BACKUP POLITIKA

OZNAKA DOKUMENTA	MT12POL01	**DATUM IZDANJA**	10-12-2023
PRIMERAK BROJ	01	**IZDANJE**	02

AUTORIZACIJA	**IME I PREZIME**	**FUNKCIJA**	**POTPIS**
PRIPREMIO	Vladimir Miladinović	Menadžera ISMS-a	
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
1	Sistem administrator
2	Menadžer za ISMS

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

Glavni cilj ove politike je pružiti dosledan okvir koji se primenjuje tokom celog procesa Back up-a.

Ova politika pokriva sledeću kontrolu:

- 8.13 Rezervne kopija informacija

4 PODRUČJE PRIMENE

Ova kontrola se odnosi na sve sisteme, ljude i procese koji čine informacioni sistem organizacije, uključujući direktore, zaposlene, dobavljače i ostale treće strane koje imaju pristup sistemima Meridian Tech d.o.o. Beograd .

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 systems), Sistem menadžmenta zaštite i bezbednosti informacija – ISO/IEC 27001:2022.

6 REFERENTNA DOKUMENTA

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

7 PREGLED

Politika Back up-a pruža osiguranje protiv gubitka podataka i ponekad je jedini način za obnovu poslovnih funkcija nakon kvara hardvera, oštećenja podataka ili sigurnosnog incidenta. Iako je politika sigurnosnih kopija tesno povezana s planom kontinuiteta poslovanja i oporavka od katastrofe, ona štiti od događaja koji su relativno vjerovatni da će se desiti, te će se u praksi koristiti češće od dokumenta o kontingencijama. Sigurnosne kopije su potrebne radi oporavka od kvara hardvera, oštećenja podataka i mogućih nesreća.

7.1 Svrha

Glavni cilj ove politike je pružiti dosledan okvir koji se primenjuje tokom celog procesa Back up-a.

Obuhvat

Ova politika se odnosi na sve podatke/informacije koji se čuvaju na serverima kompanije i smatraju se vitalnim za obavljanje poslovnih funkcija.

7.2 Odgovornost

Glavni kontakt i odgovorna osoba je System administrator.

7.3 Identifikacija ključnih podataka

Kompanija treba identifikovati koji su podaci najkritičniji za njenu organizaciju. Ovi ključni podaci trebaju biti identifikovani kako bi im se dala najviša prioritetnost tokom procesa Back Upa

Obuhvat Back upa

Podaci koji će biti deo Back upa uključuju:

- Svi podaci koji su određeni kao ključni za operacije kompanije i/ili radne funkcije zaposlenih.
- Sve informacije čuvane na korporativnim fajl serverima i email serverima, kao i operativnim sistemima i zapisnicima servera. Odgovornost korisnika je da se pobrine da se svi bitni podaci prebace na fajl server.
- Sve informacije čuvane na mrežnim serverima, što može uključivati web servere, baze podataka, kontrolere domena, firewall-ove, i servere za udaljeni pristup, itd.
- Zapisnike i konfiguraciju mrežnih uređaja poput prekidača, rutera, itd.
- Informacije čuvane na radnim stolovima zaposlenih ako administrator za sigurnosno kopiranje smatra da su takvi podaci neophodni i ako postoje sigurnosne kopije za tu svrhu.Lice zaduženo za Back up može umesto

toga odabrati da napravi kopiju standardne konfiguracije radnog stola i obnovi podatke sa fajl servera po vlastitom nahođenju.

7.4 Učestalost sigurnosnih kopija

Učestalost Back up-a je ključan korak ka uspešnom oporavku podataka. Adekvatna učestalost sigurnosnih kopija omogućiće dovoljno podataka za oporavak u slučaju incidenta.

Vrsta Sigurnosne Kopije	Učestalost	Sadržaj
Potpuna	Mesečna	Svi kritični podaci, fajlovi i sistemski podaci identifikovani u tački 8.6. ovih postupaka.
Diferencijalna	Dvonedeljna	Svi kritični podaci, fajlovi dodati ili promenjeni od poslednje potpune sigurnosne kopije.
Inkrementalna	Nedeljna	Svi kritični podaci, fajlovi dodati ili promenjeni od poslednje potpune, diferencijalne ili inkrementalne sigurnosne kopije.
Dnevna	Dnevna	Svi kritični podaci, fajlovi dodati ili promenjeni tog dana.
Snapshot Sigurnosna Kopija	-	Stanje mašine u vreme snimka, omogućavajući povratak na to stanje kasnije.
Arhivska Sigurnosna Kopija	Mesečna	Prikupljanje bezbednosnih događaja iz Event Viewer-a sa svih servera i sigurnosna kopija se pravi mesečno.

7.5 Skladištenje sigurnosnih kopija

Sigurnosne kopije predstavljaju ozbiljno pitanje svake organizacije i zahteva pažljivo razmatranje. Budući da sigurnosne kopije sadrže kritične, a često i poverljive podatke kompanije, potrebno je preduzeti odgovarajuće mere koje su usklađene s vrstom podataka koji se čuvaju.

7.6 Čuvanje Back up-a

Cuvanje Back up-a je jedan od ključnih faktora koje kompanija razmatra kako bi odredima dovoljan broj kopija potrebnih za smanjenje rizika, istovremeno čuvajući

neophodne podatke. Politika čuvanja Back upa takođe se pridržava svih zahteva postavljenih od strane naših regulatornih tela.

7.7 Skladištenje na sekundarnim lokacijama

Da bi se sprečio gubitak sigurnosnih kopija u slučaju poplava, požara ili velike katastrofe, kompanija će čuvati svoje sigurnosne kopije na odvojenoj geografskoj lokaciji.

Lokacije server:

- HQ Office Data Center o Bulevar Mihajla Pupina 10B/I, Beograd, Srbija
- HQ DR Location o SBB Telepark Data Center, Kumodraška 241, Beograd, Srbija
- Malta Data Center o BMIT LTD, 55/54 Triq Manuel Borg Gauci, Handaq, Qormi, Malta

7.8 Procedure testiranja Back upa

Testovi Back upa se sprovode svaka tri meseca (kvartalno), ili nakon svake značajne promene u bazi podataka ili softveru. Svaki identifikovani problem koji se odnosi na postupke sigurnosnih kopija će biti procenjen i, ukoliko se smatra potrebnim, CTO će implementirati promene u postupcima.

8. ODGOVORNOSTI I OVLAŠĆENJA

ISMS Menadžer je odgovoran za izdavanje Backup plana IT podršci i nadzor nad njihovim radom u vezi sa planiranjem i organizovanjem aktivnosti Politike backup-a. Za kontrolu primene politike ovlašćen je Direktor.

9. ZAPISI

Sve informacije vezane za dokumentovani postupak upravljanje rezervnim kopijama podataka i IT sistema 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
BACKUP PLAN	IS A12.ZAP01			
RESTORE	IS A12.ZAP02			

10. PRILOZI

U prilogu postupka su obrasci navedeni u nastavku:

- BACKUP PLAN ISA12ZAP01
- RESTORE ISA12ZAP02