POLITIKA ZA UDALJENI PRISTUP

OZNAKA DOKUMENTA	*MT9POL02*	**DATUM IZDANJA**	*05-12-2023*
PRIMERAK BROJ	*01*	**IZDANJE**	*02*

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

SADRAJ

.

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	Svi zaposleni
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

Ova Politika definiše standarde pri pristupu mreži kompanije Meridian Tech d.o.o. Beograd sa bilo kog mesta. Ovi standardi smanjuju potencijalne opasnosti kompanije i štetu koji bi mogla nastati prilikom neovlašćenog korišćenja njenih resursa.

Šteta uključuje: gubitak poverljivih informacija ili intelektualnog vlasništva, šteta po reputaciju kompanije, šteta po kritične sisteme itd.

Ova Politika pokriva sledeću kontrolu:

- 6.7 Rad na daljinu

4 PODRUČJE PRIMENE

Ova Politika se odnosi na sve zaposlene u organizaciji i sve saradnike, privremeno zaposlene, konsultante i druge dobavljače usluga (u nastavku dokumenta - kooperanti) koji pristupaju informacionom sistemu organizacije sa poslovnog ili privatnog kompjutera. Ova Politika odnosi se na dodeljeni pristup do informacionih sistema organizacije, uključujući i slanje email poruka i proveravanje internet resursa.

Poilitika obuhvata delove sistema za udaljeni pristup koji se odnose, ali nisu limitirane, na (navesti primere sistema koje organizacija koristi ili je moguće da će ih koristiti – npr. ISDN, ADSL, Frame Relay, MPLS, VPN, CDMA, Wireless Access Points i kablovske modeme, itd).

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.

Termin	**Definicija**
Kablovski modem (Cable Modem)	Kablovski modem je uređaj koji omogućava slanje i prijem računarskih informacija preko koaksijalnog kabla kablovske televizije. Kablovski modem prihvata ovaj koaksijalni kabl i može da prima podatke sa Interneta brzinom većom od jednog miliona bitova u sekundi.
CHAP (Challenge Handshake Authentication Protocol)	Predstavlja računarski protokol kojem je uloga da overava autentičnost i funkcioniše kao protokol u komunikacijskim mrežama.
DLCI (Data Link	Identifikator za određenu vezu za prenos podataka između dve

Connection Identifier)	krajnje tačke u Frame Relay mreži.
Dual Homing	Dvostruko navođenje može se odnositi ili na mrežni uređaj koji ima više od jednog mrežnog interfejsa, za svrhe redundancije, ili u firewall tehnologiji, dual-homing je jedna od firewall arhitektura za implementaciju preventivne sigurnosti.
Frame Relay	Jedan od najpopularnijih protokola za prenos podataka (uz Eternet i ATM). Koristi za povezivanje LAN, SNA, Internet ili čak "glasovnih" aplikacija.
Remote Access	Povezivanje sa sistemom za obradu podataka sa udaljene lokacije, na primer, preko servisa za daljinski pristup ili virtuelne privatne mreže
Split-tunneling	Istovremeni direktan pristup drugoj mreži (kao što je Internet ili kućna mreža) sa udaljenog uređaja (PC, PDA, WAP telefon, itd.) Dok je daljinski povezan sa poslovnom mrežom putem VPN tunela.
VPN	Virtuelna privatna mreža omogućava sigurnu privatnu mrežu putem javne mreže kao što je Internet, koristeći tehnologiju „tuneliranja“.

6 REFERENTNA DOKUMENTA

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

7 OPIS RADA

7.1 UDALJENI PRISTUP

Odgovornost je svih zaposlenih u organizaciji Meridian Tech d.o.o. Beograd i svih kooperanata koji imaju udaljeni pristup mrežnim resursima da osiguraju da njihov udaljeni pristup ima iste bezbednosne mere kao i pristup na radnom mestu u kompaniji.

- Organizacija kontroliše udaljeni pristup svojim sistemima.
- Šifre za login ili email ne smeju se davati nikome, čak ni članovima porodice.
- Bilo koji službeni ili lični kompjuter, koji ima udaljeni pristup sistemima, ne sme istovremeno biti povezan na drugu mrežu, osim ako to nije privatna mreža koju vi kontrolišete.
- Privatni email nalozi, ili drugi resursi ne smeju se koristiti za obavljanje službenih poslova. Time se obezbeđuje da se posao nikad ne meša sa privatnim stvarima.
- Nestandardni hardver mora biti odobren od strane Menadžera ISMS-a, i kompanija mora da odobri bezbednosne mere pri udaljenom pristupu sa tim hardverom.
- Svi kompjuteri kojima se pristupa resursima kompanije moraju da imaju poslednje verzije antivirusa.
- Sva lična oprema koja se koristi pri udaljenom pristupu sistemima kompanije mora da zadovoljava zahteve koji su propisani propisima kompanije.
- Organizacije ili pojedinci koji žele da implementiraju nestandardna rešenja za udaljeni pristup moraju da dobiju saglasnost od Menadžera ISMS-a.

- Zabranjena je upotreba javnih nezaštićenih mreža

Autorizovani korisnici mogu iskoristiti prednosti VPN komunikacije, koja omogućava zaposlenima i kooperantima Meridian Tech d.o.o. Beograd da pristupaju kompanijskom intranetu od kuće ili tokom putovanja kao i pristup serverima kompanije hostovanim na udaljenim lokacijama. To znači da je korisnik odgovoran za izbor internet provajdera (*Internet Service Provider* - ISP), instaliranje svih zahtevanih softvera i plaćanje povezanih naknada.

U skladu sa tim,

1. Odgovornost je korisnika koji imaju pristup VPN-u da se pobrinu da neovlašćenim korisnicima ne bude dozvoljen pristup internim mrežama.
2. Svi kompjuteri preko kojih se pristupa mrežama putem VPN-a moraju imati instalirane najnovije verzije antivirus softvera i *patches* operativnih sistema.
3. Korišćenjem VPN tehnologije korisnici moraju biti svesni da su njihove mašine de facto produžeci interne mreže, te da kao takve ne smeju da koriste konekciju ni za kakve druge svrhe, osim za poslovne svrhe što uključuje pružanje tehničke podrške.

4. Koristeći servis, potvrđujete da ste se složili sa datim uslovima i politikama. Ukoliko se ne slažete sa njima morate se odmah diskonektovati sa datog servisa.

Prilikom rada sa udaljenosti, ukoliko obavljanje radnih zadataka podrazumeva upotrebu dokumentovanih informacija u papirnom obliku, zaposleno lice mora obezbediti adekvatno mesto za čuvanje dokumentovanih informacija koje podrazumeva kontrolu pristupa, odnosno da je mesto odlaganja zaključano.

8 ODGOVORNOSTI I OVLAŠĆENJA

Svi zaposleni koji prekrše ovu Politiku mogu biti predmet disciplinskih mera, uključujući tu i prestanak radnog odnosa.

9 ZAPISI

Sve informacije vezane za dokumentovani postupak upravljanje udaljenim pristupom 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

10 PRILOZI

Nema.