PROCEDURA ORGANIZACIJE SISTEMA BEZBEDNOSTI

OZNAKA DOKUMENTA	*MT11PRO01*	**DATUM IZDANJA**	*01-12-2023*
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	Menadžer ISMS
2	Dispečar centar

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 procedure je da opiše koncept fizičke bezbednosti u organizaciji Meridian Tech d.o.o. Beograd. Menadžer ISMS-a, zaposleni i drugi subjekti koji učestvuju u održavanju fizičke bezbednosti organizacije, imaju odgovornost da se pridržavaju i primenjuju uputstva iz ove procedure.

Ova procedura pokriva sledeće kontrole:

- 7.1 Perimetri fizičke bezbednosti
- 7.2 Fizički pristup
- 7.3 Zaštita kancelarije, prostorije i opreme
- 7.4 Nadgledanje fizičke bezbednosti
- 7.5 Zaštita od fizičkih i pretnji iz okruženja
- 7.6 Rad u zaštićenom području
- 7.8 Položaj opreme i zaštita
- 7.11 Pomoćne komunalne funkcije za podršku
- 7.12 Sigurnost kabliranja
- 7.13 Održavanje opreme
- 7.14 Bezbedno odlaganje ili ponovna upotreba opreme

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 kompanije.

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:

QMS – (Quality management system), Sistem menadžmenta kvaliteta,

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 KONCEPT BEZBEDNOSTI

U cilju zaštite zaposlenih i imovine informacionog sistema od mogućih pretnji po fizičku bezbednost, organizacije Meridian Tech d.o.o. Beograd je uspostavilo kompleksan sistem pripravnosti i prevencije za moguće ugrožavanje bezbednosti.
Sistem bezbednosti prostorija u organizaciji se sastoji od:

- Sistema za kontrolu pristupa
- Protiv-požarnog sistema
- Fizičko-tehničkog obezbeđenja.

7.2 PERIMERTI FIZIČKE BEZBEDNOSTI

Organizacija Meridian Tech d.o.o. Beograd je odredilo 2 (broj bezbednih zona) bezbednosne zone.

- Glavni ulaz u kancelariju – glavni ulaz se koristi jednako za zaposlene u organizaciji kao i stranke. Ulazak stranke je moguće uz predhodnu najavu kod zaposlenog kog koga dolazi.
- Kancelarija Direktora - u kancelariju Direktora zaposleni mogu ulaziti jedino uz njegovo prisutstvo.
- Kancelarije osoblja - u kancelarije zaposlenih, stranke mogu ulaziti jedino uz prisutstvo zaposlenih
- Prostorija za sastanke - ova prostorija služi za održavanje sastanaka. Obzirom da u njoj često borave stranke, u ovoj prostoriji ne sme da se nalazi nikakva informacija koja je prema Pravilniku o klasifikaciji informacija klasifikovana kao ‘poverljiva’ ili ‘interna’.
- Na svim ulazima stoji uređaj za uzimanje otiska prsta (za zaposlene)/kartica kao i interfon za posetioce

7.1.1. Kontrola fizičkog ulaska

Obezbeđene prostorije su zaštićene odgovarajućim kontrolama na ulazu (otisak prsta) kako bi se osiguralo da samo ovlašćeno osoblje ima pravo pristupa.

7.1.2. Zaštita od spoljnih pretnji

Protiv-požarni aparati su uvedeni kako bi se kontrolisao požar u prostorijama. Instalirani su u svim prostorijama organizacije.

- Opasan ili zapaljiv materijal se čuva na sigurnosnom rastojanju od bezbednosnih prostorija. Potrošan kancelarijski materijal ne treba čuvati u obezbeđenim prostorijama;
- Odgovarajuća vatrogasna oprema je obezbeđena i adekvatno postavljena u prostorijama organizacije.

Pristup zgradama u kojima se nalaze kritični sistemi treba kontinuirano pratiti kako bi se otkrio neovlašćeni pristup ili sumnjivo ponašanje:

a) instaliranje sistema za video nadzor kao što je closed-circuit television za pregled i snimanje pristupa osetljivim oblastima unutar i van prostorija organizacije;

b) instaliranje, u skladu sa relevantnim važećim standardima, i periodično testiranje detektora neovlašćnog ulaska u prostorije kompanije

Dizajn sistema za praćenje treba da bude poverljiv jer otkrivanje može olakšati neotkrivene provale.

Sistemi za nadzor treba da budu zaštićeni od neovlašćenog pristupa kako bi se sprečilo da neovlašćene osobe pristupe informacijama o nadzoru, kao što su video fidovi, ili da se sistemi onesposobe na daljinu.

Kontrolna tabla alarmnog sistema treba da bude postavljena u alarmiranoj zoni i, za bezbednosne alarme, na mestu koje omogućava lak izlaz za osobu koja postavlja alarm. Kontrolna tabla i detektori treba da imaju mehanizme otporne na neovlašćene radnje. Sistem treba redovno testirati kako bi se osiguralo da radi kako je predviđeno, posebno ako se njegove komponente napajaju baterijama.

Bilo koji mehanizam za praćenje i snimanje treba da se koristi uzimajući u obzir lokalne zakone i propise, uključujući zakone o zaštiti podataka i zaštiti ličnih podataka, posebno u pogledu praćenja osoblja i perioda čuvanja snimljenih video zapisa.

7.1.3. Rad u obezbeđenim prostorijama

Prema uputstvu za kontrolu obezbeđenih prostorija, sva lica koja koriste obezbeđenu prostoriju, moraju da poštuju sledeća pravila:

- U obezbeđenu prostoriju je zabranjen ulaz bez pratnje za sva lica koja nisu na spisku za pristup obezbeđenoj prostoriji.
- Obezbeđena prostorija mora biti stalno zaključana.
- Konzumiranje hrane i pića u obezbeđenoj sobi je zabranjena.
- Premeštanje oprema i kablova se mogu izvršiti samo uz prethodne konsultacije sa odgovarajućom osobom iz IT službe;

Uputstva za rad u obezbeđenim prostorijama obuhvataju zahteve za zaposlene, izvođače radova i druge saradnike koji obavljaju svoje aktivnosti u obezbeđenim prostorijama.

Ne stavljati na raspolaganje imenika, internih telefonskih imenika i onlajn dostupnih mapa koje identifikuju lokacije objekata za obradu poverljivih informacija bilo kom neovlašćenom licu.

7.1.4. Fizičko-tehničko obezbeđenje

Sve dužnosti fizičko-tehničkog obezbeđenja obavljaju se u skladu sa ovom procedurom i drugim dokumentovanim informacijama iz uspostavljenog sistema upravljanja bezbednošću informacija ISMS.
Potrebno je obezbediti rasvetu i komunikaciju u slučaju nužde. Prekidači za slučaj nužde i ventili/prekidači za isključivanje struje, vode, plina ili drugih komunalnih usluga trebaju biti smešteni u blizini izlaza u slučaju nužde ili prostorija za opremu.
Kontakt podaci za hitne slučajeve trebaju biti zabeleženi i dostupni osoblju u slučaju prekida rada. U takvim slučajevima obaveštava se Dispečerska služba putem Skaypa koja dalje upućuje poziv odgovornim službama.

7.3 ZAŠTITA OPREME

Celokupna oprema organizacije je zaštićena od fizičkih i elementarnih pretnji i nepogoda.

7.3.1 Električno napajanje

Oprema je zaštićena od nestanka struje i drugih poremećaja usled kvara ili prestanka napajanja. Svaki računar/server koji su od strane Sistem administratora procenjeni kao najbitniji po organizaciju treba da imaju svoj UPS za bezbedan prekid programa ili kontinuirano obavljanje aktivnosti koje su kritične za poslovanje.

7.3.2 Obezbeđenje kablova

Kablovi za umrežavanje i napajanje u prostorijama gde se vrši obrada informacija se nalaze pod zemljom (podom), gde je to fizički moguće. Ukoliko nisu, onda se kablovi adekvatno zaštićuju (plastičnim kanalicama, vezuju se u snopove, radni stolovi sa sistemima za upravljanje kablovima itd.).
Kablovi i oprema su jasno identifikovani i obeleženi kako bi se greške pri rukovanju svele na minimum (npr. slučajni spoj pogrešnih mrežnih kablova ili nakon pomeranja prilikom čišćenja).

7.3.3 Održavanje opreme

Oprema se održava u skladu sa preporukama proizvođača, po propisanim specifikacijama i vremenskim intervalima. Servisiranje opreme koju obavlja treća strana (dobavljač usluga) obezbeđuje bezbednost oprema i informacija potpisivanjem Ugovora o neotkrivanju podataka.
Ukoliko se održavanje vrši sa udaljenih lokacija mora postojati sledljivost odobravanja i kontrole pristupa za daljinsko održavanje sistema i opreme organizacije.

7.3.4 Bezbednost opreme izvan prostora

Bezbednost se primenjuje i na opremi izvan kancelarijskih prostorija uzimajući u obzir različite vrste rizika rada izvan prostorija organizacije. Bez obzira na vlasništvo, za upotrebu bilo koje oprema za obradu podataka izvan prostorija organizacije, mora se dobiti ovlašćenje od strane direktora. Svi zahtevi vezano za bezbednost opreme izvan prostorija su dati u dokumentu Politika upotrebe uređaja izvan poslovnog prostora.

7.3.5 Bezbedno uklanjanje i ponovono postavljanje opreme

Svi delovi oprema koji sadrže medijume za skladištenje podataka moraju se proveriti da li su svi osetljivi podaci i licencirani softver sigurno uklonjeni. Uređaji koji sadrže osetljive informacije se fizički uništavaju ili se podaci uništavaju ili brišu koristeći tehnike koje obezbeđuju da se originalni podaci ne mogu vratiti (npr. drobljenje tupim predmetom, degausser). Standardne tehnike brisanja i formatiranja nisu preporučljive.
Nalepnice i oznake koje identifikuju organizaciju ili označavaju klasifikaciju, vlasnika, sistem ili mrežu, treba ukloniti pre odlaganja, uključujući preprodaju ili doniranje u dobrotvorne svrhe.

7.3.6 Iznosenje imovine

IKT oprema, informacije ili softver se ne smeju nositi van prostorija bez prethodnog odobrenja.

Kada je potrebno i odgovarajuće oprema se evidentira pri iznošenju i unošenju. Zahtevi su dati u dokumentu Politika upotrebe uređaja izvan poslovnog prostora.

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 fizičkom bezbednošću 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.