POLITIKA UPRAVLJANJA ODNOSIMA SA DOBAVLJAČIMA

OZNAKA DOKUMENTA	*MT15POL01*	**DATUM IZDANJA**	*12-12-2023*
PRIMERAK BROJ	*01*	**IZDANJE**	*02*

AUTORIZACIJA	**IME I PREZIME**	**FUNKCIJA**	**POTPIS**
PRIPREMIO	Vladimir Miladinović	Menadžer ISMS	
ODOBRIO	Boris Čorni	Rukovodilac IT sektora	

SADRŽAJ

1 ZAPIS O DOPUNI

Datum	Brojevi strane(a)	Detalji izmene	Broj zahteva za izmenu dokumenta

2 DISTRIBUCIJA I KONTROLA

2.1 DISTRIBUCIJA

Rb. broj	Funkcija/odeljenje
1	Sistem administrator
2	Menadžer za ISMS
3	IT služba

2.2 KONTROLA

Nekontrolisani primerci ovog dokumenta se mogu izdati zainteresovanim stranama ili kupcima organizacije shodno odluci Direktora. Održavaće se zapisi o svakom nekontrolisanom primerku. Svaki primerak će se datirati i označiti sa **„NEKONTROLISANI PRIMERAK - UNIŠTITI NAKON UPOTREBE”** na naslovnoj strani.

3 SVRHA

Svrha ovog dokumenta jeste da detaljno predstavi politiku organizacije iz oblasti upravljanja odnosima sa dobavljačima.

Kao takav, ovaj dokument predstavlja početni dizajn za poboljšanje postojećeg procesa upravljanja odnosima sa dobavljačima i ažurira se bar jednom godišnje, u skladu sa potrebama za razvojem u Meridian Tech d.o.o. Beograd .

Ova politika pokriva sledeće kontrole:

- 5.19 Bezbednost informacija u odnosima sa dobavljačima
- 5.20 Rešavanje bezbednosti informacija u okviru ugovora sa dobavljačima
- 5.21 Upravljanje bezbednošću informacija u lancu nabavke informacione i komunikacione tehnologije (IKT)
- 5.22 Nadziranje, preispitivanje i upravljanje promenama usluga dobavljača
- 5.23 Bezbednost informacija za upotrebu cloud servisa

4 PODRUČJE PRIMENE

Politika upravljanja odnosima sa dobavljačima se primenjuje u organizaciji Meridian Tech d.o.o. Beograd . U politici se ne koriste termini koje je potrebno posebno definisati.

5 TERMINI I DEFINICIJE

U cilju boljeg razumevanja ISMS-a organizacije, u nastavku su navedene definicije značajnijih pojmova koji se koriste u ovoj proceduri.

U dokumentaciji ISMS-a organizacije se koriste sledeće skraćenice:

ISMS – (Information security management Sistems), Sistem menadžmenta zaštite i bezbednosti informacija - ISO/IEC 27001:2022.

6 REFERENTNA DOKUMENTA

ISO 27001:2022 *Sistem menadžmenta bezbednošću informacija - Zahtevi*

7 OPIS RADA

7.1 Politika

Politika organizacije Meridian Tech d.o.o. Beograd , u ovoj oblasti upravljanja odnosima sa dobavljačima jeste da:
Kada je to moguće, treba postojati pismeni ugovor između uključenih strana, a organizacija Meridian Tech d.o.o. Beograd čuva primerak originala potpisanog od strane svih uključenih strana, koji se, takođe, i skenira i čuva u elektronskoj formi.

1. Ugovor uključuje:
    a. Područje primene usluge ili dobara koji se isporučuju
    b. Zavisnosti između usluga, procesa i uključenih strana
    c. Obaveze koje dobavljač mora da ispuni
    d. Ciljeve usluga/isporuke dobara
    e. Interfejs između procesa kojima upravljaju dobavljač i ostale strane
    f. Integraciju aktivnosti dobavljača sa Sistemom upravljanja bezbednošću informacija
    g. Karakteristike obima poslovanja
    h. Očekivanja
    i. Ovlašćenja i odgovornosti organizacije Meridian Tech d.o.o. Beograd
    j. Dobavljač mora da obaveštava i sastavlja izveštaje
    k. Osnove za promene
    l. proces upravljanja promenama koji osigurava unapred obaveštavanje organizacije i mogućnost da organizacija ne prihvati promene
    m. Aktivnosti i odgovronosti za očekivano ili ranije okončanje ugovora i transfer obaveza drugim stranama

- klauzule o raskidu nakon zaključenja ugovora, uključujući upravljanje evidencijama, vraćanje imovine, sigurno raspolaganje informacijama i drugom povezanom imovinom, i sve tekuće obaveze poverljivosti;

Pored navedenih elemenata pisanim sporazumom ili ugovorom treba regulisati i druga pitanja kao što su:

- opis informacija koje treba pružiti ili pristupiti i metode pružanja ili pristupa informacijama;
- klasifikaciju informacija prema klasifikacionoj šemi organizacije;
- mapiranje između vlastite klasifikacione šeme organizacije i klasifikacione šeme dobavljača;
- zakonske, statutarne, regulatorne i ugovorne zahteve, uključujući zaštitu podataka, rukovanje podacima o ličnosti (PII), prava intelektualne svojine i autorska prava i opis načina na koji će se osigurati da su ispunjeni;
- obaveza svake ugovorne strane da implementira dogovoreni skup kontrola, uključujući kontrolu pristupa, pregled učinka, praćenje, izveštavanje i proveru (audit), kao i obaveze dobavljača da se pridržava zahteva za bezbednost informacija organizacije;
- pravila prihvatljivog korišćenja informacija i druge povezane imovine, uključujući neprihvatljivo korišćenje ako je potrebno;

- procedure ili uslove za autorizaciju i uklanjanje ovlašćenja za korišćenje informacija organizacije i druge povezane imovine od strane osoblja dobavljača (npr. putem eksplicitne liste osoblja dobavljača ovlašćenog za korišćenje informacija organizacije i druge povezane imovine);
- zahtevi za bezbednost informacija u vezi sa IKT infrastrukturom dobavljača; posebno, minimalni zahtevi za bezbednost informacija za svaku vrstu informacija i tip pristupa koji služe kao osnova za pojedinačne ugovore sa dobavljačima na osnovu poslovnih potreba i kriterijuma rizika organizacije;
- obeštećenja i popravka za neuspeh izvođača da ispuni zahteve;
- zahtevi i procedure upravljanja incidentima (naročito obaveštavanje i saradnja tokom sanacije incidenta);
- zahteve za obuku i svest o specifičnim procedurama i zahtevima za bezbednost informacija (npr. za reagovanje na incidente, procedure autorizacije I slično);
- relevantne odredbe za podugovaranje, uključujući kontrole koje je potrebno implementirati, kao što je sporazum o korišćenju podisporučioce (npr. zahtev da se izlože istim obavezama isporučilaca, zahtev da se ima lista podisporučilaca dobavljača i obaveštenje pre bilo kakve promene);
- relevantne kontakte, uključujući kontakt osobu za pitanja bezbednosti informacija;
- sve zahteve za proveru, gde je to zakonski dozvoljeno, za osoblje dobavljača, uključujući odgovornosti za sprovođenje postupaka skrininga i obaveštavanja ako skrining nije završen ili ako rezultati daju razlog za sumnju ili zabrinutost;
- dokaze i mehanizme uveravanja potvrda treće strane za relevantne zahteve bezbednosti informacija u vezi sa procesima dobavljača i nezavisni izveštaj o delotvornosti kontrola, ako je potrebno;
- pravo provere (audita) procesa i kontrola dobavljača u vezi sa ugovorom
- obaveza dobavljača da periodično dostavlja izvještaj o delotvornosti kontrola i dogovor o blagovremenom ispravljanju relevantnih pitanja postavljenih u izveštaju;
- procesi rešavanja primedbi, kvarova i sukoba;
- obezbeđivanje rezervnih kopija usklađenih sa potrebama organizacije (u smislu učestalosti i vrste i lokacije skladištenja), gde to ima smisla i potrebe;
- osiguravanje dostupnosti alternativnog postrojenja (tj. mesta za oporavak od katastrofe) koje nije podložno istim pretnjama kao primarno postrojenje i razmatranja rezervnih kontrola (alternativnih kontrola) u slučaju neuspeha primarne kontrole;
- fizičke bezbednosne kontrole srazmerne klasifikaciji informacija, ako je potrebno;
- kontrole prenosa informacija radi zaštite informacija tokom fizičkog ili logičkog prenosa;
- obezbeđivanje metode bezbednog uništavanja informacija organizacije koje je uskladištio dobavljač čim više nisu potrebni;
- osiguravanje, na kraju ugovora, primopredaju podrške drugom dobavljaču ili samoj organizaciji.

2. Uloge i odnosi između glavnih dobavljača i podugovarača biće dokumentovani

Održava se redovna formalna komunikacija sa dobavljačima, a učestalost zavisi od količine posla koji se obavlja sa dobavljačem i od važnosti robe ili usluge za organizaciju Meridian Tech d.o.o. Beograd .

Lanac snabdevanja IKT proizvoda i usluga mora da reguliše sledeće:
a) definisanje zahteva za bezbednost informacija koji se primenjuju na nabavku IKT proizvoda ili usluga;
b) zahteve da dobavljači IKT usluga propagiraju bezbednosne zahteve organizacije kroz celi lanac snabdevanja ako podugovaraju delove IKT usluge koje se pružaju organizaciji;
c) zahteve da dobavljači IKT proizvoda propagiraju odgovarajuće bezbednosne prakse kroz lanac nabavke ako ti proizvodi uključuju komponente kupljene ili nabavljene od drugih dobavljača ili drugih entiteta (npr. podugovoreni programeri softvera i dobavljači hardverskih komponenti);
d) zahteve da dobavljači IKT proizvoda dostave informacije koje opisuju softverske komponente koje se koriste u proizvodima;
e) zahteve da dobavljači IKT proizvoda dostave informacije koje opisuju implementirane bezbednosne funkcije njihovog proizvoda i konfiguraciju potrebnu za njegov siguran rad;
f) implementaciju procesa praćenja i prihvatljivih metoda za potvrđivanje da su isporučeni IKT proizvodi i usluge u skladu sa navedenim bezbednosnim zahtevima. Primeri takvih metoda pregleda dobavljača mogu uključivati testiranje penetracije i dokaz ili validaciju potvrda trećih strana za operacije bezbednosti informacija dobavljača;
g) implementaciju procesa za identifikaciju i dokumentovanje komponenti proizvoda ili usluga koje su kritične za održavanje funkcionalnosti i stoga zahtevaju povećanu pažnju, kontrolu i dalje praćenje kada su izgrađene izvan organizacije, posebno ako dobavljač prepusti aspekte proizvoda ili komponenti usluge drugima dobavljačima;
h) dobijanje uveravanja da se kritične komponente i njihovo poreklo mogu pratiti kroz celi lanac snabdevanja;
i) dobijanje garancije da isporučeni IKT proizvodi funkcionišu kako se očekuje bez ikakvih neočekivanih ili neželjenih karakteristika;
j) implementaciju procesa kako bi se osiguralo da komponente dobavljača budu originalne i nepromenjene u odnosu na njihove specifikacije. Primeri mera uključuju kontrole protiv neovlaštenog pristupa, kriptografske heš verifikacije ili digitalne potpise. Praćenje performansi izvan specifikacije može biti pokazatelj neovlašćenog pristupa ili krivotvorenja. Sprečavanje i otkrivanje neovlašćenog pristupa treba da se implementira tokom više faza životnog ciklusa razvoja sistema, uključujući dizajn, razvoj, integraciju, rad i održavanje;
k) dobijanje uveravanja da IKT proizvodi postižu potrebne nivoe bezbednosti, na primer, kroz formalnu sertifikaciju ili šemu evaluacije kao što je sporazum o priznavanju zajedničkih kriterijuma;
l) definisanje pravila za razmenu informacija u vezi sa lancem snabdevanja i svim potencijalnim problemima i kompromisima između organizacije i dobavljača;

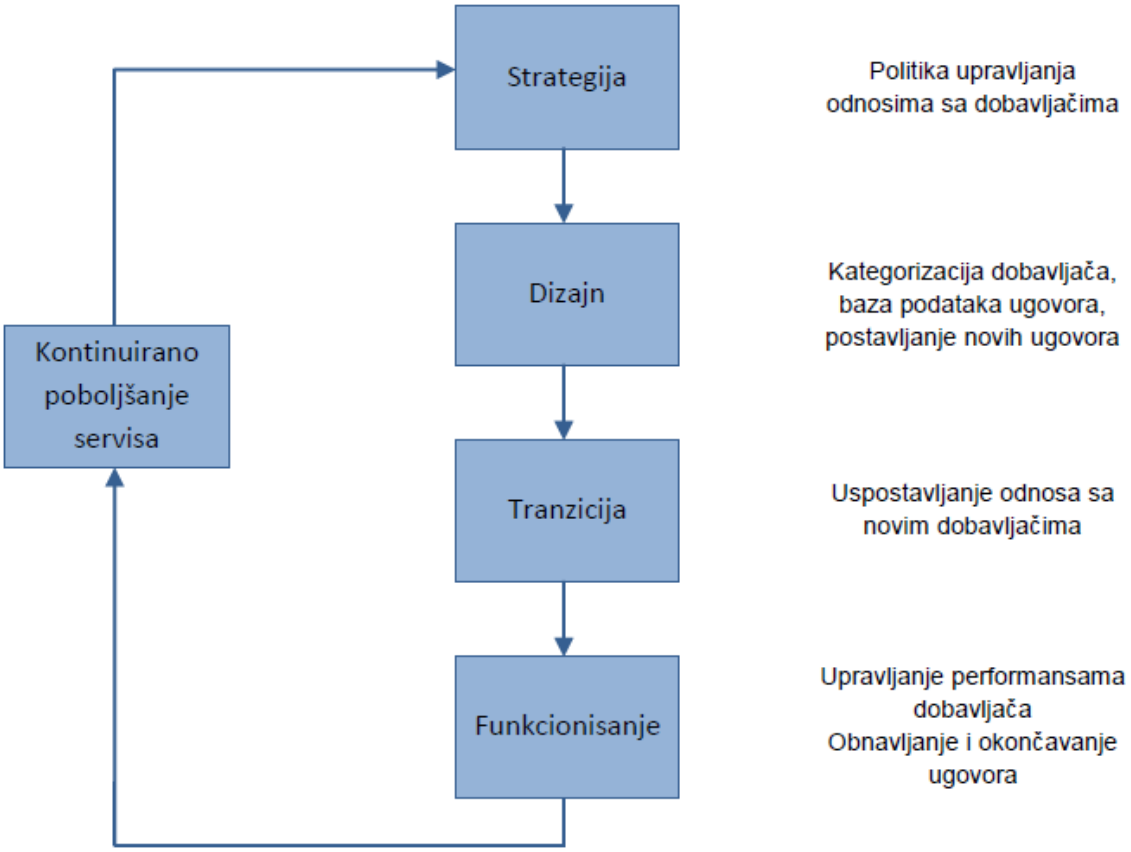
m) implementaciju specifičnih procesa za upravljanje životnim ciklusom IKT komponenti i dostupnošću i povezanim bezbednosnim rizicima.

3. Bilo kakve promene u području primene ili uslova postojećeg ugovora su dokumentovane i njima se upravlja u skladu sa procesom Upravljanje promenama.

U odeljenju koje se bavi pravnim poslovima organizacije čuvaju se originali ugovora.

7.2 Pristup upravljanju odnosima sa dobavljačima

Proces upravljanje odnosima sa dobavljačima prati sledeći pristup. Ovaj proces je u skladu sa najboljom praksom ITIL-a (IT Infrastructure Library).

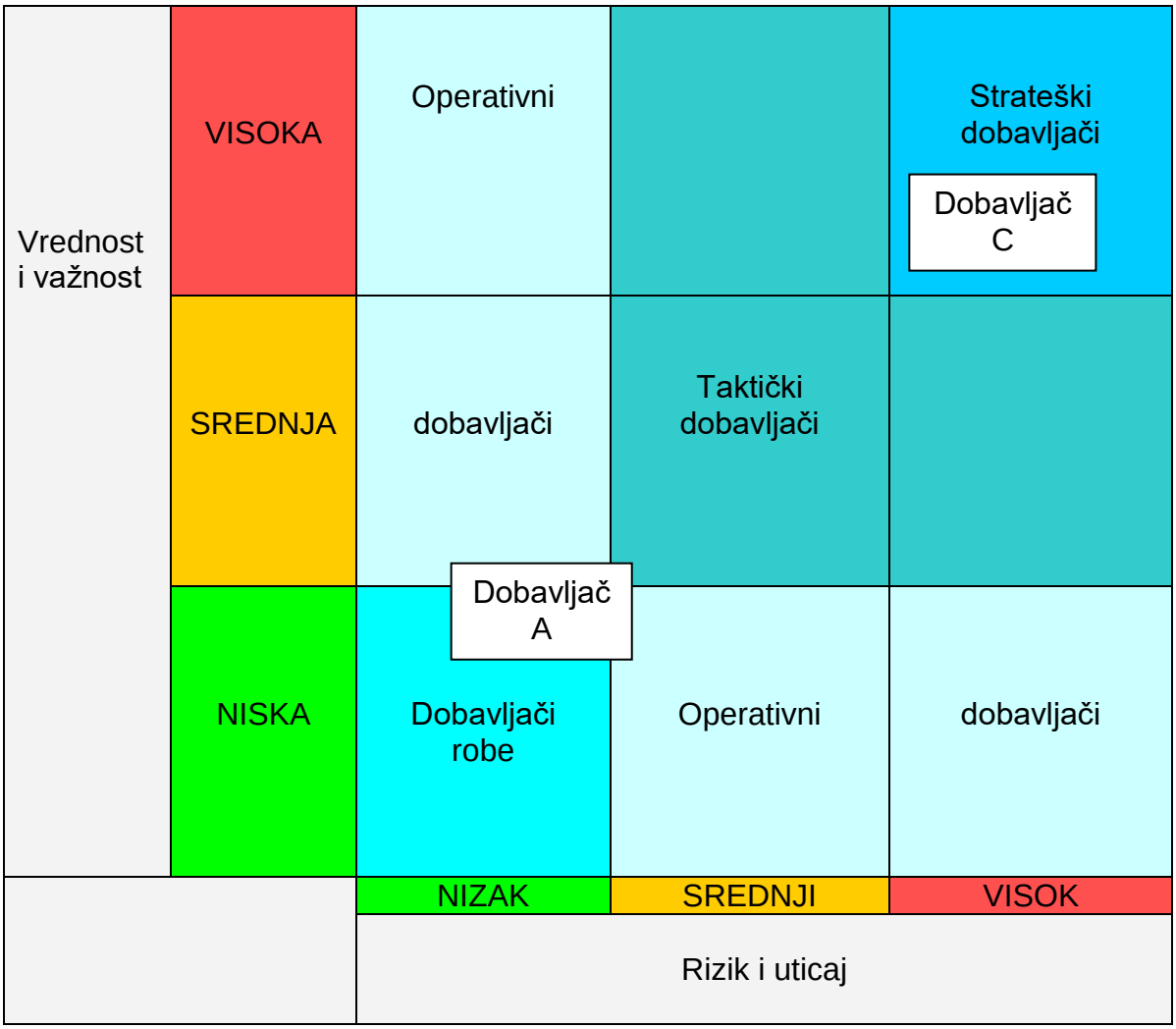


Baza podataka dobavljača i ugovora koristi se kako bi se dokumentovali datalji o proizvodima i uslugama koji se dostavljaju organizaciji Meridian Tech d.o.o. Beograd , uključujući podatke o kontaktima, nivoima servisa, podugovaračima i glavnim uslovima ugovora kao i komentari u vezi sa predviđanjima incidenata i problema po osnovu bezbednosti informacija.

7.3 Kategorizacija dobavljača

Priroda odnosa između organizacija Meridian Tech d.o.o. Beograd i dobavljača zavisi od količine novca koja se potroši na njihove dostave, kao i od prirode i važnosti proizvoda i usluga koje dostavljaju za poslovanje kompanije.

Grafikon ispod prikazuje primere položaja dobavljača u odnosu na ove atribute.



Na ovaj način svaki dobavljač je raspoređen u jednu od četiri kategorije:

1. Robni
2. Operativni
3. Taktički
4. Strateški

Preporučena učestalost sastanaka između
Organizacije Meridian Tech d.o.o. Beograd i pojedinačnih dobavljača određena je pozicijom dobavljača na ovoj matrici i prema sledećoj tabeli.

Kategorija dobavljača	Preporučena učestalost sastajanja
Robni	Nema
Operativni	Prilikom obnavljanja ugovora
Taktički	Jednom godišnje
Strateški	Mesečno/kvartalno

Svakom dobavljaču organizacije Meridian Tech d.o.o. Beograd je dodeljen jedan menadžer koji je odgovoran za zakazivanje, presedavanje i dokumentovanje sastanaka. Ime ovog pojedinca nalazi se u Bazi podataka dobavljača i ugovora.

7.4 Upravljanje performansama dobavljača

Stanje bezbednosti informacija strateških dobavljača se redovno nadzire u skladu sa preporučenom učestalošću sastanaka.

Kada je moguće, često se vrši poređenje izveštaja koji je sastavio dobavljač i onih koje je kreirala organizacija Meridian Tech d.o.o. Beograd , kako bi se proverilo da oba predstavljaju konzistentnu sliku o stanju bezbednosti informacija na obe strane.

Oba izveštaja se preispituju na sastancima sa dobavljačima i sve aktivnosti koje proizilaze sa sastanaka, predstavljaju input za **Izveštaj o neusaglašenostima** od svih rukovodilaca sektora iz svih dostupnih izvora o svim uočenim neusaglašenostima i pravi sistematizovan pregled neusaglašenosti evidentirajući ih u obrascu **Evidencija korektivnih mera**.

Proces upravljanja odnosom između organizacije i dobavljača, kao i monitoring dobavljača mora da obuhvati:

a) praćenje nivoa performansi usluga kako bi se potvrdila usklađenost sa sporazumima;

b) praćenje promena koje su izvršili dobavljači uključujući:

1) poboljšanja postojećih usluga;

2) razvoj novih aplikacija i sistema;

3) modifikacije ili ažuriranja politika i procedura dobavljača;

4) nove ili izmenjene kontrole za rešavanje incidenata u informacionoj bezbednosti i za unapređenje informacione bezbednosti;

c) praćenje promena u uslugama dobavljača uključujući:

1) promene i unapređenje mreža;

2) korišćenje novih tehnologija;

3) usvajanje novih proizvoda ili novijih verzija ili izdanja;

4) novi razvojni alati i okruženja;

5) promene fizičke lokacije uslužnih objekata;

6) promena podisporučilaca;

7) podugovaranje sa drugim dobavljačem;

d) pregled izveštaja o uslugama koje je sačinio dobavljač i organizovanje redovnih sastanka o napretku u skladu sa ugovorima;

e) sprovođenje provere (audita) dobavljača i podisporučilaca, zajedno sa pregledom izveštaja nezavisnog proveravača, ako su dostupni, i praćenjem u vezi sa identifikovanim spornim pitanjima;

f) pružanje informacije o incidentima u vezi sa bezbednošću informacija i pregleda ove informacije u skladu sa zahtevima sporazuma i svih pratećih smernica i procedura;

g) pregledanje audit tragova dobavljača i zapisa o događajima bezbednosti informacija, operativnim problemima, kvarovima, praćenju kvarova i smetnji u vezi sa isporučenom uslugom;

h) reagovanje i upravljnje svim identifikovanim događajima ili incidentima u oblasti bezbednosti informacija;

i) identifikovanje ranjivosti bezbednosti informacija i upravljanje njima;

j) proveru i nadzor aspekata bezbednosti informacija u odnosima dobavljača sa svojim dobavljačima;

k) osiguranje da isporučilac održava dovoljne servisne kapacitete zajedno sa izvodljivim planovima dizajniranim da osiguraju održavanje dogovorenih nivoa kontinuiteta usluge nakon velikih kvarova ili katastrofe;

l) osiguranje da dobavljači dodeljuju odgovornosti za pregled usaglašenosti i sprovođenje zahteva iz sporazuma;

m) redovno ocenjivanje da dobavljači održavaju adekvatne nivoe bezbednosti informacija.

7.5 Ugovorni sporovi

U slučaju ugovornog spora, trebaju se pratiti sledeće smernice:

- Finansijski direktor i finansijski tim moraju biti obavešteni o sporu
- Finansijski direktor mora dati saglasnost za sledeći korak
- Kada je prikladno, pravni savet treba da se dobije preko finansijskog direktora
- Celokupna korespondencija sa dobavljačem mora biti u pisanoj formi

Sva procena rizika po informacionu imovinu organizacije Meridian Tech d.o.o. Beograd treba se sprovesti pre bilo kojeg spora, i trebaju se postaviti planovi za nepredviđene situacije

U svako vreme nivo rizika po bezbednost informacija (time i na poslovanje) treba da bude pod kontrolom, i ako je moguće, sveden na minimum.

7.6 Okončanje pružanja servisa

Sledeći proces se primenjuje prilikom okončanja pružanja usluga ili isporuke dobara, ranijeg okončanja ili transfera pružanja usluga ili isporuke dobara:

- Okončanje pružanja usluga ili isporuke dobara zahtevaće se pismeno u skladu sa uslovima ugovora, ukoliko postoji

- Transfer drugoj strani (uključujući i in-house podršku) planiraće se putem procedura kontrole promena koje je slede
- Procena rizika po bezbednost informacija treba se sprovesti pre okončanja ili transfera servisa, i trebaju se postaviti planovi za nepredviđene situacije
- Sve budžetske implikacije moraju biti uključene u finansijski model

8 ODGOVORNOSTI I OVLAŠĆENJA

ISMS Menadžer je odgovoran za planiranje i organizovanje aktivnosti politike upravljanja odnosima sa dobavljačima. Za kontrolu primene procedure ovlašćen je Direktor.

9 ZAPISI

Sve informacije vezane za dokumentovani postupak upravljanje odnosima sa dobavljačima formiraju deo dokumentovanih informacija organizacije Meridian Tech d.o.o. Beograd. Dokumentovane informacije se moraju zadržavati i održavati u skladu sa ovim postupkom.

U realizaciji ovog postupka nastaju zapisi, odnosno dokumentovane informacije navedeni u tabeli.

Naziv	Referentna oznaka obrasca	Vreme čuvanja	Mesto čuvanja	Odgovorno lice
Baza Podataka Dobavljaca	MT15ZAP01		Arhiva nabavke	

10 PRILOZI

Nema.