POLITIKA UPOTREBE UREĐAJA I OPREME IZVAN POSLOVNOG PROSTORA

OZNAKA DOKUMENTA	*MT11POL01*	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	Rukovodioci sektora
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 se obezbedi pravilno korišćenje i zaštita prenosivih uređaja organizacije Meridian Tech d.o.o. Beograd kako bi se smanjio rizik od krađe ili gubitka uređaja i poverljivih informacija koje oni sadrže kao i da se osigura da vlasnici imaju određeni nivo odgovornosti u smislu poznavanja rizika i procedura za sprečavanje rizika prilikom upotrebe prenosivih uređaja korišćenih izvan prostorija organizacije.

Ova politika pokriva sledeću kontrolu:

- 7.9 Bezbednost imovine van poslovnih prostorija

4 PODRUČJE PRIMENE

Ova politika se odnosi na sve zaposlene koji su vlasnici laptopova i ostalih prenosivih uređaja, ili koriste privremene prenosive računare iz 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 PRAVILA ZA BEZBEDNO KORIŠĆENJE PRENOSIVIH UREĐAJA

7.1.1 Opšte uputstvo

Prenosivi uređaji koji se koriste izvan prostorija organizacije su izloženi rizicima koji se mogu smanjiti uz primenu određenih mera. Moguće pretnje su: krađa prenosive opreme i informacija, neovlašćeno otkrivanje, neovlašćen pristup internim sistemima organizacije, gubitak podataka, zaraza putem virusa.

Kada se oprema izvan poslovnih prostorija prenosi između različitih pojedinaca ili zainteresovanih strana obavezno je vođenje dnevnika koji definiše lanac nadzora za opremu uključujući najmanje ime, ulogu i organizaciju onih koji su odgovorni za opremu. Informacije koje nije potrebno preneti sa imovinom treba bezbedno izbrisati pre prenosa;

7.1.2 Briga o opremi

- Sa celokupnom opremom treba pažljivo rukovati u skladu sa preporukama proizvođača;
- Prenosivi uređaji su radna oprema i sa njom treba pažljivo postupati;
- Prenosive uređaje mogu da koriste samo zaposleni u kompaniji. Ne može ih koristiti niko drugi, bilo da su u pitanju članovi porodice, prijatelji i sl.
- Prenosivi uređaji su namenjeni prvenstveno u poslovne svrhe;

7.1.3 Odobrenje

- Nije dozvoljeno da se kompjuterska oprema i periferni uređaji **koji nisu u vlasništvu kompanije** povezuju na internu mrežu preduzeća, osim u slučaju da je odobreno od strane Menadžera ISMS-a;
- Novu opremu (tehnologije) ne treba koristiti u poslovne svrhe, sve dok se ne izvrši bezbednosna analiza i ne podese bezbednosni parametri koje je kompanija usvojila.

7.1.4 Instaliranje

Stepen zaštite prenosivih uređaja mora biti najmanje jednak stepenu zaštite kancelarijske/statičke opreme koja se koristi za istu svrhu, uzimajući u obzir rizike koji nastaju prilikom rada van organizacije.

Promene bezbednosnih opcija na prenosivim uređajima se mogu izvršiti samo od lica koja su ovlašćena od strane Menadžera ISMS-a.

7.1.5 Poverljivost

Zaposleni ne smeju čuvati poverljive poslovne informacije izvan organizacije, osim ako su sačuvani na pravilno obezbeđenim prenosivim uređajima u vlasništvu organizacije, i na određeno vreme. Korisnici su dužni da zaštite poverljive informacije preuzete iz organizacije.

7.1.6 Izveštaj o icidentima

Incidenti i problemi sa prenosivim uređajima se moraju prijaviti u najkraćem mogućem roku. U slučaju poteškoća u funkcionisanju uređaja i u slučaju bezbednosnih incidenata, mora da se obavesti Menadžer ISMS-a, u skladu sa Upravljanje Bezbednosnim Incidentima.

7.1.7 Fizička zaštita za prenosive uređaje

Zaštitne mere su uvedene da bi se sprečio neovlašćen pristup ili otkrivanje informacija koje su sačuvane ili obrađene na prenosivim uređajima. Ako postoje poverljivi dokumenti na papiru koji se koriste izvan prostorija organizacije, treba ih zaštiti na isti način kao i prenosive uređaje.

7.1.7.1 Preventive mere

Neovlašćena lica mogu čitati informacije sa ekrana kada se uređaj koristi na javnom mestu. Korisnik treba da zauzme poziciju u kojoj druga lica ne mogu da vide ekran uređaja.

Prenosive uređaje van prostorija organizacije i u organizaciji gde postoji velika frekvencija prolaznika se ne sme ostaviti bez nadzora.

7.1.7.2 Mere koje se sprovode u slučaju putovanja

Vlasnici uređaja su odgovorni za zaštitu prenosivih uređaja na sledeći način:

- Tokom putovanja prenosni uređaji se transportuju kao ručni prtljag. Da bi se računar sigurno transportovao, koristi se obložena torba za te namene.

- Prenosni uređaji se ne ostavljaju na vidnom mestu u automobilu, bez obzira da li ste u vozilu ili ne, i ne smeju se ostaviti bilo gde bez stalnog nadzora na javnim mestima.

Kada god je jedno od ovih pravila neprikladno ili nepraktično, vlasnik uređaja je odgovoran da preduzme sve razumne mere kako bi se smanjio rizik od gubitka ili oštećenja računara.

7.1.7.3 Izveštaj o ukradenoj opremi

U slučaju krađe ili gubitka prenosnih uređaja, incident se mora odmah prijaviti nadređenom rukovoiocu.

7.1.7.4 Notebookovi / laptopovi

Notebookovi / laptopovi su posebno podložni krađi ili gubljenju. Većina lopova je u potrazi za lakim profitom, ali postoji velika mogućnost zloupotrebe poverljivih informacija koje uređaji sadrže. Ukoliko se objave takve informacije, one mogu izazvati značajni finansijski i komercijalni uticaj na organizaciju, kao i narušavanje njene reputacije.

7.1.7.5 Priprema notebook/laptop računara pre davanja na korišćenje.

IT podrška je odgovoran za organizaciju pripreme notebook/laptop računara pre davanja na korišćenje.

7.1.7.6 Oprema i softver

Pre uručivanja notebook/laptop računara korisniku na upotrebu, jedino licencirani sistemski softver i licencirana korisnička oprema mogu biti instalirani, odnosno open source softver odobren za korišćenje od strane organizacije.

7.1.7.7 Podešavanje

Uređaj mora biti podešen u skladu sa bezbednosnim parametrima navedenim u ovom dokumentu u cilju sprečavanja izmena ovih konfiguracionih parametara od strane korisnika.

- Programi za zaštitu virusa moraju biti instalirani.
- Firewall mora biti podešen.
- Radi autorizacije korisnika za korišćenje laptopa podešena je prijava BIOS lozinkom i korisničkom lozinkom za prijavu na Windows. Korisnici se prijavljuju na operativni sistem koristeći detalje sadržane u korisničkom profilu.
- Svaki prenosivi računar koji će imati poverljive podatke mora imati podešen **alat za enkripciju podataka** na disku. Ako je moguće, isti metod treba primeniti i za enkripciju poverljivih podataka na mobilnim uređajima.

7.1.8 Laptop za opštu upotebu

Ukoliko je računar namenjen za više korisnika u kompaniji, pre nego što će se koristiti, postoji procedura za uklanjanje svih podaka prethodnih korisnika i uspostavljanja standardno početnog stanja.

7.1.9 Laptop za posebne namene

Ovakvi laptopovi imaju ista pravila korišćenja kao i svi drugi prenosivi uređaji sa sledećim izuzecima:

- Korisnički profili se koriste sa administratorskim privilegijama na računaru.
- Instaliranje dodatnog softvera je dozvoljeno za administratorsku svrhu kao i konfigurisanje mrežnih komponenti i test konfiguracije.

Laptop računari koje koriste lica koja nisu zaposlena u organizaciji, a povezani su na mrežu organizacije, moraju da ispune osnovne kriterijume bezbednosti. Svi prenosivi računari koji nisu u vlasništvu organizacije (pripadaju stranim dobavljačima ili saradnicima) koji hoće da se povežu na mrežu organizacije, moraju da zadovolje sledeće kriterijume:

- Umrežavanje je dozvoljeno samo uz podešavanje MS Internet Service Manager-a ili adekvatnog alata;
- Za pristup mrežnim uslugama organizacije, potvrda autentičnosti mora biti kreirana sa jedinstvenim identifikatorom za korisnika;
- Računar mora imati aktivnu zaštitu od virusa sa najnovijim antivirusnim definicijama.

7.1.10 Korisničke odgovornosti

Zaposleni organizacije postaje „vlasnik“ prenosnog uređaja na osnovu poslovnih potreba i odgovornosti u okviru organizacije. Kada se zaposlenom daje računar, on mora potpisati zapisnik o zaduženju/razduženju prenosivog računara i time se obaveže da će poštovati sve principe ovog uputstva.

Prenosivi uređaji koji se izdaju zaposlenima ostaju vlasništvo organizacije. Kada je uređaj dodeljen tada zaposleni postaje privremeni vlasnik uređaja. Nakon završetka radnog odnosa u organizaciji, lice mora da vrati uređaj njegovom rukovodiocu, i ponovo potpiše zapisnik o zaduženju/razduženju prenosivog računara. Na taj način se oslobađa od dalje odgovornosti nad računarom.

Pored opštih mera korisnici moraju biti oprezni :

- Vlasnik uređaja mora najmanje jednom mesečno, u toku radnog dana, na osam sati, da priključi uređaj na internu mrežu organizacije, kako bi se ažurirao bezbednosni softver operativnog sistema i drugi programi.
- Korisnik je dužan da obezbedi prenos podataka sa backup diska na server preko interne mreže organizacije
- Za svako povezivanje računara na računarsku mrežu, vlasnik je dužan da ažurira instalirani antivirusni program (antivirus definicije).

Pre ulaska na javnu mrežu, vlasnik mora da proveri stanje zaštite od virusa. Računaru bez instaliranog sistema zaštite od virusa koji se koristi u organizaciji, nije dozvoljeno da pristupi mreži. U slučaju otkrivanja sumnjivih promena u radu na računaru, korisnik mora odneti računar na pregled u organizaciju pre pristupa na intranet ili Internet mrežu.

- Opciju Bluetooth-a na uređaju se uključuje samo kad je to zaista neophodno i samo u vreme aktuelne veze.
- Opcija Wireless-a na uređaju se uključuje samo kad je to zaista neophodno i samo u vreme aktuelne veze. Dok je uređaj povezan na internu mrežu kompanije, wireless mora biti isključen.

U prenosive uređaje nije dozvoljeno da se ugrade dodatni uređaji u ličnoj svojini ili Bluetooth za bežično povezivanje sa drugim javnim mrežama. Takođe je zabranjeno da se menja bezbednosna instalacija i konfiguracija računara.

Prenosivi uređaji su ranjiviji od desktop računara i zahtevaju više brige. Zbog toga se preporučuje praćenje sledećih uputstava za njihovu brigu i održavanje:

- Vodite računa da ne udarite ili ispustite računar,
- Nemojte nositi predmete sa njim, koje mogu da ga oštete i ne stavljajte nikakve predmete na njega. Nosite ga u čvrstoj torbi za računare, i imajte na umu da torbe nisu namenjene za veće težine,
- Uzmite u obzir da se mrežni kabel lako može oštetiti prilikom upotrebe i čuvanja,
- Pre transporta, računar prvo mora da se ugasi i stavi u torbu za nošenje
- Izbegavajte da dodirujete ekran na notebook/laptopu
- Izbegavajte da izlažete uređaje velikim temperaturnim razlikama. Komponente su na niskim temperaturama lako lomljive, dok se na visokim deformišu
- Držite uređaj dalje od svih vrsta tečnosti. Najmanja prosuta tečnost po uređaju stvara ogromne troškove popravke i moguće gubitke podataka
- Držite sve CD/DVD-ROM, USB, memorijske i druge uređaje dalje od magnetnog zračenja. Magnetna polja mogu prouzrokovati brisanje podataka.
- Kad god je to moguće, izbegavajte gašenje računara dok je uključen glavni hard disk, jer se podaci sa diska mogu oštetiti.

7.2 MOBILNI TELFONI

Upotreba Smartphone-a je namenjena pre svega kao dodatna personalna oprema za obradu informacija na više načina, za razliku od običnog mobilnog telefona koji ima znatno skromnije mogućnosti. Pametni mobilni telefoni su moderna sredstva komunikacije i korisnici uče da ga koriste u skladu sa poslovnim potrebama i odgovornostima u organizaciji. Treba obratiti pažnju da zbog malih dimenzija i težine, pametni mobilni telefon može biti zagubljen ili ukraden. Pored toga što pametni mobilni telefoni služe za razgovor, imaju i druge funkcije u vidu audio i video snimanja, fotografisanja i čitanje e-pošte, pa postoji mogućnost da se na njima neovlašćeno čuvaju poverljivi podaci.

7.2.1 Korisničke džužnosti kod upotrebe mobilnih telefona

Pored opštih mera korisnici moraju biti oprezni u sledećem:

- Upotreba smart telefona na javnim mestima (npr. aerodromi, javni prevoz ili hotelski lobiji) mora da se obavlja na način da neovlašćena lica nemaju mogućnost da čuju razgovore. Takođe, treba da se obrati pažnja na „surfovanje preko ramena“.
- Ako smart telefon ima mogućnost Bluetooth ili Wireless (WiFi) opcija, mogu se uključiti samo kada je to zaista neophodno i samo u trenutku aktuelne veze.
- Sastanci se smatraju poverljivim, ukoliko direktor odluči učesnici na sastanku ne smeju da imaju svoje smart telefone sa sobom, već treba da ih ostave izvan prostorije za sastanke.
- Izbegavajte čitanje i čuvanje poruka iz zvaničnih mailova na smart telefonima, osim u slučaju hitne potrebe i to samo za period koji je potreban. Ako je potrebno da sačuvate poverljive podatke, proverite da li je uključena enkripcija.
- Ne ostavljajte mobilni uređaj bez nadzora u nesigurnim područjima kao što je konferencijska sala. Kada ste van organizacije, a uređaj nije u upotrebi, sklonite ga van vidokruga. Ne ostavljajte uređaj u vašem automobilu u bilo kojem vremenskom periodu, posebno ne preko noći.
- Minimalna zaštita koju je potrebno obezbediti je PIN/Password.
- Ne dozvoljava se korišćenje posovnih mobilnih uređaja članovima porodice zaposlenog.
- Ne koristite mobilne uređaje tokom vožnje (u skladu sa domaćim propisima).
- Ne generišite prekomerne i nepotrebne troškove na neke od sledećih načina:
  - odabirom pogrešnog tarifnog broja
  - konfigurisanjem nepovoljnog načina povezivanja prilikom prenosa podataka
  - neadekvatnim izborom mreže prilikom putovanja u inostranstvo
  - lični troškovi korišćenja treba da se refundiraju u slučaju gde je to potrebno

- Ne koristite aparat za uvredljiv, neprikladan sadržaj ili preteranu ličnu upotrebu uključujući (ali ne ograničavajući se na): chatovanje, igre, pornografiju ili streaming filmova.
- Mobilni uređaji su izdati prema vašoj ulozi u organizaciji; morate da nosite aparat u toku radnog vremena i obezbedite da je uređaj napunjen i spreman za upotrebu. Uređaj treba da se čuva u dobrom radnom stanju.

Mobilne uređaje vratite nakon prestanka radnog odnosa. To je imovina organizacije Meridian Tech doo, a ne lična imovina. Ako ne vratite uređaj, pokrenuće se istražna procedura, a nakon toga i prekršajna procedura za povraćaj imovine. Uređaj će biti ponovo formatiran pre preraspodele drugom korisniku.

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 upotrebom uređaja i opreme izvan poslovnog prostora 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.