POLITIKA KONTROLE PRISTUPA

OZNAKA DOKUMENTA	*MT9POL01*	**DATUM IZDANJA**	*04-12-2023*
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
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

Svrha ove Politike je da definiše kontrole pristupa koje organizacija Meridian Tech d.o.o. Beograd implementira u svom informacionom sistemu, sa ciljem omogućavanja bezbednosti informacija, sistema za obradu informacija i poslovnih procesa, a koji moraju biti kontrolisani na bazi poslovnih i bezbednosnih zahteva.

Ova politika pokriva sledeće kontrole:

- 5.15 Kontrola pristupa
- 5.16 Upravljanje identitetom
- 5.17 Informacije o autentifikaciji,
- 5.18 Prava pristupa
- 8.2 Privilegovana prava pristupa
- 8.3 Ograničenje pristupa informacijama
- 8.5 Sigurna autentifikacija

4 PODRUČJE PRIMENE

Ova Politika se odnosi na sve zaposlene u organizaciji, kao i na sve dobavljače usluga, konsultante, privremeno zaposlene, tj. na sve kooperante organizacije.

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 OPIS RADA

7.1 KONTROLA PRISTUPA

Organizacija kontroliše pristup informacionim sistemima na tri nivoa: fizičkom, organizacionim i tehnološkom nivou. Politika kontrole pristupa je bazirana i definisana u saglasnosti sa poslovnim zahtevima, uzimajući u obzir Politiku sistema upravljanja bezbednošću informacija.

Fizička zaštita je ostvarena kontrolom pristupa bezbednosnim zonama, uz čuvanje zapisa o svakome ko ulazi i ostaje unutar ovih zona (otisak prsta). Zaštita je postavljena za štampanu dokumentaciju, svaki server, kompjuter i mrežnu opremu koja ima posebnu vrednost za kompaniju.

Organiuaciona zaštita je ostvarena usvajanjem politika, procedura i dokumentacije za sva korisnička prava pristupa na nivou celog sistema. Zaštita je implementirana od strane IT podrške.

Tehnološka zaštita je ostvarena u svakom delu informacionog sistema upotrebom svih tehnoloških sredstava i mogućnosti. Zaštita je nadgledana upotrebom softverskih rešenja, hardverom i mrežnim protokolima.

Glavni princip na kome je zasnovana kontrola pristupa jeste da je **sve zabranjeno osim onog što je eksplicitno dozvoljeno**. Sa ciljem lakše kontrole, monitoringa i definisanje nivoa pristupa, sistem kontrole pristupa je podeljen na nekoliko delova:

- Pristup radnim stanicama (korisnički operativni sistem)
- Pristup domain resursima
- Pristup mrežnim resursima
- Pristup aplikacijama
- Pristup sistemskim resursima i bazi podataka

Direktni nadređeni će poslati formalni zahtev putem e-maila za svakog korisnika, precizno navodeći nivo pristupa svakom sistemu. Nakon dodele pristupa, Dispečerska služba će odgovoriti mejlom pružajući potrebne podatke za pristup sistemima. Nakon što su dodeljena prava ona se upisuju u tabelu Kontrola pristupa, koju vodi Menadžer za ISMS.

Prava pristupa mogu se menjati usled promene pozicije ili potrebe u okviru projekta, pri čemu princip ostaje isti kao kod dodeljivanja naloga.

Tabela kontrola pristupa obuhvata osnovne podatke kao što su:

- ID
- User name
- Informaciju o tržištu
- Pristup izveštajima i sistemtskim aplikacijama

U slučaju kada zaposleni bude preraspoređen sa jedne pozicije na drugu ili napusti kompaniju, prava pristupa informacionim sistemima moraju biti promenjena ili ukinuta u

roku od jednog radnog dana. Zahtev za promenu ili ukidanje prava pristupa upućuje se od strane neposrednog rukovodioca prema Dispečerskoj službi. Nakon procesa, korisnik se briše iz tabele Kontrole pristupa.

7.1.1 Server soba

Pristup server sobi je strogo ograničen i dozvoljen samo autorizovanim osobama preko identifikacije otiskom prsta.

7.1.2 Revizija korisničkih privilegija pristupa

Menadžer ISMS-a redovno vrši proveru korisničkih prava pristupa svakih 12 meseci ili u kraćim intervalima, posebno kada dolazi do napuštanja radnog mesta, novih zaposlenih, promena radnih pozicija itd.
Provera korisničkih prava pristupa se pravi redovno kako bi se omogućila efektivna kontrola pristupa informacijama i IT servisima.

7.1.3 Indetifikacija i potvrda naloga

Korisnička prava pristupa su definisana u saglasnosti sa poslovnim i ugovornim zahtevima tako da se predviđaju sankcije, ukoliko neko pokuša neovlašćeno da pristupi informacijama. Proces identifikacije i potvrde identiteta korisnika obuhvata sledeće:

- Jedinstveni korisnički nalog: ID, koriste se za identifikaciju korisnika. Upotreba grupnih ID-a će biti dozvoljena samo u slučaju da je to potrebno za određene poslovne operacije, ali prethodno odobrene od strane neposrednog rukovodioca i ISMS Menadžera.
- Pre nego što se dozvoli pristup informacionom sistemu ili IT servisu potrebna je potvrda od strane neposrednog rukovodioca.
- Redovno se proverava da li je nivo odobrenog prava pristupa u saglasnosti sa poslovnim potrebama.

Prava pristupa korisnicima koji su promenili poziciju ili su napustili organizaciju su deaktivirana. U slučaju višemesečnog bolovanja ili porodiljskog odsustva, status korisnika unutar aplikacije Dispečar označava se kao neaktivan.

U slučaju kada zaposleni napusti radno mesto ili uređaj u obavezi su da zaključaju uređaj.

7.1.4 Postupak u slučaju napuštanja radnog mesta

Kada zaposleni napusti radno mesto ili uređaj, obavezan je da se odjavi sa svih naloga i zaključa uređaj.

7.1.5 Izolacija osetljivih informacija

Pristup izolovanim osetljivim sistemima je kontrolisan korišćenjem Tabele Kontrole pristupa. Prava pristupa se proveravaju i odobravaju od strane neposrednog rukovodioca, a implementiraju od strane Dispečerske službe.

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 pravom pristupa 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

U prilogu postupka su obrasci navedeni u nastavku:

- Tabela pristupa BACK OFFICE aplikacije
- Tabelas pristupa ATLAS aplikacije