Politike i protokoli za medije

Zaštita podataka o ličnosti i digitalna sigurnost

Zaštita podataka o ličnosti

Politika privatnosti je dokument koji je potrebno izraditi sa ciljem da se publici kojoj je namjenjena daju informacije o tome zbog čega i na koji način rukovalac koristi i obrađuje podatke o ličnosti tih lica.

Dužnost obavještavanja proizilazi iz zakonske obaveze kontrolora[1] da unaprijed pruže zakonom propisane informacije licima čiji se podaci prikupljaju. Kako bi tražene informacije bile unaprijed dostupne zainteresovanim licima, standardna praksa je da politika privatnosti bude javno objavljena na sajtu rukovaoca.

Tekst ispod je primjer obrasca kojim rukovalac može opisati obrade podataka o ličnosti koje prikuplja putem svoje web stranice u okviru politika privatnosti. Naslovi ovog primjera prate obavezne informacije koje je rukovalac dužan da pruži prema Zakonu o zaštiti ličnih podataka i drugim važećim propisima.

U fusnota ase nalaze objašnjenja kako da se ovaj primjer prilagodi za potrebe konkretnog rukovaoca. U tom smislu, potrebno je da se u okviru svake tačke (naslova) unesu informacije koje su relevantne za konkretnog rukovaoca, uključujući i informaciju o tome da se neke obrade ne vrše. Nakon finaliziranja teksta sa potrebnim informacijama fusnote je potrebno izbrisati.

Ukoliko rukovalac ne prikuplja lične podatke, preporuka je da na web stranici objavi obavještenje u kojem se to i konstatuje.

Primjer konkretne politika privatnosti koji su izrađeni u skladu sa ovim preprukama, a koje je izradila SHARE Fondacija iz Srbije se nalaze ovdje.

Preuzmite dokument politika privatnosti u Word dokumentu.

[1] Svaki javni organ, fizičko ili pravno lice, agencija ili drugi organ koji samostalno ili zajedno sa drugim vodi, obrađuje i utvrđuje svrhu i način obrade ličnih podataka na osnovu zakona ili propisa.

Politika privatnosti

U daljem tekstu se možete informisati o tome u kojim situacijama, za koje svrhe i na koji način dole navedeni rukovalac obrađuje podatke o ličnosti, a uzimajući u obzir informacije koje su rukovaoci dužni da predoče prema odredbama Zakona.[2]

1) Identitet i kontakt podaci rukovaoca

<Naziv>
<Adresa>
<Grad, Država>

2) Kontakt podaci rukovaoca u vezi sa zaštitom podataka o ličnosti

<navesti kontakt podatke>

3) Svrha obrade, izvor podataka i pravni osnov za obradu[3]

Svrha[4]	***Vrsta[5] i izvor podataka[6]***	***Pravni osnov[7]***
<navesti svrhu obrade podatka>	<navesti načine prikupljanja i izvore podataka za ovu svrhu>	<navesti pravni osnov za obradu podatka za ovu svrhu>
<navesti svrhu obrade podatka>	<navesti načine prikupljanja i izvore podataka za ovu svrhu>	<navesti pravni osnov za obradu podatka za ovu svrhu>

ili

[2] Predložak predstavljen u ovom poglavlju treba uskladiti sa tačno određenim podacima o ličnosti koje je organuzacija koja radi na uspostavljanju politika privatnosti dužna predočiti, a u skladu sa Zakonom o zaštiti ličnih podataka te države.

[3] Informacije u okviru ovog naslova mogu biti date tekstualno ili u obliku tabele. U finalnom dokumentu je potrebno obrisati tabelu, odnosno narativni tekst, u zavisnosti od toga o kojoj se od te dvije forme daju informacije u okviru ovog naslova.

[4] Svrha može biti na primjer: davanje komentara na sajtu; popunjavanje kontakt forme na sajtu; učestvovanje u anketama; prijava na newsletter; registracija na sajt; doniranje rukovaocu, itd.

[5] Vrste podataka mogu biti na primjer: ime; email adresa; telefon; IP adresa; sadržaj komentara ili poruke; broj bankovnog računa, itd.

[6] Podaci se mogu prikupljati direktno od lica koje ih daje rukovaocu – na primjer tako što ih lice samo upisuje na sajtu, ili indirektno – na primjer iz javno dostupnih izvora.

[7] Pravni osnov za obradu može biti pristanak lica, legitimni interes rukovaoca, ugovor koji rukovalac ima sa licem ili ispunjenje zakonskih obaveza rukovaoca. Ukoliko niste sigurni, potrebno je da po pitanju odgovarajućeg pravnog osnova konsultujete pravnika.

<u formi narativnog teksta navesti / opisati posebno svaku svrhu, informaciju o tome na koji način su prikupljeni podaci za ispunjenje te svrhe i po potrebi o kojim podacima se radi, kao i koji je pravni osnov za svaku posebnu svrhu>

4) Primaoci podataka o ličnosti[8]

Podatke o ličnosti rukovalac deli sa <navesti primaoce podataka tj. organizacije sa kojima se podaci dele>.

5) Iznošenje podataka o ličnosti u drugu državu[9]

Podaci o ličnosti se obrađuju u <navesti zemlje u kojima se podaci čuvaju / hostuju>.

6) Rok čuvanja podataka o ličnosti tj. kriterijumi za njegovo određivanje[10]

<navesti rok čuvanja podataka, tj. trenutak nakon kog se podaci brišu, pri čemu ukoliko ima više svrha, potrebno je navesti različite rokove za svaku od svrha obrade>.

7) Prava lica na koje se podaci odnose

Bilo koje lice na koje se podaci koje obrađujemo odnose ima pravo da zahtjeva od rukovaoca:

- da ga istinito i potpuno obavijesti o obradi njegovih podataka;
- pravo na uvid i/ili kopiju podataka koji se na njega odnose;
- pravo na ispravku i dopunu pogrešnih ili nepotpunih podataka, u bilo koje vreme;
- pravo na brisanje, kome se može udovoljiti u skladu sa zakonskim uslovima, odnosno kada: podaci o ličnosti više nisu neophodni za ostvarivanje svrhe zbog koje su prikupljeni ili na drugi način obrađivani; lice na koje se podaci odnose je podnijelo prigovor na obradu po osnovu legitimnog interesa rukovaoca, a nema drugog pravnog osnova za obradu; podaci o ličnosti su nezakonito obrađivani; podaci o ličnosti moraju biti izbrisani u cilju izvršenja zakonskih obaveza rukovaoca;
- pravo na ograničenje obrade, kome se može udovoljiti ukoliko su ispunjeni propisani uslovi: ako je lice na koje se podaci odnose osporilo tačnost podataka o ličnosti, a rukovaocu je potrebno vrijeme koje mu omogućava da provjeri tačnosti; ako je obrada nezakonita, a lice se protivi brisanju i umesto brisanja zahtjeva ograničenje upotrebe podataka; rukovaocu više nisu potrebni

---

[8] Uneti primaoce podataka, sa kojima rukovalac deli podatke (radi razumevanja, preporuka je da se navede i razlog zbog kojih se podaci dele). To mogu biti poslovni saradnici, povezana privredna društva ili organizacije, kurirske službe, pravni i finansijski konsultanti, nadležni državni organi, itd. Ukoliko nema primalaca sa kojima se podaci o ličnosti dele, tako u okviru ovog naslova treba i napisati.

[9] Unijeti informacije o tome u kojim se sve zemljama obrađuju podaci. Po potrebi provjeriti gde je web stranica hostovana. Ukoliko se podaci obrađuju u zemljama koje se ne smatraju adekvatnim prema mjerodavnim propisima, navesti pravni osnov za prenos podataka u neadekvatne zemlje.

Na primjer: *Podaci o ličnosti se obrađuju u Srbiji i u Indiji. Prenos podataka u Indiju, koja se ne smatra zemljom koja obezbeđuje adekvatan nivo zaštite podataka, regulisan je i obezbeđen Standardnim ugovornim klauzulama.*

[10] Primjeri za rok čuvanja mogu biti: podaci o ličnosti koje dajete prilikom ostavljanja komentara se čuvaju trajno tj. ne brišu se kao ni sami komentari; email koji ste dali u cilju slanja newletter-a se briše kada se odjavite; podaci koje dajete u kontakt formi na web stranici se čuvaju najviše godinu dana od slanja poruke.

podaci o ličnosti za ostvarivanje svrhe obrade, ali ih je lice zatražilo u cilju podnošenja, ostvarivanja ili odbrane pravnog zahteva; ili je lice već podnelo prigovor na obradu, a u toku je procenjivanje da li pravni osnov za obradu od strane rukovaoca preteže nad interesima lica;

- prenos podataka u mašinski čitljivoj formi, koje postoji u slučajima kada je to primenljivo, tj. ako je to tehnički moguće jer su podaci mašinski čitljivi i kada je pravni osnov za obradu pristanak lica ili ugovorni odnos sa licem na koje se podaci odnose.
- pravo da u bilo kom trenutku povuče svoj pristanak na obradu određenih podataka, ukoliko je pristanak pravni osnov za obradu.

Lice takođe ima pravo na prigovor, ukoliko lice na koje se podaci odnose smatra da legitimni interes rukovaoca na osnovu kog se podaci obrađuju nije opravdan, odnosno da ugrožava prava, slobode i interese tog lica.

U slučaju da se vrši automatizovana obrada podataka o ličnosti i donošenje odluka, lice ima pravo na ljudsku intervenciju, kao i pravo na izražavanje stava o odluci ili osporavanje odluke.

8) Pravo da se podnese pritužba

Lice ima pravo da na postupanje rukovaoca podnese pritužbu nadležnom organu u skladu sa Zakonom države u kojoj rukovalac posluje.

9) Postojanje automatizovanog donošenja odluke, uključujući profilisanje[11]

Rukovalac ne vrši automatizovano donošenje odluka, niti profilisanje, na osnovu podataka o ličnosti.

10) Politika kolačića[12]

<U ovom naslovu je dat samo primjer kako rukovalac može opisati korišćenje kolačića na svojoj web stranici. Ukoliko želite da koristite donji tekst, potrebno ga je prilagoditi konkretnoj web stranici>.

"Kolačić" je mali podatak koji web stranica može poslati vašem pretraživaču, a koji se onda može čuvati na hard disku. Ako ste zabrinuti zbog vaše privatnosti i korištenja tehnologije "kolačići", možete podesiti pretraživač da vas obavijesti kada primite "kolačić". Kolačići vam mogu pomoći da budete efikasniji i da

[11] Mediji najčešće ne vrše profilisanje (pravljenje jedinstvenih profila) i automatizovano donošenje odluka o pravima i interesima posjetilaca svojih web stranica (donošenje odluka bez ljudske intervencije, već samo putem „algoritama“). Ukoliko rukovalac to ipak radi, ovde je potrebno jasno i razumljivo objasniti svrhe i načine na koje se takva obrada vrši.

[12] Ukoliko koristite kolačiće koji mogu da dovedu do direktne ili posredne identifikacije određenih korisnika vaše web stranice (putem bilo kog jedinstvenog identifikatora), korištenje takvih kolačića se takođe smatra obradom podataka o ličnosti.
U tom slučaju, potrebno je prvo da odredite da li postoje neki kolačići za koje imate legitimni interes da ih koristite (poput strogo neophodnih kolačića), što je u tom slučaju pravni osnov za obradu podataka.
Sve ostale kolačiće je moguće koristiti samo na osnovu pristanka posjetioca web stranice.
Stoga je tada potrebno i preporučljivo da omogućite pop-up opciju u kojoj bi posjetioci web stranice imali mogućnost da odbiju sve kolačiće koji se ne mogu pravdati legitimnim interesom, poput analitičkih, marketinških i kolačića trećih strana.

imate koristi od funkcija «memorije», na primjer kada web stranica pamti vaš jezik na kome ste pregledali stranicu iz prethodne posjete. Kolačići vam omogućavaju da sačuvate svoje preferencije, da sačuvate proizvode i usluge i da prilagodite stranice.

Rukovalac koristi kolačiće na svom sajtu u cilju pružanja usluga i funkcionalnosti svojim korisnicima. Možete ograničiti ili onemogućiti upotrebu kolačića preko svog internet pretraživača, ali bez kolačića nećete moći da koristite sve funkcionalnosti sajta.

Postoje različite vrste kolačića, a prema kriterijumu ko postavlja kolačiće na web stranicu razlikujemo:

- kolačiće prve strane (first party cookies) – kolačići koje postavlja rukovalac kada koristite web stranicu, i
- kolačići trećih strana (third party cookies) – kolačići koje postavlja neka druga organizacija kada koristite web stranicu (neke web stranice mogu takođe sadržati sadržaje sa drugih stranica koji mogu postaviti sopstvene kolačiće).

Što se tiče namjene, koristimo sljedeće vrste kolačića na sajtu:

- Strogo neophodni kolačići – ovi kolačići koji su neophodni za upravljanje statusom vaše veze.
- Funkcionalni kolačići - ovi kolačići omogućavaju internet stranici da zapamti vaše prethodne radnje kako bi vam pružio napredne funkcionalnosti.
- Analitički kolačići - ovi kolačići nam omogućavaju da prikupljamo podatke o vašem korištenju internet stranice u cilju poboljšanja njenog učinka i dizajna. Da biste onemogućili kolačiće Google analitike, preuzmite i instalirajte ovaj dodatak.
- Marketinški kolačići - ovi kolačići koji se koriste za prikupljanje različitih informacija o vašoj posjeti našoj stranici, kao što su informacije o sadržaju koji ste pregledali, vezama koje ste pratili, vašem pretraživaču, uređaju ili IP adresi.

Digitalna sigurnost

Interne sigurnosne poltike

Digitalna sigurnost je od ključnog značaja za medijske organizacije i fizička lica koji ih čine, odnosno novinare i druge zaposlene, kao i izvore sa kojima novinari dolaze u kontakt prilikom istraživanja. Kako bi korištenje tehnologije prilikom obavljanja njihovog posla bilo što sigurnije, mediji bi trebalo da usvoje odgovaraju'e politike i procedure koje će im u tome pomoći. U slučaju tehničkih incidenata, kao što su napad na web stranicu medija ili preuzimanje naloga, ove politike mogu biti od pomoći da se šteta po resurse organizacije spriječi ili makar svede na minimum.

U zavisnosti od kapaciteta i rasursa organizacije, u kreiranju internih sigurnosnih politika se podrazumijeva učešće menadžmenta, uredništva, članova tima zaduženih za IT, kao i novinara i drugih zaposlenih koji posjeduju naprednije tehničke vještine koje mogu prenijeti drugima. Obuka i edukacija zaposlenih su značajne kako bi se procedure i politike primjenjivale, a da se pritom redovni procesi rada ne remete.

Svaki interni dokument u oblasti digitalne sigurnosti treba prilagoditi realnim potrebama i mogućnostima organizacije, da bude precizan i razumljiv svim interesnim stranama. Interne politike moraju biti dostupne u elektronskoj formi samo članovima tima, dakle ne javn. U te svrhe se mogu koristiti platform za internu komunikaciju poput Mattermost, Rocket.Chat, Element kako bi zaposleni u slučaju nedoumica ili rada van prostorija organizacije imali pristup dokumentaciji i mogli da se konsultuju sa kolegama ili osobama koje su nadležne za nadzor primjene politika, npr. urednici.

Primjeri internih dokumenata su politika lozinki, politika korištenja službenih e-mail adresa i pratećih naloga, kao i sigurnosni plan.

Politika lozinki

Cilj dokumenta ispod je da pomogne organizacijama da kreiraju jedinstvenu politiku za korištenje i upravljanje lozinkama, kako bi se obezbijedile jasne procedure. Politika lozinki omogućava organizaciji i njenim članovima sigurno kreiranje, korištenje, skladištenje i modifikaciju lozinki, koje predstavljaju osnovni mehanizam autentifikacije, odnosno zaštite organizacionih resursa od neovlaštenog pristupa.

_____ (Naziv organizacije)

1. Ova politika se primenjuje na lozinke (passwords) u upotrebi za zaštitu naloga, uređaja, dokumenata, baza podataka i drugih resursa kojima upravlja _____ (Naziv organizacije).

2. Jedna lozinka se ne smije koristiti za zaštitu više različitih resursa. Lozinke se ne smiju javno prikazivati i djeliti sa neautorizovanim osobama.

3. Ukoliko postoji tehnička mogućnost, neophodno je uvesti dvostruku verifikaciju prijave (2-step verification) na svaki resurs kojim upravlja _____ (Naziv organizacije).

4. Promjena svih lozinki za resurse kojima upravlja _____ (Naziv organizacije) vrši se na period od _____ meseci.

5. Lozinke moraju biti duge najmanje 15 karaktera, moraju sadržati posebne karaktere (npr. znaci interpunkcije), velika slova, mala slova i cifre. Lozinke ne smiju sadržati podatke o ličnosti zaposlenih (npr. imena, prezimena, datume rođenja, brojeve telefona, adrese stanovanja) niti njima bliskih lica (npr. članova uže porodice).

6. Za naročito osjetljive resurse (npr. baze koje sadrže podatke naročito osjetljive prirode: žrtve nasilja, zdravstveno stanje, seksualno opredjeljenje itd) neophodno je uvesti zaštitne fraze (passphrases) koje čine nizovi nasumično odabranih riječi u kombinaciji sa drugim obaveznim elementima za lozinke iz tačke 5. ove politike. Zaštitne fraze moraju da budu dužine najmanje 20 karaktera.

7. Lice u organizaciji zaduženo za administriranje lozinkama je _____ (ime i prezime, radno mesto).

8. Po dodjeli lozinke za naloge koji se koriste za poslove i aktivnosti _____ (Naziv organizacije), kao što su recimo službeni e-mail nalozi, zaposleni su dužni da datu lozinku promjene u skladu sa ovom politikom odmah pošto je dobiju od nadležnog lica koje je kreiralo nalog (npr. tehnički administrator) i dodjelio ga zaposlenom. Nove lozinke moraju biti generisane i skladištene u menadžeru lozinki.

9. Lozinke i zaštitne fraze se čuvaju u posebnim aplikacijama namjenjenim isključivo za upravljanje lozinkama (npr. KeePass, KeePassXC) koje čuvaju bazu lozinki na lokalnoj memoriji uređaja.

Čuvanje lozinki u internet pretraživačima (internet browsers) i na stranicama za online čuvanje lozinki nije dozvoljeno.

10. Pravljenje rezervne kopije baze lozinki koja se čuva na eksternoj memoriji (npr. eksterni hard disk, USB) se vrši prilikom svake izmjene lozinki i zaštitnih fraza (dodavanje novih ili mjenjanje starih) i obavezno se u nazivu fajla označava datum kada je napravljena.

11. U slučaju da zaposleni primjeti ili posumnja da je bilo koji resurs kojim upravlja _____ (Naziv organizacije) kompromitovan, odmah će o tome obavestiti nadređenog i promjeniti lozinku ili zaštitnu frazu za taj resurs, a ukoliko je riječ o resursu koji se zajednički koristi obavijestit će lice u organizaciji zaduženo za administriranje lozinkama.

12. Ova politika stupa na snagu ____ dana od dana donošenja.

Datum:_____ Ovlašteno lice organizacije:_____

Mjesto:_____

Politika korištenja email-a i pratećih naloga

Pomoću dokumenta ispod organizacije mogu da kreiraju jedinstvenu politiku za korištenje i upravljanje službenim e-mail nalozima i sa njima povezanim nalozima (tj. kompletnih paketa usluga za produktivnost koje nude provajderi kao što su Google ili Microsoft) kako bi bilo jasno u koje svrhe mogu da se koriste, kome se dodjeljuju, kako se postupa prilikom odlaska članova tima iz organizacije i tome slično. Politika naloga omogućava organizacijama i njenim članovima da nalozima u vlasništvu organizacije upravljaju na načine koji smanjuju moguće rizike u pogledu digitalne sigurnosti i koriste ih u skladu sa propisanim svrhama.

Naziv i adresa organizacije

Politika korištenja email i pratećih naloga _____ (naziv organizacije)

U ovoj politici su sadržani uslovi korištenja email i pratećih naloga na internet domenima u vlasništvu _____, i to: _____ (upisati domene, npr. organizacija.rs) (u daljem tekstu: domeni _____).

1. Email i prateći nalozi kreirani za potrebe rada, obavljanja prakse i volontiranja u _____ su u vlasništvu _____.

2. _____ upravlja nalozima i izdaje ih na korišćenje licima koja su u radnom odnosu u _____, licima koja su na praksi i licima koja volontiraju.

3. Lice kome je izdat email nalog koristi nalog i _____ nema uvid u sadržaj tog naloga niti u njegove prateće dijelove (cloud storage, kolaborativni dokumenti i sl).

4. Nalozi na domenima _____ se koriste isključivo u svrhe koje odredi _____.

5. U slučaju prestanka odnosa između _____ i lica kome je izdat nalog, vlasništvo naloga ostaje kod _____.

6. _____ će ostaviti rok od 30 dana od dana prestanka odnosa da lice kome je izdat nalog prikupi iz naloga sav sadržaj koji smatra da će mu biti potreban.

7. Poslije isteka roka od 30 dana od prestanka odnosa nalog će biti izbrisan, a kopija sadržaja arhivirana za potrebe _____.

8. Politika stupa na snagu danom donošenja.

9. Lica kojima su dodeljeni nalozi će biti obaveštena o svakoj budućoj izmjeni ove politike.

Mjesto i datum, Odgovorno lice

_____

Sigurnosni plan

Sigurnosni plan ima za cilj da pomogne organizacijama da kreiraju preventivne i reaktivne mjere u pogledu tehničkih incidenata, razmotre moguće rizike i prijetnje po tehničku infrastrukturu organizacije, propišu procedure i korake u slučaju suočavanja sa različitim vrstama tehničkih incidenata, itd. Iako nije moguće predvidjeti scenario svakog pojedinačnog tehničkog napada, posjedovanje sigurnosnog plana može spriječiti ili umanjiti štetu i pomoći da se izvrši sanacija.

Prilikom izrade sigurnosnog plana, obratite pažnju na sljedeće:

Ciljevi: postavite realističan primarni cilj ili više sekundarnih ciljeva, kako bi propisane mjere zaista bile primjenjene zarad postizanja datih ciljeva.

Pretnje i rizici: razmislite o mogućim scenarijima ugrožavanja digitalne sigurnosti vaše organizacije i njenih članova, to će vam pomoći da preciznije identifikujete moguće prijetnje i rizike po digitalnu sigurnost i bolje se pripremite za suočavanje sa njima.

Preventivni koraci: navedite realistične korake koje možete da preuzmete u vezi sa zaštitom digitalne sigurnosti, uzimajući u obzir prijetnje, rizike i kapacitete same organizacije (tehničke, organizacione i kadrovske).

Koraci u slučaju incidenta: razmotrite moguće scenarije incidenta (npr. neovlašteno preuzimanje naloga na društvenim mrežama) i definišite neophodne korake u datim situacijama. Iako nije realistično predvidjeti sve scenarije, odaberite nekoliko za koje smatrate da su najrealističniji da se ostvare ili koji su se već dogodili vašoj organizaciji.

Preporučeni uređaji i oprema: napravite listu hardverskih i softverskih rješenja koja imaju dobru reputaciju i recenzije i preporučena su od strane ekspertske zajednice. Imajte na umu kapacitete organizacije, a ukoliko niste sigurni šta bi vašim potrebama najviše odgovaralo, potražite eksterni savet.

Primjena internih procedura: opišite konkretno primjenu vaših bezbednosnih procedura na više primera incidenata za koje smatrate da su najrealističniji da se ostvare ili sa kojima ste ranije imali iskustva u organizaciji.

Sigurnosni plan

CILJ	**Unaprijediti digitalnu sigurnost organizacije kao cjeline i njenih pojedinačnih članova**
PRIJETNJE I RIZICI	• Kompromitacija podataka o ličnosti i poverljivih informacija (dokumenti, prepiske...) • Kompromitacija tehničke infrastrukture i resursa organizacije • Gubitak kontrole nad infrastrukturom i podacima kao rezultat
PREVENTIVNI KORACI	• Pristup infrastrukturi i resursima organizacije (serveri, mrežna oprema, nalozi na društvenim mrežama, admin paneli web stranica, itd.) omogućen samo određenim licima i zaštićen jakim lozinkama koje se čuvaju u posebnim aplikacijama za tu namenu (password managers, npr. KeePass) • Usvojena politika lozinki organizacije • Dvostruka autentifikacija (2-step authentication) uključena na svim korisničkim nalozima koji je podržavaju. • Naročito osetljive podatke (npr. informacije o žrtvama seksualnog nasilja) čuvati enkriptovane, na posebnim uređajima koji se ne koriste za svakodnevni rad. • Uređaji zaposlenih zaštićeni lozinkama/pin kodovima • Redovno pravljenje rezervnih kopija podataka (backup) na lokalnim uređajima (npr. eksterni hard diskovi) i/ili onlajn (na serveru organizacije ili na cloud uslugama, npr. Dropbox, Google Drive, OneDrive...). **Međutim, naročito osetljive podatke o ličnosti i druge povjerljive informacije ne treba čuvati na cloud servisima.** • Za razmjenu poverljivih informacija koristiti enkriptovane e-mailove (PGP) i chat aplikacije (Signal).

KORACI U SLUČAJU INCIDENTA	• Što prije obavestiti nadležne kolege (administratore zadužene za tehničku infrastrukturu u organizaciji) i tehničku podršku (npr. hosting kompaniju) i pratiti njihove instrukcije • Prikupiti sve dostupne informacije o incidentu (vrijeme, mjesto, aktivnosti u toku incidenta, IP adrese, logovi, screenshots, posljednje ispravne konfiguracije...) kako bi se utvrdila šteta i posljedice • Obavijestiti posebne/sektorske timove za reakciju u slučajevima cyber incidenata, poput Nacionalnog CERT-a (Computer Emergency Response Team) • Prijaviti incident nadležnim državnim organima • Provjeriti posljednju dostupnu verziju podataka/konfiguracije sistema radi pokušaja vraćanja u prethodno stanje i rekonstrukcije
PREPORUČENI UREĐAJI I OPREMA	• Mobilni telefoni sa instaliranim enkriptovanim chat aplikacijama (Signal) • Računari: instaliran i redovno ažuriran anti-virus softver, kao i svi ostali softveri koji se koriste • Računari: instaliran menadžer lozinki (npr. KeePass, KeePassXC) • Računari: instaliran softver za enkripciju hard diska (VeraCrypt) • Kreirani PGP ključevi za mejlove zaposlenih i instaliran odgovarajući softver (npr. Thunderbird, Gpg4Win, Mailvelope) • Browsers: Mozilla Firefox, instalirani dodaci (HTTPS Everywhere, Privacy Badger, uBlock Origin, minerBlock, Facebook Container) ili Brave na kome se mogu instalirati verzije dodataka za Google Chrome • Na uređajima instaliran pouzdan VPN (npr. Mullvad, ProtonVPN) i Tor Browser

PRIMJENA INTERNIH PROCEDURA (PRIMJER)	Među zaposlenima je primjećeno je da je web stranica organizacije nedostupna ili da se teško učitava 1. Provjeriti dostupnost stranice na servisu “Down For Everyone Or Just Me” (https://downforeveryoneorjustme.com/) i internet konekciju 2. Izvršiti skeniranje svih računara i uređaja anti-virus softverom 3. Ukoliko se utvrdi da nije riječ o tehničkom problemu, zaposleni obavještava tehničkog administratora organizacije lično ili putem sigurnog kanala komunikacije (Signal čet, enkriptovana email poruka) 4. Administrator, u saradnji sa tehničkom podrškom, izvršava provjeru infrastrukture i ukoliko se utvrdi da je došlo do neuobičajenog saobraćaja, neovlaštenog pristupa ili druge povrede integriteta informacionog sistema, vrši prikupljanje digitalnih dokaza 5. Slijedi pokušaj povraćaja podataka/povraćaj funkcionalnosti pomoću rezervnih kopija i/ili posljednjih dobrih konfiguracija 6. Slijedi utvrđivanje vrste napada i pravne kvalifikacije, obavještavanje nadležnih organa i pripremanje podnesaka (npr. krivične prijave) u saradnji sa posebnim/sektorskim timovima