PRAVILA PRENOSA PODATAKA

OZNAKA DOKUMENTA	*MT19POL01*	**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

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	System administrator
2	Menadžer za ISMS
3	Svi zaposleni03,

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 ove politike jeste da uspostavi pravila prenosa informacija, bez obzira u kom obliku se informacije nalaze.

4 PODRUČJE PRIMENE

Ova politika se primenjuje na sve zaposlene i angažovana lica kojima upravlja organizacija. ISMS menadžer će biti odgovoran za sprovođenje 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 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 Prenos informacija – opšte smernice

Organizacija treba da saopšti svoju politiku prenosa informacija svim relevantnim zainteresovanim stranama. Pravila definisana za svaki pojedinačni sporazum o zaštiti informacija u tranzitu moraju odražavati klasifikaciju uključenih informacija. Kada se informacije prenose između organizacije i trećih strana, ugovor mora da sadrži i bezbednosne zahteve za prenos informacija (uključujući autentifikaciju primaoca), mere nadzora uspostavljanja i održavanja kako bi se informacije zaštitile u svim oblicima u tranzitu.

Prenos informacija se vrši elektronskim prenosom, fizičkim prenosom medija za skladištenje i verbalnim prenosom.

Za sve vrste prenosa informacija, pravila definisana u ugovorima moraju uključivati:

a) kontrole za zaštitu prenetih informacija od presretanja, neovlašćenog pristupa, kopiranja, modifikacije, pogrešnog usmeravanja, uništavanja i uskraćivanja usluge, uključujući nivoe kontrole pristupa koji su srazmerni klasifikaciji uključenih informacija i sve posebne kontrole neophodne za zaštitu osetljivih informacija, kao što su korišćenje kriptografske tehnike;
b) kontrole kako bi se obezbedila sledljivost i neporecivost, uključujući održavanje lanca čuvanja informacija tokom tranzita;
c) identifikaciju odgovarajućih kontakata u vezi sa transferom, uključujući vlasnike informacija, vlasnike rizika, lica odgovorna za bezbednosti, po potrebi;
d) ovlašćenja i odgovornosti u slučaju incidenata bezbednosti informacija, kao što je gubitak fizičkih medija za skladištenje ili curenje podataka;
e) korišćenje dogovorenog sistema obeležavanja za osetljive ili kritične informacije, obezbeđujući da se oznake razumeju i da su informacije adekvatno zaštićene;
f) pouzdanost i dostupnost usluge transfera;
g) politike ili smernice specifične za predmet o prihvatljivom korišćenju sredstava za prenos informacija;
h) uputstva za čuvanje i odlaganje svih poslovnih zapisa, uključujući poruke;
i) razmatranje svih drugih relevantnih zakonskih, statutarnih, regulatornih i ugovornih zahteva u vezi sa prenosom informacija (npr. zahtevi za elektronske potpise).

Elektronski transfer

Sigurnosna pravila pri korišćenju sredstava elektronske komunikacije za prenos informacija:

a) otkrivanje i zaštita od zlonamernog softvera koji se može preneti korišćenjem elektronskih komunikacija;
b) zaštita prenetih osetljivih elektronskih informacija u obliku priloga;

c) sprečavanje slanja dokumenata i poruka u komunikacijama na pogrešnu adresu ili broj
d) dobijanje odobrenja pre korišćenja eksternih javnih usluga kao što su trenutne poruke, društvene mreže, deljenje datoteka ili skladištenje u cloud servisu;
e) jači nivoi autentifikacije prilikom prenosa informacija putem javno dostupnih mreža;
f) ograničenja u vezi sa elektronskim sredstvima komunikacije;
g) savetovanje osoblja i drugih zainteresovanih strana da ne šalju usluge kratkih poruka (SMS) ili trenutne poruke sa kritičnim informacijama jer ih mogu pročitati na javnim mestima (a samim tim i neovlašćena lica) ili uskladištiti na uređajima koji nisu adekvatno zaštićeni;

Prenos fizičkih medija za skladištenje

Sigurnosna pravila prilikom prenosa fizičkih medija:
a) odgovornosti za kontrolu i obaveštavanje o prenosu, otpremi i prijemu;
b) obezbeđivanje tačnog adresiranja i transporta poruke;
c) pakovanje koje štiti sadržaj od bilo kakvog fizičkog oštećenja do kojeg bi moglo doći tokom transporta i u skladu sa specifikacijama proizvođača, korišćenje minimalnih tehničkih standarda za pakovanje i transport (npr. korišćenje neprozirnih koverata);
d) spisak ovlašćenih pouzdanih kurira koji je dogovoren od strane relevantnog rukovodioca;
e) standarde identifikacije kurira;
f) u zavisnosti od stepena klasifikacije informacija u medijumu za skladištenje koji se transportuje, koristiti kontrole koje su očigledne ili otporne na neovlašćenu upotrebu;
g) procedure za proveru identifikacije kurira;
h) odobrena lista trećih lica koja pružaju usluge transporta ili kurirske usluge u zavisnosti od klasifikacije podataka;
i) vođenje dnevnika za identifikaciju sadržaja medija za skladištenje, primenjenu zaštitu, kao i evidentiranje liste ovlašćenih primalaca, vremena predaje licima koja vrše transport i prijema na odredištu.

Verbalni prenos

Bezbedonosna pravila za verbalni prenos informacija:
a) poverljivi verbalni razgovori se ne smeju voditi na javnim mestima ili putem nesigurnih kanala komunikacije jer ih mogu čuti neovlašćena lica;
b) ne ostavljati poruke koje sadrže poverljive informacije na telefonskim sekretaricama ili glasovne poruke jer ih neovlašćena lica mogu reprodukovati, uskladištiti na komunalnim sistemima ili pogrešno uskladištiti kao rezultat pogrešnog biranja;
c) izvršiti pregled do odgovarajućeg nivoa da ne dođe do prisluškivanja;
d) obezbediti da se primenjuju odgovarajuće kontrole prostorija (npr. zvučna izolacija, zatvorena vrata);
e) započnite sve osetljive razgovore sa odricanjem odgovornosti kako bi polaznici znali nivo klasifikacije i sve zahteve za rukovanje onim što će čuti.

7.2 EMAIL

Email je postao jedan od ključnih poslovnih alata, kako u internoj tako i u komunikaciji sa klijentima i dobavljačima. Međutim, zbog svoje fleksibilnosti i opšte dostupnosti, korišćenje email-a sa sobom nosi i brojne značajne rizike, te svi korisnici moraju biti na oprezu i moraju usvojiti dobru praksu prilikom slanja i primanja email-a.

Ova politika govori o načinu upotrebe email-a u okviru organizacije Meridian Tech d.o.o. Beograd uključujući i listu stvari koje smeju i koje ne smeju da se rade. Primenjuje se na sve email-ove bez obzira na sredstva ili lokaciju sa kojih se koristi, npr. putem mobilnih uređaja ili van kancelarije.

Email nam je na raspolaganju, kako bi nam pomogao u poslovanju organizacije. Ipak, moći ćete koristiti email i za neke lične potrebe, ali isključivo u skladu sa ovom politikom.

Ukoliko ne razumete smisao ove politike ili Vam nije jasno na koji način se ona odnosi na Vas, trebali biste se obratiti Vašem nadređenom menadžeru.

7.3 Ugovori o poverljivosti ili neotkrivanju podataka

Neophodno je obezbediti da svi pružaoci usluga, koji pružaju usluge sa pristupom osetljivim ili poverljivim podacima, budu vezani Ugovorom o neotkrivanju podataka (NDA) i da prođu proceduru odgovarajuće provere kadrova, u skladu sa zakonima i politikama i procedurama organizacije.

NDA treba da pokrije najmanje sledeće tačke:

- opis informacija koje treba zaštititi (osetljivi podaci, relevantni zapisi, itd.),
- trajanje: obaveza poverljivosti traje neograničeno,
- aktivnosti koje su obavezne nakon isteka Ugovora o poslovnoj saradnji,
- odgovornosti i aktivnosti koje treba sprovesti kako bi se izbeglo neovlašćeno otkrivanje informacija,
- dozvoljeni obim upotrebe poverljivih informacija,
- pravo na reviziju i kontrolne aktivnosti,
- postupak prijave neovlašćenog otkrivanja informacija,
- uslove vraćanja/otkrivanja poverljivih informacija,
- očekivane aktivnosti u slučaju kršenja Ugovora,
- postupak prijave povrede poverljivosti u skladu sa zahtevima zakona.

Prilikom utvrđivanja zahteva za poverljivost ili sporazume o neotkrivanju podataka koji uključuju pristup određenim osetljivim ili poverljivim podacima, konsultuje se vlasnik podataka.

Nije dozvoljeno otkrivati, dostavljati ili prenositi osetljive i poverljive podatke bilo kojoj trećoj strani bez pisane saglasnosti vlasnika podataka (uključujući e-poštu) i pod uslovom da je treća strana upoznata sa poverljivom prirodom takvih podataka i obavezuje se da obezbedi zaštitu takvih podataka u skladu sa bezbednosnim politikama organizacija. Vlasnik podataka upravlja i dokumentuje ove procedure.

Osetljivi i poverljivi podaci moraju biti zaštićeni od potencijalnih zlonamernih lica.

7.4 Slanje i prijem elektronskih poruka

Korišćenje elektronske pošte (e-pošte) nije dozvoljeno za slanje osetljivih i poverljivih podataka.
Ukoliko je potrebna razmena relevantnih zapisa, npr. za potrebe provere, ovi zapisi se čuvaju i stavljaju na raspolaganje trećoj strani putem bezbednog i zaštićenog preuzimanja. S obzirom da se link za preuzimanje može primiti i putem e-pošte putem mobilnog telefona ili tableta, uvek je potrebno poslati napomenu sa vezom kojom će primaoca obavestiti o važećim ograničenjima u vezi sa pristupom relevantnim zapisima.
Alternativa gore navedenom je da je dozvoljen prenos relevantnih zapisa u obliku šifrovanih priloga e-pošte. U tom slučaju, kripto-ključ se šalje preko alternativnog kanala komunikacije (npr. SMS).
U određenim situacijama, za ovaj vid prenosa može se razmotriti korišćenje prenosivih medija (npr. USB stick) umesto elektronske pošte, s tim da se mora voditi računa o odlaganju, čuvanju i uništavanju ovih medija u skladu sa relevantnom politikom. Menadžer bezbednosti informacija odobrava ovu vrstu upotrebe.

Prilikom poslovne komunikacije uvek treba da se koristi email adresa organizacije. Za ove svrhe ne biste smeli koristiti ličnu email adresu. Uvek se trebaju imati u vidu smernice za slanje poverljivih informacija (informacije klasifikovane kao Poverljive, interne i javne) prilikom njihovog slanja email-om.

Svi email-ovi poslati sa email adrese organizacije ostaju u vlasništvu organizacije Meridian Tech d.o.o. Beograd i smatraju se delom korporativnih zapisa. Svi email-ovi smatraju se zvaničnim oblikom komunikacije organizacije i u skladu s tim, prema njima se treba tako i odnositi.

Organizacija zadržava pravo da nadgleda i proverava korišćenje email-a od strane ovlašćenih korisnika, kako bi ocenila usaglašenost sa ovom politikom. Ovo se obavlja u skladu sa važećim zakonima.

Brisanje email-a sa pojedinačnog naloga ne mora da znači da je on trajno uklonjen iz IT sistema organizacije, što znači da se taj email može još uvek preispitati i proveriti.

Korisnik treba biti svestan da ne postoji garancija da će poruka stići do primaoca ili da će je baš on pročitati, kao i da poruka može biti drugačije protumačena u zavisnosti od kulture, uloge pa čak i raspoloženja pojedinca koji je čita. Zato uvek treba da razmislite da li je email pravi način za prenošenje date informacije i da li je možda neki drug način komunikacije, poput telefona, prikladniji, pogotovo ako je poruka hitna ili kompleksna.

Posebna pažnja mora se obratiti prilikom slanja email-a koji sadrži poverljive informacije, kako bi se sprečilo da se greškom pošalje neovlašćenom primaocu. Obratite pažnju na automatsko popunjavanje polja primaoca gde na osnovu samo nekoliko unetih znakova sistem predlaže adresu primaoca.

Ne koristite opciju automatskog prosleđivanja, npr. dok ste na odmoru, jer postoji mogućnost da se poverljive informacije proslede primaocu koji nema dovoljan stepen zaštite nepohodan za date informacije.

Korisnici bi trebali izbegavati slanje nepotrebnih poruka širokoj grupi primaoca, naročito onoj koja imaju veliku cirkulaciju kao što je “opšta lista” svih zaposlenih. Kada je to neophodno, takvi email-ovi treba da se proslede putem odeljenja za komunikaciju u organizaciji.

Email-ove poslate sa email adrese organizacije treba shvatiti na isti način kao i druge formalne metode komunikacije. Ništa što bi moglo da pokvari reputaciju organizacije ili da utiče na njen odnos sa dobavljačima, klijentima ili ostalim zainteresovanim stranama ne sme da se pošalje u javnost.

Konkretno, korisnici ne bi smeli slati email-ove koji sadrže materijale koji su klevetnički, nepristojni, nisu u skladu sa politikom organizacije o ravnopravnosti polova i pravom na različitost ili koji primalac na bilo koji način može smatrati neprikladnim. Ukoliko niste sigurni da li poruka koju nameravate da pošaljete spada u ovu kategoriju, molimo Vas da se konsultujete sa Vašim nadređenim menadžerom pre slanja email-a.

Zvanična email adresa organizacije ne sme se koristiti za:

- distribuciju neovlašćenog komercijalnog ili reklamnog materijala, lančanih pisama ili bilo koje vrste neželjene pošte (junk mail) ostalim organizacijama
- slanje materijala koji narušava prava intelektualne svojine (posebno autorska i srodna prava) drugih osoba ili organizacija
- aktivnosti koje štete ili uništavaju podatke ostalih korisnika ili na neki drugi način ometaju poslovanje drugih korisnika
- distribuciju uvredljivih, opscenih ili neprikladnih slika, podataka ili drugih materijala, ili svih podataka koji mogu da dovedu do opscenih ili neprikladnih slika ili materijala
- slanje bilo čega što je kreirano ili lako može da izazove neprijatnost ili nepotrebnu nervozu ostalih
- prenos uvredljivih, pretećih ili nasilničkih poruka drugima
- slanje materijala koji diskriminiše ili podstiče diskriminaciju bilo koje grupe na osnovu rase, pola, seksualne opredeljenosti, materijalnog statusa, invaliditeta, političkih ili verskih uverenja
- prenos klevetničkog materijala ili lažnih tvrdnji varljive prirode
- aktivnosti koje uključuju privatnost ostalih korisnika
- slanje anonimnih poruka – tj. bez jasne identifikacije pošiljaoca
- sve ostale aktivnosti koje utiču ili mogu da utiču na ugled organizacije

Ukoliko primite neželjenu (*junk mail*) ili *spam* poštu, preporučuje se da je izbrišete bez otvaranja. Ne odgovarajte na ove poruke, jer ćete na taj način potvrditi validnost Vaše adrese pošiljaocu, što će rezultirati daljom neželjenom komunikacijom.

7.5 Čuvanje informacija na prenosivim medijima

Mediji na kojima se čuvaju podaci uključuju, između ostalog:

- Hard diskovi (interni i eksterni),
- CD,
- DVD,
- optički diskovi,
- USB memorijske kartice,
- Čitači medijskih kartica,
- MP3/MP4 plejeri,
- digitalne kamere,
- rezervne trake,
- audio trake (uključujući diktafone i telefonske sekretarice).

Prenosivi računarski mediji su zaštićeni da bi se sprečila šteta, krađa ili neovlašćeni pristup.
Tokom transporta, mediji na kojima se čuvaju podaci zaštićeni su od neovlašćenog pristupa, zloupotrebe ili korupcije.
Sistemska dokumentacija je zaštićena od neovlašćenog pristupa.
Primer dokumentacije koju treba zaštititi uključuje, između ostalog, opise:

- Aplikacija,
- Procesi,
- Procedura,
- Struktura podataka,
- Detalji autorizacije.

Ako je prikladno, treba koristiti fizičke kontrole, kao što su šifrovani ili zaključani specijalizovani koferi. Treba voditi računa o tome da mediji koji više nisu potrebni budu bezbedno uklonjeni kako bi se sprečilo curenje informacija.
Korisnicima je zabranjeno korišćenje USB uređaja u privatne svrhe. Zabranjeno je snimanje osetljivih i poverljivih dokumenata na USB bez prethodnog odobrenja. Svi spoljni uređaji, kao što su USB, eksterni diskovi i drugi prenosivi mediji, podložni su zloupotrebi i stoga je svaki zaposleni odgovoran za dodeljene medije. Medij je zabranjeno ostavljati bez nadzora i obavezno ga čuvati u skladu sa uputstvima proizvođača. Svaki medijum će biti označen u svrhu identifikacije.

7.6 Transport medijuma za prenos informacija

Svaki medijum koji se transportuje mora biti zaštićen od neovlašćenog pristupa, zloupotrebe ili oštećenja integriteta informacija sadržanih na medijumu.
U situacijama kada prevoz obavljaju eksterna lica (ili organizacije), obavezno je potpisivanje ugovora koji obavezuje poštovanje određenih bezbednosnih procedura (Non-Disclosure Agreement - NDA). Kad god je primenljivo, koristiće se šifrovanje podataka ili specijalne zaključane kutije ili koferi.

7.7 Procena rizika

Lica ovlašćena da upravljaju rizicima vrše procenu rizika kako bi utvrdile bezbednosne kontrole potrebne za zaštitu informacija tokom njihovog životnog ciklusa, na primer:

- kreiranje informacija (klasifikacija)
- obrada (provera ulaznih podataka, provera integriteta podataka)
- skladištenje (odvajanje)
- prenos (šifrovanje, neporecivost)
- uništavanje (bezbedno brisanje i fizičko uništavanje).

Vlasnik podataka odobrava procenu rizika pojedinačnog sistema.

7.8 Održavanje vašeg naloga

Vašem mailbox-u (poštanskom sandučiću) je ograničena veličina. To je urađeno, kako bi se sprečilo prelaženje kapaciteta čuvanja podataka i kako bi se obezbedila isplativa upotreba email-a.

Trebali biste održavati Vaš email nalog tako da ostane u okviru ograničenja mailbox-a, koristeći se kada je to moguće, opcijom arhiviranja poruka koja je dostupna na većini email programa. Ukoliko se Vaš mailbox napunio, kontaktirajte IT podršku za savet po ovom pitanju.

Kada je moguće, koristite linkove u email porukama umesto da šaljete kompletne kopije fajlova u prilogu, naročito ako se poruka šalje velikom broju primalaca. Na ovaj način sprečiće se zatrpavanje mailbox-ova ostalih korisnika i izbeći mogući prekidi u poslovanju.

Postoji sistemsko ograničenje veličine email-a koje iznosi 30Mb . Ukoliko iz opravdanih poslovnih razloga budete morali da pošaljete veliki email, obratite se IT podršci za savet.

Kompjuterski virusi i zlonamerni softveri su mali programi koji mogu negativno da utiču na Vaš kompjuter i Vaše korišćenje Interneta, a mogu i da izlože poverljive organizacione informacije ekstremnom riziku. Takvi virusi mogu se nenamerno preuzeti ili instalirati putem email-a primljenog u Vaš inbox. Organizacija je obezbedila antivirus softver koji se nalazi na svim kompjuterima koji imaju pristup mreži, i koji treba da registruje sve viruse pre nego što se oni instaliraju.

Ukoliko mislite da je Vaš kompjuter zaražen virusom ili Vam je poslat email za koji sumnjate da sadrži virus, odmah prijavite problem IT podršci. Ne otvarajte nijedan prilog za koji sumnjate da sadrži virus.

Pored toga, ne smete:

- email-om slati fajlove za koje znate da su zaraženi virusom
- preuzimati podatke ili programe bilo koje vrste sa neproverenih izvora
- isključiti ili rekonfigurisati instalirani antivirus sistem koji se nalazi na kompjuteru preko kojeg pristupate email-u
- proslediti obaveštenje o virusu bilo kome, osim IT podršci

IT podrška je obezbedila da se svi email-ovi na ulasku u mrežu i kod *host*-a testiraju na viruse, i kada je to moguće, upotrebiće dva nezavisna načina testiranja na viruse.

Ukoliko je virus slučajno ili namerno poslat drugoj organizaciji, Meridian Tech d.o.o. Beograd se može proglasiti odgovornim, ukoliko se prenos pokaže kao rezultat nemarnosti.

7.9 Email nadzor

Upotreba email-a unutar sistema organizacije se nadgleda i beleži centralno, kako bi se:

- efektivno planiralo i upravljalo kapacitetima resursa
- procenila usaglašenost sa politikama i procedurama
- osiguralo da se standardi održavaju
- sprečile i primetile kriminalne radnje
- istražilo neovlašćeno korišćenje

Nadzor vrši osoblje koje je posebno ovlašćeno za to. Procedura stalnog nadzora primenjuje se na svim korisnicima i može podrazumevati i proveru sadržaja email poruka.

Ukoliko menadžer posumnja da korisnik zloupotrebljava email, trebao bi kontaktirati ISMS menadžera. Sve slične prijave biće ispitane u skladu sa dokumentovanim procedurama i, kada je to moguće, pruženim dokazima. Postoji zahtev da se takve informacije saopšte i regulatornim i zakonodavnim telima u skladu sa zakonom.

Korisnik ne sme da pristupi email nalogu drugog korisnika, osim ako nije dobio dozvolu od vlasnika naloga ili od nadređenog menadžera. U ovakvom slučaju to mora biti isključivo iz opravdanog poslovnog razloga i može se pristupiti samo email-ovima koji se smatraju značajnim za dato pitanje.

8 ODGOVORNOSTI I OVLAŠĆENJA

ISMS menadžer je odgovoran za upravljanje bezbednosnim procenama za organizaciju u skladu sa utvrđenim zahtevima. Svi sistemi koji su pod upravljanjem organizacije sa zahtevima koji odstupaju od ovih smernica moraju da podnesu zahtev za izuzeće od smernica na razmatranje i potencijalno odobrenje.
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 prenosa podataka 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.