



# VZPOSTAVITEV CENTRALNEGA PODATKOVNEGA SKLADIŠČA IN ANALITSKIH ORODIJ

Tehnične zahteve

ELES, d.o.o.

## 1 Vsebina

1	Vsebina .....	I
2	Definicije pojmov in kratic.....	II
3	Uvod .....	3
4	Predmet naročila .....	4
5	Splošno .....	4
5.1	Omejitve in posebnosti .....	5
6	Obseg del .....	5
6.1	Vzpostavitev okolja (Generalne zahteve): .....	5
6.2	Vzpostavitev standardov razvoja in dodatna orodja in zahteve: .....	6
6.3	Izobraževanje .....	7
7	IT zahteve.....	7
7.1	Splošne zahteve .....	7
7.2	Tehnične in varnostne zahteve.....	9
7.2.1	Splošne tehnične zahteve: .....	9
7.3	Tehnične zahteve pri namestitvi v oblaku (najem storitve) .....	9
7.3.1	Minimalne varnostne zahteve za storitve v oblaku .....	11
7.4	Varna arhitektura in razvoj.....	12
8	Dogovor o nivoju izvajanja storitev.....	14
8.1	Definicija pojmov .....	14
8.2	Izvajanje podpore in vzdrževanja .....	15
8.3	Nivo izvajanja storitev .....	18
8.3.1	Določanje prioritete izvajanja storitev .....	18
8.3.2	Čas obratovanja storitev in odzivni časi .....	19
8.4	Pogodbena kazen za izvajanje podpore in vzdrževanja .....	20

## 2 Definicije pojmov in kratic

BC	Business Connect
BI	Poslovna inteligenca (Business Intelligence)
D365	Dynamics 365
DWH	Centralno podatkovno skladišče (Data Warehouse)
ETL	Extract Transform Load

### 3 Uvod

ELES je kot sistemski operater prenosnega omrežja v Republiki Slovenije zadolžen za prenos električne energije. Tega zagotavlja z neprekinjenim upravljanjem omrežja, strokovnim vzdrževanjem in razvojem. Storitve prenosa električne energije izvaja za potrebe tako slovenskega kot tudi mednarodnega trga z električno energijo.

ELES se je zavezal k optimizaciji dela, procesov in modernizaciji informacijskega sistema in se odločil za uvedbo modernega poslovnega sistema ERP in modernega sistema za podporo upravljanja s sredstvi ter operativnega delovanja.

Z vpeljavo novih naprednih sistemov (D365, BC,...) se je izkazala potreba po naprednem sistemu (BI orodju), ki nam bo omogočal pridobivanje in združevanje podatkov iz različnih informacijskih virov ter pripravo podrobnih analiz in naprednih poročil.

Uporabnik bo lahko z naprednim orodjem sam kreiral prilagodljive interaktivne vizualizacije podatkov na enostaven »povleci in spusti« način. Svoje predstavitve bo lahko delil med ostale uporabnike. Iz centralnega mesta za upravljanje z dovoljenji bo lahko nadziral, kaj lahko ostali uporabniki v njegovi predstavitvi vidijo. Dovoljenja bomo lahko določili za skupine ali neposredno za uporabnika.

V primeru, da bo želel uporabnik v svoji predstavitvi prikazati podatke, ki trenutno niso zajeti v sistem, se bo lahko z uporabo ustreznega vmesnika, ki ga bo nudilo orodje, povezal na kateri koli drug ustrezen vir podatkov, kasneje pa bo lahko od ustreznih služb zahteval, da se manjkajoči podatki dodajo v DWH. Te podatke bo lahko uporabnik nato vključil v svoje predstavitve ali zgradil popolnoma novo predstavitev, za katero bo lahko določil ustrezna dovoljenja in jo nato posredoval ostalim uporabnikom.

Uporabnik bo lahko vse zgoraj naštetе funkcionalnosti izvedel sam brez predhodnega tehničnega znanja. Tako se bo lahko uporabnik osredotočil na tisto, kar je pomembno – na podatke in iz njih pridobil uporabne informacije. Te informacije bodo uporabniku zaradi naprednih algoritmov in samega naprednega delovanja sistema, predstavljene v odzivnem času.

Z naprednim sistemom bo uporabnik dobil potrebne informacije iz aktualnih podatkov, ki bodo pripravljene po sodobnih metodologijah in predstavljene na uporabniku razumljiv in jasn način. Lahko bo pregledoval »živa« poročila in izvajal analize na realnih podatkih. Napredni uporabnik bo lahko tudi dodajal svoje podatke ali vire podatkov in jih vključil v že obstoječo analizo. Lahko bo izdelal tudi popolnoma novo poročilo oziroma analizo. Izdelke bo lahko shranjeval v datoteke ali jih neposredno delil z drugimi.

## 4 Predmet naročila

Predmet naročila je nabava, implementacija, vzdrževanje naprednega poročevalskega sistema in licenc ter usposabljanje uporabnikov in administratorjev v družbi ELES d.o.o. za potrebe vodstva.

- implementacija tehnološke platforme za postavitev DWH na ravni družbe.
- izdelava tehničnih standardov in postopkov izgradnje storitev poslovne inteligence/analitike ELES.
- opis postopkov implementacije uporabniških zahtev poslovne inteligence/analitike.
- nabava dodatne oz. licenčne programske opreme drugih proizvajalcev za vzpostavitev enotne platforme za DWH
- izdelava integracijskih vmesnikov in povezav ter umestitev platforme v obstoječ poslovno informacijski sistem ELES.
- implementacija poslovnih pravil, analiz za notranje naročnike.
- izdelava tehnične in uporabniške dokumentacije.
- izobraževanje administratorjev za delo z DWH.

Naročnikova obstoječa infrastruktura temelji na Microsoftovi programski opremi v MS Azure. V sklopu obstoječe pogodbe z proizvajalcev bo naročnik zagotovil najem potrebne programske opreme (PaaS in SaaS, predvidene storitve MS Fabric, Purview, Azure DevOps, Power BI in ostali standardni gradniki za vzpostavitev okolja oz. primerljive).

V kolikor izvajalec predvideva uporabo dodatnih oz. drugih komponent (t.i. »third-party« programska oprema (programska oprema, ki je na voljo v sklopu Azure Marketplace oz. ostala licenčna programska oprema) in lastno razvita programska oprema jo izvajalec mora vključiti v sklopu svoje ponudbe.

Naročnik ima pravico, da v sklopu začetnega obsega in priprave BI Arhitekture od izvajalca zahteva uporabo standardnih SaaS in PaaS gradnikov MS Azure, saj je za naročnika ključno da sledi dobrim praksam in sodobnim standardom uporabe oblačne rešitve.

## 5 Splošno

Sistem bo namenjen zbiranju podatkov, obdelavi in pregledovanju le-teh ter po potrebi izpisovanju poročil družbe Eles (skupine Eles). Sistem mora omogočati spremljanje delovanja in migracije podatkov ter javljati napake, ki so nastale pri dnevni migraciji podatkov.

### AVTORSKE PRAVICE

Izvajalec je ob predaji tistega dela predmeta pogodbe, ki predstavlja avtorsko delo, najkasneje do izdaje Potrdila o prevzemu, dolžan izročiti naročniku vso dokumentacijo, ki jo je izvajalec pripravil zanj po tej pogodbi.

Izvorna koda:

Izvorno kodo programske opreme mora izvajalec predati na nosilcu podatkov oz. v Eles Azure okolju (Dev Ops), ki ga je mogoče prebrati na sistemu naročnika. Priložiti mora tudi pripadajočo dokumentacijo, ki podrobno pojasnjuje aplikativno rešitev in podatkovno strukturo informacijske rešitve.

Pogodbeni stranki se dogovorita, da izvajalec na naročnika prenese izključno pravico predelave programske opreme tako, da je naročniku omogočen dostop s polnimi pravicami do vzdrževanja, dopolnjevanja in spreminjanja programske opreme.

Pri standardni programski opremi, katere pravice ima tretja oseba, izvirne kode ni potrebno predati.

## SLOVENSKI JEZIK

Izobraževanje in uporabniška dokumentacija v slovenskem jeziku.

### 5.1 Omejitve in posebnosti

Izvajalec mora pri izvedbi del upoštevati:

- obstoječe poslovno okolje v podjetju naročnika (tudi okolje v oblaku),
- obstoječe podatke v informacijskih sistemih naročnika,
- obstoječe varnostne sheme naročnika,
- obstoječo zakonodajo (Energetski zakon, Zakon o gospodarskih družbah, Slovenski računovodski standardi, Mednarodni računovodski standardi),
- varnostno politiko naročnika,
- osvežitev, prenos, transformacija informacijskih podatkov mora biti časovno usklajena z drugimi opravili na sistemih. Naročnik in izvajalec natančno določita urnike implementacije sistema.

## 6 Obseg del

Izvedba storitev:

1. Načrtovanje in analiza
2. Priprava BI Arhitekture in BI skrbništva
3. Vzpostavitev okolij
4. Vzpostavitev standardov razvoja
5. Implementacija analitične rešitve:
  - a. Skupne dimenzije
  - b. Kadrovska evidenca in obračun
6. Izobraževanje
7. Podpora in vzdrževanje sistema

### 6.1 Vzpostavitev okolja (Generalne zahteve):

- Okolje mora biti postavljeno skladno z ELES Azure landing-zone specifikacijami.
- Okolje za gostovanje sistema bo treba v celoti konfigurirati v okviru ELES Azure oblaka.
- Konfigurirano okolje mora ustrezati vsem Microsoft priporočenim najboljšim praksam, varnostnim zahtevam in omejitvam ter v celoti podpirati razvojni življenjski cikel, tj. razvojno, testno in produkcijsko okolje.
- Konfigurirano okolje se mora varno povezovati z notranjim omrežjem Eles.
- Implementacija rešitve mora biti izvedena v skladu s smernicami metodologije Microsoft CAF (Microsoft Cloud Adoption Framework za Azure).
  - Infrastruktura kot koda (implementacija preko skript BICEP; verzioniranje,...)
  - Integracija CI/CD (CI - Continuous Integration in CD - Continuous Deployment) z uporabo Azure DevOps."
- Integracij z obstoječo infrastrukturo Sentinel, Defender, .....
- Sistem bo potrebno implementirati z iskanjem najboljše zmogljivosti z optimalno količino virov. Arhitektura rešitve se lahko prilagodi med izvajanjem, kolikor je potrebno, da se doseže najbolj optimalen rezultat glede na stroške virov, implementacijo in podporo, hitrost delovanja itd.

Učinkovitost in optimizacija rešitve bosta nenehna naloga v vseh fazah projekta (tudi v sklopu podpore in vzdrževanja). Pričakuje se, da bo dobavitelj zagotovil najboljše prakse, vpoglede in priporočila za optimizacijo zmogljivosti rešitve in Azure stroška ter implementacijo zahtevanih sprememb in izboljšav.

## 6.2 Vzpostavitev standardov razvoja in dodatna orodja in zahteve:

- Implementacija zbiranja podatkov v Azure Monitor.
- Zagotoviti ustrezní nivo varnosti in upravljanja nad podatki:
  - o Vzpostavitev upravljanja in centralnega pregleda (preko administratorskega portala in poročil) nad podatki in okoljem: data lineage, data protection, certification, catalog integration
  - o Integracija z Defender for Cloud Apps in Azure Active Directory.
- Definiranje postopkov za konfiguracijo okolja in upravljanje sprememb znotraj Azure DevOps.
- Vzpostavitev standardov razvoja za potrebe podpore za skupinsko delo, obvladovanje napak, obveščanje napak:
  - o Enotnega imenovanja (standarde poimenovanja objektov)
  - o Beleženje dogodkov
- Vzpostavitev naprednega ogrodja (angl. Framework), ki omogoča učinkovito integracijo podatkov iz podatkovnih virov z naslednjimi lastnostmi:
  - o ETL postopek mora omogočati delna polnjenja podatkov, enostavno kontrolo postopka, ponovljivost, sledljivost idr.
  - o Možnost časovnega nastavljanja proženja ETL postopkov.
  - o Možnost ročnega proženja dela ETL postopka na zahtevo.
  - o Samodejno obveščanje o stanju izvedbe ETL skrbnikom sistema (uspešno, neuspešno ...).
  - o Razhroščevanje (angl. debugging) pri razvoju ETL postopkov.
- Vzpostavitev in razvoj podporne aplikacije za določanje definicij in poslovnih pravil s strani skrbnikov vsebinskih področij . Aplikacija mora omogočati kreiranje vnosnih mask na enostaven način (brez programiranja). Primeri uporabe:
  - o Kreiranje in upravljanje uparjalnih tabel (generičen vmesnik - možnost opredelitve preslikav med npr. konti in postavkami izkazov brez poseganja skrbnika sistema BI ali zunanjih izvajalcev).
  - o Kreiranje in upravljanje pravil ETL postopka: parametri, definicije grupiranja, definicije hierarhij (generičen vmesnik - Možnost uporabniškega oblikovanja hierarhij (agregacije) po meri).
- Vzpostavitev rešitve mora temeljiti na sodobnem pristopu organizacije podatkov v enotni podatkovni platformi (t.i. Data LakeHouse arhitektura), znotraj platforme se morajo podatki poenotiti v Delta Parquet formatu. Nad temi podatki mora biti omogočeno izvajanje procesiranja za različne odjemalce oz. analitične scenarije.
- Vzpostavljena rešitev mora omogočiti integracijo z MS Purview za pripravo kataloga podatkov in zaščito podatkov (Purview Information Protection).
- Vzpostavitev Azure Monitoring in Azure Notification
- Vzpostavitev uporabniške podpore za delo (generiranje osnovne kode in funkcij za dostop do podatkov, pomoč pri pripravi analiz in poročil) z uporabo AI funkcionalnosti na način pogovorne komunikacije (Primer: Copilot)
- Uporaba Power BI za pripravo poročil in analiz.
- Možnost analiziranja podatkov v Excelu z direktno povezavo na podatkovno platformo.

## 6.3 Izobraževanje

Usposabljanje bo zajemalo:

- Izobraževanje za končne in ključne uporabnike. Izobraževanje se izvede sproti ločeno za vsako vsebinsko področje. Pri tem se za vsako vsebinsko področje izvede delavnico, ki zajema najmanj predstavitev uporabe Power BI in predstavitev uporabe analitičnega modela nad referenčnimi Power BI poročili. Uporabniki po delavnici izvedejo preizkušanje referenčnih poročil. Po preizkušanju se organizira sestanek oz. delavnico, na kateri se naslovi morebitne nejasnosti in pomanjkljivosti.
- Izobraževanje za skrbnike sistema poslovnega obveščanja. Skrbnike sistema se mora izobraziti in jim predstaviti, kako vzdrževati rešitev BI. Ob zaključku izobraževanja morajo skrbniki osvojiti znanje za samostojno delo in spremembe v rešitve BI (ETL, analitični model, Power BI, nadzorna aplikacija za urejanje definicij in poslovnih pravil).

## 7 IT zahteve

### 7.1 Splošne zahteve

- Vsi grafični vmesniki omogočajo enostavno, intuitivno in pregledno uporabniško izkušnjo;
- Sistem mora omogočati dostop iz mobilnih naprav z kontrolo z MS Intune in Conditional Access politikami;
- Sistem mora omogočati enostavno, intuitivno in pregledno uporabniško izkušnjo tudi na mobilnih napravah;
- Nadzorni programski vmesnik (Monitoring in Obveščanje (Notification)) zagotavlja enostavne preglede in obveščanje:
  - nad izmenjavami podatkov z ostalimi sistemi;
  - prikazom napak v procesu (sporočilna lista potrjenih/nepotrjenih napak),
  - trenutnega stanja sistema,
- enostavna navigacija, uporabniški meniji, zagotovitev bližnjic do najpogosteje uporabljenih poročil;
- priprava in možnost uporabe vnaprej pripravljenih poročil, statistik in evidenc;
- vgrajena validacijska pravila (logične kontrole opozarjanja na nepravilne vnose podatkov in zamrznitev nadaljevanja izračunov/javljanje nekonsistenc v primeru nevpisanih/neveljavnih podatkov);
- možnost prenosa dokumentov (poročil, evidenc, statistik) v MS Office okolje.
- Ponudnikova rešitev mora biti usklajena z arhitekturo in operativnim modelom ELES Azure Learning Zone (ALZ) (Vsebine dokumenta si lahko ponudnik ogleda na lokaciji naročnika v okviru razpisnega postopka).
- Model storitve
  - Storitve najema v SaaS oz. v kolikor to ni mogoče oz. na voljo v kombinaciji PaaS in SaaS
- Ponudnik storitev
  - Azure
- Izbor regije na podlagi
  - Zakonodaje (EU model klavzule)
  - Razpoložljivost storitve
  - Razpoložljivost območja razpoložljivosti
  - Cenovna politika
- Okolja
  - Razvojno in testno



- Produkcijsko

Vezano na poglavje 6.1 bo potrebno implementirati z iskanjem najboljše zmogljivosti z optimalno količino virov naročnik dopušča možnost da Razvojno in Testno okolje uporabljata določene skupne storitve oz. podatke.

- Omrežje
  - Izpostavljenost
    - Javno/Zasebno
      - Javno –Viri so na voljo na javnih IP končnih točkah
      - Zasebno –Viri so na voljo na zasebnih IP končnih točkah in objavljeni prek centralnega varnostnega elementa
    - Standardni upoštevani postopki objave aplikacij ELES
      - Azure Application Gateway, požarni zid Azure, itd...
    - Zahteve po protokolu odjemalca
      - HTTPS (443), itd...
      - Zahtevana omrežna vrata za vse sestavne dele rešitve
    - Zahteva certifikata
      - Javno CA potrdilo
    - Hibridno omrežje
      - Zahteve hibridnega omrežja (npr. Spredaj v oblaku – Zadaj v podjetju)
      - Segmentacija/izolacija omrežne pod mreže in velikosti pod mrežij
  - Omrežna zakasnitev
    - Aplikacija mora delovati znotraj območja Zahodna Evropa ali Severna Evropa
- Ponudnik mora zagotoviti arhitekturni diagram
- Ponudnik mora zagotoviti landing-zone postavitev za vsak gradbeni blok arhitekture
- Model implementacije
  - Zahteva po kodi IaC (npr. BICEP)
  - Zahteva po razvoju (npr. YAML)
- Zahteve HA / DR
  - Arhitektura vključuje načrt visoke razpoložljivosti in/ali obnovitve po nesreči
- Zmogljivost
  - Arhitektura vključuje načrt zmogljivosti in kapacitete na podlagi vstopa ELES
- Upravljanje in vodenje
  - Ponudnik mora zagotoviti, da je upravljanje in vladanje del projekta
- Upravljanje
  - Spremljanje
  - Opozorila
  - Varnostno kopiranje
  - Upravljanje posodobitev
  - Upravljanje sprememb in sledenje spremembam
- Pravno
  - v primeru obdelave osebnih podatkov je potrebna skladnost z odredbo GDPR in ZVOP2
  - skladnost z Zakon o informacijski varnosti (ZInfV)
  - skladnost z NIS2 direktivo
- Varnost
  - Omrežna varnost (FW, AppGW, WAF, IDS, IDP, DDoS, ...)
  - Varnost podatkov (v mirovanju / med prenosom)
  - Zasebnost podatkov
  - Klasifikacija podatkov
  - Upravljanje identitet in dostop

- Potrebna dovoljenja za vloge lastnika/skrbnika/uporabnika rešitve
- Potrebni drugi varnostni principi, na primer upravljana identiteta, storitveni principi, registracija aplikacij

## 7.2 Tehnične in varnostne zahteve

Naročnik zahteva namestitev sistema v oblačno okolje naročnika (uporaba oblačnih storitev, ki jih naročnik že najema (Microsoft Azure)).

### 7.2.1 Splošne tehnične zahteve:

- Vse povezave, ki se uporabljajo za izmenjavo podatkov preko javnega omrežij, morajo biti šifrirane.
- Uporabniški vmesnik mora biti izveden kot spletna aplikacija oz. kot mobilna aplikacija na mobilnih napravah. Objavljena mora biti preko varne povezave (https).
- Uporabniški vmesnik mora delovati na brskalniku Microsoft Edge brez namestitve vtičnikov oz. preko mobilne aplikacije na mobilnih napravah.
- Sistem mora beležiti dnevniške zapise in revizijske sledi.
- Sistem mora beležiti in omogočati pošiljanje dnevniških zapisov in revizijskih sledi v obliki syslog.
- Storitve je lahko dostopna uporabniku zgolj po njegovi predhodni enolični identifikaciji. Zahteva ne velja za tisti del objavljenih storitev, za katere naročnik zahteva, da je na voljo splošni publiki (npr: javna spletna stran)
- Prijava v storitev (avtentikacija) mora potekati na način, ki onemogoča nepooblaščen razkritje ali uporabo avtentikacijskih podatkov.
- Šifriranje podatkov in komunikacij (tam kjer je prisotno), mora biti izvedeno s sodobnimi močnimi šifrirnimi algoritmi in metodami. Uporaba šibkih šifrirnih algoritmov in metod ne sme biti mogoča.
- Uporabniški vmesnik mora podpirati uporabo sistema enkratne prijave (SSO).
- Sistem mora podpirati standardne vmesnike za integracijo z MFA sistemi
- Sistem mora podpirati standardne vmesnike za integracijo z IM sistemi
- Izdelan mora biti tehnični arhitekturni dokument (HLD, LLD), ki mora zajemati najmanj:
  - o blokovna shema gradnikov sistema
  - o njihova povezanost in soodvisnost,
  - o opisani in označeni komunikacijski protokoli in smer prometa
  - o opisane morajo biti integracijske točke in načini integracije z obstoječimi inf. sistemi naročnika
- Rešitev mora omogočiti delovati v visoko razpoložljivostnem načinu (HA)

## 7.3 Tehnične zahteve pri namestitvi v oblaku (najem storitve)

Sistem mora podpirati avtentikacijo z uporabo Azure Aktivnega imenika (MS Entra ID).

Za nastavljanje pravic dostopa mora biti možno uporabiti varnostne skupine v Azure Aktivnem imeniku.

Prometni tokovi naj se vzpostavljajo od naročnika proti ponudniku storitev, če je podatkovni tok dvosmeren ali samo v smeri od ponudnika storitve proti naročniku mora biti za komunikacijo uporabljen »Site 2 Site IPSec VPN«

Izvajalec storitve je dolžan naročnika nemudoma (v roku 2 ur po tem, ko je zaznal incident) obvestiti o varnostnih incidentih v katerih so ali bi lahko bili ogroženi podatki naročnika in njegovih uporabnikov.

Izvajalec mora ob prenehanju uporabe storitve v oblaku zagotoviti naročniku možnost pridobitve njenih podatkov na enostaven način in v obliki, ki ji omogoča nadaljnjo uporabo ali pretvorbo podatkov v drugo ustrezno obliko.

Ponudnik lahko za napisane zahteve predlaga nadomestno rešitev. Naročnik lahko nadomestno rešitve zavrne in ponudbo označi kot neustrezno.

Izvajalec mora pripraviti šolanja za uporabnike in administratorje sistema. Po koncu šolanj morajo uporabniki in administratorji sistema osvojiti znanje za samostojno delo s sistemom.

Izvajalec pripravi tudi vso potrebno tehnično in uporabniško dokumentacijo. Katero dokumentacijo in o vsebini se naročnik in izvajalec dogovorita po podpisu pogodbe.

### 7.3.1 Minimalne varnostne zahteve za storitve v oblaku

#### Namen minimalnih varnostnih zahtev

Poglavje določa minimalne varnostne zahteve za storitve v oblaku, ki so vključene v sklopu ponudbe in jih naročnik še ne najema. Na osnovi minimalnih varnostnih zahtev za storitve v oblaku se naročnik odloča ali bo določeno storitev v oblaku sprejel v uporabo ali ne. Navedene minimalne varnostne zahteve predstavljajo zgolj osnovni okvir za odločanje.

#### Varnostne zahteve za storitve v oblaku

Varnostne zahteve za varnostno kategorijo storitve v oblaku so opredeljene v spodnji tabeli.

Varnostna zahteva
Centralizirano upravljanje identitete uporabnikov (kreiranje uporabnikov, nastavljanje njihovega profila, ukinitve uporabniškega imena).
Upravljanje avtentikacijskih podatkov uporabnikov (določanje politike gesel, načini avtentikacije, ...).
Storitev je mogoče uporabljati zgolj po predhodni enolični identifikaciji uporabnika (prijava v storitev, uporaba določenega identifikatorja, ki ga ni mogoče podvajati ...).
Prijava v storitev (avtentikacija) mora potekati na način, ki onemogoča nepooblaščen razkritje ali uporabo avtentikacijskih podatkov (npr. z uporabo šifriranja komunikacije, OTP, ...).
Možnost integracije prijave v storitev z uporabo AD uporabniških imen brez posredovanja gesel (ali njihovih odtisov) izvajalcu storitve v oblaku (npr. uporaba modelov zaupanja, federacije ...).
Komunikacija med uporabnikom in storitvijo v oblaku mora biti šifrirana.
Uporabnikom je mogoče dodeljevati nivoje dostopa oz. funkcionalnosti storitve.
Pri storitvah, ki omogočajo različne funkcionalnosti in nivoje dostopa za različne uporabnike, mora biti možnost delegiranega upravljanja z nivoji dostopa in funkcionalnostmi storitve.
Izvajalec storitve v oblaku ima veljaven certifikat ISO 27001 ali drug ustrezen certifikat s področja informacijske varnosti.
Naročnik je omogočeno izvajanje presoje informacijske varnosti ponudnika storitve v oblaku ali mu je na razpolago vpogled v poročilo neodvisne revizije informacijske varnosti, ki je bila izvedena pri ponudniku storitve v oblaku.
Naročnik je seznanjen s seznamom pogodbenih podizvajalcev izvajalca storitve v oblaku.
Z izvajalcem storitve v oblaku mora biti podpisana pogodba po obdelavi osebnih podatkov.
Osební podatki se hranijo v podatkovnih centrih znotraj držav EU območja oz. v državah za katere je IP-RS izdal mnenje, da zagotavljajo ustrezen nivo varstva osebnih podatkov. Enaka zahteva velja tudi za varnostne kopije teh podatkov oz. redundantne podatkovne centre.
Podatki (ki niso osebni podatki), ki se obdelujejo ali hranijo med izvajanjem storitve v oblaku, se nahajajo v podatkovnih centrih znotraj držav EU območja oz. v državah za katere je IP-RS izdal mnenje, da zagotavljajo ustrezen nivo varstva osebnih podatkov. <sup>1</sup> Enaka zahteva velja tudi za varnostne kopije teh podatkov oz. redundantne podatkovne centre.
Izvajalec storitve v oblaku izvaja aktivnosti obdelave osebnih podatkov v skladu s Splošno EU uredbo o varstvu osebnih podatkov (GDPR)
Šifriranje podatkov in komunikacij (tam kjer je prisotno), mora biti izvedeno s sodobnimi močnimi šifrirnimi algortmi in metodami. Uporaba šibkih šifrirnih algortimov in metod ne sme biti mogoča.
Uporabnikovi podatki se hranijo (v kolikor je za to potreba) pri ponudniku storitve v oblaku v šifrirani obliki.
Zagotavljanje izpolnjevanja zahtev LI in DR v skladu z veljavno zakonodajo.

<sup>1</sup> Kljub temu, da tukaj ne gre za obdelavo osebnih podatkov, se tudi za ostale potrebe uporablja isti seznam držav

<b>Varnostna zahteva</b>
Naročnik ima možnost dostopa (neposredno ali posredno prek določenih storitev ponudnika) do revizijskih sledi dostopov in uporabe storitve v oblaku.
Naročnik ima možnost pridobitve in prenosa revizijskih sledi obdelav osebnih podatkov.
Izvajalec storitve je dolžan naročnika nemudoma obvestiti o varnostnih incidentih v katerih so ali bi lahko bili ogroženi podatki naročnika oz. njegovih uporabnikov.
Storitev ima pogodbeno določen SLA.
Storitev omogoča (v naprej definirano obdobje) dostop do podatkov tudi po prekinitvi pogodbe med družbo in izvajalcem storitve v oblaku.
Storitev ima v pogodbi določen najdaljši čas v katerem se pri izvajalcu storitve nepovratno pobrišejo podatki (po poslani zahtevi za brisanje ali po prekinitvi uporabe storitve), vključno s kopijami podatkov na varnostnih kopijah in/ali redundantnih podatkovnih centrih.
Družba ima ob prenehanju uporabe storitve v oblaku možnost pridobitve njenih podatkov na enostaven način in v obliki, ki ji omogoča nadaljnjo uporabo ali pretvorbo podatkov v drugo ustrezno obliko.

## 7.4 Varna arhitektura in razvoj

Pri načrtovanju, razvoju, spremembah in vzdrževanju storitev, sistemov in/ali posameznih delov ter komponent je potrebno upoštevati varnostne usmeritve. Pri razvoju aplikacij je zagotavljanje informacijske varnosti ključnega pomena v vseh fazah razvojnega cikla, od analize zahtev, varnega načrtovanja, upravljanja in vzdrževanja ter ni odvisno od uporabljene projektne metodologije (slap, agile, ipd.). Pri razvoju je potrebno upoštevati priporočila, dobre prakse in standarde s področja razvoja:

- aplikacijski varnostni življenjski cikel (Secure Software Development Lifecycle - SSDLC);
- raba aplikacijskih varnostnih metrik (npr. OWASP);
- standard ISO/IEC 27034 – varnost aplikacij;

Načela varnega načrtovanja/razvoja tako vključujejo vsaj:

- Načelo varnega pristopa že v fazi načrtovanja (Security by design), kjer je vsaka storitev, sistem in njegove posamezne komponente, zasnovana na podlagi in s poudarkom na varnosti. Ob načrtovanju se posveča veliko pozornost morebitnim tveganjem namernih napadov in nepooblaščenih posegov ter z dobro zasnovo zmanjšuje posledice zaznanih morebitnih varnostnih tveganj. Upošteva se delitev kibernetnega prostora družbe na posamezne smiselne dele (cone), za katere veljajo enaka varnostna pravila.
- Načelo krčenja obsega možnega napada (Attack surface reduction): to je zmanjševanje vpliva in števila tveganj, z namenom zniževanja napadalčeve zmožnosti za izrabo varnostnih ranljivosti in potencialnih varnostnih ranljivosti v sistemih, komponentah in/ali storitvah. Načelo vsebuje oziroma se dopolnjuje z principi varnega razvoja programske opreme, načelom najmanjšega nivoja pravic, načelom minimalnih funkcionalnosti sistemov, ipd.
- Načelo najmanjšega nivoja pravic, potrebnih za nemoteno izvajanje dela (Minimal need-to-know), to pomeni, da se vsaki komponenti ITK sistemov in vsakemu uporabniku dodelijo najnižje možne pravice, ki jih potrebujejo za delo (izvršitev zelenega ukrepa ali dostopa). Pravice in možnost dostopa se omejuje tudi uporabnikom z upravljavskimi pravicami in programom za upravljanje informacijskega sistema in sicer na najmanjšo mero, še potrebno za izvedbo njihovih nalog oziroma funkcij. Aplikacije in omrežne storitve se ne zaženejo pod skrbniškimi privilegiji, temveč samo z golim minimumom potrebnih dostopovnih pravic.
- Načelo omejevanja dostopa (Least Privilege Access Principle - LPAP), to pomeni, da mora biti tako povezljivost (dostop) do vsakega sistema in/ali posamezne komponente in sama povezljivost posameznega sistema in/ali komponente upravljana, nadzorovana in omejena. Neposreden dostop do svetovnega spleta je omogočen le tam, kjer je nujno potreben. Z varnostno občutljivih con je dostop, do zunanjih sistemov in svetovnega spleta, prepovedan.
- Načelo razmejitev dolžnosti oziroma ločevanja vlog (duty segregation policy).

- Načelo ločevanja razvojnih, testnih in produkcijskih okolij in v njih uporabljenih podatkov.
- Načelo neprekinjenega varnega poslovanja, kjer se že ob zasnovi sistema upošteva ocena tveganja in zagotovi zmožnost izdelave varnostnih kopij in upošteva principe za zagotavljanje odpornosti
- Načelo vzpostavitve jasne odgovornosti skupine ali posameznika v kibernetnem okolju družbe (Establish responsibility)
- Umeščanje informacijskih sredstev, sistemov in storitev v primerne varnostne cone, to pomeni da je potrebno posamezno sredstvo, sistem ali storitev, glede na zunanje zahteve (zakon, pogodbe, ipd) in/ali ocenjenega učinka na družbo ali posameznike, v primeru ogrožanja ali izgube zaupnosti, celovitosti ali razpoložljivosti, umestiti v primerno varnostno cono. Vsaka cona ima svoja specifična varnostna pravila. Neposredne povezave med informacijskimi sredstvi ali sistemi, ki so več kot dve coni narazen praviloma niso dovoljene.
- Načelo minimalnih funkcionalnosti sistemov (Least functionality): na sistem namestimo samo za njihov namen nujno potrebno programsko opremo in ga prilagodimo na način najmanjših, a za osnovni namen še zadostnih, nastavitvev (konfiguracij).
- Načelo poglobljene obrambe (Defence-in-depth principle), Načelo poglobljene obrambe: varnostnih tveganj se ne rešuje z enim samim slojem zaščite ampak se omejijo z izvajanjem postopnih, večstopenjskih in dopolnilnih varnostnih ukrepov - če kdo zaobide en sloj zaščite, zaščito ponujajo preostali zaščitni sloji.
- Načelo podvojenosti (Redundancy principle), kjer je celoten ITK sistem zasnovan tako, da odpoved posameznih komponent ne vpliva (poslabša) na varnost. S tem preprečimo nastanek napake na enem mestu (Single point of failure)
- Načelo ničelnega zaupanja (0 trust model), kjer ne predvidevamo varnosti posameznega elementa, ali zahteve, neglede na to kakšna je, iz kje izvira, kje ima ponor. Načelo ničelnega zaupanja od nas zahteva ravnanje: «nikoli ne zaupaj, vedno preveri».
- Skrb za nenehno utrjevanje (Hardening) storitev, sistemov in komponent v kibernetnem okolju
- družbe, kar pomeni rabo orodij, tehnik in dobrih praks, za zniževanje ranljivosti programske in strojne opreme.
- Raba in upravljanje kriptografskih kontrol in mehanizmov za zagotovitev:
  - Avtentikacije oziroma overjanja (ang. authentication): zagotoviti moramo verifikacijo resničnosti identitete (uporabnika in/ali informacijske komponente/sistema) in verifikacijo resničnosti izvora podatkov in informacij. Praviloma se za dostop do informacijskih virov in storitev družbe uporabljajo domenski računi in večfaktorska avtentikacija;
  - Zaupnosti (ang. confidentiality) in tajnosti (ang. secrecy): z ustreznimi postopki šifriranja moramo zagotoviti zaupnost povezave med uporabnikom in prejemnikom, pri čemer moramo zagotoviti zaščito podatkov in informacij, ki se ob tem izmenjajo;
  - Celovitosti podatkov (ang. integrity): zagotoviti moramo istovetnost podatkov, to pomeni, da podatki od svojega nastanka niso bili kakorkoli spremenjeni oziroma, da sprememba, ne more biti neopažena;
  - Preprečevanje zanikanja dejanj (ang. non-repudiation): zagotoviti moramo nezmožnost zanikanja izvora podatkov in preprečiti možnost ponarejanja opravljenih storitev (npr: prepovedana raba skupnih računov – »shared accounts«);
  - Kontrole dostopa za sredstev in storitev (ang. access control): zagotoviti zaščito pred nedovoljeno uporabo virov, ki so dosegljivi preko omrežja. Potrebno je upoštevati pravila dostopa in identiteto uporabnika.

Vsi ITK sistemi in njihove posamezne komponente (aplikacije, operacijski sistemi, virtualizacijske platforme, firmware, BIOS, sistemi za nadzor in upravljanje, ipd.) morajo omogočati nameščanje varnostnih popravkov. Istovetnost varnostnih popravkov, posodobitev in definicij (podpisov) mora biti mogoče preveriti z uporabo kriptografskih mehanizmov.

Dobavitelj mora zagotavljati varnostne popravke tako dobavljenega sistema in/ali komponent ter imeti razvit proces upravljanja varnostnih popravkov celotnega sistema in njegovih posameznih komponent, kot tudi za v sistemu vključenih in uporabljenih komponent drugih dobaviteljev (third party). Dobavitelj mora imeti razvit sistem upravljanja z varnostnimi popravki, ki mora omogočati nadzor in upravljanje testiranja varnostnih popravkov, njihovo namestitvev in izdelavo potrebne dokumentacije.

Dobavitelj mora omogočati tehničnemu skrbniku sistema oziroma zunanjemu ponudniku storitev vzdrževanja, samostojno nameščanje varnostnih popravkov in posodobitev.

## 8 Dogovor o nivoju izvajanja storitev

### 8.1 Definicija pojmov

**Storitve** so naročnikove storitve, ki jih naročnik izvaja za svoje uporabnike

**Storitve podpore in vzdrževanja** so storitve, izvajalca, namenjene podpori in vzdrževanju strojne in programske opreme opredeljene v pogodbi s katero naročnik izvaja storitve za svoje uporabnike.

**Katalog storitev** je evidenca storitev s pripadajočimi opisnimi podatki.

**Nivo storitev** je določen način izvajanja storitve podpore in vzdrževanja, kjer so zajeti parametri, način in čas izvajanja storitev podpore in vzdrževanja.

**Storitveni center (SC)** je enotna vstopna točka za komunikacijo med izvajalcem in naročnikom.

**Komunikacijski kanal**, je oblika komunikacije med naročnikom in enotno vstopno točko SC izvajalca. Te oblike so:

- telefon, GSM,
- elektronska pošta,
- portal.

Vsi naštetih komunikacijski kanali so dvosmerni.

**Informacija** je skupek dejstev, ki se nanašajo na posamezno storitev in opisujejo stanje te storitve ali z njo povezanih dogodkov.

**Dogodek** Sprememba stanja, ki je pomembna s stališča upravljanja storitve ali konfiguracijskega elementa. Izraz se uporablja tudi kot opozorilo ali obvestilo, ki ga kreira storitev, konfiguracijski element ali orodje za spremljanje. Dogodek praviloma zahteva odziv osebja zadolženega za obratovanje IKT in pogosto temu sledi vpis incidenta.

**Incident** je dogodek, ki pomeni nenačrtovano prekinitve ali zmanjšanje kakovosti storitve. Incident je tudi napaka v konfiguracijskem elementu, ki še ne vpliva na storitev, kot je okvara ene komponente sistema, zmanjša pa zanesljivost storitve.

**Zanesljivost** je merilo ki pove koliko časa zmore storitev ali nek konfiguracijski element delovati brez prekinitve. Običajno se meri kot povprečni čas med odpovedma (MTBF) ali kot povprečni čas med izpadoma storitve (MTBSI). Izraz se lahko uporablja tudi za opredelitev verjetnosti, da bo storitev delovala kot zahtevamo.

**Vpliv** – je pojem oz. objektivno merilo s katerim se določi vpliv posameznega dogodka na poslovanje oz. uporabo storitve. Z vplivom lahko določimo, koliko dogodek vpliva na delovanje storitev in poslovanje.

**Nujnost** – je pojem oz. objektivno merilo s katerim določamo, kako hitro je potrebno odpraviti incident in zagotoviti ponovno normalno delovanje storitve.

**Prioriteta** – je pojem oz. objektivno merilo s katerim na osnovi določene nujnosti in vpliva določimo vrstni red reševanja incidentov, problemov, storitvenih zahtev in zahtev za spremembo. Prioriteto določi naročnik na podlagi vpliva in nujnosti.

**Problem** je nepoznan vzrok za nastanek enega ali več incidentov na storitvah.

**Problemski tip** je klasifikator problematike, s katerim določimo vrsto aktivnosti in z generičnimi parametri opredelimo vsebino problematike. Na osnovi problemskega tipa se določi ali je klic naročnika



vezan za incidente oz. zahteve, z njim opredelimo tudi specifičnosti iz kataloga storitev vezane na različne ravni storitve.

**Znana napaka** je odkrit vzrok za nastanek incidentov. Znana napaka je tako rekoč rešitev problema, ki ponuja začasno ali stalno rešitev.

**Storitveni zahtevek** je uradni zahtevek uporabnika za neko storitev. Na primer: zahtevek za informacijo ali nasvet, zahtevek za odpravo incidenta, zahtevek za rešitev problema, zahtevek za novo storitev. Storitveni zahtevek je lahko vezan na zahtevek za spremembo kot del procesa reševanja zahtevka.

**Zahteva za spremembo, sprememba** je zahteva, kjer naročnik poda zahtevo za dodajanje nove funkcionalnosti in vsebine oz. s katero se spremeni, doda ali odvzame funkcionalnost ali vsebina obstoječe storitve. Sprememba pomeni tudi spreminjanje kapacitete in razpoložljivosti storitve. Spremembe se klasificirajo na osnovi obsega in se lahko obravnavajo kot projektno delo. Spremembe niso standardne storitvene zahteve. Sprememba pomeni tudi kreiranje novih storitev.

**Odzivni čas** je čas v katerem se prijava incidenta, prijava problema, storitvena zahteva in zahteva za spremembo vpiše v sistem, klasificira, določi osnovna problematika, storitev, sistemski sklop ali okvarjena strojna oz. programska oprema. Po izteku tega časa mora izvajalec storitve kompetentno pristopiti k odpravi incidenta oz. k zagotavljanju izvedbe storitvene zahteve. Mejniki odzivnega časa je povratna informacija naročniku, ki vsebuje:

- zaporedno številko odprtega incidenta, problema, zahteve za spremembo oz. storitvene zahteve, ki je hkrati tudi identifikacijska številka za nadaljnjo komunikacijo;
- podatke o določitvi storitve, okvarjenega sistemskega sklopa, strojne ali programske opreme;
- določena mora biti prioriteta, kot derivat med vplivom in nujnostjo
- določena mora biti generična vsebina problematike

**Čas obratovanja** določi časovni interval razpoložljivosti storitve naročniku. Časovni roki za izračun SLA parametrov tečejo samo znotraj tega časovnega intervala.

**Pomoč naročniku** je nasvet ali interaktivno spremljanje uporabe storitve, ki ga izvajalec posreduje naročniku. Pomoč naročniku vključuje tudi prenos izvajalčevega znanja.

**Programska oprema** je vsa programska oprema, ki mora biti nameščena na strojni opremi (postavljenem v delovno okolje) za izvajanje storitev.

**Odbor za analizo in odobritev sprememb**, je skupina, ki je določena stalno oz. se zasedba te skupine spreminja glede na kompleksnost spremembe. V skupini sodelujejo člani naročnika in izvajalca, ki s svojimi kompetencami lahko presodijo kakšen vpliv bo imela sprememba na obstoječe stanje storitev in na poslovanje.

**Odprava incidenta** pomeni zagotovitev prvotno določenega delovanja storitve z zagotavljanjem končne ali pa nadomestne rešitve.

**Vzdrževanje** so standardne vnaprej določene aktivnosti s katerimi se zagotavlja kvalitetno delovanje opreme in storitev, kot tudi preventivno odkrivanje vzrokov za nastanek incidentov ali pa potreb za izvajanje sprememb v smislu povečanja kapacitete. Aktivnosti vezane na redno vzdrževanje se izvajajo in dokumentirajo v sklopu izvajanja storitvenih zahtev.

**Delovniki** so vsi dnevi od ponedeljka do petka, ki niso v Republiki Sloveniji priznani kot praznik.

**Prazniki** so dnevi, ki so v Republiki Sloveniji priznani kot dela prosti dnevi.

## 8.2 Izvajanje podpore in vzdrževanja

Opis storitev podrobneje opredeljuje storitve, ki so predmet te pogodbe.



### **Dosegljivost strokovnjaka izvajalca**

- dajanje informacij povezanih s posamezno storitvijo in opremo,
- pomoč naročniku pri uporabi storitve in opreme.

### **Sprejem in odprava incidentov**

- prijava incidentov preko želenega komunikacijskega kanala
- sprejem incidentov in dokumentiranje vsebine problematike
- vezava incidentov na specifično storitev, sistemski sklop, sistem in opremo
- določanje problemskega tipa incidentov
- reševanje incidentov – vzpostavitev normalnega delovanja storitve
- poročanje o incidentu (vzrok, kako se je incident odpravil..)

### **Reševanje problemov**

- prijava problemov
- proaktivno odkrivanje in odpravljanje problemov
  - analiza trendov dogodkov na sistemih in sistemskih sklopih
  - priprava predlogov za izboljšave
- reaktivno odkrivanje in odpravljanje problemov
  - odkrivanje problemov in dokumentiranje vsebine
  - raziskovanje problematike
  - pripravo podlag za odpravo vzrokov iz problematike

### **Izvajanje storitvenih zahtev**

- prijava storitvenih zahtev
- sprejem zahtev in dokumentiranje vsebine
- klasifikacija zahtev glede vsebine
- vezava storitvenih zahtev za specifično storitev, sistemski sklop, sistem in opremo
- izvajanje zahtev na obstoječih storitvah, sistemskih sklopih, sistemih in opremi
- dokumentiranje izvedenih storitev

### **Izvajanje zahtev za spremembo**

- prijava zahtev za spremembo
- sprejem in dokumentiranje zahtev za spremembo
- kategorizacija zahtev za spremembo glede na obseg in kompleksnost
- vezava zahtev za spremembo na specifično storitev, sistemski sklop, sistem in opremo
- določanje prioritete sprememb
- analiza zahtev za spremembo glede na obstoječe stanje – organiziranje odbora za analizo in odobritev sprememb.
- določanje vpliva sprememb glede na izvajanje obstoječih storitev in poslovanje
- planiranje izvedbe spremembe skupaj z naročnikom
- razvoj spremembe
- testiranje spremembe
- implementacija spremembe
- stabilizacija spremembe in izobraževanje naročnika
- dopolnitev obstoječe dokumentacije storitve, systemskega sklopa, sistema in opreme glede na spremembo.

### **Redno vzdrževanje in upravljanje**

- redni pregled in spremljanje delovanja opreme, sistemov in storitev
- vzdrževanje obstoječih skript posameznih storitev
- izvajanje posodobitev in nameščanje varnostnih popravkov po navodilih proizvajalca na najnovejšo verzijo oz. na verzijo dogovorjeno z naročnikom
- izdelava mesečnih poročil o izvajanju vzdrževanja in stanju sistemskih sklopov, sistemov, opreme in storitev.
- stalen avtomatski nadzor nad delovanjem sistemskih sklopov in sistemov.

### **Nadomestna oprema**

- Izvajalec bo za naročnika imel v pripravljenosti nadomestno opremo.
- Nadomestna oprema bo zadovoljevala takojšnjo zamenjavo okvarjene opreme vsakega sistema, ki je predmet vzdrževanja te pogodbe.
- Izvajalec bo nadomestno opremo uporabil, zamenjal takoj v primeru, da ugotovi okvaro na produkcijski opremi.
- Izvajalec bo zamenjavo izvedel v skladu z parametri ravni storitve.

### **Poročanje o izvajanju storitev**

- izvajalec bo mesečno zagotavljal poročila o izvajanju storitev podpore in vzdrževanja in stanju storitev, sistemskih sklopov in sistemov. Poročilo o opravljenih storitvah je obvezna priloga k računu. Izvajalec enkrat letno pripravi skupno poročilo o delovanju sistema in izvajanju storitev

## **1. KOMUNIKACIJA IN KONTAKTNI PODATKI**

Naročnik prijavi storitveni zahtevek preko enega izmed komunikacijskih kanalov:

- telefon
- e-pošta
- portal

Odzivni čas in čas za rešitev prične teči od trenutka prijave napake s strani naročnika.

Ponudnik kontaktira naročnika preko enega izmed sledečih komunikacijskih kanalov:

- telefon: 01 473 2020
- e-pošta: [sos-itk@eles.si](mailto:sos-itk@eles.si)

### 8.3 Nivo izvajanja storitev

#### 8.3.1 Določanje prioritete izvajanja storitev

Tabela za določitev stopnje NUJNOSTI.

STOPNJA NUJNOSTI	Opis
URGENTNO	<ul style="list-style-type: none"> <li>Prizadet je sistem oz. storitev in je ni mogoče več uporabljati.</li> <li>Uporaba sistema ali storitve je zahtevana v najkrajšem možnem času.</li> <li>Od časa ponovne vzpostavitve delovanja sistema ali storitve je odvisno nadaljnje izvajanje poslovanja oziroma zagotavljanje dogovorjene kvalitete poslovanja v podjetju.</li> </ul>
NUJNO	<ul style="list-style-type: none"> <li>Prizadet je sistem ali storitev vendar je uporaba možna v omejenem obsegu, omejeni funkcionalnosti oz. omejeni kapaciteti.</li> <li>Sistem deluje v razpoložljivem načinu (namesto v visoko razpoložljivem načinu). Obstaja bojazen, da se bo izgubila funkcionalnost tudi rezervnega sistema.</li> <li>Poslovanje je moteno,</li> <li>Delovanje storitve ali sistema je časovno občutljivo</li> </ul>
STANDARDNO	<ul style="list-style-type: none"> <li>Na sistemu ali storitvi je odkrita napaka.</li> <li>Poslovanje je lahko moteno vendar delovanje storitve ali sistema ni časovno občutljivo.</li> </ul>
NIZKO	<ul style="list-style-type: none"> <li>Kategorija se dodeljuje dogodkom in zahtevam, ki ne vplivajo na poslovanje. V primeru, ko je incident odpravljen in je potrebno opazovanje ali nadaljnje raziskovanje.</li> </ul>

Tabela za določitev stopnje VPLIVA

STOPNJA VPLIVA	Opis
IZREDEN	<ul style="list-style-type: none"> <li>Dogodek ali zahteva ima vpliv na delovanje storitve, od katere je v odvisno veliko število uporabnikov oz. ima veliko poslovno pomembnost.</li> <li>Uporaba storitve je onemogočena vsem uporabnikom.</li> <li>Poslovanje je lahko ogroženo ali onemogočeno.</li> </ul>
VISOK	<ul style="list-style-type: none"> <li>Dogodek ali zahteva ima vpliv na delovanje storitve, od katere je v tem trenutku odvisno samo del uporabnikov oz. ima delno veliko poslovno pomembnost.</li> <li>Uporaba storitve je onemogočena večini uporabnikov.</li> <li>Poslovanje je omejeno.</li> </ul>
NORMALNO OMEJEN	<ul style="list-style-type: none"> <li>Dogodek ali zahteva ima omejen vpliv.</li> <li>Uporaba storitve je omogočena, vendar je dogodek omejen na določen sistemski sklop ali del programske opreme.</li> <li>Dogodek je lahko omejen tudi na skupino uporabnikov, v celoti pa je večini uporaba storitve omogočena.</li> <li>Poslovanje je lokalno omejeno.</li> </ul>
LOKALEN	<ul style="list-style-type: none"> <li>Dogodek ali zahteva ima izredno omejen vpliv na posameznega uporabnika ali na posamezen del sistema, strojne oz. programske opreme.</li> </ul>

Matrika za določanje PRIORITETE na podlagi nujnosti in vpliva

VPLIV/NUJNOST	Nizko	Standardno	Nujno	Urgentno
Izreden vpliv	4	2	1	1
Visok vpliv	4	3	2	1
Normalno omejen	4	3	2	2
Lokalen	4	4	3	3

### 8.3.2 Čas obratovanja storitev in odzivni časi

#### Dosegljivost strokovnjaka izvajalca

Čas za odzivnost	Čas za odgovor	Čas obratovanja
2h	4 h	Delavnik 8:00 – 16:00

#### Sprejem in odprava incidentov:

Prioriteta	Opis	Čas za odzivnost	Čas do rešitve	Čas obratovanja
1	Kritično	1 h	4 h	24/7
2	Visoka	2 h	8 h	24/7
3	Srednja	4 h	24 h	Delavnik 8:00 – 16:00
4	Nizka	4 h	24 h	Delavnik 8:00 – 16:00

#### Reševanje problemov:

Prioriteta	Opis	Čas za odzivnost	Čas do rešitve	Čas obratovanja
1	Kritično	2 h	24 h	Delavnik 8:00 – 16:00
2	Visoka	2 h	24 h	Delavnik 8:00 – 16:00
3	Srednja	4 h	48 h	Delavnik 8:00 – 16:00
4	Nizka	4 h	48 h	Delavnik 8:00 – 16:00

#### Izvajanje storitvenih zahtev:

Prioriteta	Opis	Čas za odzivnost	Čas do rešitve	Čas obratovanja
1	Kritično	4 h	24 ur	Delavnik 8:00 – 16:00
2	Visoka	4 h	48 ur	Delavnik 8:00 – 16:00
3	Srednja	4 h	5dni	Delavnik 8:00 – 16:00
4	Nizka	4 h	5dni	Delavnik 8:00 – 16:00

#### Izvajanje zahtev za spremembo:

Prioriteta	Opis	Čas za odzivnost	Čas do rešitve	Čas obratovanja
1	Kritično	2 h	Skladno z dogovorom	Delavnik 8:00 – 16:00
2	Visoka	2 h	Skladno z dogovorom	Delavnik 8:00 – 16:00
3	Srednja	4 h	Skladno z dogovorom	Delavnik 8:00 – 16:00
4	Nizka	4 h	Skladno z dogovorom	Delavnik 8:00 – 16:00

#### Redno vzdrževanje in upravljanje:

Opis	Čas za odzivnost	Čas do rešitve	Čas obratovanja
------	------------------	----------------	-----------------

Analiza sistema	1 dan	Skladno z dogovorom	Delavnik 8:00 – 16:00
Nameščanje nove verzije programske opreme	1 dan	Skladno z dogovorom	Delavnik in prazniki 8:00 – 16:00
Nameščanje kritičnih popravkov programske opreme	4h	Skladno z dogovorom	24/7

#### 8.4 Pogodbena kazen za izvajanje podpore in vzdrževanja

Če je izvajalec po svoji krivdi v zamudi z izpolnitvijo svojih obveznosti, ima naročnik pravico zahtevati od izvajalca pogodbeno kazen. Pogodbena kazen se izračunava če se storitve ne izvajajo časovnih okvirjih dogovorjenimi s to pogodbo.

Pogodbena kazen je dolžan izvajalec plačati naročniku v roku 8-ih dni od datuma izstavitve zahtevka za plačilo kazni oz. se znesek lahko pobota z izstavljenim računom če se stranki tako dogovorita.

Pogodbena kazen za neizvajanje storitev v dogovorjenih časovnih rokih za posamezne storitve je:

##### Dosegljivost strokovnjaka izvajalca

Čas za odzivnost	Čas za odgovor
Za vsako začeto prekoračeno uro 5€	Za vsako začeto prekoračeno uro 10€

##### Sprejem in odprava incidentov:

Prioriteta	Opis	Čas za odzivnost	Čas do rešitve
1	Kritično	Za vsako začeto prekoračeno uro 5€	Za vsako začeto prekoračeno uro 20€
2	Visoka	Za vsako začeto prekoračeno uro 5€	Za vsako začeto prekoračeno uro 20€
3	Srednja	Za vsako začeto prekoračeno uro 5€	Za vsako začeto prekoračeno uro 10€
4	Nizka	Za vsako začeto prekoračeno uro 5€	Za vsako začeto prekoračeno uro 10€

##### Reševanje problemov:

Prioriteta	Opis	Čas za odzivnost	Čas do rešitve
1	Kritično	Za vsako začeto prekoračeno uro 5€	Za vsako začeto prekoračeno uro 20€
2	Visoka	Za vsako začeto prekoračeno uro 5€	Za vsako začeto prekoračeno uro 20€
3	Srednja	Za vsako začeto prekoračeno uro 5€	Za vsako začeto prekoračeno uro 10€
4	Nizka	Za vsako začeto prekoračeno uro 5€	Za vsako začeto prekoračeno uro 10€

##### Izvajanje storitvenih zahtev:

Prioriteta	Opis	Čas za Odzivnost	Čas do rešitve
1	Kritično	Za vsako začeto prekoračeno uro 5€	Za vsako začeto prekoračeno uro 10€
2	Visoka	Za vsako začeto prekoračeno uro 5 €	Za vsako začeto prekoračeno uro 10€
3	Srednja	Za vsako začeto prekoračeno uro 10€	Za vsako začeto prekoračen dan 5€

4	Nizka	Za vsako začeto prekoračeno uro 5€	Za vsako začet prekoračen dan 5€
---	-------	------------------------------------	----------------------------------

**Izvajanje zahtev za spremembo:**

Prioriteta	Opis	Čas za Odzivnost	Čas do rešitve
1	Kritično	Za vsako začeto prekoračeno uro 5€	Za vsako začeto prekoračeno uro 10€
2	Visoka	Za vsako začeto prekoračeno uro 5€	Za vsako začeto prekoračeno uro 10€
3	Srednja	Za vsako začeto prekoračeno uro 5€	Za vsako začet prekoračen dan 10€
4	Nizka	Za vsako začeto prekoračeno uro 5€	Za vsako začet prekoračen dan 10€

**Redno vzdrževanje in upravljanje:**

Opis	Čas za odzivnost	Čas do rešitve
Analiza sistema	Za vsako začet prekoračen dan 5€	Za vsako začet prekoračen dan 10€
Nameščanje nove verzije programske opreme	Za vsako začet prekoračen dan 5€	Za vsako začet prekoračen dan 10€
Nameščanje kritičnih popravkov programske opreme	Za vsako začeto prekoračeno uro 5€	Za vsako začet prekoračen dan 20€