KLASIFIKACIJA INFORMACIJA

OZNAKA DOKUMENTA	*MT8PRO01*	**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
3	

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 ovog dokumenta je da definiše i opiše pravila za klasifikaciju informacija, u kojim će različite vrste informacija biti zaštićene na različite načine. Informacije treba da se klasifikuju sa odgovarajućom klasifikacijom koja određuje potrebu, prioritete i očekivani stepen zaštite u radu sa informacijama. Informacije su različitog stepena osetljivosti i kritičnosti. Da bi se odredio odgovarajući nivo zaštite i posebne mere za bezbednost, treba koristiti šeme za klasifikaciju informacija opisane u ovom dokumentu.

Sva pitanja u vezi ovog dokumenta trebaju se uputiti Menadžeru ISMS-a.
Ova procedura pokriva sledeću kontrole:

- 5.12 Klasifikacija informacija,
- 5.13 Oznacavanje informacija

4 PODRUČJE PRIMENE

Ova Politika se odnosi na sve vrste informacija, neovisno na kom medijumu i u kojem obliku se čuvaju. Takođe, namenjena je svim zaposlenim licima i kooperantima koji imaju pristup informacionom sistemu, i drugom obliku arhiviranja podataka.

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 KLASIFIKACIJA INFORMACIJA

Sistem klasifikacije Meridian Tech d.o.o. Beograd klasifikuje informacije u tri nivoa. Najniži nivo 1 je najmanje osetljiva informacija a najviši nivo 3 je najosetljivija informacija.

7.1.1 Koncepti

- Svi podaci (informacije) moraju imati vlasnika.
- Vlasnik je zadužen za klasifikaciju svojih podataka (informacija).
- Svaki podatak (informacija) mora biti klasifikovan u jednom od nivoa (od 1 do 3), u zavisnosti od zakonskih obaveza, procedura i politika Meridian Tech d.o.o. Beograd, troškova održavanja i poslovnih potreba.
- Ako vlasnik nije siguran u kom nivou treba klasifikovati informaciju, treba da se koristi nivo 3.
- Vlasnik mora da definiše kome je dozvoljen pristup informacijama za koje je on odgovoran.
- Vlasnik mora redovno da prati klasifikaciju informacije u slučaju da informacije promene nivo klasifikacije u toku vremena, promene pravila (interna i/ili eksterna), u slučaju promene načina obrade ili bilo koje druge promene u radu sa informacijama.
- Vlasnik je odgovoran za svoje podatke i mora da obezbedi ili traži da budu obezbeđene sve fizičke, tehničke i / ili administrativne mere zaštite.
- Sve informacije moraju biti klasifikovane i nivo klasifikacije treba biti zapisan barem na naslovnoj strani, bez obzira na vrstu medijuma na kome se nalaze informacije.

Kada informacija dobije svoju klasifikaciju, ona mora da podržava sva pravila te klase, i svih podređenih. Svaki nadređeni nivo sadrži zahteve podređenih nivoa. Na primer, ako se informacija svrstava u klasu 3, onda mora da prati direktive klase 1, 2 i 3 podsistema. Ako sistem sadrži podatke iz različitih klasa, mora biti klasifikovan u skladu sa potrebama najviše klase, ili biti podeljen na dva tipa (dve klase).

7.1.2 Javne informacije (PODACI) (NIVO 1)

Informacije iz ovih sistema mogu postati javne bez ikakvih implikacija za Meridian Tech d.o.o. Beograd (tj. podaci nisu poverljivi i dostupni su celokupnoj javnosti). Integritet podataka je od vitalnog značaja. Nemogućnost davanja usluga zbog napada na ove podatke je prihvatljiv rizik.

Primeri: Javno objavljene informacije koje je objavio Meridian Tech d.o.o. Beograd i brošure dostupne široj javnosti, web serveri na Internetu, javni cenovnici itd.

7.1.3 Interne informacije (NIVO 2)

Eksterni (spoljašnji) pristup ovim podacima treba potpuno zabraniti, ali ako se desi da se ovi podaci javno predstave, posledice nisu kritične (npr. Meridian Tech d.o.o. Beograd se može javno kompromitovati, ali ne može pretrpeti velike štete). Integritet i dostupnost podataka je važna, ali ne i kritična. Interni pristup podacima nije selektivan, dostupni su za celu kompaniju.

Primeri za ovu vrstu podataka mogu se naći u dokumentaciji, politikama, uputstvima, opštim poslovnim dokumentima, procedurama, telefonskim imenicima Meridian Tech d.o.o. Beograd i slično.

7.1.4 Poverljive informacije (NIVO 3)

Podaci iz ove klase imaju najveću vrednost i kritičnost u okviru Meridian Tech d.o.o. Beograd i zaštićeni su od spoljnjeg i unutrašnjeg pristupa. Pristup je ograničen samo na određene grupe zaposlenih naznačenih od vlasnika informacije. Ako neovlašćena lica imaju pristup ovim informacijama, to može da utiče na rad Meridian Tech d.o.o. Beograd i može izazvati finansijski gubitak, obezbediti značajnu korist konkurenciji ili može da izazove pad poverenja od strane kupaca. Integritet, poverljivost i dostupnost podataka je od vitalnog značaja.

Primeri: Određene baze podataka, plate, lični podaci o zaposlenima, računovodstvene evidencije, zapisnici sa raznih sastanaka i odbora, mnogo poverljivih podataka klijenata i poverljivih sporazuma.

7.2 DOSTUPNOST INFORMACIJA PREMA KLASI

Dostupnost informacija prema klasifikaciji je definisana da kontroliše i obezbedi dostupnost tim informacijama. Preventivne mere će smanjiti mogućnost pada sistema i plan za kontinuitet poslovanja, smanjiti vreme nedostupnosti nakon bilo kakvog incidenta.

Klasa	**1**	**2**	**3**
Maksimalna dozvoljena vremena nedostupnosti informacija	1 sedmica	2 dana	1 dan
Dostupnost u danima	ponedeljak - nedelja	pon-pet	pon- sub
Dostupnost u časovima	24 sata	8:00 do 16:00	8:00 do 16:00
Očekivana raspoloživost u procentima	80%	90%	95%

7.3 POTREBE ZA SVAKU KLASU

7.3.1 Javni podaci (NIVO 1)

Čak i oni podaci koji nisu osetljivi na svim sistemima Meridian Tech d.o.o. Beograd moraju imati minimalni nivo bezbednosti (pogotovo ako se sa njima radi u mreži). Ako se ova zaštita ne ispuni, Nivo 1 može da se koristiti kao polazna tačka za napad na neke od internih ili poverljivih sistema Nivoa 2 i/ili 3.

Potrebe za Nivo 1 se zasnivaju na procedurama koje slede, ali i na "zdravom razumu":

- Potrebno je instalirati antivirusni program
- Ovi podaci treba da budu dostupni samo ovlašćenom osoblju za njihovu obradu i uvek moraju da imaju lozinku.
- Treba da se primeni automatsko zaključavanje ekrana sa lozinkom za zaštitu posle 15 minuta

- Treba da se ograniči pristup za upisivanje i uređivanje ovih podataka (samo pojedini korisnici su odgovorni za održavanje i samo oni imaju privilegiju da uređuju, a drugi samo da čitaju).

7.3.2 Interni podaci (NIVO 2)

Podaci iz nivoa 2 imaju dodatne potrebe zaštite:

- Potrebna je identifikacija, autentifikacija i autorizacija korisnika podataka
- Ovlašćenja za kontrolu pristupa i privilegije (ko može da uređuje/edituje, zapisuje, briše, čita): kontrolu pristupa definiše vlasnik između nominovanih korisnika (ili korisničkih grupa i predloženih objekata)
- Obuhvataju sve potrebe iz Nivoa 1
- Pomoćna sredstva koja sadrže informacije ne smeju se prenositi bez odobrenja relevantnog lica, prenos vrši ovlašćeno lice ili isključivo preko proverenih organizacija za transport robe.
- Pomoćna sredstva moraju biti uskladištena na nacin koji sprecava slucajno ili namerno uništenje ili na način koji može skratiti vek trajanja imovine.
- Pomoćnu imovinu zaposleni moraju vratiti po prestanku radnog odnosa ili ako više nema potrebe da ih koriste u vezi sa radnim zadacima.
- Pomoćna imovina mora biti uništena na takav način da nije moguće povratiti informacije koje su bile na uređaju. Prethodno se sve informacije i ostala prateća oprema koja se nalazi na uređaju mora se bezbedno preneti na odgovarajuću lokaciju.

7.3.3 Poverljivi podaci (NIVO 3)

Podaci iz nivoa 3 su najviši nivo klasifikacije i imaju sledeće potrebe zaštite:

- Zaštita i kontrola pristupa
- Identifikacija, autentifikacija i autorizacija mora biti na nivou korisnika, a ne na nivou grupe. Kontrola pristupa i privilegija mora biti na nivou korisnika
- Mora se redovno testirati bezbednost
- Odgovornost za korisnika: svaki korisnik je odgovoran za svoje postupke. Treba se obezbediti logovanje, praćenje i izveštavanje o bilo kakvim nelegalnim aktivnostima. Audit ruta (Audit trails) moraju biti zaštićeni.
- Ponovna upotreba sredstva: sredstva koja se koriste od strane zaposlenih moraju se reinicijalizirati pre upotrebe od strane drugog lica. Ne sme se dozvoliti kompromitovanje bezbednosti pri ponovnoj upotrebi.

- Prenos podataka: kada programi komuniciraju jedni sa drugima i razmenjuju informacije iz ove klase, moraju imati kontrolu za poverljivost i integritet.
- Za određene aplikacije može biti neophodno da se napravi kontrola da informacija dolazi od pošiljaoca, a ne od nekog drugog. To se zove nemogućnost poricanja ("non-repudation") pošiljaoca. Isto važi i za nemogućnost poricanja primaoca, da postoji kontrola da je informacija stigla do korektnog primaoca.
- Podaci sačuvani na papiru ili drugim medijumima moraju biti bezbedno čuvani, zaključani i sa kontrolom pristupa samo za ovlašćene zaposlene.
- Obuhvataju sve potrebe Nivoa 1 i Nivoa 2.
- Pomoćna sredstva na kojima se nalaze informacije tokom prenosa moraju biti šifrovana i obezbeđena u jakim i za to namenjenim torabama ili pakovanju koje je dizajnirano da zaštiti pomoćno sredstvo od mogućeg oštećenja.
- Pomoćna sredstva koja se čuvaju moraju biti šifrovana i zaključana u sefovima ili drugim određenim oblastima gde je pristup strogo kontrolisan i gde su onemogućena neovlašćena lica.
- Pomoćna sredstva moraju biti fizički uništena čvrstim predmetom (na primer čekićem) ili visokom temperaturom na takav način da nije moguće povratiti informacije koje su bile na uređaju. Odlaganje na ovaj način uništenih uređaja može se vršiti samo u saradnji sa ovlašćenim specijalizovanim verifikovanim organizacijama za otkup elektronskog otpada sa kojima organizacija ima formalno pravni ugovor.

7.4 UPOTREBA, OBRADA I OZNAČAVANJE INFORMACIJA

Upotreba, obrada i označavanje informacija vrši se u skladu sa klasifikacionom šemom (oznaka1-3) i potrebama za svaku klasu.

Označavanje informacija mora biti prema utvrđenim pravilima. Sve informacije moraju imati oznaku za klasifikaciju, osim javnih informacija.

Mora se implementirati sistem za označavanje automatski generisanih podataka. Tu se klasifikacija mora definisati još u fazi programiranja.

Podaci u elektronskom formatu, razvijeni u bilo kojem korisničkom alatu (koji se ne generišu direktno iz sistema) moraju imati elektronske oznake za klasifikaciju u svakom dokumentu.

Za sve ostale informacije (izlazne-ulazne) na papiru ili drugim medijima, koriste se dopunska sredstva za označavanje klasifikacije (pečati, potpisi, stikeri, itd).

Kada određeni podaci (informacije) više nisu potrebni i moraju biti uništeni, to mora biti urađeno u skladu sa nacionalnim zakonom i važećim pravilima i propisima nadležnih organa.

Ako se trebaju uništiti informacije u elektronskom obliku na pojedinim medijumima, oni treba da budu uništeni pravilno u zavisnosti od medijuma i internih politika i procedura.

Ukoliko medijumi nisu za dalju upotrebu treba da budu uništeni fizički sa nemogućnošću za svako dalje korišćenje. Ako su medijumi za ponovnu upotrebu (HDD diskovi, USB…) treba primeniti savremene tehničke procedure mnogostrukog brisanja i dva puta provere, koji će potvrditi odsustvo bilo kakvog zapisa na medijumu.

Ako je informacija zapisana na papiru, mora biti uništena pomoću odgovarajućeg uređaja za uništavanje papira. To važi za sve klase (1 -3).

7.4.1 Način označavanja

Sve informacije koje se nalaze u informacionom sistemu Meridian Tech d.o.o. Beograd moraju biti jasno obeležene stepenom klasifikacije. Ovaj znak bi trebalo da bude lako vidljiv i da jasno i nedvosmisleno pokazuje nivo klasifikacije informacija. Javne informacije nemaju posebnu oznaku za klasifikaciju.

Za informacije generisane u organizaciji sa standardnim editorima teksta koje se koriste u elektronskoj i/ili papirnoj verziji, nivo klasifikacije je naveden u zaglavlju/headeru dokumenta u sekciji "klasifikacija".

Informacije generisane u okviru organizacije bez korišćenja standardnog šablona i koriste se u elektronskoj i / ili papirnoj formi, nivo klasifikacije je naveden na prvoj strani dokumenta.

Informacije generisane u organizaciji, a koje postoje samo u elektronskom obliku (forma, pregled, izveštaj iz aplikacije), nivo klasifikacije mora da je označen na svakom ekranu aplikacije.

Za informacije koje dolaze izvan Meridian Tech d.o.o. Beograd nivo klasifikacije se označava sa posebnim pečatom za tu svrhu ili drugim načinom obeležavanja, i pečatira se od strane vlasnika dokumenta na prvoj strani.

Za informacije koje dolaze izvan Meridian Tech d.o.o. Beograd u elektronskoj formi, nivo klasifikacije smatra se najvišim (Nivo 3).

Informacije koje se generišu u Meridian Tech d.o.o. Beograd i čuvaju na eksternim sistemima imaju nivo klasifikacije 3 (Nivo 3).

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 klasifikacijom informacija 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.