KRIPTOGRAFSKA POLITIKA

OZNAKA DOKUMENTA	*MT10POL01*	**DATUM IZDANJA**	*09-12-2023*
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	Rukovodici IT 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

Sa ciljem zaštite poverljivosti, autentičnosti i integriteta informacija, usvaja se Kriptografska politika za potrebe organizacije Meridian Tech d.o.o. Beograd.

Ova Politika pokriva sledeću kontrolu:

- 8. 24 Upotreba kriptografije

4 PODRUČJE PRIMENE

Ova politika se primenjuje na sve poslovne procese organizacije koje zahtevaju kriptozaštitu prema sledećim principima:

- upotreba kriptografskih kontrola širom organizacije treba da bude potpuno kontrolisana, uključujući opšte principe pod kojima poslovne informacije treba da budu zaštićene;
- na osnovu procene rizika, potreban nivo zaštite treba da bude identifikovan uzimajući u obzir vrstu, snagu i kvalitet algoritma za šifrovanje;
- treba definisati upotrebu enkripcije za zaštitu informacija koje se transportuju mobilnim uređajima, prenosivim medijima ili preko komunikacionih linija;
- opredeliti pristup upravljanju ključevima, uključujući metode koje se bave zaštitom kriptografskih ključeva i oporavak šifrovanih informacija u slučaju gubljenja, kompromitovanja ili oštećenja ključeva;
- odrediti uloge i odgovornosti, tj. ko je odgovoran za :
  1) sprovođenje politike;
  2) upravljanje ključevima, uključujući i generisanje ključeva;
- primeniti standarde koji moraju biti usvojeni za efikasno sprovođenje u celoj organizaciji (koje se rešenje koristi za koje poslovne procese).

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 PRIMENA KRIPTOGRAFSKIH KONTROLA

7.1 PRIMENA KRIPTOGRAFSKIH KONTROLA

Ukoliko sprovedena analiza rizika ukazuje da je neophodno primeniti kriptografiju u cilju tretmana rizika s obzirom na visok nivo rizika i uticaj na poslovanje organizacije Meridian Tech d.o.o. Beograd, organizacija će implementirati kriptografske kontrole za zaštitu informacija i pri tom će uzeti u obzir sledeće:
Prilikom primene kriptografske politike organizacije, treba uzeti u obzir propise i nacionalna ograničenja koja se mogu primeniti na upotrebu kriptografskih tehnika (kao i pitanja prekograničnog protoka šifrovanih informacija).

Primena kriptografskih kontrola može da se koriste za postizanje sledećih ciljeva informacione bezbednosti:

a) poverljivosti: koristeći šifrovanje informacija da se zaštite osetljive ili kritične informacije, da se čuvaju ili da se prenose;

b) integriteta/autentičnosti: koristeći digitalne potpise ili autentifikaciju putem kodova prosleđenih sms porukama (vremenski token itd.) da bi se proverila autentičnost (provera identiteta pošiljaoca) ili integritet (sprečavanje neovlašćene izmene) čuvanih ili prenošenih osetljivih ili kritičnih informacija;

c) neporecivosti: koristeći kriptografske tehnike da se obezbedi dokaz koji sprečava entitet da poriče predašnje obaveze ili akcije (npr. ugovor preko Interneta);

Donošenje odluke o tome da li je kriptografsko rešenje primereno treba posmatrati kao deo šireg procesa procene rizika i izbora kontrola. Ova procena se zatim može koristiti za određivanje da li je kriptografska kontrola prikladna, koja vrsta kontrole treba da se primeni i za koju svrhu i poslovne procese. Pri izboru odgovarajuće kriptografske kontrole od kripto-specijalliste treba zatražiti savet kako bi se na najbolji način dostigli ciljevi politike bezbednosti informacija.

7.1.1 Upravljanje ključevima

Politika treba da obuhvati zahteve za upravljanje kriptografskim ključevima tokom celog njihovog životnog ciklusa, uključujući generisanje, čuvanje, arhiviranje, preuzimanje, distribuciju, povlačenje i uništavanje ključeva.
Kriptografski algoritmi, dužine ključa i prakse korišćenja treba da budu izabrani u skladu sa najboljom praksom. Svi kriptografski ključevi treba da budu zaštićeni od izmena i gubitka. Pored toga, za tajne i privatne ključeve potrebna je zaštita od neovlašćenog korišćenja. Oprema koja se koristi za generisanje, skladištenje i arhiviranje ključeva treba da bude fizički zaštićena.

Sistem upravljanja ključevima treba da se zasniva na dogovorenom skupu standarda, procedura i bezbednih metoda za:

- generisanje ključeva za različite kriptografske sisteme i različite aplikacije;
- izdavanje i pribavljanje sertifikata javnog ključa;
- distribuciju ključeva namenjenih licima, uključujući kako ključevi treba da se aktiviraju kada budu primljeni;
- čuvanje ključeva, uključujući kako ovlašćenim korisnicima omogućiti pristup ključevima;
- promene ili ažuriranje ključeva, uključujući pravila o tome kada ključevi treba da se menjaju i kako će to biti urađeno;
- postupanje sa kompromitovanim ključevima;
- oduzimanje ključeva uključujući kako treba da se povuku ili deaktiviraju ključevi, na primer kada su ključevi ugroženi ili kada korisnik napusti organizaciju (u tom slučaju ključevi takođe treba da budu arhivirani);
- oporavak ključeva koji su izgubljeni ili oštećeni;
- pravljenje rezervnih kopija ili arhiviranje ključeva;
- uništavanje ključeva;
- logovanje i reviziju aktivnosti u vezi sa upravljanjem ključevima.

Da bi se smanjila verovatnoća nepravilnog korišćenja, datume aktivacije i deaktivacije za ključeve treba definisati tako da mogu da se koriste samo za vremenski period definisan u odgovarajućoj politici upravljanja ključevima. Pored bezbednog upravljanja tajnim i privatnim ključevima, verodostojnost javnih ključeva takođe treba uzeti u obzir. Ovaj proces potvrde verodostojnosti može da se uradi koristeći sertifikate javnih ključeva, koji se obično izdaju od strane sertifikacionog tela, koje bi trebalo da bude priznata organizacija sa odgovarajućim uspostavljenim kontrolama i procedurama da se obezbedi potreban stepen poverenja.

Sadržaj sporazuma o nivou usluga (SLA - Service Level Agreement) ili ugovora sa spoljnim dobavljačima kriptografskih usluga, npr. od samog sertifikacionog tela, treba da pokrije pitanja odgovornosti, pouzdanosti usluga i vremena odziva za pružanje tih usluga.

7.1.2 Uloge i odgovornosti

Dodeljene su uloge i odgovornosti za:

1) sprovođenje pravila za efikasno korišćenje kriptografije:

Uloga: Sistem administartor

2) upravljanje ključevima, uključujući generisanje ključeva

Uloga: Sistem administartor

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 kriptografskim kotrolama i kriptografskim ključevima 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.