



REPUBLIKA HRVATSKA

**MINISTARSTVO RADA, MIROVINSKOGA SUSTAVA,
OBITELJI I SOCIJALNE POLITIKE**

PROTOKOL O PRISTUPU I KORIŠTENJU INFORMACIJSKIH SUSTAVA

Sadržaj

1. Definicije i pojmovi	2
2. Obveznici primjene Protokola o pristupu i korištenju informacijskih sustava	4
3. Uporaba računalne opreme i programske podrške	5
4. Autentifikacija i politika lozinki	7
5. Uporaba informacijsko-komunikacijske infrastrukture	9
6. Uporaba Interneta i elektroničke pošte.....	11
7. Edukacija korisnika	15
8. Kibernetički incident	16
9. Upoznavanje korisnika s Protokolom	17

Na temelju članka 26. i 29. Zakona o kibernetičkoj sigurnosti (Narodne novine broj 14/24) i članaka 38. i 42. Uredbe o kibernetičkoj sigurnosti (Narodne novine broj 135/24) donosi se sljedeći

PROTOKOL O PRISTUPU I KORIŠTENJU INFORMACIJSKIH SUSTAVA

1. Definicije i pojmovi

1. U ovom dokumentu koriste se sljedeći pojmovi:

- **Administrator:** osoba zadužena za tehničko održavanje računala, pojedinih programa ili sustava (mogu se koristiti i pojmovi kao: *sistem inženjer*, *superuser* ili *root*);
- **Adresa elektroničke pošte:** isto što i *e-mail adresa*, jedinstvena adresa korisnika koja se korisnicima otvara za potrebe obavljanja radnih zadataka i poslovnih procesa te poslovnog komuniciranja (npr.: josip.ivic@mrosp.hr) a vezana je uz korisnički račun; u posebnim slučajevima mogu biti otvorene i grupne adrese elektroničke pošte (kao distribucijska ili mailing lista ili kao zaseban sandučić ili mailbox);
- **Autentifikacija:** proces provjere i potvrđivanja identiteta korisnika; način na koji se provjerava prijavljuje li se u aplikaciju ili u sustav osoba koja mu zaista ima pravo pristupiti; ovom provjerom identiteta korisniku se omogućava da pristupa onim funkcijama i sadržajima koji su mu odobreni; najčešći je način autentifikacije unos korisničkog imena i lozinke;

Uz autentifikaciju vezan je i pojam **Multifaktorska autentifikacija (MFA)**: sigurnosni proces koji zahtijeva više od jednog načina potvrde identiteta korisnika; umjesto da se koriste samo korisničko ime i lozinka, MFA traži dodatne informacije kako bi bilo sigurno da se radi o legalnom korisniku; neki od faktora autentifikacije mogu biti SMS kod, kod kojeg generira posebna aplikacija, pametna kartica, sigurnosni USB ključ, otisak prsta, prepoznavanje lica i slično; dodatni načini autentifikacije čine korisnički račun i cijeli sustav sigurnijima;

- **Distribucijska lista:** formalno ima oblik adrese elektroničke pošte s tim da se sva elektronička pošta koja pristigne na tu adresu distribuira (prosljeđuje) na adrese elektroničke pošte korisnika koji su navedeni u listi; elektroničke poruke dolaze u njihov sandučić i ne čuvaju se na drugom mjestu zato što adresa elektroničke pošte za distribucijsku listu nema svoj sandučić (mailbox);
- **Informatičko-komunikacijska infrastruktura (ili informacijsko-komunikacijska infrastruktura):** poslužiteljska i komunikacijska oprema i prijenosni sustavi koji se

temelje na stalnoj infrastrukturi, uključujući programsku podršku i upravljačke programe; također ju čini svaki uređaj od kojih jedan ili više njih programski izvršava automatsku obradu digitalnih podataka koji se obrađuju, pohranjuju, dobivaju ili prenose;

- **Kibernetička sigurnost:** sve aktivnosti koje su nužne za zaštitu od kibernetičkih prijetnji mrežnim i informacijskim sustavima, korisnicima tih sustava i drugim osobama na koje one utječu;
- **Kibernetički incident (ili samo incident):** događaj koji ugrožava dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili usluga koje mrežni i informacijski sustavi nude ili kojima omogućuju pristup;
- **Korisnik:** svaka fizička osoba koja pristupa računalnoj opremi i mreži Ministarstva i institucija, koja koristi programsku podršku ili poslovne baze podataka kojima upravlja Ministarstvo ili institucije kojima je Ministarstvo osnivač;
- **Korisničko ime:** isto što i *log in*, *account name*, *user name* i slično, skraćeno ime korisnika definirano na računalu, pojedinim programima ili na sustavu a služi za pristup pojedinim resursima informacijskog sustava;
- **Korisnički račun:** skup koji se sastoji od korisničkog imena i lozinke s točno definiranim pravima za rad na računalu, pojedinim programima ili na sustavu;
- **Lanac sreće:** elektronička poruka koja na svojem kraju traži da ju prosljedite jednom ili više korisnika;
- **Poslovne aplikacije:** programi koji služe za vođenje pojedinih poslovnih procesa unutar informacijskog sustava;
- **Privilegirana prava:** prava za rad s aplikacijama, dijelovima sustava ili cijelim sustavima (aplikativnim, računalnim ili komunikacijskim), koja pojedini korisnici mogu dobiti uz standardna prava koja imaju ostali korisnici; može se raditi o različitim nivoima administratorskih prava ili o dozvoli za pristup i korištenje funkcionalnosti koje ne bi trebali ili smjeli koristiti svi korisnici;
- **Privitak:** isto što i *attachment*, dokument koji je u obliku datoteke poslan putem elektroničke pošte;
- **Programska podrška:** skup svih računalnih programa potrebnih za rad i kontrolu računalnih sustava te skup svih sistemskih, operativnih, uslužnih i aplikativnih programa;
- **Računalna oprema:** računala i drugi elektronički uređaji za unos, pohranu, obradu, prijenos i prikaz podataka;
- **Rizici kibernetičke sigurnosti:** mogućnosti gubitka podataka ili pristupa usluzi ili poremećaji uzrokovani incidentom, koji imaju vjerojatnost da do tog incidenta dođe te štetu koju za korisnike informacijskog sustava takav incident može uzrokovati.

2. Obveznici primjene Protokola o pristupu i korištenju informacijskih sustava

1. Protokol o pristupu i korištenju informacijskih sustava osnovni je dokument koji definira pravila pristupa i korištenja informacijskih sustava u Ministarstvu rada, mirovinskoga sustava, obitelji i socijalne politike (u daljnjem tekstu: Ministarstvo) i drugim ustanovama i institucijama koje u svom radu koriste informatičko-komunikacijsku infrastrukturu i informacijske sustave (u daljnjem tekstu: Institucije) čiji je vlasnik i kojima upravlja Ministarstvo. Cilj je zaštititi podatke koji se nalaze u informacijskim sustavima, osobe čiji su podaci prikupljeni, građane i Institucije za koje se obavljaju usluge pomoću informacijskih sustava kojima upravlja Ministarstvo te same korisnike koji pristupaju informacijskim sustavima i poslovne procese kojima upravljaju Ministarstvo i Institucije.
2. Protokol se primjenjuje u Ministarstvu i svim Institucijama koje u svom radu koriste informatičko-komunikacijsku infrastrukturu i informacijske sustave čiji je vlasnik i kojima upravlja Ministarstvo.
3. Protokol su obavezni provoditi svi korisnici informacijskih sustava koji koriste informatičko-komunikacijsku infrastrukturu i informacijske sustave čiji je vlasnik i kojima upravlja Ministarstvo.
4. U Institucijama ne postupanje u skladu s ovim Protokolom bez da za to postoje opravdani razlozi predstavlja povredu službene dužnosti, dok će Ministarstvo to regulirati Pravilnikom o unutarnjem redu.

3. Uporaba računalne opreme i programske podrške

1. Računalna oprema koristi se za poslovne procese korisnikovog radnog mjesta.

Korisnik računala koje pristupa računalnoj mreži kojom upravlja Ministarstvo nije vlasnik tog računala nego se njime, kao opremom koja je u vlasništvu Ministarstva ili Institucije, služi u okviru posla koji obavlja.

Pristup podacima za koje korisnik nema ovlaštenje nije dozvoljen.

2. Svaki korisnik za rad s računalnom opremom, s razine operacijskog sustava, posjeduje svoj korisnički račun (vlastito korisničko ime i lozinku). Anonimne aktivnosti u korištenju sustava nisu dozvoljene.

Ministarstvo može za pojedine sustave ili dijelove sustava propisati korištenje multifaktorske autentifikacije (MFA) kada se osim korištenja korisničkog imena i lozinke za prijavu koristi još neki drugi način autentifikacije.

3. Svaki korisnik poslovnim aplikacijama koje koriste poslovne baze podataka pristupa vlastitim korisničkim imenom i lozinkom koju mu, na zahtjev voditelja njegove organizacijske jedinice, dodjeljuje administrator poslovne aplikacije.
4. Osoba kojoj je dodijeljen korisnički račun s administratorskim pravima taj račun smije koristiti samo za zadatke koje nije moguće napraviti bez administratorskog pristupa. U svim ostalim situacijama dužan je koristiti svoj redovan korisnički račun.
5. Korisnik je odgovoran za sve aktivnosti unutar računalne opreme i poslovnih aplikacija koje su obavljene s njegovim korisničkim imenom.
6. Prilikom privremenog napuštanja radnog mjesta korisnik je dužan onemogućiti da računalnoj ili programskoj opremi mogu pristupiti druge osobe bez ponovne prijave uporabom korisničkog imena i lozinke ili drugog dozvoljenog načina autentifikacije.
7. Prilikom duljeg napuštanja radnog mjesta korisnik je dužan ugasiti računalnu opremu ako mu to nije drugačije naloženo od strane nadređenih osoba ili zaposlenika organizacijske jedinice Ministarstva nadležne za informatičke poslove. Izuzetak mogu biti situacije kada operativni sustav ili sustav upravljanja bazama podataka pokrene nadogradnju ili postupak oporavka što može biti dugotrajan postupak i za vrijeme kojeg nije preporučljivo gasiti računalno.
8. Nije dopuštena instalacija i kopiranje ili umnožavanje programske podrške bez odobrenja organizacijske jedinice Ministarstva nadležne za informatičke poslove. Nije dopušteno korištenje programa ili elektroničkih dokumenata nad kojima postoji autorsko pravo ako korisnik, institucija u kojoj je zaposlen ili Ministarstvo nema regulirano pravo njihovog korištenja.

Sva programska podrška koja se postavlja na računala i drugu informatičko-komunikacijsku opremu mora imati legalnu licencu (pravo korištenja) ako je to primjenjivo.

9. Nisu dozvoljene izmjene postavki operacijskog sustava od strane korisnika ili drugih neovlaštenih osoba bez suglasnosti organizacijske jedinice Ministarstva nadležne za informatičke poslove.
10. Organizacijska jedinica Ministarstva nadležna za informatičke poslove može pružati informatičku podršku samo za programe za koje je licence nabavilo Ministarstvo. Za programe koje su nabavile pojedine Institucije organizacijska jedinica Ministarstva nadležna za informatičke poslove ne pruža informatičku podršku.
11. Za kreiranje i zatvaranje korisničkih računa, odnosno za promjenu pojedinih ovlasti i prava na razini operativnog sustava zadužena je organizacijska jedinica Ministarstva nadležna za informatičke poslove a za kreiranje, zatvaranje i promjenu pojedinih ovlasti za rad s poslovnim aplikacijama i bazama podataka zaduženi su administratori poslovnih aplikacija. Potrebu promjene ovlasti i prava za pojedine korisnike ovoj organizacijskoj jedinici pisanim putem šalje neposredno nadređeni rukovoditelj korisnika.
12. Udaljeni pristup do računalne opreme i poslovnih podataka uporabom računalnih mreža može se dozvoliti samo uz korištenje opreme koju je instalirala organizacijska jedinica Ministarstva nadležna za informatičke poslove i koja je pod njenim nadzorom ili koju je pregledala i suglasila se s njenom uporabom za udaljeni pristup.
13. O problemima u radu računalne opreme te eventualnim ugrozama iste, korisnik mora obavijestiti neposredno nadređenog rukovoditelja i organizacijsku jedinicu Ministarstva nadležnu za informatičke poslove. Kontakt podaci nalaze se na Intranet stranici it.mrosp.hr.
14. Probleme u radu koji zahtijevaju intervenciju organizacijske jedinice Ministarstva nadležne za informatičke poslove korisnici u Institucijama prijavljuju preko HelpDesk aplikacije kojoj mogu pristupiti s Intranet stranice it.mrosp.hr, a korisnici iz Ministarstva s Intranet stranice intranet.mrosp.hr.
15. Korisnik će prekinuti korištenje aplikacija koje pristupaju poslovnim bazama podataka ako na računalu na kojem radi nije instaliran ili se redovito ne ažurira program za zaštitu od virusa i drugog zlonamjernog softvera. O tome odmah mora obavijestiti organizacijsku jedinicu Ministarstva nadležnu za informatičke telefonski ili preko HelpDesk aplikacije i čekati njihove daljnje upute.

Način na koji korisnici mogu prepoznati je li na računalu instaliran i ažuriran program za zaštitu od virusa i drugog zlonamjernog softvera opisan je na Intranet stranicama it.mrosp.hr u dijelu kojem se pristupa preko izbornika *Kako i zašto*.

4. Autentifikacija i politika lozinki

1. Zbog utvrđene visoke razine kibernetičkih sigurnosnih rizika, Ministarstvo je dužno provoditi naprednu razinu mjera upravljanja kibernetičkim sigurnosnim rizicima. Jedan je od zahtjeva iz Uredbe o kibernetičkoj sigurnosti (Narodne novine br. 135/24) da se na svim mrežnim i informacijskim sustavima za pristup u kojima se koriste lozinke kao sredstvo autentifikacije vodi politikom „najjačih mogućih lozinki“ koja mora biti u skladu s trenutnim dobrim praksama.
2. Duljina lozinki koje se koriste u informacijskim sustavima i informatičko-komunikacijskom sustavu Ministarstva treba biti najmanje 14 znakova i to poštujući sljedeća pravila:
 - Minimalno jedan znak mora biti malo slovo
 - Minimalno jedan znak mora biti veliko slovo
 - Minimalno jedan znak mora biti znamenka između 0 i 9
 - Minimalno jedan znak mora biti poseban znak (točka, zarez, upitnik, uskliknik, znak računskih operacija, =, #, \$, %, &, /, (,), -, _, @)
 - Lozinka ne smije sadržavati ime ili prezime korisnika
 - Lozinka se ne smije ponavljati unazad 24 promjene.
3. Korisnici administratorskih lozinki ili lozinki koje omogućavaju neka privilegirana prava moraju koristiti lozinku koja ima najmanje 16 znakova poštujući pravila iz prethodne točke.
4. Lozinka se obavezno mora promijeniti najkasnije 5 mjeseci nakon prethodnog postavljanja.
5. Korisnici se moraju s posebnom pažnjom odnositi prema dodijeljenim mu pristupnim podacima. Obavezni su svoje korisničko ime ili lozinku primjereno čuvati od mogućnosti da postanu dostupne drugim osobama. Ne smiju ih ostavljati zapisanima na radnom stolu, računalu ili na drugim mjestima gdje ih mogu pronaći i vidjeti druge osobe.

Svoje korisničko ime i lozinku korisnik ne smije ustupati drugim osobama, niti se u svom radu smije koristiti korisničkim imenom i lozinkom koji mu nisu dodijeljeni.

Druge osobe, bez obzira na funkciju i položaj u odnosu na korisnika, ne smiju od njega tražiti da im povjeri svoje lozinke.

Iznimno (korisnik je odsutan ili ne može pristupiti sustavu, korisnik ne može obavljati zadatke koje je potrebno žurno izvršiti i slično), ako to nalaže potreba posla, uz prethodnu suglasnost nadređenog rukovoditelja, korisnik će ustupiti na korištenje svoje korisničko ime i lozinku ili će za rad koristiti tuđe korisničko ime i lozinku. Nadređeni rukovoditelj koji je dao suglasnost da druga osoba koristi tuđe korisničko ime i lozinku dužan je osigurati da tijekom njenog korištenja ne dođe do zloupotrebe. U tom slučaju odgovornost za sve postupke nastale kao posljedica korištenja tuđeg korisničkog imena

i lozinke snosi osim korisnika za čijeg je korištenja došlo do kibernetičkog incidenta i rukovoditelj koji je dao suglasnost.

Odmah po prestanku potrebe korištenja tuđeg korisničkog imena i lozinke, korisnik čije je korisničko ime bilo korišteno mora promijeniti lozinku. Ako on to nije u mogućnosti napraviti, rukovoditelj koji je dao suglasnost dužan je od administratora sustava ili organizacijske jedinice Ministarstva nadležne za informatičke poslove zatražiti izmjenu lozinke.

6. Za pristup informatičko-komunikacijskoj infrastrukturi Ministarstva izvan lokalne računalne mreže obavezno je koristiti VPN (Virtual Private Network). Za korištenje VPN-a obavezna je multifaktorska autentifikacija, a način i vrstu odredit će Ministarstvo.
7. Multifaktorska autentifikacija za VPN pristup informatičko-komunikacijskom sustavu Ministarstva obavezna je i za sve vanjske korisnike i pružatelje usluga koji joj imaju potrebu i dozvolu pristupati.
8. Na isti način kako je to propisano za uporabu i čuvanje lozinke, korisnik se mora s posebnom pažnjom odnositi i prema dodijeljenom mu multifaktorskom načinu pristupa informacijskim sustavima i informatičko-komunikacijskoj infrastrukturi kako im neovlaštene osobe ne bi mogle pristupiti.

5. Uporaba informacijsko-komunikacijske infrastrukture

1. Računalna mreža smije se koristiti samo za potrebe poslova koje korisnik obavlja u okviru svojih radnih zadataka i poslovnih procesa.
2. Poslovne baze podataka koje sadrže osobne podatke ne smiju se nezaštićene slati putem računalne mreže ili medija za prijenos ili pohranu podataka. Takvi se podaci prethodno moraju kriptirati.
3. Gosti i poslovni partneri ne smiju koristiti računalnu mrežu Ministarstva na kojoj se nalaze poslovne aplikacije i baze podataka. Iznimka su osobe kojima je pristup računalnoj mreži potreban radi obavljanja poslova od značaja za informacijsko-komunikacijski sustav, osobe koje testiraju, održavaju, ispravljaju nedostatke ili nadograđuju informacijske sustave ili informatičko-komunikacijski sustav te osobe koje imaju ovlast nadzora, inspekcije ili drugih vidova kontrole pojedinih poslovnih procesa za koje se koristi odgovarajuća programska podrška. Odobrenje za pristup informacijsko-komunikacijskoj infrastrukturi u ovakvim slučajevima daje odgovorna osoba službe ili više organizacijske jedinice za čiju potrebu se treba omogućiti pristup informacijsko-komunikacijskoj infrastrukturi, a pri tome osoba koja dobije odobrenje za rad na računalu u mreži Ministarstva mora prethodno potpisati izjavu o tajnosti podataka ako to već nije ranije napravila.
4. Korisnici računalnu mrežu smiju koristiti samo opremom konfiguriranom prema uputama dobivenim od organizacijske jedinice Ministarstva zadužene za informatičke poslove. Privatnom opremom (uključujući i mobilne uređaje) korisnici mogu pristupati računalnoj mreži samo uz odobrenje odgovorne osobe službe ili više organizacijske jedinice za čiju potrebu je potrebno koristiti ovu opremu, i prema uputama koje će dobiti od organizacijske jedinice Ministarstva zadužene za informatičke poslove.

Privatnom opremom nije dozvoljeno pristupati poslovnim aplikacijama i bazama podataka.

5. Svakom se korisniku iz Ministarstva na poslužiteljima može otvoriti osobna mapa za pohranu datoteka koje koristi za obavljanje svojih radnih zadataka i poslovnih procesa. Toj mapi može pristupiti samo korisnik za kojeg je ona napravljena.
6. Voditelji organizacijskih jedinica u Ministarstvu mogu od organizacijske jedinice zadužene za informatičke poslove pisanim putem zatražiti otvaranje dijeljenih mapa za pohranu i razmjenu datoteka za pojedine organizacijske jedinice ili grupe korisnika.

Voditelji organizacijskih jedinica u institucijama za svoj redovan rad mogu zatražiti otvaranje dijeljenih mapa na vlastitoj dostupnoj infrastrukturi od osobe ili firme koja obavlja informatičke poslove za potrebe te institucije ako ona nema zaposlene vlastite stručnjake.

7. Organizacijska jedinica Ministarstva zadužena za informatičke poslove zadužena je za pohranu sigurnosnih kopija podataka (backup) koje se nalaze na računalnoj infrastrukturi kojom upravlja.

Izradu sigurnosnih kopija podataka koje se nalaze na računalnoj infrastrukturi institucije može propisati njen rukovoditelj. Uspostavu i provođenje takvog sustava mogu izvoditi osobe ili firme koje obavljaju informatičke poslove za potrebe te institucije ako ona nema zaposlene vlastite stručnjake.

8. Za podatke koje korisnik pohrani na svom računalu odgovoran je korisnik. Organizacijska jedinica Ministarstva zadužena za informatičke poslove ne snosi nikakvu odgovornost za podatke koji su spremljeni na lokalnim računalima korisnika.
9. O problemima u radu računalne mreže te uočenim eventualnim ugrozama korisnik mora obavijestiti organizacijsku jedinicu Ministarstva zaduženu za informatičke poslove.
10. Odgovorna osoba institucije koja koristi informacijski sustav kojim upravlja Ministarstvo odredit će službenika koji će biti zadužen organizacijskoj jedinici Ministarstva zaduženoj za informatičke poslove slati obavijesti o prestanku radnog odnosa ili druge vrste angažmana osoba koje su imale pristup informacijskom sustavu. Pisanu obavijest potrebno je poslati odmah po prestanku radnog odnosa ili druge vrste angažmana. Tim će se osobama odmah po primitku obavijesti onemogućiti pristup resursima informacijskog sustava.

Svi elektronički zapisi u dodijeljenim osobnim mrežnim mapama ili na računalu koje je korišteno bit će obrisani u roku od četrnaest dana po primitku obavijesti, osim ako to drugačije ne naloži nadređena osoba. Ovo se odnosi i na sve e-mail poruke koje su pohranjene u osobnom sandučiću elektroničke pošte na e-mail poslužitelju kojim upravlja Ministarstvo.

Ako je razlog prestanka radnog odnosa, službe ili druge vrste angažmana prelazak u drugu ustanovu socijalne skrbi koja također koristi informacijski sustav kojim upravlja Ministarstvo, potrebno je to navesti u pisanoj obavijesti. U tom slučaju korisniku će se omogućiti daljnje korištenje informacijskog sustava i informatičko-komunikacijske infrastrukture, a u sustavu će biti evidentirana pripadnost drugoj instituciji.

Službenik koji je određen za slanje obavijesti za svoju instituciju može ju poslati u obliku prijave preko HelpDesk aplikacije kojoj se pristupa s Intranet stranice it.mrosp.hr.

11. Uz ovaj Protokol, za pojedine dijelove informacijskog sustava mogu biti propisane dodatne upute ili protokoli koji predstavljaju nadopunu ovog Protokola.

6. Uporaba Interneta i elektroničke pošte

1. Korisnik treba voditi računa o pravilima ponašanja korisnika Interneta. Zabranjuje se pregledavanje mrežnih stranica s pornografskim sadržajem ili drugim oblicima socijalno neprihvatljivog sadržaja.
2. Ako se zbog pregledavanja ili preuzimanja multimedijalnih sadržaja ili drugih datoteka usporava rad drugih korisnika s poslovnim aplikacijama i bazama, korisnik i njegov nadređeni rukovoditelj trebaju organizirati da se pregledavanje ili preuzimanje tih sadržaja provodi u vrijeme kada neće ometati rad drugih korisnika.
3. Korisnici informacijskih sustava Ministarstva i institucija u svrhu službene komunikacije obavezno moraju koristiti službeno im dodijeljenu adresu elektroničke pošte.
4. Korisnik za pristup elektroničkoj pošti smije upotrijebiti samo svoje osobno korisničko ime. Pojedini korisnici mogu biti ovlašteni za pristup grupnim adresama elektroničke pošte (primanje ili primanje i slanje elektroničke pošte) koje se kreiraju prema zahtjevu odgovornih osoba za obavljanje posebnih aktivnosti ili poslova.
5. Korisnik elektroničke pošte odgovoran je za sve aktivnosti nastale s njegove adrese elektroničke pošte kao i za aktivnosti nastale tijekom njegovog pristupa elektroničkoj pošti namijenjenoj posebnim aktivnostima ili poslovima Ministarstva i institucija. Korisnik nikada i nikome ne smije otkrivati korisničko ime i lozinku za pristup računalnoj opremi jer se može iskoristiti za pristup korisnikovom sustavu elektroničke pošte. Ako korisnik smatra da mu je lozinka ugrožena (poznata drugim osobama) obavezan ju je odmah promijeniti.
6. Ministarstvo je vlasnik cjelokupne elektroničke pošte koja se šalje i prima pomoću računa elektroničke pošte koje je dodijelilo. Nadređeni rukovoditelj od korisnika uvijek može zatražiti uvid u elektroničku poštu koja se nalazi na tim računima. U slučaju zloupotrebe elektroničke pošte nadređeni rukovoditelj može zatražiti zatvaranje računa elektroničke pošte koji koristi njegov zaposlenik. Ako je zahtjev opravdan, organizacijska jedinica Ministarstva nadležna za informatičke poslove onemogućit će pristup računu.
7. Korisnik sustava elektroničke pošte ne smije slati poruke elektroničkom poštom osobama koje ne poznaje, ukoliko oni sami to od korisnika nisu zatražili ili ako to nije sastavni dio radnih zadataka koje obavlja.
8. Neke adrese elektroničke pošte mogu predstavljati grupu ljudi pa korisnik sustava elektroničke pošte to treba imati u vidu glede sadržaja poruke koju šalje.
9. U poruci elektroničke pošte korisnik se uvijek treba predstaviti svojim imenom i prezimenom, nazivom radnog mjesta ali i nazivom i adresom sjedišta Ministarstva, odnosno institucije.
10. Svi korisnici ispod svog potpisa u porukama elektroničke pošte trebaju obavezno imati sljedeći tekst, na hrvatskom i na engleskom jeziku, odricanja od odgovornosti:

Ova elektronička poruka i njeni prilozi mogu sadržavati povlaštene i/ili povjerljive informacije. Molimo Vas da poruku ne čitate ako niste njen naznačeni primatelj. Ako ste ovu poruku primili greškom, molimo Vas da o tome obavijestite pošiljatelja te da izvornu poruku i njene privitke obrišete bez čitanja ili bilo kakvog pohranjivanja. Svaka je neovlaštena upotreba, distribucija, reprodukcija ili priopćavanje ove poruke nije dozvoljena. S obzirom na nepostojanje potpune sigurnosti e-mail komunikacije, - - NAZIV INSTITUCIJE - - ne može bezrezervno preuzeti odgovornost za sadržaj ove poruke, odnosno za posljedice radnji koje bi proizašle iz informacija koje se nalaze u poruci. - - NAZIV INSTITUCIJE - - ne preuzima odgovornost za eventualnu štetu nastalu uslijed zaraženosti e-mail poruke virusom ili drugim zlonamjernim programom, ometanja prijenosa podataka i elektroničkih poruka kao i pogrešne ili zakašnjele dostave poruke do koje je došlo uslijed tehničkih problema. - - NAZIV INSTITUCIJE - - zadržava pravo nadziranja i pohranjivanja e-mail poruka koje se šalju iz ili pristižu u - - NAZIV INSTITUCIJE - -.

Molim ne ispisujte ovaj e-mail osim ako je to zaista potrebno.

This e-mail and its attachments may contain inside and/or confidential information. Please do not read the message if you are not its intended recipient. If you have received this message in error, please inform the sender and delete the original message and its attachments without reading or storing it in any way. Any unauthorized use, distribution, reproduction or communication of this message is prohibited. Due to the lack of complete security of e-mail communication, - - NAME OF THE INSTITUTION - - does not assume responsibility for the content of this message, i.e. for the consequences of actions that would result from the information provided. --NAME OF THE INSTITUTION-- does not take responsibility for any damage caused by infection of this e-mail message with a virus or other harmful program, unauthorized interference, erroneous or delayed delivery of the message due to technical issues. - - NAME OF THE INSTITUTION - - reserves the right to monitor and store e-mail messages sent from -- NAME OF THE INSTITUTION - - or arrive in it.

Please do not print out this e-mail unless it is highly necessary.

11. Organizacijska jedinica Ministarstva zadužena za informatičke poslove omogućit će svim korisnicima računa elektroničke pošte na domenama kojima upravlja automatsko dodavanje poruke o odricanju od odgovornosti na kraju elektroničke poruke.

Korisnici koji u svojim potpisima već imaju napisanu poruku o odricanju od odgovornosti trebaju je obrisati.

12. U kontekstu poruke elektroničke pošte korisnik uvijek mora voditi računa da primatelj može biti osoba čiji se jezik, kultura ili način komunikacije mogu znatno razlikovati od njegovog.
13. Kontaktira li korisnik s inozemstvom, s državama u kojim se ne koriste dijakritički znakovi (č, ć, đ, š, ž), potrebno je izbjegavati njihovo korištenje u poruci elektroničke pošte i dokumentima jer ona kod tih primatelja vjerojatno neće biti vidljiva. U tom slučaju za zamjenu se može koristiti č=c, ć=c, đ=dj, š=s, ž=z.
14. Pri imenovanju datoteka za privitak, zbog kompatibilnosti između računalnih operativnih sustava, preporuka je izbjegavati korištenje hrvatskih dijakritičkih znakova (č, ć, đ, š, ž) kao i dugačke nazive.

15. Korisniku sustava elektroničke pošte zabranjeno je:

- slanje komercijalnih oglasa (*spam mail*)
- slanje veće količine nezatraženih poruka (koje nisu rezultat radnih zadataka koje korisnik obavlja) na istu adresu elektroničke pošte, slanje poruka kojim se zahtijeva ili sudjeluje u tzv. lancima sreće
- lažno predstavljanje u sustavu elektroničke pošte
- krivotvorenje zaglavlja poruke elektroničke pošte
- uznemiravanje putem poruka elektroničke pošte u bilo kojem obliku
- činiti radnje koje predstavljaju kršenje pozitivnih domaćih i međunarodnih propisa.

16. Pri slanju privitaka bilo bi dobro da je korisnik upoznat s time da primatelj na svome računalu ima odgovarajuće aplikacije kojima te dokumente može pregledati. Pri slanju privitaka pošiljatelj je dužan voditi računa da ne krši autorska prava, poslovnu tajnu ili pozitivne propise.

17. Korisnik ne smije elektroničkom poštom slati nezaštićene osjetljive i povjerljive podatke (poput tajnih ili povjerljivih dokumenata, dijelova poslovnih baza podataka, pina kartice ili lozinke za pristup računalnom sustavu, osobnih podataka itd.) zato što je standardna elektronička poruka nezaštićeni medij za prijenos informacija i podataka.

18. Ako se osobni podaci za službenu upotrebu šalju elektroničkom poštom, na vrhu elektroničke poruke obavezno treba staviti napomenu kako se radi o podacima za službenu upotrebu, odnosno oznaku "Neklasificirano". Također, osobne podatke je potrebno kriptirati. Ako nije dostupan neki od profesionalnih programa, za kriptiranje se može koristiti program za arhiviranje koji ima opciju kriptiranja arhivirane datoteke. Minimalna duljina lozinke koju je potrebno postaviti treba biti 14 znakova. Lozinku je potrebno primatelju poslati drugim komunikacijskim kanalom (npr. SMS porukom) umjesto elektroničkom poštom.

Ako je potrebno poslati pristupne podatke za neki od informacijskih sustava ili za informatičko-komunikacijsku infrastrukturu, onda se nikada ne smije učiniti da se svi podaci šalju elektroničkom poštom. Elektroničkom poštom može se poslati korisničko ime dok se lozinka može poslati drugim komunikacijskim kanalom (npr. SMS porukom).

19. Korisnik nikada ne smije otvarati privitak ili odabirati poveznicu (link) ako nije siguran da su oni namijenjeni njemu ili ako ima sumnju u vjerodostojnost poruke ili adrese elektroničke pošte s koje mu je poruka upućena. Takve poruke elektroničke pošte može prosljediti organizacijskoj jedinici Ministarstva zaduženoj za informatičke poslove radi upute što dalje treba učiniti s tom porukom.

20. Obavezno je periodično brisanje ili arhiviranje elektroničke pošte (kako iz mape *Ulazna pošta*, tako i iz mapa *Poslano* i *Obrisano*). Ovakvim postupanjem izbjegavaju se

upozorenja o prekoračenom limitu prostora za pohranu elektroničkih poruka i omogućuje se nesmetan rad poslužitelja elektroničke pošte.

Veličina sandučića elektroničke pošte korisnika uvjetovana je mogućnostima sustava, te se mogu uvesti ograničenja. U slučaju približavanja granici ograničenja korisnik dobiva automatiziranu poruku elektroničkom poštom od računalnog sustava Ministarstva o približavanju granici ograničenja. Nakon prekoračenja veličine prostora, sustav automatski onemogućava daljnje primanje i slanje pošte sve dok korisnik dovoljno ne isprazni sandučić elektroničke pošte. Privitke (dokumente, fotografije i sl.) u poruci elektroničke pošte korisnik treba koristiti onda kada je to neophodno i paziti na njihovu veličinu.

Maksimalna je veličina privitka koju korisnik elektroničke pošte Ministarstva može poslati 35 MB, međutim, za korisnike elektroničke pošte izvan Ministarstva ta veličina ovisi o njihovom pružatelju usluga elektroničke pošte i postavljenim ograničenjima. To znači da e-mail poruka koja ima priloge veće od ograničenja primateljeva e-mail poslužitelja neće biti dostavljena primatelju.

7. Edukacija korisnika

1. Ministarstvo će za sve korisnike informacijskih sustava i informatičko-komunikacijske infrastrukture organizirati edukacije o aktualnim kibernetičkim prijetnjama, načinima prepoznavanja kibernetičkih prijetnji, najboljim kibernetičkim sigurnosnim praksama, te o osnovnim praksama kibernetičke higijene i podizanja svijesti o rizicima i kibernetičkim prijetnjama.

Sudjelovanje na ovim edukacijama obavezno je za sve korisnike bez obzira na radno mjesto, funkciju, položaj i radno iskustvo.

Svaki korisnik obavezan je jednom u najviše tri godine pohađati edukaciju s novostima o aktualnim kibernetičkim prijetnjama i njihovom prepoznavanju.

2. Službenik zadužen za slanje obavijesti organizacijskoj jedinici Ministarstva zaduženoj za informatičke poslove (isti službenik koji se navodi u poglavlju 5. *Uporaba informacijsko-komunikacijske infrastrukture* u točki 10.) redovito će ju obavještavati o zaposlenicima za koje je potrebno održati edukaciju.

Obavijesti se šalju najmanje svakih 6 mjeseci ili po zahtjevu organizacijske jedinice Ministarstva zadužene za informatičke poslove elektroničkom porukom na adresu ks.edukacije@mrosp.hr ili na način koji odredi organizacijska jedinica Ministarstva zadužena za informatičke poslove.

3. Sadržaj edukacije donosi organizacijska jedinica Ministarstva zadužena za informatičke poslove.
4. Organizacijska jedinica Ministarstva zadužena za informatičke poslove povremeno će organizirati radionice za povećanje digitalnih kompetencija i učinkovito korištenje pojedinih programa i programskih alata. Rukovoditelji institucija trebaju omogućiti zainteresiranim korisnicima prijavu i sudjelovanje na radionicama.

8. Kibernetički incident

1. U slučaju sumnje na kibernetički incident ili u slučaju da je neosporno došlo do kibernetičkog incidenta, korisnik koji o tome ima saznanja treba odmah, bez odgode, obavijestiti organizacijsku jedinicu Ministarstva zaduženu za informatičke poslove.

Ako je korisnik koji je uočio kibernetički incident ujedno zaposlenik neke od institucija koje koriste informacijske sustave i informatičko-komunikacijsku infrastrukturu kojom upravlja Ministarstvo, o kibernetikom incidentu odmah mora obavijestiti i odgovornu osobu u svojoj instituciji.

U slučaju da se kibernetički incident dogodio na dijelu sustava kojim upravlja Ministarstvo (informacijski sustavi i informatičko-komunikacijska infrastruktura kojima upravlja Ministarstvo) obavezu prijave incidenta preko nacionalne platforme PiXi (nacionalne platforme za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima) preuzima Ministarstvo.

Ako se kibernetički incident ili sumnja na kibernetički incident dogodio na informacijskom sustavu koji koristi institucija ali njome ne upravlja Ministarstvo, institucija je obavezna sama prijaviti sumnju ili incident putem platforme PiXi ili e-mailom prema NCSC-HR (Nacionalni centar za kibernetičku sigurnost) pri SOA-i.

Institucije koje osim informatičko-komunikacijske infrastrukture Ministarstva, koriste pristup i infrastrukturu drugih tijela (na primjer domenu skole.hr kojom upravlja CARNet), ako dođe do sumnje ili incidenta na toj domeni ili infrastrukturi dužni su odmah po otkrivanju obavijestiti vlasnika domene i tijelo koje upravlja infrastrukturom te postupiti sukladno dogovoru.

2. U slučaju pojave kibernetičkog incidenta na informacijskim sustavima ili informatičko-komunikacijskoj infrastrukturi kojima upravlja Ministarstvo, Ministarstvo će postupiti prema Proceduri postupanja u slučaju kibernetičkog incidenta.
3. Ako je tijekom rada na informacijskom sustavu došlo do pogreške koja ima štetne posljedice za druge osobe ili institucije, korisnik koji je to primijetio obavezan je odmah o tome izvijestiti onoga tko je oštećen, a zatim i administratora sustava te organizacijsku jedinicu Ministarstva zaduženu za informatičke poslove.

9. Upoznavanje korisnika s Protokolom

1. Organizacijska jedinica Ministarstva zadužena za informatičke poslove svakom novom korisniku informacijskog sustava, nakon otvaranja korisničkog računa poslat će e-mail u kojem će biti priložen Protokol kao i poveznica za stalni pristup aktualnoj verziji.
2. Prilikom izmjene sadržaja Protokola, organizacijska jedinica Ministarstva zadužena za informatičke poslove elektroničkom poštom obavijestit će sve korisnike informacijskih sustava o napravljenoj izmjeni, a obavijest će biti postavljena i na Intranet stranicama it.mrosp.hr koje su dostupne svim korisnicima i na kojima se nalazi objavljen tekst Protokola.

KLASA: 650-01/25-03/08

UR.BROJ: 524-02-03-01/6-25-1

Zagreb, 16.10.2025.

