiske incidente. Izvajalec pa pripravi in vzdržuje ustrezno in potrebno dokumentacijo, ki jo zahteva načrt na kibernetiske incidente.
- Na strežniškem nivoju pa na sodobnih in podprtih verzijah sistemov Microsoft Windows Server ali sodobni distribuciji sistema Linux.
- Vsi oddaljeni dostopi morajo biti varni, šifrirani in časovno omejeni skladno z zahtevami naročnika.
- Imajo implementirane rešitve za zaščito pred DDoS napadi (v primeru, da ima izvajalec v vzdrževanju tudi infrastrukturo).

#### 4. Neprekinjeno poslovanje in obvladovanje tveganj vezano na informacijske sisteme

**Obvladovanje tveganj v primeru izpada informacijskega sistema je ključnega pomena za informacijski sistem, ki je identificiran kot kritični sistem in del kritične infrastrukture v UKCL.**

Zahtevana stopnja delovanja SLA za kritične sisteme je razpoložljivost 99,9%.

Za kritične sisteme/servise je potrebno zagotoviti spremljanje (monitoriranje) v avtomatičnem načinu 24/7 z aktivnimi mehanizmi obveščanja (mail, SMS,...).

Zahteve in smernice, ki jih mora zagotavljati izvajalec za vzpostavitev sistema neprekinjenega poslovanja (Business Continuity) in obvladovanja tveganj (Risk Management) za informacijski sistem, ki je identificiran kot del kritične infrastrukture. Namen je zagotoviti, da organizacija lahko nadaljuje svoje ključne poslovne funkcije tudi v primeru motenj ali izpada.

***Za zagotovitev neprekinjenega poslovanja in varnosti informacijskega sistema mora izvajalec skrbeti za načrtovanje v zvezi z zagotavljanjem neprekinjenega poslovanja in obvladovanja tveganj (Recovery Time Objective – RTO):***

- **Avtomatizirane skripte**

Uporaba avtomatiziranih skript za namestitve in konfiguracijo infrastrukture. Zagotovitev konsistentnosti vzpostavitve celotnega produkcijskega in testnega okolja.

- **Uravnoteženje obremenitve (Load Balancing)**

Razporeditev prometa med več instancami zabojsnikov (kontejnerjev) za zagotavljanje, da noben servis ni preobremenjen in da okvara enega ne vpliva na celoten sistem.

- **Konfiguracijske datoteke**

Namestitvene skripte in ostale konfiguracijske datoteke (če se uporabljajo) se hranijo z orodji za upravljanje s kodo, tako da je vedno na voljo zadnja verzija potrebnih konfiguracij. Omogočati mora tudi vpogled v zgodovino sprememb konfiguracije.

- **Obveščanje in spremljanje (Monitoring)**

Monitoring sistema, ki na nivoju vsakega servisa, ki se izvaja v zabojsniku sporoča svoje zdravstveno stanje IS (Health Check). V primeru nedelujočega zabojsnika so implementirani mehanizmi, ki nezdrav zabojsnik avtomatično resetirajo. Samodejno obveščanje skrbnikov o težavah za hitro ukrepanje.

- **Failover sistemi (Cluster sistem)**

Servisi sistem se morajo izvajati v zabojsnikih z več instancami, kar pomeni da obstaja redundanca, ki tudi ob izpadu ene instance zagotavlja neprekinjeno delovanje IS.



- **Neprekinjena zaščita podatkov (Continuous Data Protection - CDP)**

Omogočati mora sprotno varnostno kopiranje podatkov, kar omogoča obnovitev podatkov do točno določenega časa.

- **Posodabljanje**

Redno posodabljanje in nadgradnje aplikativne programske opreme.

- **Povezljivost, robustnost in dosegljivost sistema**

Glede na kritičnost mora imeti sistem/servis določeno stopnjo redundance. Uporaba predlaganih tehnologij, kot so zabojniki (tehnološke smernice), omogoča enostavno umestitev in integracijo teh servisov z orodji za doseganje visoke razpoložljivosti, kot so Kubernetes, Docker Swarm, Service Fabrics.

**Izvajalec mora v primeru kritičnega izpada vzpostaviti informacijski sistem (Recovery Point Objective – RPO) in obnoviti podatke v času izpada.**

V primeru kritičnega izpada informacijskega sistema UKCL se čas potreben za ponovno vzpostavitev informacijskega sistema opredeljen v SLA.

Skupni čas ponovne vzpostavitve delovanja celotnega sistema odvisen od časa ponovne vzpostavitve in delovanja vseh teh kritičnih delov, ki so v integraciji z drugimi izvajalci v okolju UKCL.

## 5. Lokacija podatkov

Vsi podatki za produkcijska okolja morajo biti locirani na strežnikih v profesionalnem podatkovnem centru (angl. »Data center«) v UKC Ljubljana. Vse povezave med strežniki (testni in produkcijski) in izvajalcem morajo biti enkriptirane in preko namenskih VPN-ov. V primeru, da je lokacija podatkov in aplikacij izven UKC Ljubljana in se izvajajo servisi v omrežje UKC Ljubljana morajo biti povezave ustrezno zaščitene (IPsec protokol).

## 6. Rok hrambe

Rok hrambe mora biti nastavljen za vsak poslovni proces ločeno in v skladu s pravnim redom RS.

## 7. Pogodba o zagotavljanju nivoja storitev (SLA - Service level agreement)

Izbrani izvajalec mora z naročnikom skleniti dogovor o zagotavljanju nivoja storitev (SLA), ki je sestavni del razpisne dokumentacije ali opisano v strokovnih zahtevah razpisa.

Predstavlja nivo storitev (v nadaljnjem besedilu: SLA ali "Sporazum") med izvajalcem in naročnikom za zagotavljanje storitev IT, potrebnih za podporo in vzdrževanje informacijskega sistema.

**Odzivni časi in časi za odpravo napake se lahko razlikujejo od spodaj omenjenih časov, če so drugače opredeljeni v pogodbi oziroma v razpisni dokumentaciji ali če se naročnik in izvajalec za dotični primer drugače dogovorita.**

#### 7.1 Napaka

Napaka pomeni vsako negativno odstopanje v funkcionalnosti, videzu ali delovanju informacijskega sistema, ki ni v skladu z zahtevami, opredeljenimi v strokovnih zahtevah (priloga pogodbe), ali z zahtevami, ki so bile naknadno dogovorjene z izvajalcem in izvedene v obliki nadgradenj, ali ki deluje v nasprotju z navodili za uporabo informacijskega sistema.

#### 7.2 Odzivni čas

Odzivni čas je čas, ki preteče od prejema poročila o napaki do trenutka, ko izvajalec začne popravljati napako.

#### 7.3 Čas reševanja

Ciljni čas reševanja je čas, ki preteče od trenutka, ko izvajalec začne odpravljati napako (izteče se odzivni čas), do trenutka, ko je napaka odpravljena (ali je zagotovljena delujoča alternativna rešitev).

#### 7.4 Ciljni čas okrevanja (Recovery Point Objective)

Ciljni čas okrevanja je najdaljše ciljno obdobje, v katerem se lahko podatki (transakcije) izgubijo iz informacijskega sistema zaradi večjega incidenta.

#### 7.5 Klasifikacija napak

Napake se razvrstijo glede na njihovo resnost. Obstajajo štirje razredi resnosti:

##### **Razred 1 = 'Kritična napaka'**

Kritična napaka pomeni, če napaka ogroža varnost ali končnim uporabnikom onemogoča uporabo informacijskega sistema.

Zgledi napak te vrste so:

- vsaj polovica uporabnikov ne more uporabljati informacijskega sistema;
- podatki niso procesirani, so narobe sprocesirani oz. netočni;
- za napako ni nadomestne rešitve »workaround«;
- napaka povzroča nedelovanje informacijskega sistema ali občutno zmanjšuje performance delovanja.

##### **Razred 2 = 'Večja napaka'**

Večja napaka pomeni, če napaka končnim uporabnikom onemogoča uporabo funkcij ali dela funkcij in ni bila odpravljena s ponujeno rešitvijo in je zato uporaba informacijskega sistema omejena.

Zgledi napak te vrste:

- pogosta prekinitve delovanja informacijskega sistema in njegovih komponent ali periodična zaustavitve delovanja;
- pripravljen obhod »workaround« je neustrezen ali neučinkovit;
- zmožnosti delovanja informacijskega sistema so zmanjšane do te mere, da uporabniki ne morejo uporabljati sistema zaradi predolgega časa odziva na izvajanje storitev.

### **Razred 3 = 'Manjša napaka'**

Manjša napaka pomeni, če napaka ne preprečuje uporabe funkcij in če obstaja obvozna rešitev za napako.

Zgledi napak te vrste:

- napake, za katere obstaja primerna obvozna pot (ti. »workaround«), ki ne vpliva resno na operacije in performančne zmožnosti informacijskega sistema;
- napake, ki uporabniku onemogočajo rabo določenega postopka, zavajajoči uporabniški vmesnik;
- izguba dela funkcionalnosti ali fleksibilnosti, ki ne vpliva pomembno na končne uporabnike.

### **Razred 4 = 'Napaka dokumentacije ali vizualne skladnosti'**

Napaka dokumentacije ali vizualne skladnosti pomeni vsako napako v dokumentaciji. Napaka dokumentacije ali vizualne skladnosti obstaja v primeru neskladnosti med dokumentacijo, vizualnim videzom sistema in terminologijo.

Naročnik lahko nemoteno uporablja informacijski sistem.

Zgledi napak te vrste:

- kozmetične napake;
- manjša izguba fleksibilnosti;
- uporabnik ugotovi napako, vendar napačne funkcionalnosti ne uporablja in tako ne trpi posledic.

Glede na to, da naročnik informacijski sistem uporablja v produkciji, mora izvajalec zagotavljati ekipo strokovnjakov za celotno obdobje trajanje pogodbe, ki skrbijo za nemoteno delovanje, razvoj in nadgradnje. V sklopu vzdrževanja mora izvajalec zagotavljati reševanje napak in odpravljanje anomalij v delovanju informacijskega sistema, ter preventivno opozarjati na potencialno zmanjšanje zmožnosti delovanja in izpadov.

#### **7.6 Odzivni časi in časi za odpravo napak**

Odzivni čas je čas, ki preteče od prejema prijave napake, do trenutka, ko izvajalec začne z odpravljanjem napake. Čas za odpravo napake je tisti čas, ki preteče od prejema zahteve za odpravo napake, do takrat, ko je izvajalec odpravil napako. Odzivni čas na prijavo napak in čas za odpravo napake je odvisen od tipa napake.

Odzivni čas za prijavo napak oziroma incidentov v rednem delovnem času (ponedeljek do petek med 8 in 16 uro):

Tip napake	Odzivni čas	Čas za odpravo napake
Razred 1 – Kritična napaka	1 ura	<p><b>**4 ure</b></p> <p>Ponovna vzpostavitev storitve v naslednjih 4 urah po tem, ko je izvajalec obveščen o napaki. Izvajalec bo delal, dokler napaka ne bo odpravljena.</p> <p>Naročnik in izvajalec se bosta dogovorila o načrtu za izredne razmere, ki bo veljal, dokler se naročnik in izvajalec ne dogovorita, da je napaka odpravljena.</p>
Razred 2 – Večja napaka	4 ure	<p>8 ur</p> <p>Ponovna vzpostavitev storitve v naslednjih 8 urah po tem, ko je izvajalec obveščen o napaki. Izvajalec bo delal, dokler napaka ne bo odpravljena.</p>
Razred 3 – Manjša napaka	8 ur	<p>24 ur</p> <p>Ponovna vzpostavitev storitve v naslednjih 24 urah po tem, ko je izvajalec obveščen o napaki. Izvajalec bo delal, dokler napaka ne bo odpravljena.</p>
Razred 4 – Napaka dokumentacija ali vizualne skladnosti	12 ur	<p>48 ur</p> <p>Ponovna vzpostavitev storitve v naslednjih 48 urah po tem, ko je izvajalec obveščen o napaki. Izvajalec bo delal, dokler napaka ne bo odpravljena.</p>

**\*\*Nenehno poskušanje oziroma 4 ure**

Odzivni čas za prijavo napak oziroma incidentov in čas za odpravo napak oziroma incidentov izven delovnega časa:

- ponedeljek do petek med 16. in 8. uro zjutraj,
- sobota, nedelja in dela proste dni pa je 24/7.

Za prijavljene napake razreda 1 in 2 (kritične napake in večje napake) se časi odziva in odprave napak izračunavajo v časovnem oknu 24/7/365.

Časi odziva in odprave napak se izračunavajo znotraj normalnega delovnega časa od 6:30 16:30 ure za prijavljene napake razreda 3 in 4.

*Primer:*

- prijava napake s prioriteto 1 se izvede v torek ob 15:00. Reševanje incidenta se mora pričeti isti dan do 16:00. napaka mora biti razrešena naslednji delovni dan (sreda) do 16:00 ure.
- prijava napake s prioriteto 3 se izvede v torek ob 15:00. Reševanje napake se mora pričeti najkasneje v sredo ob 15. uri, napaka mora biti razrešena pet delovnih dni kasneje do 15.00 ure.

Nenehno poizkušanje razen v primerih, ko je za napako potrebna zamenjava dela strojne opreme ali popravek sistemske opreme in je čas odprave napake pogodbeno določen oziroma zagotovljen s strani principala (IBM,...).

## **8. Zagotovitev delovanja informacijskega sistema**

Izvajalec mora vzdrževati in izboljševati uporabo programa ter izpolnjevati nove zahteve funkcionalnosti, ki jih zahteva naročnik skladno z dobrimi praksami v IKT industriji.

Garancijska doba za odpravo napak za storitve, opravljene v okviru dopolnilnega vzdrževanja, ki posegajo v področje funkcionalnosti sistema, je 12 mesecev od naročnikove potrditve izvedbe naročila. Odpravljene napake storitev oziroma na storitvah, ki so opravljene v okviru dopolnilnega vzdrževanja, so po preteku 12 mesecev od naročnikove potrditve izvedbe naročila predmet osnovnega vzdrževanja sistema.

Izvajalec je dolžan dopustiti in omogočiti naročniku učinkovit nadzor nad kvaliteto opravljenih storitev. Naročnik ima pravico v času veljavnosti te pogodbe angažirati strokovnjake - poznavalce tehnologije in revizorje informacijskih sistemov, za presojo kakovosti opravljenih storitev (kakovost rešitev, ustreznost procesa izdelave, testiranja in dobave rešitev, ustreznost rešitev z vidika varovanja podatkov). V primeru takšnih presoj je izvajalec dolžan sodelovati s temi strokovnjaki in jim omogočiti dostop do tehnične dokumentacije in izvorne kode.

Naročnik je dolžan izvedbo presoje napovedati najmanj 8 dni pred presojo. V kolikor se med presojo ugotovijo neskladnosti, stroške revizije krije v celoti izvajalec.

Naročnik uporablja za podporo in upravljanje ITSM procesov (storitveni zahtevki, incidenti, problemi, spremembe, SLA in upravljanje IT sredstev) aplikacijo za upravljanje storitev IBM Maximo Control Desk (Maximo IT). Naročnik zahteva, da izvajalec redno beleži in rešuje vse zahtevke, incidente, spremembe ter ostale procese in mesečno poroča o dejansko opravljenem delu, njegovi vsebini in obsegu v naročnikovi aplikaciji IBM Maximo Control Desk (Maximo IT). V primeru, da zunanji izvajalec že ima vzpostavljen lasten sistem za beleženje, mora izvajalec na lastne stroške zagotoviti integracijo z IBM Maximo Control Desk (Maximo IT).

## 9. Ukrepanje in rezultati

Ko izvajalec prejme prijavo o napaki, potrdi status in vsebino zadevne napake v "odzivnem času" (kot je opredeljen v nadaljevanju). Izvajalec opravi oceno zahtevnosti posamezne zahteve. Po potrebi lahko izvajalec skupaj z naročnikom oceni zapletenost posamezne zahteve in se odloči, kako nadaljevati. Izvajalec obvesti naročnika o predvidenem datumu odprave napake in o potrebnih dejavnostih, ki jih je treba pri tem izvesti.

Izvajalec se odzove z akcijskim načrtom, namenjenim odpravi napake. Dejanski zahtevani odzivni čas je odvisen od resnosti napake in je naveden v SLA.

Odprava napake lahko pomeni tudi implementacija alternativne začasne rešitve, ki jo mora potrditi naročnik.

Po odpravi napake izvajalec o njeni odpravi obvesti naročnika oziroma se navedeno uredi v okviru ustrezne informacijske rešitve obveščanja o napaki.

**V primeru, da izvajalec prekorači odzivni čas ali čas za odpravo napake, so posledice opredeljene v pogodbi.**

## 10. Poročilo o delovanju platforme in odpravi napak

Izvajalec je dolžan naročniku predložiti poročilo o napaki, iz katerega bo razviden vzrok nastanka napake, predviden čas odprave napake ter obrazložitev napake. Poročilo je izvajalec dolžan v primeru kritičnih napak predložiti nemudoma po prijavi napake oziroma najkasneje v roku 24 ure po odpravi. V primeru nekritičnih napak je izvajalec dolžan poročilo predložiti naročniku najkasneje v roku 48 ur po odpravi napake.

Če izvajalec oceni, da bo odprava kritične napake trajala več kot štiri ure, mora o tem obvesti naročnika.

## 11. Preverjanje skladnosti izvajalca s smernicami

### • Nadzor s strani naročnika

Naročnik ima pravico izvajati nadzor nad delovanjem izvajalca, da se prepriča o skladnosti izvajalčevih aktivnosti s standardi in zahtevami, določenimi v zakonu informacijske varnosti, ter dobrimi praksami v industriji informacijskih in komunikacijskih tehnologij (IKT), kakor tudi s trenutnimi tehnološkimi smernicami ter s smernicami informatike UKC Ljubljana.

### • Obseg nadzora

Nadzor zajema pregled izvajalčevih notranjih postopkov, varnostnih mehanizmov, upravljanja z informacijami in pristopov k obvladovanju tveganj, ki vplivajo na zaupnost, celovitost in razpoložljivost informacijskih sistemov ter storitev, ki jih izvajalec zagotavlja naročniku. Obseg, metodologija in oblika nadzora je v izključni domeni naročnika (npr. samoocenitveni vprašalnik,...).

- **Dostop do dokumentacije in evidenc**

Izvajalec mora naročniku ali pooblaščenim predstavnikom omogočiti dostop do vse relevantne dokumentacije, evidenc, ter podatkov o delovanju svojih sistemov in praksah, ki omogočajo preverjanje skladnosti z Zakonom o informacijski varnosti ter industrijskimi standardi.

- **Ukrepi in priporočila**

V primeru, da se ob nadzoru ugotovi neskladnost ali pomanjkljivosti, mora izvajalec v roku, dogovorjenem z naročnikom, odpraviti neskladnosti in slediti naročnikovim priporočilom za izboljšanje, skladno s tehnološkimi smernicami in dobrimi praksami v IKT industriji.

- **Poročilo o izvedenem nadzoru**

Po izvedenem nadzoru naročnik lahko pripravi poročilo, ki vsebuje ugotovitve, priporočila ter morebitne roke za izvedbo popravnih ukrepov. Izvajalec mora v roku, določenem v poročilu, zagotoviti odpravo morebitnih ugotovljenih neskladnosti in o tem obvestiti naročnika.

- **Varovanje poslovnih skrivnosti**

Vse informacije, ki jih naročnik pridobi med nadzorom, so zaupne narave in jih mora naročnik obravnavati kot poslovno skrivnost izvajalca, razen če zakon določa drugače.

- **Kršitev določil nadzora**

V primeru, da izvajalec ne omogoči nadzora ali ne odpravi ugotovljenih neskladnosti, si naročnik pridržuje pravico do uvedbe dodatnih ukrepov, vključno z morebitno prekinitvijo pogodbe, če so neskladnosti take narave, da pomembno vplivajo na izvajanje storitev.