POLITIKA KORISNIČKIH ŠIFRI

OZNAKA DOKUMENTA	*MT9POL03*	**DATUM IZDANJA**	*02-12-2023*
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	IT podrška
2	IT administrator

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

Šifre su važan deo bezbednosti informacija. One su prva linija zaštite cele infrastrukture organizacije Meridian Tech d.o.o. Beograd. Svi zaposleni u organizaciji (uključujući i saradnike i dobavljače usluga i ostale kooperante) su odgovorni da preduzmu neophodne mere, nabrojane u nastavku, pri izboru i zaštiti svojih korisničkih šifri.

Svrha ove Politike je da uspostavi standard pri kreiranju jakih šifri i zaštita istih.

Ova politika pokriva sledeću kontrolu:

- 5.17 Informacije o autentifikaciji

4 PODRUČJE PRIMENE

Ova Politika važi za sve zaposlene u organizaciji koji imaju ili su odgovorni za korisnički profil (ili bilo koji drugi oblik pristupa koji zahteva šifru) na bilo kom sistemu koji pripada organizaciji, ima pristup mrežnoj infrastrukturi ili čuva poverljive informacije organizacije.

Takođe, odnosi se na sve podizvođače, konsultante, privremeno zaposlene, dobavljače i ostale koje se u nastavku nazivaju kooperantima kompanije, koji imaju ili su odgovorni za korisnički profil (ili bilo koji drug oblik pristupa koji zahteva šifru) na bilo kom sistemu koji pripada organizaciji, ima pristup mrežnoj infrastrukturi ili čuva poverljive informacije 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 UPOTREBA KORISNIČKIH ŠIFRI

1. Sistemske šifre se menjaju prema potrebi
2. Preporuka je da se korisničke šifre ne menjaju, osim ako postoji indikacija da je došlo do kompromitovanja šifre, stogo je zabranjeno deliti svoju šifru. Nakon dobijanja početne šifre korisnik je u obavezi da postavi novu šifru. Za pristup e-mailu postoji dvostruka indetidikacija sifra i Microsoft Authenticator
3. Korisnički profili koji imaju pristup na sistemskom nivou dodeljeni kroz pripadnost određenoj grupi ili program imaju unikatnu šifru različitu od svih profila koji poseduje taj korisnik,
4. Ubacivanje šifre u email poruku ili u drugu formu elektronske komunikacije je zabranjeno, osim ako nije kriptovano,
5. Sve šifre na korisničkom i sistemskom nivou moraju da se usklade sa uputstvima u nastavku,

7.2 UPUTSTVA

7.2.1 Generisanje uputstva pri kreiranju šifre

Organizacija koristi šifre iz različitih razloga. Neki od njih su uobičajeni i odnose se na korisničke šifre, web profile, email profile ili zaštitu ekrana.

Zaposleni u organizaciji ili kooperanti moraju biti svesni koji je pravi način pri kreiranju jakih šifri, a samim tim moraju da koriste sledeća uputstva:

- Šifra ne sme da sadrži deo ili celo korisničko ime. Deo korisničkog imena je definisan kao tri ili više povezanih alfanumeričkih znakova ograničenih sa strane praznim mestom ili bilo kojim od sledećih znakova: comma (,), period (.), hyphen (-), underscore (_), ili number sign (#).
- Šifra mora biti dužine od najmanje 8 znakova
- Šifra mora da sadrži znakove iz bar tri od sledeće četiri kategorije:
  - Latinična velika slova (A do Z)
  - Latinična mala slova (a do z)
  - Osnovnih 10 cifri (0 do 9)
  - Nealfanumeričke znakove kao što su : uzvičnik (!), dolar ($), taraba (#), ili procenat (%).
- Šifra ne treba da sadrži reč u bilo kom jeziku, slengu, dijalektu, žargonu itd.
- Šifra ne treba da bude bazirana na ličnoj informaciji, imenima članova porodice itd.
- Šifra ne treba da bude zapisana ili čuvana online

Loše, slabe šifre imaju sledeće karakteristike :

- Sastoje se od manje od 8 znakova
- Sastoje se od reči koja se nalazi u rečniku
- Sastoje se od često upotrebljavane reči, na primer:
  - Imena članova porodice, ljubimaca, prijatelja, saradnika, omiljenih likova itd.
  - Kompjuterskih pojmova i imena, komandi, sajtova, kompanija, hardver, softver.
  - Reči : Organizacija i geografski pojmovi kao što su “sanjose,” “sanfran” i slično.
  - Rođendani ili druge lične informacije kao što su adresa i telefonski broj
  - Reč ili niza znakova kao što su aaabbb, qwerty, zyxwvuts, 123321, itd.
- Bilo koja od gore navedenih kombinacija zapisani po obrnutom redosledu
- Bilo koja od gore navedenih sa predznakom ili praćena bilo kojim brojem

Šifre moraju biti kreirane tako da se lako pamte. Jedan od načina da se ovo uradi je da se kreira šifra bazirana na naslovu omiljene pesme, afirmacije ili druga fraze. Na primer, fraza može biti , “This May Be One Way To Remember” a šifra bi bila : “TmB1w2R!” ili “Tmb1W>r~” ili bilo koja druga varijacija.

Napomena: Nemojte da koristite bilo koji od navedenih primera za šifre!

7.2.2 Standardi za zaštitu šifre

1. Šifre za korisničke profile u organizaciji ne koriste se za drugi neposlovni pristup (lični ISP profil, lični email itd). Uvek kada je to moguće, ne treba se koristiti ista šifra za pristup različitim delovima sistema.
2. Poslovne šifre ne smeju se nikome govoriti. Sve šifre su osetljive, poverljive poslovne informacije.
3. Ovo je lista stvari koje se ne smeju raditi:
   - Nemojte otkrivati šifru nikome putem telefona
   - Nemojte okrivati šifru u email poruci
   - Nemojte pričati o šifri u prisustvu ostalih
   - Nemojte otkrivati koja bi mogla da bude vaša šifra (moje prezime i slično).
   - Nemojte otkrivati šifru odgovaranjem na razne upitnike ili ankete
   - Nemojte otkrivati šifru članovima porodice
   - Nemojte da otkrivate šifru kolegama kad idete na odmor
   - Nemojte da zapisujete šifru i da je čuvate u kancelariji
   - Nemojte da čuvate šifre u fajlu na kompjuteru bez enkripcije
   - Nemojte da koristite opciju “Remember Password” u aplikacijama kao što su Eudora, Outlook, ili Netscape Messenger

Definisane informacije o autentifikaciji koje su unapred definisane ili obezbeđene od strane dobavljača se menjaju odmah nakon instalacije sistema ili softvera

Ako neko zahteva šifru, on će biti upućen ovom dokumentu ili IT podršci / System administratoru.

Ako neko od zaposlenih ili kooperatora sumnja da je njegov korisnički profil ili šifra narušen, treba da prijavi sigurnosni incident nadređenom mendžeru, a on Dispečer službu ili system admonistratora kako bi on preduzeo adekvatne mere i odmah promeniti šifru. Organizacija ili neko od ovlašćenih, s vremena na vreme može da proba probijanje ili nagađanje šifri, i ako je šifra probijena ili pogođena prilikom ovogo testa, korisnik je primoran da promeni šifru.

U situaciji kada korisnik zaboravi svoju šifru, treba se obratiti nadređenom. Nadređeni potom šalje zahtev Dispečerskoj službi putem mejla za izdavanje nove šifre. U slučaju da korisnik više puta unese pogrešnu šifru, nalog mu se automatski blokira. Nadređeni ponovo podnosi zahtev putem mejla Dispečerima za dobijanje nove šifre.

7.3 STANDARDI PRI RAZVOJU APLIKACIJA

Projektanti softvera i developer-i moraju osigurati da njihovi programi sadrže sledeće bezbednosne mere:

1. Kada je to primenjljivo, aplikacije će podržavati autentifikaciju pojedinačnih korisnika, ne grupa.
2. Aplikacije neće pokazivati šifre u čistoj formi, već će biti maskirane.
3. Aplikacije će omogućiti neku formu upravljanja pravima pristupa (autorizacija), tako da ako neko preuzme funkcije drugog radnika neće biti potrebno da zna njegove šifre.

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 korisničkim šiframa 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.