BYOD (Bring Your Own Device) POLITIKA

OZNAKA DOKUMENTA	*MT6POL02*	**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

SADRŽAJ 2

1. ZAPIS O DOPUNI 3

2. DISTRIBUCIJA I KONTROLA 4

2.1 DISTRIBUCIJA 4

2.2 KONTROLA 4

3. SVRHA 5

4. PODRUČJE PRIMENE 5

5. TERMINI I DEFINICIJE 5

6. REFERENTNA DOKUMENTA 5

7. OPIS RADA 5

7.1 POLITIKA 6

7.2 AKSIOMI POLITIKE (VODEĆI PRINCIPI) 6

7.3 DETALJNI ZAHTEVI POLITIKE 7

8. ODGOVORNOSTI I OVLAŠĆENJA 8

9. ZAPISI 9

10. PRILOZI 9

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

Zaposleni koji preferiraju korišćenje IT opreme u ličnom vlasništvu za potrebe posla, moraju biti eksplicitno ovlašćeni da to mogu činiti. Takođe, mora da se obezbedi bezbednost korporativnih podataka u istoj meri kao i korišćenjem korporativne IT opreme, tj. ne sme da se korišćenjem privatne opreme uvedu neprihvatljivi rizici (kao što je malware software) na korporativnu mrežu time što korisnici ne uspevaju da obezbede sopstvenu opremu.

4 PODRUČJE PRIMENE

Ova politika je deo okvira korporativnog upravljanja. To je posebno važno za zaposlene koji žele da koriste POD-ove (Personally Owned Device) za potrebe posla. Ova politika se odnosi i na treće strane koje deluju u sličnom svojstvu prema našim zaposlenima bez obzira da li su eksplicitno vezani (npr. ugovorne odredbe i uslovi) ili su već navikli (npr. generalno se drže etičkih standarda i prihvatljivog ponašanja) da se pridržavaju naših politika bezbednosti informacija..

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 bezbednošću informacija - ISO/IEC 27001:2022.

6 REFERENTNA DOKUMENTA

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

7 OPIS RADA

7.1 POLITIKA

Za razliku od informaciono-komunikacionih (IKT) uređaja u vlasništvu organizacije, uređaji u ličnom vlasništvu (POD) su IKT uređaji u vlasništvu zaposlenih lica ili trećih lica, kao što su dobavljači, konsultantske kuće ili izvođači na radovima održavanja. Ovlašćeni zaposleni i treća lica mogu izraziti želju da koriste svoje POD-ove za potrebe posla, na primer generisanja i primanja poslovnih telefonskih poziva i tekstualnih poruka na svojim ličnim mobilnim telefonima, koristeći svoje tablet računare za pristup, čitanje i odgovaranje na poslovne e-mailove ili rad od kuće (home-office). BYOD način rada je povezan sa brojnim rizicima po informacionu bezbednost, kao što su:

- Gubitak, obelodanjivanje ili korupcija korporativnih podataka na POD-ovima;

- Incidenti uključuju pretnje ili kompromitovanje korporativne IKT infrastrukture i drugih informacionih sredstava (npr. malware infekcijom ili hakovanjem);

- Neusaglašenost sa važećim zakonima, propisima i obavezama (npr. privatnost ili piraterija);

- Prava intelektualne svojine prekršena za korporativne informacije stvorene, skladištene, obrađene ili komunicirane na POD-ovima u toku rada za organizaciju.

Zbog zabrinutosti rukovodstva o rizicima po bezbednost informacija u vezi sa BYOD načinom rada, pojedinci koji žele da se opredele za BYOD moraju biti autorizovani od strane menadžmenta i moraju unapred eksplicitno prihvatiti uslove navedene u ovoj politici. Menadžment zadržava pravo da ne autorizuje pojedince ili da povuče ovlašćenje, ako smatra da BYOD nije prikladan i u najboljem interesu organizacije. Organizacija će nastaviti da pruža svoj izbor IKT uređaja koji su u potpunosti u vlasništvu i upravljani od strane kompanije, a neophodni su za potrebe rada, tako da nema prisile za bilo koga da se opredeljuje da koristi BYOD način rada, ako odluči da ne učestvuje u takvom sistemu korišćenja opreme.

7.2 AKSIOMI POLITIKE (VODEĆI PRINCIPI)

Organizacija i vlasnici i korisnici POD-ova dele odgovornosti za bezbednost informacija. Ništa u ovoj politici ne utiče na vlasništvo organizacije nad korporativnim informacijama, uključujući svu sa radom povezanu intelektualnu svojinu stvorenu u toku rada na POD-ovima.

7.3 DETALJNI ZAHTEVI POLITIKE

Korporativni podaci jedino mogu da se kreiraju, obrađuju, čuvaju i komuniciraju na ličnim uređajima koji se pokreću pomoću izabranog (od strane kompanije) klijentskog softvera za upravljanje mobilnim uređajima (Mobile Device Management - MDM). Uređaji koji ne koriste MDM (uključujući uređaje koji ne mogu da pokreću MDM, one na kojima su vlasnici odbili da dozvole da se instalira MDM sa pravima i privilegijama neophodnim da bi pravilno radili i onih na kojima je MDM onemogućen ili izbrisan posle instalacije) mogu da se povežu sa definisanom Internet mrežom za goste, ali im neće biti odobren pristup korporativnom LAN-u. Ovi uređaji ne smeju da se koriste za kreiranje, modifikovanje, čuvanje ili komuniciranje korporativnih podataka. Kontrolom i zaštitom podataka i konfiguracionim podešavanjima za sve mobilne uređaje u mreži, MDM može da smanji troškove podrške i poslovne rizike. Namera MDM-a je da se optimizuje funkcionalnost i sigurnost komunikacija mobilne mreže uz minimiziranje troškova i zastoja.

1. POD-ovi moraju da koristite odgovarajuće oblike autentikacije uređaja odobrenih u skladu sa informacionom bezbednošću, kao što su to digitalni sertifikati kreirani za svaki konkretan uređaj. Digitalni sertifikati ne smeju da se kopiraju ili prenose između POD-ova.
2. BYOD korisnici moraju da koriste odgovarajuće oblike autentikacije korisnika odobrenih u skladu sa informacionom bezbednošću, kao što su to user ID, lozinke i autentifikacioni uređaji (token).
3. Sledeće klase ili vrste korporativnih podataka nisu pogodne za BYOD i nije dozvoljeno na POD-ovima:
   - Sve klasifikovan POVERLJIVO ili iznad;
   - Druge korporativne informacije trenutno klasifikovane kao visoko vredne ili osetljive koje će verovatno biti klasifikovane kao interne ili iznad;
   - Velike količine korporativnih podataka (tj. veće od 4 GB združene na jednom POD-u ili storage uređaju).
4. Organizacija ima pravo da kontroliše svoje informacije. Ovo uključuje pravo na backup, povraćaj, modifikaciju, određivanje pristupa i/ili brisanja korporativnih podataka bez pozivanja na vlasnika ili korisnika POD-a.
5. Organizacija ima pravo da zapleni i forenzički ispita bilo koji POD, ukoliko veruje da sadrži, ili da je sadržao, korporativne podatke kada je to neophodno za istražne ili kontrolne svrhe.
6. Pogodan antivirusni softver mora biti pravilno instaliran i pokrenut na svim POD-ovima.
7. POD korisnici moraju da obezbede da se dragoceni korporativni podaci kreirani ili modifikovani na POD-ovima redovno bekupuju povezivanjem na mrežu preduzeća i vrši se sinhronizacija podataka između POD-a i mrežnog diska.
8. Bilo koji POD korišćen za pristup, smeštaj ili obradu osetljivih informacija mora enkriptovati podatke prenošene preko mreže (npr. korišćenjem SSL ili VPN), dok se čuvaju na POD-u ili na posebnom medijumu za skladištenje.
9. Pošto IT osoblje nema resurse ili stručnost da podrži sve moguće uređaje i softvere, POD-ovi koji se koriste za BYOD dobiće ograničenu podršku, ali samo za poslovne svrhe.

10. Iako zaposleni imaju razumna očekivanja o privatnosti nad svojim ličnim podacima na svojoj ličnoj opremi, pravo organizacije da kontroliše svoje podatke i upravlja POD-ovima može povremeno dovesti do toga da osoblje podrške nenamerno pristupi ličnim podacima zaposlenih. Da bi se smanjila mogućnost takvog otkrivanja ličnih podataka, POD korisnicima se savetuje da njihove lične podatke odvoje od poslovnih podataka na POD-u npr. u odvojenim direktorijumima, sa jasnim nazivom (npr. "Privatno" i "BYOD").
11. Nije dozvoljeno kršenje prava na privatnost drugih ljudi, na primer, korišćenje POD-ova za audio-video snimanje na poslu.

8 ODGOVORNOSTI I OVLAŠĆENJA

ISMS tim sa ISMS menadžerom je odgovoran za održavanje ove politike i savetovanje uopšte o kontrolama bezbednosti informacija. Tim je odgovoran za izdavanje digitalnih sertifikata za autentikaciju autorizovanih POD-ova, kao i za praćenje bezbednosti mreže pri neovlašćenom pristupu, neprikladnom mrežnom saobraćaju itd. U sprezi sa drugim korporativnim funkcijama, ISMS tim je takođe odgovoran za pokretanje edukativnih aktivnosti da se podigne svesnost i razumevanje obaveza identifikovanih u ovoj politici.

IT osoblje je odgovorno za upravljanje bezbednošću korporativnih podataka i konfigurisanje bezbednosti na autorizovanim POD-ovima koristeći MDM. Takođe je izričito odgovorno za obezbeđivanje bezbednosti MDM softvera i pratećih procedura, kako bi se smanjio rizik od hakerske eksploatacije MDM za pristup mobilnim uređajima.

IT osoblje je odgovorno za pružanje ograničene podrške za BYOD na POD-ovima, ali samo za pitanja u vezi sa poslom. Incidente informacione bezbednosti koji su zahvatili POD-ove korišćene za BYOD treba odmah prijaviti na uobičajen način.

Svi relevantni zaposleni su odgovorni za poštovanje ove i drugih korporativnih politika svo vreme.

Interni auditor je ovlašćen da proceni usklađenosti sa ovim i drugim korporativnim politikama u bilo kom trenutku.

9 ZAPISI

Sve informacije vezane za dokumentovani postupak Upravljanje upotrebom privatnih uređaja u poslovne svrhe 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.