POLITIKA BEZBEDNOSTI PRENOSIVIH UREĐAJA

OZNAKA DOKUMENTA	*MT6POL01*	**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	

Ovaj dokument je vlasništvo organizacije Meridian Tech d.o.o. Beograd i njegov sadržaj ne sme se saopštavati neovlašćenim osobama, ili osobama van organizacije bez pismene saglasnosti Menadžera ISMS-a.

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	Direktor
2	Menadžer ISMS
3	Svi zaposleni u organizaciji

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 opisuje kontrole neophodne za minimiziranje bezbednosnih rizika, koji se odnose na prenosive uređaje u organizaciji Meridian Tech d.o.o. Beograd .

Svi kompjuterski sistemi su izloženi bezbednosim rizicima. Laptop uređaji i drugi prenosivi uređaji su osnovno sredstvo za rad, ali mogućnost njihovog prenosa čini ih posebno ranjivima na fizičke pretnje ili krađu.

Ne zaboravljajte da šteta od ovih napada nije samo vrednost hardvera, već i vrednost svih podataka koji se nalaze na njemu. Mi smo veoma zavisni od kompjuterskih sistema koji nam omogućavaju potrebne informacije bilo kada i bilo gde. Šteta koja bi se uzrokovala prilikom neovlašćenog pristupa informacijama ili promena tih informacija je višestruko veća nego vrednost samog hardvera.

Ova Politika se poziva na druge Politike bezbednosti, ali su informacije koje sadrži direktno namenjene korisnicima laptopova i drugih prenosnih uređaja, i u slučaju poklapanja, ova Politika uvek ima prednost.

Ova politika pokriva sledeće kontrole:

- 8.1 Krajnji korisnicki uredjaji,
- 7.10 Uređaji za skladištenje,
- 7.14 Sigurno odlaganje ili ponovna upotreba opreme

4 PODRUČJE PRIMENE

Ova Politika se odnosi na sve laptopove i prenosive uređaje koji su vlasništvo organizacije, bez obzira da li se koriste u kancelariji, kod kuće ili na drugoj lokaciji. Takođe, odnosi se na sve zaposlene i kooperante koje imaju pristup informacionom sistemu.

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 FIZIČKE KONTROLE ZA PRENOSNE UREĐAJE

- Fizička bezbednost prenosivih uređaja je lična odgovornost svakog vlasnika uređaja.
- Prenosivi uređaji se čuvaju u vidnom polju vlasnika uvek kada je to moguće. Posebna pažnja je neophodna na javnim mestima kao što su aerodromi, železničke stanice, restorani ili neka druga javna mesta.
- Prenosivi uređaji se moraju zaključavati uvek kada se ne koriste, preporučljivo u jakim pregradama, fiokama ili sefovima. Ovo se radi u kućnim uslovima, na poslu ili u hotelu. Prenosivi uređaji se nikada ne smeju ostavljati na vidnom mestu u automobilima.
- Laptopovi se moraju nositi i čuvati u posebnim torbicama ili jakim koferima kako bi se smanjio rizik od slučajnih oštećenja.
    - Podaci o modelu, serijskom broju i inventarnom broju trebaju se čuvati. Ukoliko je laptop ukraden, odmah se obaveštava Policija i nadređena osoba, ili ako nije moguće odmah onda u najkraćem mogućem roku.

7.2 KONTROLE PROTIV NEOVLAŠTENOG PRISTUPA INFROMACIJAMA NA PRENOSIVIM UREĐAJIMA

- Softver za enkripciju se koristi na svim prenosivim uređajima ukoliko je analiza rizika pokazala potrebu za tim. Takođe, potrebne su jake enkripcione šifre. Za više informacija u vezi enkripcije pročitajte dokument MT10POL01 Kriptografija. Ako je prenosivi uređaj ukraden ili izgubljen, enkripcija omogućava veoma efikasnu zaštitu podataka koji se nalaze na njemu.
- Poslovni prenosivi uređaji su dodeljeni za upotrebu ovlašćenim korisnicima. Oni se ne smeju pozajmljivati ili koristiti od strane prijatelja ili porodice.
- Ostavljanje prenosivog uređaja sa aktivnim ekranom na njemu treba izbegavati. U tom slučaju laptopovi se uvek gase, izloguju ili se zaključava ekran.

7.3 DRUGE KONTROLE ZA PRENOSIVE UREĐAJE

7.3.1 Neutarizovan softver

Download, instalacija ili korišćenje neautorizovanog softvera je strogo zabranjeno. Neautorizovan softver može da uzrokuje ozbiljne ranjivosti u sistemu kao i da utiče na rad vašeg laptopa. Softverski paketi koji omogućavaju da kompjuter bude kontrolisan sa

udaljene lokacije i takozvani ‘hacking tools’ (npr. network sniffers i password crackers) su strogo zabranjeni osim ako nisu striktno odobreni od strane menadžmenta zbog poslovnih aktivnosti.

7.3.2 Nelicencirani softver

Većina softvera, osim ako nije posebno definisan kao “freeware” ili “public domain software”, može da se instalira i koristi ako je plaćena licenca. Shareware ili probni paketi moraju biti obrisani ili licencirani na kraju test perioda. Neki softveri su limitirani za privatnu upotrebu od strane pojedinaca dok drugi zahtevaju plaćanje licenci. Pojedinci i kompanije redovno se suočavaju sa tužbama zbog korišćenja nelicenciranog softvera.

7.3.3 Zakoni, regulativa i politike

Korišćenje prenosivih uređaja mora da bude u saglasnosti sa relevatnim zakonima, regulativom i politikama koji se odnose na korišćenje laptopova i informacija. Licenciranje softvera je već bilo pomenuto, a propisi o zaštiti podataka o ličnosti su drugi primer regulative sa kojom se mora usklađivati korišćenje informacione imovine.

7.3.4 Nedozvoljeni sadržaj

Kompanija neće tolerisati nedozvoljene sadržaje kao što su pornografija, rasizam, slike, video ili email poruke koje mogu da prouzrukuju agresiju ili nesigurnost. Ovi sadržaji se ne smeju čuvati, koristiti, kopirati ili prenositi na laptopu. Menadžer ISMS-a povremeno proverava mrežu i sisteme u vezi sa ovim materijalima i prati upotrebu Interneta. On obaveštava Direktora, ako primeti da neko često krši ova pravila, i tada se inicira disciplinski postupak. Ukoliko dobijete nedozvoljene sadržaje putem email poruke ili drugim putem, iste se moraju odmah ukloniti sa sistema. U slučaju kada se slučajno otvori nedozvoljeni sajt, korisnik treba koristiti opciju BACK ili da zatvori prozor odmah. Ako kosirnik dobija puno spam poruka o tome mora obavestiti odgovornu osobu.

Osetljive informacije ne treba čuvati duže nego što je potrebno da bi se smanjio rizik od neželjenog otkrivanja.
Prilikom brisanja informacija o sistemima, aplikacijama i uslugama treba uzeti u obzir sledeće:
a) odabir metode brisanja (npr. elektronsko prepisivanje ili kriptografsko brisanje) u skladu sa poslovnim zahtevima i uzimajući u obzir relevantne zakone i propise;
b) evidentiranje rezultata brisanja kao dokaza;
c) kada koristite pružaoce usluga brisanja informacija, pribavljanje dokaza o brisanju informacija od njih.

Kada treća lica čuvaju informacije organizacije u njeno ime, organizacija treba da razmotri uključivanje zahteva za brisanje informacija u ugovore sa trećim stranama kako bi ih sprovela tokom i po prestanku pružanja takvih usluga (na primer Cloude servis).

S obzirom da se bezbedno brisanje nekih uređaja (npr. pametnih telefona) može postići samo uništavanjem ili korišćenjem funkcija ugrađenih u ove uređaje (npr. „vraćanje fabričkih podešavanja“), organizacija treba da izabere odgovarajući metod u skladu sa klasifikacijom informacija kojom rukuje takvi uređaji.

7.3.5 Oprema za mobilni rad – nabavka, adekvatnost i posdrška

Kada se razmatra korišćenje ili nabavka mobilne opreme koja će se možda koristiti i za upravljanje poverljivim informacijama, važno je obezbediti: - Kada se uređaj koristi za upravljanje podacima organizacije od strane spoljnih saradnika ili obrnuto, da uređaj zadovoljava sve postavljene sigurnosne zahteve; - Uređaj je tehnički sposoban da pruži prihvatljivu zaštitu podataka koji se čuvaju, preuzimaju ili postavljaju na uređaj. Postojaće dostupna adekvatna tehnička podrška kako bi obezbedili da uređaj može da bude podešen i korišćen na takav način koji čuva poverljivost podataka. Od tehničkog osoblja zaposleni će dobiti savete i podršku u vezi sa uređajima i softverom.

7.3.6 Upravljanje prenosivim uređajima

Da bi se obezbedila sigurnost uređaji moraju aktivno biti održavani u smislu konfiguracije i upravljanja. Enkripcija ne sprečava pristup podacima ukoliko je sistem zaražen ili hakovan. Potrebno je obezbediti da uređaji imaju instaliran automatski ažuriran antivirusni softver kada je to primenljivo. Prisustvo malware-a, kao što su virusi i crvi mogu da predstave pretnju zaštiti podataka na uređaju. Operativni sistem koji se nalazi na uređaju mora da bude podržan od strane proizvođača i da ima instalirane sigurnosne zakrpe za operativni sistem i ostale instalirane softverske aplikacije. Gde je primenljivo, obezbediti da uređaji imaju ispravno konfigurisan firewall softver. Potrebno je konfigurisati korisnička prava na najmanja moguća. Obezbediti da za normalne poslovne aktivnosti korisnik nema administratorsko pravo pristupa. Administracija je odgovorno za vođenje evidencije o svim mobilnim uređajima. Evidencija o uređajima treba da sadrži podatke koji su neophodni da bi se uređaj i/ili korisnik nedvosmisleno identifikovali, kao što su proizvođač, model, serijski broj, korisnik koji je zadužio uređaj i njegov jedinstveni matični broj i slično.

7.3.7 Ponovno dodeljivanje, popravka i uklanjanje opreme

Podaci sa prenosnog uređaja moraju biti uklonjeni pre nego što se on pozajmi ili dodeli drugom licu. Podaci se uklanjaju odmah po vraćanju uređaja. Podaci moraju biti obrisani na siguran način kada se uređaj uklanja. Kada mobilni uređaj popravlja druga

organizacija postoje dve opcije u vezi sa ličnim ili poverljivim podacima koji se nalaze na uređaju: Ukloniti podatke sa uređaja pre popravke ili održavanja; Uposliti firmu koja će imati ugovornu obavezu da upravlja podacima na siguran način. U slučaju da se pronađe mobilni uređaj čiji nestanak je prijavljen, IT osoblje izvršiće pregled uređaja i utvrditi da li on može biti ponovo korišćen za rad na daljinu ili ne.

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 bezbednošću prenosivih uređaja 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.