UPRAVLJANJE PODACIMA I INFORMACIJAMA

OZNAKA DOKUMENTA	*MT20POL01*	**DATUM IZDANJA**	*22-12-2023*
PRIMERAK BROJ	*01*	**IZDANJE**	*01*

AUTORIZACIJA	**IME I PREZIME**	**FUNKCIJA**	**POTPIS**
PRIPREMIO	Vladimir Miladinović	Menadžer ISMS-a	
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 6

7.1 Sprečavanje curenja podataka 6

7.2 Brisanje informacija 7

7.2.1 Metode brisanja 7

7.3 Maskiranje podataka 8

8 ODGOVORNOSTI I OVLAŠĆENJA 9

9 ZAPISI 9

10 PRILOZI 10

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/odeljenje
1	Sistem administrator
2	Menadžer za ISMS
3	IT služba

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 upravljanja informcijama i podacima, kao i procesom brisanja i maskiranja podataka je da doprinese otkrivanju i sprečavanju neovlašćenog raspolaganja informacijama od strane pojedinaca ili sistema, spreči nepotrebno izlaganje osetljivih informacija, uključujući i podatke o ličnosti, i da se pridržava zakonskih, statutarnih, regulatornih i ugovornih zahteva za poverljivost i brisanje informacija.

4 PODRUČJE PRIMENE

Ova politika se primenjuje na svepodatke i informacije u IT sistemu, i na drugi način skladištene, kojima upravlja organizacija. Primenjuje na sve zaposlene u organizaciji.

ISMS menadžer će biti odgovoran za sprovođenje bezbednosti u skladu sa zahtevima ove politike.

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 Sistems), Sistem menadžmenta bezbednošću informacija - ISO/IEC 27001:2022.

6 REFERENTNA DOKUMENTA

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

7 OPIS RADA

7.1 Sprečavanje curenja podataka

Alati za sprečavanje curenja podataka dizajnirani su za identifikaciju podataka, praćenje korišćenje i kretanja podataka i preduzimanje radnji za sprečavanje curenja podataka (npr. upozoravanje korisnika na njihovo rizično ponašanje i blokiranje prenosa podataka na mobilne uređaje za skladištenje).

Sprečavanje curenja podataka inherentno uključuje praćenje komunikacije osoblja i aktivnosti na mreži, a time i poruka eksternih strana, što moze da izazove pravnu zabrinutost, koju treba razmotriti pre primene alata za sprečavanje curenja podataka. U tom smislu moraju se konsultovati svi zakoni koji se odnose na privatnost, zaštitu podataka, zapošljavanje, presretanje podataka i telekomunikacije koji su primenjivi na praćenje i obradu podataka u kontekstu sprečavanja curenja podataka.

Organizacija mora razmotriti sledeće kako bi smanjila rizik od curenja podataka:

- identifikaciju i klasifikaciju informacija
- praćenje mogućih kanala curenja podataka (npr. e-pošta, prenos dokumenata, mobilni uređaji i prenosni uređaji za skladištenje);
- aktivnosti kako bi se sprečilo curenje informacija.

Alati za sprečavanje curenja podataka trebali bi se koristiti za:

- identifikovanje i nadzor osjetljivih informacija koje su pod rizikom od neovlašćenog otkrivanja;
- otkrivanje zloupotrebe osjetljivih informacija;
- blokiranje aktivnosti korisnika ili mrežnog prenosa koji otkrivaju osetljive informacije.

Organizacija mora odrediti nivo dozvoljenih radnji prilikom obrade podataka, na primer da li ima dozvolu da kopira ili otpremi podatke, putem mreže ili na uređaje i medije za skladištenje izvan organizacije. Ako zaposleni imaju ograničenja u procesu obrade podataka, organizacija mora implementirati tehnologiju kao što su alati za sprečavanje curenja podataka ili konfigurisati postojeće alate koji omogućavaju korisnicima da imaju uvid i da vrše određene aktivnosti nad podacima (na primer unos podataka), a posebno ako ih vrše sa udaljenih lokacija, ali sprečavaju kopiranje i skladištenje izvan kontrole organizacije.

Svaki izvoz podataka mora biti odobren od strane vlasnika podataka a korisnike će se smatrati odgovornim za svoje postupke u odnosu na podatke.

Svako nedozvoljeno snimanje ili fotografisanje ekrana je strogo zabranjeno.

Rezervne kopije moraju biti zaštićene kao i orginalni podaci (na primer kontrola pristupa i fizička zaštita medija za skladištenje na kojima se čuva rezervna kopija).

Sprečavanje curenja podataka takođe treba uzeti u obzir prilikom zaštite od nezdrave konkurencije i zlonamernih lica. Zaštititi podatke koji mogu biti interes za špijunažu ili mogu su kritične za društvo u celini. Radnje za sprečavanje curenja podataka mogu podrazumevati obrnuti društveni inženjering ili korišćenje tehnika koje podrazumevaju privlačenje napadača i preusmeravanje na drugu stranu.

7.2 Brisanje informacija

Osetljive informacije neće se čuvati duže nego što je potrebno za smanjenje rizika od neželjenog otkrivanja, dužina čuvanja informacija ili kriterijumi za donošenje odluke o vremenskom okviru biće definisani kroz dokumenta za upravljanje dokumentovanim informacijama.

Prilikom brisanja informacija o sistemima, aplikacijama i uslugama treba uzeti u obzir sledeće:

- odabir metode brisanja u skladu sa zahtevima poslovanja i uzimajući u obzir relevantne zakone i propise;
- evidentiranje rezultata brisanja kao dokaza;
- kada koristite pružaoce usluga za brisanja informacija, pribavljanje dokaza o brisanju informacija od njih.

Kada treće strane skladište informacije organizacije u njeno ime, organizacija treba da uključi zahteve za brisanje informacija u ugovore sa trećim stranama kako bi ih sprovela tokom i nakon prestanka pružanja takvih usluga.

7.2.1 Metode brisanja

U skladu sa poslovnim zahtevima i uzimajući u obzir relevantno zakonodavstvo i propise, organizacija će izbrisati osetljive informacije kada više ne budu potrebne:

- konfigurirati sistem za sigurno uništavanje informacija kada više nisu potrebne;
- brisanje zastarelih verzija, kopija i privremenih datoteka na svim lokacijama;
- korišćenje odobrenog, sigurnog softvera za brisanje za trajno brisanje informacija kako bi se osiguralo da se informacije ne mogu oporaviti pomoću specijalnih alata za oporavak ili forenzičkih alata;
- korišćenje odobrenih, sertifikovanih pružalaca usluga bezbednog odlaganja;
- korišćenje mehanizama za odlaganje koji odgovaraju vrsti medija za skladištenje koji se odlaže.

Kako bi se izbeglo nenamerno izlaganje osetljivih informacija kada se oprema isporučuje dobavljačima, osetljive informacije će biti zaštićene uklanjanjem pomoćne memorije (npr. hard diskova) i memorije pre nego što oprema napusti prostorije organizacije.

S obzirom na to da se sigurno brisanje pametnih telefona može postići samo uništavanjem ili korišćenjem funkcija ugrađenih u te uređaje (npr. "vraćanje fabričkih postavki"), koje u većini slučajeva uključuju trajno uklanjanje svih informacija na uređaju, organizacija će razmotriti koji metod će primeniti prema riziku.

U slučaju brisanja većeg broja važnih informacija, biće generisan službeni zapisnik o brisanju informacija.

7.3 Maskiranje podataka

Kada je zaštita osetljivih podataka, posebno podataka o ličnosti, važna, organizacija će razmotriti skrivanje takvih podataka korišćenjem tehnika kao što su maskiranje podataka, pseudonimizacija ili anonimizacija.

Tehnike pseudonimizacije koristit će se za podatke o ličnosti kada je važno sačuvati identifikatore, ali je potrebno ograničiti njihov pristup određenoj grupi osoba.

Anonimizacija će se koristiti za trajno uklanjanje identifikatora podataka o ličnosti, u slučaju korišćenja podataka u statističke ili analitičke svrhe gde identifikatori više nisu potrebni.

Mogu se koristit i dodatne tehnike maskiranja:

- enkripcija;
- poništavanje ili brisanje karaktera pojedinačnih znakova;
- različite brojeve i datume;
- zamena;
- zamena vrednosti sa njihovim hash-om.

Pri odabiru tehnika maskiranja podataka, organizacija će uzeti u obzir sledeće:

- ne odobravanje pristupa korisnicima svim podacima, stoga dizajniranje maskiranja kako bi korisniku prikazali samo minimalne potrebne podatke;
- h) slučajevi kada neki podaci ne bi trebali biti vidljivi korisniku za neke zapise iz skupa podataka;
- kada su podaci prikriveni, a postoji razumna osnova za mogućnost da korisnici ne mogu videti da li su podaci prikriveni;
- j) sve zakonske ili regulatorne zahteve.

Prilikom korišćenja maskiranja podataka, pseudonimizacije ili anonimizacije, u obzir će se uzeti sljedeće:

- stepen jačine maskiranja, pseudonimizacije ili anonimizacije podataka prema upotrebi obrađenih podataka;
- kontrola pristupa obrađenim podacima;
- sporazumi ili ograničenja u korišćenju obrađenih podataka;
- zabrana poređenja obrađenih podataka sa drugim informacijama u cilju identifikacije lica na koje se podaci odnose (PII);
- praćenje davanja i prijema obrađenih podataka.

8 ODGOVORNOSTI I OVLAŠĆENJA

Svaki sektor je odgovoran za upravljanje podacima kojima raspolaže. Vlasnici podataka su dužni da upravljaju brisanjem i maskiranjem podataka čiji su vlasnici. Druga lica u organizaciji ne smeju da brišu podatke bez odobrenja vlasnika imovine ili drugog ovlašćenog relevantnog lica. Sa tehnikama brisanja i maskiranja mora biti upoznat ISMS menadžer.
Svaki pokušaj osoblja da zaobiđe ili na drugi način povredi ovu politiku ili bilo koju prateću politiku tretiraće se kao kršenje bezbednosti i podleže istrazi. Rezultati istrage mogu povlačiti pismenu opomenu, suspenziju, prekid, a moguće i krivične i/ili građanske kazne.

9 ZAPISI

Sve informacije vezane za dokumentovani postupak upravljanje odnosima sa dobavljačima 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.