



**HRVATSKI INSTITUT ZA POVIJEST
POLITIKA INFORMACIJSKE SIGURNOSTI**

Zagreb, veljača 2025.

Na temelju članka 40. Statuta Hrvatskog instituta za povijest ravnatelj Hrvatskog instituta za povijest donosi sljedeću Politiku informacijske sigurnosti.

1. Opće odredbe

Pojmovi (u smislu ove Politike):

Povjerljivi podaci/dokumentacija: podaci namijenjeni ograničenom krugu ovlaštenih osoba (npr. osobni podaci, ugovori, interne odluke).

Osjetljivi podaci: podaci čije bi neovlašteno otkrivanje/izmjena mogla uzrokovati štetu Institutu ili pojedincima (uključuje i osobne podatke).

Zaštićena područja / sigurne zone: prostori s ograničenim pristupom zbog smještaja kritične opreme ili povjerljive dokumentacije.

Osjetljivi prostori: prostori u kojima se obrađuju/pohranjuju povjerljivi podaci ili se nalazi kritična oprema.

Svrha i ciljevi Politike: Ovom se Politikom utvrđuju pravila zaštite informacijskih sustava i opreme Instituta s ciljem osiguranja povjerljivosti, integriteta i dostupnosti podataka u njegovu radu.

Politika definira prihvatljiva i neprihvatljiva ponašanja pri korištenju informacijske tehnologije, jasno raspodjeljuje zadatke i odgovornosti sudionika te propisuje mjere u slučaju kršenja pravila.

Dokument je pisan razumljivim, službenim jezikom i prilagođen je akademskom okruženju. Provodeći ovu Politiku, Institut nastoji uspostaviti ravnotežu između liberalnog pristupa rada u znanstvenoj zajednici i potrebe za zaštitom sustava i opreme – naglasak je na edukaciji korisnika, uz minimalnu uporabu restriktivnih mjera nužnih za sigurnost.

Područje primjene: Politika se primjenjuje na sve informacijske resurse Instituta (Zagreb i Slavonski Brod) – svu računalnu i mrežnu opremu koja se nalazi u prostorijama Instituta, sav instalirani softver te sve mrežne usluge Instituta.

Pravila ove Politike obvezna su za sve osobe koje koriste informacijske sustave i opremu Instituta: sve zaposlenike Instituta i vanjske suradnike (ugovorne osobe) kojima je omogućen pristup sustavima i opremi Instituta.

(Napomena: Institut ne obuhvaća studente u svojem radu, pa se pravila vezana uz studente navode samo ako su primjenjiva.) Vanjske tvrtke ili osobe angažirane ugovorom za održavanje opreme ili usluga također su obvezne pridržavati se ove Politike.

Obuhvat domena i servisa: Politika se primjenjuje na sve informacijske resurse pod nadzorom Instituta, uključujući domene i mrežna sjedišta: isp.hr, hipzg.hr, hipsb.hr te povezane servise (repositorij, izdavačke platforme, web, e-pošta). Službena elektronička komunikacija provodi se isključivo putem institutske domene (@isp.hr / @hipzg.hr / @hipsb.hr). Generičke adrese trećih pružatelja (npr. Gmail) koriste se samo prijelazno i bez obrade osobnih ili povjerljivih podataka, uz obvezan 2FA (dvorazinsko ili višerazinsko sigurnosno potvrđivanje) i arhiviranje; cilj je njihovo postupno ukidanje u službenoj elektroničkoj komunikaciji.

Načela i usklađenost: Provedba Politike temelji se na načelima pouzdanosti, integriteta i dostupnosti informacija te poštovanju zakona Republike Hrvatske i EU-a. Posebno se vodi računa o usklađenosti s propisima iz područja zaštite osobnih podataka (GDPR) i sigurnosti informacijskih sustava. Ova Politika

stupa na snagu danom donošenja, a objavljuje se na mrežnim stranicama Instituta radi upoznavanja svih korisnika.

2. Organizacija upravljanja sigurnošću informacija

Raspodjela odgovornosti: Za učinkovitu primjenu ove Politike nužno je jasno odrediti uloge i odgovornosti svih sudionika te osigurati da svatko zna svoj posao i za što odgovara.

U tu svrhu Institut uvodi sljedeće uloge: korisnici informacijskih usluga, glavni korisnici pojedinih aplikacija, davatelji informatičkih usluga (sustavni i mrežni administratori) te po potrebi imenovani voditelj sigurnosti ili povjerenstvo za sigurnost. U nastavku su definirane odgovornosti pojedinih skupina.

2.1. Korisnici informatičkih usluga

Korisnicima se smatraju sve osobe koje se u svojem radu služe računalima, informacijskim sustavima i mrežnim uslugama Instituta, unose ili obrađuju podatke, ali nisu zadužene za održavanje sustava. Svaki korisnik mora biti svjestan svoje uloge u unaprjeđenju sigurnosti ukupnog sustava.

Osnovne dužnosti korisnika su:

- **Pridržavanje pravila prihvatljivog korištenja:** Računala i mreža Instituta smiju se koristiti isključivo za zakonite svrhe i aktivnosti u skladu s etičkim normama te internim pravilima Instituta. Zabranjena je uporaba institutske IT opreme za bilo kakve nedopuštene, ilegalne ili neetičke radnje.
- **Odabir sigurnih zaporki:** Korisnik je dužan odabrati kvalitetnu zaporku (lozinku) i povremeno ju mijenjati. Preporučuje se minimalna duljina zaporke od 8 znakova (nikako manje od 6), uz korištenje kombinacije velikih i malih slova, brojeva i drugih znakova. Ne smiju se koristiti opće riječi (posebice ne one iz rječnika), imena bliskih osoba, kućnih ljubimaca, datumi i sl., jer se takve zaporkе lako otkriju socijalnim inženjeringom. (Detaljna pravila za zaporkе propisana su u posebnom Pravilniku o rukovanju zaporkama.)
- **Zaštita zaporki:** Korisnik mora čuvati tajnost svoje zaporke. Zaporka se ni u kojem slučaju ne smije otkriti drugoj osobi, pa ni sistem administratoru. Zaporkе se ne smiju zapisivati na papiriće zalijepljene na monitore, držati u nezaključanim ladicama ili općenito ostavljati na dostupnim mjestima. U slučaju zaboravljene zaporke korisnik treba kontaktirati administratora radi postavljanja nove.
- **Odgovornost za čuvanje podataka:** Svaki korisnik koji stvara ili obrađuje podatke dužan je pobrinuti se za njihovo sigurno čuvanje. Važne podatke potrebno je redovito sigurnosno kopirati. Korisnik treba zatražiti od IT službe uspostavu automatske izrade sigurnosnih kopija (backup) ili ih sam izrađivati, u skladu s internim pravilima o izradi sigurnosnih kopija.
- **Zaštita službenih dokumenata:** Elektronički dokumenti smatraju se službenima jednako kao i pisani, stoga ih je potrebno odgovarajuće zaštititi. Povjerljivi elektronički dokumenti moraju biti pohranjeni na sigurnoj lokaciji (npr. na poslužitelju uz kontrolu pristupa) i zaštićeni od neovlaštenog uvida, jednako kao i papirnati dokumenti.

Korisnici su također dužni prijaviti svaki sigurnosni incident ili sumnju na incident (npr. pojava virusa, neovlašten pristup, gubitak podataka, kvarovi opreme) čim ga uoče da bi se problem brže riješio i spriječila veća šteta. Detaljan postupak prijave i rješavanja incidenata definiran je u Pravilniku o rješavanju sigurnosnih incidenata.

2.2. Glavni korisnik aplikacije

Za svaku važniju poslovnu aplikaciju koju Institut koristi (npr. aplikacija za računovodstvo, matične evidencije i sl.) ravnatelj imenuje glavnoga korisnika aplikacije. Glavni korisnik je tipično voditelj odsjeka ili osobe zadužene za to poslovno područje (npr. voditelj računovodstva za financijsku aplikaciju).

Odgovornosti glavnog korisnika uključuju: provjeru točnosti i integriteta podataka koje djelatnici unose u sustav; provjeru ispravnosti i sigurnosti same aplikacije; upravljanje korisničkim pristupima aplikaciji (dodjela i oduzimanje ovlasti za pristup podacima); te suradnju s informatičkom službom i dobavljačem aplikacije na održavanju sigurnosti. Glavni korisnik kontaktira proizvođača softvera radi nabave nadogradnji i ispravaka, zahtijeva ugradnju sigurnosnih mehanizama i sl.

Ukratko, glavni korisnik osigurava da se aplikacija koristi na pravilan i siguran način i da se njome obrađeni podaci štite od neovlaštenih izmjena.

2.3. Davatelji informatičkih usluga (administratori)

Pod davateljima informatičkih usluga podrazumijevaju se djelatnici (ili ugovorni serviseri) zaduženi za tehničko održavanje i administriranje računalne i mrežne opreme te informacijskih sustava Instituta. U Hrvatskom institutu za povijest to su sistem inženjer, odnosno specijalisti informatičke službe i informatički referent koji je CARNET sistem inženjer. Administratori su odgovorni za ispravan i neprekidan rad informacijskog sustava Instituta, kao i za provedbu svih mjera zaštite definiranih ovom Politikom i pratećim pravilnicima.

Za sustave i mrežnu opremu koji su smješteni kod vanjskog pružatelja usluga (npr. cloud infrastruktura, poslužitelji, backup, IP telefonija) odgovornost za održavanje i administriranje snosi ugovorni partner u skladu s ugovorom o pružanju usluga. Administratori Instituta u tim slučajevima imaju pravo pristupa i nadzora, ali nisu primarno odgovorni za tehničko održavanje.

Odgovornosti administratora obuhvaćaju:

Administriranje računala: Svako računalo i poslužitelj mora imati imenovanog odgovornog administratora, koji se brine o ispravnoj instalaciji i konfiguraciji softvera. Administratori moraju konfigurirati svako računalo na siguran način – primjenjujući sve dostupne sigurnosne zakrpe proizvođača softvera, postavljajući odgovarajuće postavke vatrozida, liste pristupa, filtre mrežnog prometa i druge zaštitne mehanizme.

Posebnu pozornost dužni su posvetiti uređajima i poslužiteljima koji obavljaju kritične funkcije ili sadržavaju vrijedne i povjerljive informacije – takvi sustavi moraju biti zaštićeni od neovlaštenog pristupa na najvišoj razini.

Praćenje sustava: Administratori svakodnevno nadziru rad sustava – provjeravaju systemske zapisnike (logove), prate korištenje mrežnih servisa i aktivnosti korisnika, da bi na vrijeme uočili nedopuštene aktivnosti ili probleme.

Ako opaze nešto sumnjivo ili incident, dužni su o tome odmah obavijestiti voditelja sigurnosti (ili odgovornu osobu) i po potrebi pomoći u istrazi i otklanjanju problema.

Svaki incident treba dokumentirati radi lakšeg sprječavanja sličnih situacija ubuduće. Ako je riječ o ozbiljnom incidentu koji može predstavljati kršenje zakona, administrator je dužan obavijestiti

nadležna tijela (Nacionalni CERT za kibernetičke incidente, Ministarstvo unutarnjih poslova Republike Hrvatske (MUP).

Zaštita privatnosti i povjerljivosti: Administratori tijekom obavljanja posla mogu doći u doticaj s povjerljivim podacima korisnika. Obvezni su čuvati tajnost svih informacija do kojih dođu te poštovati privatnost korisnika sustava. Da bi se to osiguralo, svaki administrator i vanjski serviser mora potpisati Izjavu o čuvanju povjerljivih informacija (ugovor o povjerljivosti) prije nego što dobije pristup sustavima Instituta.

Također, administratori ne smiju nikad od korisnika tražiti njihove osobne zaporke – stručan administrator može riješiti tehnički problem i ako ne zna korisničku lozinku (uz uvjet da se na osobnom računalu korisnika nalazi administratorski račun postavljen od institutskih administratora).

Poštovanje pravila struke: Administratori su dužni primjenjivati općeprihvaćene stručne standarde pri administriranju sustava, paziti da tehničke intervencije minimalno ometaju funkcionalnost sustava te da svaka promjena bude u skladu s internim pravilima i procedurama Instituta. Administratori ne smiju samoinicijativno isključivati sigurnosne mehanizme (npr. antivirusni program, zapisivanje logova i dr.) na sustavima osim privremeno i uz opravdan razlog, o čemu moraju obavijestiti nadređenog.

(Napomena: Ako napredni korisnik želi sam administrirati svoje računalo, mora za to dobiti odobrenje i potpisati izjavu da će se pridržavati pravila administriranja. U tom slučaju prema njemu će se primjenjivati sva pravila koja vrijede za administratore sustava.)

2.4. Voditelj sigurnosti informacijskog sustava

Institut može imenovati voditelja informacijske sigurnosti (engl. Chief Security Officer – CSO) – osobu posebno zaduženu za organizaciju i nadzor provođenja mjera sigurnosti. Poželjno je da to bude iskusna i stručna osoba iz informatičke službe, s dobrim poznavanjem tehnologije i sposobnošću komunikacije i vođenja ljudi. Voditelj sigurnosti koordinira sve aktivnosti vezane uz sigurnost informacijskih sustava. Voditelj informacijske sigurnosti je osoba – radnik zaposlen(a) na radnom mjestu Informatički specijalist.

Njegove glavne zadaće su:

- izrada i ažuriranje pisanih pravilnika i procedura za sigurnost (poput ove Politike i njezinih priloga)
- nadzor nad mrežom i servisima: kontinuirano praćenje stanja mrežne infrastrukture i poslužiteljskih sustava, u suradnji s mrežnim i sistem administratorima, radi uočavanja sigurnosnih incidenata i ranjivosti
- obuka korisnika i osoblja: organizacija edukacije zaposlenika i administratora o sigurnosnim principima, pravilnoj uporabi sustava, zaštiti podataka i sl.
- podizanje svijesti korisnika o pravilima „računalne higijene” i poticanje dobre sigurnosne prakse
- suradnja s upravom: redovito izvještavanje uprave Instituta o stanju informacijske sigurnosti te predlaganje mjera za poboljšanje (nabava opreme, ulaganje u obuku, donošenje novih pravila)
- sudjeluje i u planiranju nabave nove računalne opreme ili razvoja softvera kako bi se osiguralo da sigurnosni zahtjevi budu ispunjeni
- reagira na incidente – vodi postupke kod većih sigurnosnih incidenata – organizira istragu, te komunicira s vanjskim tijelima po potrebi. U slučaju ozbiljnijih incidenata voditelj sigurnosti osigurava da se slijede procedure iz Pravilnika o rješavanju sigurnosnih incidenata.

2.5. Povjerenstvo za sigurnost (opcija)

Ako se ocijeni svrsishodnim, ravnatelj Instituta može odlukom osnovati povjerenstvo za sigurnost informacijskih sustava. Povjerenstvo bi činili predstavnici uprave (pomoćnik ravnatelja), voditelj informacijske sigurnosti, radnik zaposlen na radnom mjestu Informatički referent i radnik zaposlen na radnom mjestu Tajnik Instituta.

Zadaće povjerenstva uključuju: razmatranje izvješća o stanju sigurnosti i predlaganje mjera za poboljšanje (npr. nabava opreme, organizacija dodatne edukacije), odobravanje provođenja službenih istraga u slučaju ozbiljnih incidenata te periodično podnošenje izvješća ravnatelju o stanju informacijske sigurnosti i potrebnim aktivnostima.

Povjerenstvo može razmatrati i donositi nove prateće pravilnike (poput politika za pojedine podsustave) da bi osnovna sigurnosna politika ostala ažurna, ali općenita, dok se detaljna pravila lakše dopunjavaju prema potrebi.

U slučaju osnivanja povjerenstva, njegove odluke i preporuke bit će dokumentirane i obvezujuće za sve djelatnike nakon odobrenja ravnatelja Instituta.

2.6. Primjena u podružnicama

Ova Politika jednako se primjenjuje na Podružnicu Slavonski Brod.

Primjenjuju se jedinstveni standardi za sigurnost i upravljanje sustavima, uključujući zajedničku evidenciju opreme i koordinaciju mjera zaštite. U slučaju servisa i sustava koji se održavaju kod vanjskog pružatelja usluga vrijede ista pravila i ugovorne obveze kao i za središnjicu Instituta.

Službena korespondencija vodi se isključivo preko @isp.hr / @hipzg.hr / @hipsb.hr; generičke adrese trećih pružatelja ukidaju se po planu prijelaza.

3. Pravila upravljanja sustavom i mrežom

3.1. Administriranje računalne opreme

Institut osigurava da sva računala i poslužitelji budu ispravno administrirani i zaštićeni. Svaki sustav ima odgovornog administratora: za opremu u prostorijama Instituta to su interni administratori, a za sustave i poslužitelje smještene kod vanjskog pružatelja usluga odgovornost snosi ugovorni partner u skladu s ugovorom.

Naprednim korisnicima može se dopustiti administriranje vlastitih računala isključivo uz pismeno odobrenje i potpisivanje izjave o poštovanju pravila, čime prihvaćaju sve odgovornosti administratora.

Administratori moraju konfigurirati sustave tako da budu maksimalno zaštićeni od napada izvana i iznutra – redovito instalirati sigurnosne nadogradnje i zacrpe prema preporukama proizvođača, koristiti odgovarajuće antivirusne programe i vatrozidne postavke, postaviti kontrolu pristupa, filtriranje mrežnog prometa i druge mjere zaštite.

Posebna pozornost posvećuje se računalima koja obavljaju ključne funkcije ili čuvaju povjerljive podatke – njih treba dodatno osigurati protiv neovlaštenog pristupa.

Praćenje i evidencija: Administratori su dužni pratiti rad sustava – provjeravati systemske logove, nadzirati iskorištenost resursa i ponašanje korisnika – da bi na vrijeme otkrili eventualne sigurnosne prijetnje ili nepravilnosti.

O svim većim uočenim problemima ili kršenjima pravila odmah obavještavaju voditelja sigurnosti. Administratori vode evidenciju o svim konfiguracijskim promjenama na sustavima i intervencijama te tu evidenciju pohranjuju na sigurno mjesto radi pregleda i audita po potrebi.

U svojem radu administratori i ostalo IT osoblje poštuju privatnost korisnika i čuvaju povjerljivost korisničkih podataka.

Bilo kakav uvid u korisničke datoteke ili komunikacije administratori obavljaju isključivo u skladu s pravilima nadzora (poglavlje 4.2.) i uz odobrenje nadležnih.

3.2. Upravljanje mrežom i pristupom

Mrežna infrastruktura: Ako Institut posjeduje vlastitu računalnu mrežu i komunikacijsku opremu, mora definirati pravila tko upravlja mrežom i konfigurira mrežnu opremu, dodjeljuje IP adrese, kreira virtualne mreže (VLAN) i sl.

Dio mrežne opreme (switchevi, routeri, IP telefonija) održava i konfigurira vanjski ugovorni partner. U tim slučajevima administratori Instituta imaju pravo nadzora i obvezu koordinacije, dok je tehnička odgovornost na vanjskoj tvrtki.

Osoba zadužena za mrežu mora voditi točan popis svih mrežnih priključaka i uređaja u mreži, uključujući i prijenosna računala ako se priključuju.

Priključivanje udaljenih korisnika: Ako Institut omogućuje udaljeni rad (npr. zaposlenicima od kuće ili na terenu pristup institucijskim sustavima), potrebno je donijeti poseban pravilnik o radu na daljinu. Svi koji rade na daljinu moraju biti upoznati s tim pravilima.

Mora se osigurati da korištenje privatnog računala za spajanje na institutske mreže ne ugrozi sigurnost – npr. zahtijevanjem upotrebe VPN-a, jakih zaporki, redovitog ažuriranja i antivirusne zaštite na osobnom uređaju. Povjerljivi podaci na udaljenom računalu moraju biti jednako zaštićeni kao da se nalaze u zgradi Instituta.

Priključivanje gostujućih računala: Institut definira pravila za spajanje na mrežu vanjskih uređaja koje donose posjetitelji, vanjski suradnici, predavači, serviseri i sl. Nije dopušteno da takve osobe samoinicijativno priključuju svoja računala u internu mrežu Instituta, zbog rizika širenja zloćudnog softvera ili provođenja zlonamjernih radnji (prisluškivanje mrežnog prometa, neovlašteno prikupljanje podataka itd.).

Institut može odrediti posebna mrežna priključna mjesta (ili gostujuću bežičnu mrežu) izolirana od interne mreže, gdje je dozvoljeno spajanje gostujućih računala.

Mrežna konfiguracija treba spriječiti da s tog segmenta mreže gosti mogu pristupiti ostalim resursima Instituta.

Bežična mreža: Ako Institut koristi bežičnu (Wi-Fi) mrežu za pristup internetu ili lokalnoj mreži, mora osigurati da neovlaštene osobe ne mogu pristupiti internim resursima preko bežične veze niti prisluškivati promet. Bežična mreža mora biti odgovarajuće šifrirana (min. WPA2 ili noviji standard) i zaštićena autentikacijom korisnika.

Preporučuje se uspostava odvojenog bežičnog segmenta za goste koji je logički odijeljen od interne mreže. Ako Institut uvodi bežičnu mrežu, donijet će poseban pravilnik koji definira vrste enkripcije, obvezni softver, postupke za izdavanje i čuvanje ključeva i lozinki i sl.

Postojeću bežičnu mrežu Instituta postavila je i održava vanjska tvrtka u skladu s ugovorom o pružanju usluga. Za sigurnosne postavke i održavanje mrežne opreme odgovoran je vanjski pružatelj, dok administratori Instituta nadziru korištenje i poštovanje pravila pristupa.

3.3. Podjela mrežnih zona

Radi lakše zaštite, institutsku računalnu mrežu i opremu preporučljivo je podijeliti na sigurnosne zone prema razini dostupnosti podataka.

Dio informacijskih servisa i infrastrukture Instituta nalazi se kod vanjskih pružatelja usluga (npr. hosting web stranice, cloud poslužitelji, VPN servisi i drugi mrežni resursi). Održavanje tih sustava u domeni je ugovornih partnera, uz obvezu poštovanja ove Politike i važećih sigurnosnih standarda.

- Zona javnih servisa (DMZ - engl. Demilitarized Zone) – obuhvaća opremu koja pruža javno dostupne usluge (npr. web poslužitelj javne web stranice, DNS poslužitelj, javni mail gateway itd.). DMZ označava izdvojeni mrežni segment smješten između interne mreže i interneta, namijenjen pružanju javnih servisa uz dodatne sigurnosne mjere.
- Intranet (privatna mreža) – obuhvaća internu mrežu Instituta, uključujući interne poslužitelje, servise i aplikacije. Ova je zona zaštićena od vanjskog pristupa i namijenjena isključivo ovlaštenim korisnicima Instituta.
- Extranet – obuhvaća produžetke interne mreže otvorene za mobilne korisnike ili povezivanje izdvojenih lokacija i vanjskih partnera. Tu spadaju, primjerice, VPN pristup za vanjske suradnike ili veze institutske mreže s partnerskim ustanovama u zajedničkim projektima. Extranet predstavlja povećan rizik jer pruža prolaz u zaštićenu internu mrežu, stoga se pristup mora strogo kontrolirati ugovorima (za vanjske tvrtke) i tehničkim mjerama (npr. VPN s dvofaktorskom autentikacijom, odvojen segment mreže za vanjski pristup i dr.).

(Napomena: Institut će po potrebi izraditi zasebne sigurnosne pravilnike za pojedine zone – npr. pravilnik za DMZ, za udaljeni pristup – da bi administratori imali jasne upute za zaštitu tih dijelova sustava.)

3.4. Upravljanje softverom i licenciranjem

Legalnost softvera: Na svim računalima Instituta smije biti instaliran samo legalno nabavljen i licenciran softver. Korištenje neovlaštenog (piratskog) softvera strogo je zabranjeno jer predstavlja kršenje autorskih prava i zakona.

Povreda ovih odredbi može Institutu nanijeti materijalnu i moralnu štetu, pa će odgovorne osobe snositi disciplinske i zakonske posljedice.

Instalacija softvera: Institut imenuje jednu ili više odgovornih osoba za instalaciju softvera i praćenje licencijskih obveza.

Zaposlenici ne smiju samoinicijativno instalirati programe na službena računala. Ako korisniku za obavljanje posla treba određeni novi program za rad, dužan je obratiti se administratorima uz obrazloženje potrebe, da bi se program nabavio i instalirao na pravilan način.

Poštovanje licencijskih prava: Svi korisnici moraju se pridržavati odredbi licencijskih ugovora za softver koji koriste te poštovati autorska prava. Svaki zaposlenik potpisuje Izjavu o prihvatljivom korištenju, pri čemu potvrđuje da je upoznat s ovim pravilima i da će ih se pridržavati.

Time Institut prebacuje odgovornost za eventualno kršenje zakona o autorskom pravu na nesavjesnog korisnika.

Drugim riječima, ako zaposlenik svjesno instalira ili koristi nelegalan softver, snosit će osobnu odgovornost za posljedice.

Ažuriranje softvera: Administratori su dužni pratiti objave dobavljača softvera i pravodobno instalirati sigurnosna ažuriranja i nove verzije ključnih programa. Posebno se to odnosi na operativne sustave, poslužiteljske servise te antivirusne definicije. Korištenje zastarjelih verzija softvera može ugroziti sigurnost sustava, pa će Institut planirati nadogradnju ili zamjenu zastarjelih aplikacija u suradnji s korisnicima i prema financijskim mogućnostima.

3.5. Fizička sigurnost i zaštita opreme

Kontrolirani pristup prostorima: Prostorije Instituta dijele se prema stupnju pristupa na: otvorene za javnost, zatvorene za javnost (dostupne samo zaposlenicima) i posebno zaštićene prostore s ograničenim pristupom unutar kruga zaposlenika.

Uprava Instituta dužna je popisati sve prostorije koje spadaju u zaštićena područja (npr. mrežni ormar, poslužiteljska soba ako postoji, arhiv, prostor s povjerljivom dokumentacijom) i uspostaviti kontrolu pristupa za takve prostore. Pristup zaštićenim prostorima imaju samo ovlaštene osobe, prema popisu ovlaštenih djelatnika koji se vodi i ažurira.

Osobe na ulazu Instituta moraju imati uvid u popis ovlaštenih djelatnika i vršiti izdavanje/primanje ključeva uz evidenciju, ili se mora implementirati tehnički kontroliran pristup (npr. kartice/ključ).

Đio kritične opreme (npr. mrežni poslužitelji i backup mediji) smješten je kod vanjskog pružatelja usluga, pri čemu odgovornost za njihovu fizičku sigurnost i održavanje snosi ugovorni partner, u skladu s ugovorom o pružanju usluga.

Sigurne zone: Kritična ICT oprema (npr. mrežni poslužitelji ključnih servisa, komunikacijska oprema glavnog čvora mreže, backup mediji s osjetljivim podacima) trebala bi biti fizički smještena u posebno zaštićenim prostorijama – sigurnim zonama, bilo da se nalazi u prostoru Instituta ili u okruženju vanjskog pružatelja usluga (cloud infrastruktura).

U takve zone dopušten je ulaz samo ovlaštenom osoblju. Pristup mrežnoj i komunikacijskoj opremi dopušten je administratorima i tehničarima isključivo kad je to potrebno za održavanje ili nadzor sustava. U slučaju postojanja poslužiteljske sobe, u nju se ulazi samo po potrebi, u skladu s pravilima kontrole pristupa.

Sigurne zone moraju imati dodatne mjere zaštite: zaključavanje, protuprovalni i protupožarni sustav, klimatizaciju, nadzor vlage, neprekidno napajanje (UPS) itd., jer je kontinuitet rada tih sustava od kritične važnosti.

Zaštita opreme od havarija: Sva važna informatička oprema mora biti zaštićena od uobičajenih opasnosti: prekida napajanja, prenapona, požara, poplave i sl. Električne instalacije u prostorima u kojima se nalazi mrežna ili poslužiteljska oprema moraju biti izvedene kvalitetno i redovito

provjeravane; preporučuje se korištenje UPS uređaja, a po potrebi i agregata za struju, da bi se osigurao neprekidan rad ključne opreme.

U prostorijama u kojima se nalazi mrežna ili druga bitna informatička oprema ne smiju se držati zapaljive tekućine ili eksplozivne tvari.

Treba razmotriti i druge moguće probleme poput pregrijavanja, poplave (curenje vode) – npr. ne držati opremu u podrumu sklonom poplavama, osigurati klimatizaciju i protupožarne aparate i sl., da bi se smanjila mogućnost štete i ubrzao oporavak u slučaju incidenta.

Vanjske tvrtke u prostorima Instituta: Povremeno je nužno dopustiti pristup prostorijama i opremi Instituta i osobama iz vanjskih tvrtki ili institucija – radi servisiranja opreme, održavanja sustava, podrške, edukacije, zajedničkih projekata, konzultacija itd.

U takvim slučajevima Institut će s vanjskim partnerom ugovorom urediti obvezu poštovanja svih sigurnosnih pravila Instituta.

Za vanjske partnere koji održavaju dio informatičke infrastrukture (npr. cloud poslužitelje, mrežnu opremu, backup sustave) vrijede iste odredbe o povjerljivosti i sigurnosnim pravilima kao i za zaposlenike Instituta.

Ugovorom ili posebnim sporazumom regulirat će se i dozvoljeni opseg pristupa koji se odobrava trećoj strani – uključujući fizički pristup određenim prostorijama, pristup računalnoj opremi te logički (mrežni) pristup potencijalno povjerljivim informacijama.

Svaka vanjska osoba koja dolazi u dodir s povjerljivom opremom, podacima ili sigurnom zonom Instituta mora prethodno potpisati Izjavu o čuvanju povjerljivih informacija (NDA).

Vanjske osobe bez ovlasti ne smiju se kretati same u osjetljivim prostorima Instituta. Ako radni zadatak zahtijeva da neovlaštena osoba (npr. serviser) mora boraviti u zaštićenom prostoru bez stalne pratnje djelatnika Instituta, to je dopušteno samo uz provođenje nadzora (npr. videonadzor prostora tijekom rada serviser).

Institut može od vanjske tvrtke zatražiti popis svih osoba koje će dolaziti raditi u prostoru Instituta i inzistirati da se nenajavljene zamjene osoblja unaprijed jave.

Prilikom dolaska, odgovorna osoba Instituta ima pravo tražiti identifikaciju osoblja vanjske tvrtke (izvršitelja) i usporediti s najavljenim imenima, te uskratiti pristup osobama koje nisu na popisu. U slučaju teže povrede pravila od vanjskog izvršitelja, Institut može zatražiti da se ta osoba ukloni iz daljnjeg rada za Institut, a ako je povreda ozbiljna – i raskinuti ugovor s tom vanjskom tvrtkom.

3.6. Inventarizacija i zaštita opreme

Popis i vlasništvo opreme: Sva računalna i mrežna oprema koja se koristi u Institutu mora biti evidentirana u inventurnom popisu. Institut vodi ažurirani popis opreme s osnovnim podacima: opis uređaja, lokacija, proizvođač/model, serijski ili inventarski broj, osnovni konfiguracijski podaci te naznaka vlasništva opreme.

Naime, dio opreme može biti u vlasništvu partnerskih institucija (npr. CARNET-a ili Ministarstva znanosti, obrazovanja i mladih), a dana je Institutu na korištenje.

Institut se brine o svojoj opremi kojom raspolaže s jednakom pažnjom, bez obzira na vlasnika – kao dobar gospodar, štiti ju od oštećenja i krađe.

Ako se u Institutu nalazi oprema u vlasništvu druge institucije, ovlaštenim osobama te institucije mora se omogućiti pristup toj opremi radi održavanja.

Odgovornost za opremu: Za fizičku sigurnost cjelokupne informatičke opreme odgovoran je ravnatelj Instituta, koji ovlasti i odgovornosti dalje delegira na rukovoditelje ustrojstvenih jedinica ili pojedine zaposlenike. Svaka primopredaja opreme na brigu potvrđuje se potpisom – čime djelatnik (korisnik) preuzima odgovornost za tu opremu.

Npr., računala u uredima odgovornost su pojedinih korisnika/uprave, mrežni uređaji odgovornost su administratora.

Institut će razraditi procedure za sprječavanje krađe i oštećenja opreme. Npr., na izlazu iz zgrade (porti) provjeravat će se iznosi li netko opremu iz Instituta te posjeduje li za to potrebnu dokumentaciju (odobrenje, otpremnicu, radni nalog za servis i sl.).

Svi će zaposlenici biti upoznati s obvezom čuvanja opreme te će nastojati spriječiti neovlašteno iznošenje opreme ili materijala. Služba nabave ili računovodstvo brinut će se o osiguranju vrednije opreme od rizika (požara, elementarnih nepogoda, provale i sl.).

3.7. Osiguranje neprekidnosti poslovanja

Institut poduzima mjere za očuvanje podataka i kontinuiteta rada u slučaju nezgoda ili poremećaja (kvarovi opreme, požar, elementarne nepogode, ljudske pogreške itd.). Ključna mjera je redovita izrada sigurnosnih kopija (backup) svih važnih informacija i konfiguracija softvera.

Odredit će se koje točno podatke treba sigurnosno kopirati (poslovne dokumente, baze podataka istraživanja, korisničke profile, konfiguracije servera, sandučice e-pošte i sl.) te učestalost sigurnosnog pohranjivanja (dnevno, tjedno, mjesečno - ovisno o kritičnosti), koja se za sustave kod vanjskog pružatelja usluga utvrđuje od strane pružatelja usluga, a za ostale sustave utvrđuje u suradnji voditelja informacijske sigurnosti, odgovornog rukovoditelja ustrojstvene jedinice i IT službe. Preporučuje se imati više kopija koje se čuvaju na različitim lokacijama, idealno u vatrootpornim ormarima ili sefovima.

Za poslužitelje, mrežne servise i datotečne sustave koji se nalaze kod vanjskog pružatelja usluga, sigurnosne kopije izrađuje i održava ugovorni partner, u skladu s ugovorenim obvezama i definiranim sigurnosnim standardima.

Jedna kopija može se čuvati unutar Instituta, a druga na odvojenoj sigurnoj lokaciji (npr. u drugoj zgradi ili kod vanjskog pružatelja usluga putem ugovorenog cloud backup rješenja).

Za sustave kod vanjskog partnera Institut se oslanja na njihove procedure i dokumentaciju vezanu uz backup. Institut može definirati interna pravila za backup korisničkih računala i drugih podataka koji se pohranjuju lokalno, uključujući obvezu korisnika da radne dokumente pohranjuju na lokacije koje se redovito sigurnosno kopiraju.

Obveza čuvanja povjerljivosti odnosi se i na podatke u backupu jednako kao i na originalne podatke. Backup mediji (npr. trake ili diskovi) čuvaju se pod ključem i imaju kontrolirani pristup, u skladu sa sigurnosnim procedurama vanjskog pružatelja usluga.

Institut će izraditi plan oporavka (disaster recovery) za sustave i procese pod svojom nadležnošću te definirati aktivnosti koje treba poduzeti radi obnove poslovanja u slučaju prekida rada.

Za sustave koji se nalaze kod vanjskog pružatelja usluga, plan oporavka provodi sam pružatelj, u skladu sa svojim sigurnosnim procedurama i ugovorenim obvezama, dok Institut u svojem planu definira komunikaciju, odgovornosti i korake koji se poduzimaju u suradnji s pružateljem usluga.

Te će se procedure dokumentirati i čuvati da bi u slučaju odsutnosti odgovorne osobe drugi djelatnici mogli postupiti u skladu s planom. Plan oporavka definira aktivnosti i redosljed obnove rada ključnih funkcija, kontaktne informacije za hitne slučajeve te prema potrebi nabavu zamjenske opreme ili suradnju s vanjskim pružateljem usluga na vraćanju servisa u rad.

Periodički (najmanje jednom godišnje) testirat će se ispravnost sigurnosnih kopija i provesti proba oporavka sustava, bilo interno ili u suradnji s vanjskim pružateljem usluga. Proba oporavka provodi se na zasebnoj testnoj opremi ili u laboratorijskim uvjetima, a nikako na produkcijskoj opremi tijekom radnog vremena, da ne bi ometala redovan rad.

Rezultati testova backupa i oporavka dokumentiraju se i analiziraju radi poboljšanja procedura.

3.8. Upravljanje istraživačkim podacima i repozitorijem

Institut koristi nacionalnu infrastrukturu za digitalne repozitorije (Dabar/Srce) te nacionalni informacijski sustav znanosti CroRIS. Odgovornost Instituta odnosi se na upravljanje sadržajem i metapodacima unutar vlastitog institucionalnog repozitorija, što uključuje uloge repozitorskog administratora, urednika zbirke i autora/vlasnika podataka.

Institut osigurava primjenu minimalnih standarda upravljanja istraživačkim podacima RDM – Research Data Management minimum (opis skupa, pravni temelj, licenca, metapodaci, plan čuvanja, anonimizacija osobnih podataka), takedown postupak (privremeno uklanjanje spornog sadržaja do odluke), kao i pravila embarga i verzioniranja zapisa. Administratori i urednici repozitorija obvezni su koristiti dvofaktorsku autentikaciju (2FA) u skladu s pravilima Srca.

Tehničke sigurnosne mjere poput sigurnosnih kopija (backup), provjere integriteta podataka (fixity provjere, checksum) i održavanja aplikacijske infrastrukture osigurava Srce kroz Dabar sustav.

4. Nadzor, kontrola i usklađenost

4.1. Pravo nadzora i privatnost

Institut zadržava pravo nadzora nad svojim informacijskim sustavima, u mjeri nužnoj za zaštitu svojih resursa. Ovlaštene osobe Instituta smiju nadzirati: instalirani softver i podatke pohranjene na umreženim računalima Instituta, kao i način korištenja institutskih računala i mreže.

Nadzor se smije provoditi isključivo u sljedeće svrhe:

- radi osiguranja integriteta, povjerljivosti i dostupnosti informacija i resursa Instituta
- radi provođenja istrage u slučaju sumnje da je došlo do sigurnosnog incidenta
- radi provjere usklađenosti korištenja informacijskih sustava sa zahtjevima ove Politike i drugih propisa.

Nadzor mogu obavljati samo osobe koje Institut za to posebno ovlasti (npr. voditelj sigurnosti, članovi povjerenstva za sigurnost). Pri provođenju nadzora, ovlaštene osobe dužne su maksimalno poštovati privatnost i dostojanstvo korisnika i njihovih osobnih podataka.

Međutim, ako se tijekom nadzora otkrije da je korisnik kršio ovu Politiku ili zakon, Institut više ne može jamčiti povjerljivost informacija otkrivenih u toj istrazi – te se one mogu upotrijebiti kao dokaz u stegovnom postupku ili pred sudom, u skladu sa zakonom.

4.2. Postupak nadzora i kontrole

Opseg nadzora: Nadzorna pravila odnose se na svu računalnu opremu u prostorima Instituta i opremu spoenu na mrežu Instituta, na sav softver instaliran na službenim uređajima te na sve mrežne servise koji se koriste u sklopu informacijskog sustava Instituta.

Pravila moraju poštovati svi zaposlenici i vanjski suradnici koji koriste IT opremu Instituta, kao i ugovorne organizacije koje pružaju IT usluge Institutu.

Suradnja korisnika: Svi korisnici obvezni su surađivati s ovlaštenim osobama za nadzor, tako da im na zahtjev pruže potrebne informacije i omogućće pristup prostorijama, uređajima i datotekama bitnim za provođenje nadzora.

To uključuje, primjerice, obvezu da korisnik na zahtjev ovlaštene osobe otključa svoj službeni uređaj ili stavi na raspolaganje dokumente od interesa za istragu. Isto se odnosi i na administratore računala i servisa – oni su dužni pružiti pomoć sigurnosnom specijalistu tijekom istrage (npr. ustupiti log zapise, konfiguracijske datoteke i sl.)

Dozvoljeni obuhvat kontrole: Ovlašteni sigurnosni tim ima pravo, u okviru istrage:

- pristupiti svakoj računalnoj opremi Instituta na razini korisnika ili sustava (od korisničkih radnih stanica do poslužitelja)
- pregledati svaku informaciju pohranjenu ili generiranu na institutskoj opremi, bilo u elektroničkom ili pisanom obliku, kao i informacije koje su putem institutske opreme prenesene (npr. mrežnim putem)
- ući u radne prostore (urede, laboratorije, sigurne zone) u svrhu nadzora opreme
- interaktivno nadzirati mrežni promet Instituta i bilježiti prometne podatke (paketne logove) radi analize
- koristiti alate za udaljeni nadzor i administraciju (npr. remote desktop, AnyDesk, VPN pristup ili slične sustave), uz poštovanje sigurnosnih pravila.

Nepridržavanje: Zaposlenik koji odbije suradnju pri nadzoru ili se ogлуši o ova pravila može snositi disciplinske posljedice. Institutu je na raspolaganju mjera uskraćivanja prava korištenja mreže i usluga (privremeno ili trajno) korisniku koji onemogućuje nadzor.

U slučaju težeg ili ponovljenog kršenja pokrenut će se stegovni postupak u skladu s općim aktima Instituta.

4.3. Obrada osobnih podataka u prodaji knjižnih izdanja i periodičkih publikacija u internetskoj trgovini

Kod online narudžbi u internetskoj trgovini (web shopu) Institut prikuplja isključivo nužne podatke (minimalizacija), uz pravni temelj, informiranje ispitanika, rokove čuvanja i prava ispitanika.

Prijenos podataka je šifriran (TLS). Podaci o karticama ne pohranjuju se na sustavima Instituta; naplata se obavlja preko certificiranog procesora plaćanja (PCI-DSS). Institut vodi evidenciju o izvršenim kupnjama putem sustava WooCommerce, bez pohrane punih brojeva kartica (PAN-ova).

5. Mjere i sankcije u slučaju kršenja pravila

Svi zaposlenici i suradnici dužni su se pridržavati odredbi ove Politike i njezinih pratećih pravilnika. Kršenje pravila predstavlja povredu radne obveze i može dovesti do stegovnih mjera. Kod manjih propusta primijenit će se načelo postupne korekcije – zaposleniku će se ukazati na grešku i pružiti dodatna edukacija (npr. savjetovanje o izradi sigurnije zaporke).

Međutim, ponovljeno ignoriranje sigurnosnih pravila ili teži propust koji ugrozi integritet sustava rezultirat će formalnim stegovnim postupkom.

Stegovne mjere mogu uključivati: opomenu pred otkaz, premještaj na drugo radno mjesto, gdje je manja mogućnost ugrožavanja IT sustava, pa sve do redovitog ili izvanrednog otkaza ugovora o radu, ovisno o težini povrede.

Ako je povredu počinio vanjski suradnik ili tvrtka, Institut može raskinuti suradnju odnosno ugovor o djelu/usluzi s tom osobom ili tvrtkom. Primjerice, ako zaposlenik vanjske tvrtke izazove sigurnosni incident kršenjem pravila, Institut će zahtijevati od te tvrtke da odmah ukloni tu osobu iz svih poslova za Institut.

U slučaju teže povrede, Institut će pokrenuti postupak raskida ugovora s tom tvrtkom i potraživati naknadu štete ako je primjenjivo.

Teško kršenje sigurnosnih mjera (npr. namjerno oštećenje podataka, neovlašteno iznošenje povjerljivih informacija, instalacija zlonamjernog softvera) može predstavljati i kazneno djelo prema Kaznenom zakonu. U takvim slučajevima Institut će, osim internih mjera, o događaju obavijestiti nadležne državne institucije i staviti im na raspolaganje rezultate provedene interne istrage.

Prilozi sigurnosne politike

(Napomena: Slijede posebni pravilnici koji čine sastavni dio Politike informacijske sigurnosti Instituta. Oni detaljno razrađuju pojedina područja sigurnosti: zaporke, e-poštu, antivirusnu zaštitu, antispam, postupanje s incidentima i povjerljivim informacijama. Ovi se pravilnici primjenjuju zajedno s glavnim dokumentom Politike.)

PRAVILNIK O RUKOVANJU ZAPORKAMA

Svrha: Ovaj Pravilnik propisuje pravila za odabir, korištenje i zaštitu zaporki (lozinki) kojima se štite korisnički računi i podaci. Sigurna zaporka osnovna je obrana sustava: kompromitiranjem jedne slabe zaporke napadač može steći neovlašten pristup i ugroziti cijeli sustav. Često korisnici misle da njihovo računalo „nema ništa važno“, no dovoljno je da jedan račun bude probijen pa da napadač dobije uporište za napad na ostale resurse – lanac puca na najslabijoj karici.

Današnja računala mogu brzo pogoditi ili probiti jednostavne zaporke, a ljudi teško mogu zapamtiti vrlo složene zaporke.

Ovaj Pravilnik nastoji uspostaviti ravnotežu između sigurnosti i praktičnosti. Svaki je korisnik dužan primjenjivati ova pravila o zaporkama i time doprinositi ukupnoj zaštiti sustava.

Područje primjene: Pravila se odnose na sve djelatnike i vanjske suradnike Instituta koji koriste informatičke resurse za svoj rad. Administratori sustava dužni su tehnički provesti namještanje ovih pravila na svim sustavima koji to omogućavaju (npr. postaviti minimalne duljine zaporki, isteke i sl.).

Pravila za zaporke:

- minimalna duljina zaporke: Zaporka mora imati najmanje 8 znakova. Prekratke zaporke lako je odgonetnuti „brutalnom silom“. Iako je propisan minimum od 8 znakova, preporučuje se koristiti još duže zaporke (12 i više znakova) kad god je moguće;
- složenost znakova: Zaporka treba biti kombinacija velikih i malih slova, brojeva i posebnih znakova. Ne smije biti obična riječ iz rječnika na bilo kojem jeziku. Preporuka je uzeti neku lako pamtljivu frazu pa ju modificirati – primjerice, zamijeniti određena slova brojevima ili znakovima (npr. „h0bo3niCa“ umjesto „hobotnica“);
- zabrana jednostavnih pojmova: Nije dopušteno koristiti opće ili lične pojmove kao zaporke – poput vlastitog imena ili prezimena, imena djece ili kućnih ljubimaca, datuma rođenja, broja telefona i sl. Takve se zaporke vrlo lako otkriju metodama socijalnog inženjeringa i pogađanjem;
- trajanje zaporke: Korisnik treba zaporku redovito mijenjati, najmanje svaka 3 mjeseca (90 dana), a po potrebi i češće. Česta promjena smanjuje šansu da zaporka bude provaljena;
- nije dopušteno izmjenjivati stalno dvije iste zaporke naizmjenično – takvim trikovima izigrava se svrha promjene zaporke;
- sistemski softver (domenski kontroler) bit će podešen da forsira promjenu zaporke svakih 90 dana i da onemogućiti korištenje stare zaporke prilikom postavljanja nove.

Povjerljivost zaporke: Zaporka je strogo tajna. Korisnik odgovara za čuvanje tajnosti svoje zaporke i ne smije ju odati nijednoj neovlaštenoj osobi – uključujući kolege i nadređene, pa čak ni IT administratoru.

Administratori ne smiju tražiti od korisnika da im oda svoju lozinku; u slučaju potrebe, mogu privremeno postaviti novu zaporku ili dodijeliti korisniku ovlasti bez traženja postojeće lozinke. Korisnik treba biti oprezan i na moguće pokušaje krađe zaporke (phishing) – npr. hakeri se mogu lažno predstaviti kao administratori i tražiti da im korisnik „potvrdi” svoju lozinku.

Na takve upite korisnik se nikad ne smije odazvati.

Pohranjivanje zaporke: Zaporke se ne smiju zapisivati na papiriće koje držimo uz računalo (ispod tipkovnice, zalijepljene na monitor i sl.) niti spremati u nezaključane ladice.

Ako korisnik treba zapis da bi zapamtio složenu zaporku, treba ga čuvati na sigurnom mjestu (zaključana bilježnica, šifrirana datoteka u računalu i sl.). Preporuka je koristiti pouzdane password manager alate za čuvanje lozinki u šifriranom obliku.

Zaboravljena ili kompromitirana zaporka: Ako korisnik zaboravi zaporku ili posumnja da je otkrivena, dužan je odmah obavijestiti administratora. Administrator će provesti postupak resetiranja zaporke i omogućiti korisniku postavljanje nove. Ako postoji sumnja da je zaporka kompromitirana (npr. korisnik je uočio neovlašten pristup svojem računu), potrebno je incident prijaviti prema proceduri i smatrati stari ključ nevažećim.

Administratorske obveze: Administratori sustava dužni su provesti tehničke mjere za provođenje ovih pravila gdje je to moguće. Na sustavima i aplikacijama koji podržavaju tu mogućnost postaviti će se minimalna duljina zaporke (8 znakova) i zaključavanje korisničkog računa nakon 3 neuspjela pokušaja prijave.

Također će se aktivirati automatski mehanizam isteka zaporki nakon 90 dana i zabrana ponovne uporabe barem posljednjih nekoliko korištenih zaporki.

Administratori će povremeno (npr. jednom godišnje) provesti provjeru poštuju li korisničke zaporke ova pravila – na način koji ne otkriva stvarne zaporke korisnika (npr. audit alatom koji ispituje složenost lozinki ili pokušaj probijanja hash zapisa lozinki uz odobrenje uprave).

Nepridržavanje: Korisnici koji zanemaruju ova pravila o zaporkama ugrožavaju sigurnost informacijskog sustava.

Institut će nastojati edukacijom utjecati na korisnike da kreiraju sigurne zaporke te će ih upozoravati na propuste. Međutim, u slučaju ponovljenog kršenja pravila (npr. korisnik više puta namjerno postavlja slabe zaporke) Institut može protiv te osobe pokrenuti stegovni postupak. Zaposlenik također može biti premješten na radno mjesto s manjim ovlastima i pristupom, gdje neće moći ugroziti integritet sustava i podataka.

PRAVILNIK O KORIŠTENJU ELEKTRONIČKE POŠTE

Uloga e-pošte: Elektronička pošta nezaobilazan je dio svakodnevne komunikacije, poslovne i privatne. Komuniciranje e-poštom na Institutu zahtijeva osviještenost o svim aspektima ove komunikacije s obzirom na moguće posljedice.

Protokol SMTP (Simple Mail Transfer Protocol), na kojem se temelji slanje e-pošte, u svojim začecima nije bio dizajniran s naglaskom na sigurnost.

Nadalje, u korištenju e-pošte javljaju se i problemi uzrokovani ljudskim faktorom – korisnici često nisu svjesni svih „zamki“ koje postoje pri slanju poruka. Ovaj Pravilnik najprije ukratko opisuje tipične rizike e-komunikacije, a zatim propisuje pravila za sigurno i primjereno korištenje službene e-pošte.

1. Rizici tehnološke prirode („nesigurnost protokola“)

Poruke e-pošte putuju internetom u obliku običnog teksta, slično razglednici – moguće ih je relativno lako presresti i pročitati, pa čak i izmijeniti sadržaj tijekom prijenosa.

Krivtvođenje adrese pošiljatelja vrlo je jednostavno – nikada ne možete biti potpuno sigurni tko je stvarno poslao e-poruku jer se polje „From:“ može falsificirati.

Protokoli za preuzimanje pošte (POP3, IMAP) u osnovnoj verziji šalju korisničko ime i zaporku nešifrirano, kao običan tekst, pa se i one mogu prislušivati.

Zbog toga je nužno, gdje god je moguće, koristiti kriptografske protokole – npr. SSL/TLS za siguran prijenos podataka, te opcijski PGP/GPG za šifriranje samog sadržaja poruka.

2. Rizici uzrokovani slučajnim greškama („nezgode“)

Lako je moguće kliknuti na pogrešnu ikonu ili odabrati pogrešnu opciju u poštanskom programu. Česta greška je pritiskanje „Reply All“ umjesto „Reply“, čime povjerljiva poruka namijenjena jednom primatelju odlazi na veći broj adresa (svim članovima grupe). Takvu grešku nije moguće poništiti – jednom poslana poruka više se ne može zaustaviti.

Također je čest slučaj da se odabere pogrešna e-adresa primatelja iz adresara, osobito u programima koji automatski dopunjavaju adrese dok tipkate. U brzini se može odabrati pogrešno ime slično onomu koje zapravo želite, pa poruka odlazi pogrešnoj osobi.

Pogrešno adresiranje: Moguće je i da pošiljatelj pogrešno upiše adresu – e-poruka tada može završiti kod neočekivanog primatelja, ili uopće ne biti dostavljena ako adresa ne postoji.

3. Rizici u komunikaciji („nesporazumi“)

Ljudi često pišu e-poruke ležernijim, neformalnim stilom, kao da razgovaraju. Međutim, druga strana (primatelj) možda ne poznaje pošiljatelja dobro i ne shvaća ton poruke na isti način. To može dovesti do nesporazuma. Zato službenu korespondenciju uvijek treba voditi u službenom, pristojnom tonu, uz jasnu konstrukciju rečenica.

Službena e-adresa korisnika sadržava naziv Instituta (@isp.hr, @hipzg.hr ili hipsb.hr). Stoga svaka poruka izvana nosi ime Instituta. Primatelj može privatnu prepisku shvatiti kao službeni dopis ili vaše osobno mišljenje zamijeniti za službeni stav ustanove.

Preporuka je uvijek jasno naznačiti kad iznesene tvrdnje predstavljaju vaš osobni stav, npr. frazom „Ovo je moje privatno mišljenje“ u poruci.

4. Rizici otkrivanja informacija („curenje povjerljivih poruka“)

E-poruka namijenjena jednom primatelju vrlo se lako može proslijediti drugima – bilo zlonamjerno (s ciljem da se naškodi osobi ili Institutu), bilo iz nehaja (netko prosljedi poruku, a da ne zatraži dozvolu autora), bilo slučajno (pogreškom, npr. pritiskom na pogrešan gumb).

Zbog toga se poslovne dopise s osjetljivim informacijama preporučuje označiti kao povjerljive. Time se primatelja formalno obvezuje na diskreciju i pažljivije postupanje s takvom porukom. (Primjer: u e-poruci klijentu u naslov poruke dodati oznaku „[POVJERLJIVO]“.)

U slučaju sigurnosnog incidenta ili interne istrage moguće je da će ovlaštene osobe morati čitati sadržaj poruka koje su izvorno bile zamišljene kao privatna komunikacija. Institut jamči da će čuvati povjerljivost takvih poruka koliko god je to moguće, ali ne može jamčiti potpunu privatnost ako sadržaj poruka bude služio kao dokazni materijal u stegovnom postupku ili pravnom procesu.

Drugim riječima, ako koristite službenu e-adresu za osobnu prepisku, budite svjesni da u iznimnim situacijama ni takva komunikacija možda neće ostati potpuno privatna.

5. Radna etika i ekonomika vremena

Velika količina e-poruka dnevno može znatno odvlačiti pozornost i oduzimati radno vrijeme. Stoga korisnici trebaju ograničiti broj neposlovnih i zabavnih poruka tijekom radnog vremena: ne koristiti službenu e-poštu za prosljeđivanje viceva, lančanih srećaka i sličnog – takve poruke zatrpavaju sandučice i nepotrebno troše vrijeme primatelja.

Lančane poruke i hoax: Upozoravamo da mnoge „lančane srećke“ ili dramatični apeli koji kruže e-poštom sadržavaju lažne informacije. Često im je cilj navesti ljude da prosljeđuju poruku (npr. izmišljene peticije, lažne humanitarne akcije ili teorije zavjere) ili čak da ih prevare na novčanu uplatu („pomozite bolesnom djetetu“, „posudite novac nekom strancu“ itd.). Korisnici trebaju biti skeptični prema takvim masovnim porukama.

Spam: Neželjena komercijalna pošta (spam) također predstavlja problem – opterećuje mrežne resurse interneta i troši vrijeme korisnika, čak i ako takve poruke brišete bez čitanja.

Institut će na poslužitelju e-pošte primjenjivati filtre protiv spama, ali i korisnici su obvezni da sami ne šalju takve poruke. Slanje bilo kakvih neovlaštenih masovnih poruka s adresa Instituta strogo je zabranjeno.

6. Poštovanje autorskih prava

Svaka napisana e-poruka smatra se autorskim djelom po zakonu, i pripada osobi koja ju je napisala. Stoga prosljeđivanje tuđe e-poruke drugim primateljima zahtijeva dozvolu njezina autora (pošiljatelja). Nemojte automatski proslijediti privatnu poruku, a da ne pitate pošiljatelja smije li se to učiniti.

Prilozi (attachmenti) koji se šalju uz e-poruku mogu sadržavati materijale zaštićene autorskim pravom – glazbu, filmove, skenirane članke i sl. Primajući i šaljući takve materijale bez dozvole, možete sebe i Institut izložiti tužbama zbog povrede autorskih prava. Osobito je zabranjeno koristiti službenu e-poštu za razmjenu piratskog sadržaja (softvera, muzike, videozapisa).

Uzimajući u obzir sve navedene rizike, korištenje službene elektroničke pošte smatra se rizičnom aktivnosti, pa se od korisnika zahtijeva pridržavanje sljedećih pravila:

- službeni korisnički račun: Svakom zaposleniku Institut će otvoriti službenu e-adresu na institutskoj domeni za obavljanje posla. Taj račun namijenjen je prvenstveno poslovnoj komunikaciji.
- ograničena privatna upotreba: Dozvoljeno je koristiti službenu e-adresu u razumnom opsegu i za privatne potrebe, ali samo ako to ne ometa obavljanje posla i ne krši ostala pravila. Privatne poruke treba slati u manjem broju i po mogućnosti izvan najkritičnijeg radnog vremena. Institut zadržava pravo nadzirati ukupni opseg korištenja u privatne svrhe i reagirati ako ono prelazi razumne granice.
- reprezentacija Instituta: Prilikom slanja poruka imajte na umu da nastupate kao član Instituta. U komunikaciji uvijek koristite primjeren, profesionalan stil izražavanja. Nemojte pisati poruke u afektu, nepristojnim ili uvredljivim tonom. Također ne zaboravite dodati službeni potpis s osnovnim podacima (ime, položaj, naziv Instituta, kontakt). Ako iznosite osobne stavove u raspravama, jasno naznačite da je riječ o vašem privatnom mišljenju, a ne stavu Instituta.
- poštujujte „netiketu“: Pridržavajte se općih pravila pristojnog ponašanja na internetu (netiquette). Službena e adresa Instituta ne smije se koristiti za slanje sadržaja koji je uvredljiv, uznemirujući, pornografski, diskriminirajući ili na bilo koji način neprimjeren. Strogo je zabranjeno korištenje e-pošte za seksualno ili drugo uznemiravanje kolega ili bilo koje osobe.
- zabrana lančanih i spam poruka: Nije dopušteno slanje lančanih pisama ili bilo kakvih masovnih poruka koje mogu opterećivati mrežne resurse ili oduzimati radno vrijeme primateljima. Zabranjeno je i slanje spam poruka reklamnog ili sličnog sadržaja putem institutske e-pošte. U slučaju primanja sumnjivih ili lančanih poruka korisnici ih ne smiju prosljeđivati, a mogu ih prijaviti IT službi ako ih učestalo dobivaju.
- dokumentarna vrijednost: Svaka službena e-poruka smatra se dokumentom te podliježe propisima o čuvanju poslovne dokumentacije. Službene e-poruke (npr. važni nalozi, odluke, dogovori projekata) potrebno je arhivirati i čuvati određeno vrijeme (prema zakonu ili internom aktu o arhiviranju), jednako kao što bi se čuvao dopis na papiru. Korisnici su dužni takve poruke (ili njihove ispise) pohraniti u odgovarajuću evidenciju ako su dio poslovnog procesa.
- antivirusna kontrola pošte: Sve e-poruke koje pristižu na poslužitelj Instituta automatski se skeniraju antivirusnim programom. Ako se u prilikov ili tekstu poruke pronađe virus, poruka neće biti isporučena primatelju – poslužitelj će ju staviti u karantenu, a i pošiljatelj i primatelj dobit će obavijest o zaraženoj poruci. Poruka u karanteni čuva se određeno vrijeme (npr. mjesec dana) i potom trajno briše ako primatelj ne zatraži da mu se preda (uz prethodno čišćenje).
- antispam filtriranje: Institut zadržava pravo filtriranja ulaznih poruka s ciljem zaustavljanja spama. To može uključivati odbacivanje poruka s poznatih neželjenih adresa, premještanje sumnjivih poruka u „spam“ mapu ili njihovo privremeno zadržavanje u karanteni na serveru. Korisnicima se preporučuje da također koriste mogućnosti označavanja spama u svojem e-klijentu i ne otvaraju sumnjive poruke.
- istrage i uvid u poštu: U slučaju službene istrage sigurnosnog incidenta ovlaštene osobe Instituta smiju pregledati sve sadržaje na službenom računaru zaposlenika, uključujući i e-poruke, ako postoji opravdana sumnja da je to potrebno. Naravno, to će se činiti uz poštovanje povjerljivosti, ali korisnici moraju biti svjesni da zloraba službene e-pošte poništava očekivanje privatnosti (vidi poglavlje 4.1. ove Politike).
- arhiviranje i brisanje: Sandučići e-pošte zaposlenika imaju ograničen kapacitet. Korisnici trebaju voditi računa o arhiviranju starih poruka – poruke koje su dio poslovnog procesa treba arhivirati lokalno (npr. spremanjem izvan sandučića) i čuvati propisani period, a ostale starije poruke povremeno brisati da bi se oslobodio prostor na poslužitelju. IT služba može, uz

prethodnu najavu, automatski brisati poruke starije od određenog roka iz pojedinih mapa (osim arhivskih).

Postupak dodjele e-adrese: Pri svojem zaposlenju novi djelatnik dužan je zatražiti od administratora mail poslužitelja otvaranje korisničkog računa elektroničke pošte. Zahtjev mora sadržavati ime i prezime osobe koja zahtijeva otvaranje korisničkog računa elektroničke pošte. Navedeni postupak identičan je za AAI@edu identitet kojim se ostvaruje mogućnost korištenja različitih mrežnih resursa (CroRIS, Office365, pristup WoS, Scopus, JSTOR bazama, SRCE akademija itd.).

Pri prestanku radnog odnosa zaposlenika, neposredni rukovoditelj dužan je najkasnije u roku od 7 dana zatražiti zatvaranje korisničkog računa te osobe. Iznimka se primjenjuje na zaposlenike koji nakon odlaska u mirovinu nastavljaju sudjelovati kao suradnici na projektima Instituta.

Administrator će nakon odjave zaposlenika zatvoriti sandučić, uz mogućnost postavljanja automatske obavijesti o promjeni adrese ili prosljeđivanja pošte drugoj ovlaštenoj osobi na određeno vrijeme, ako tako odredi uprava.

Vanjski suradnici na projektu mogu dobiti privremenu e-adresu na institutskoj domeni, uz odobrenje ravnatelja i na određeno vrijeme. Ta se adresa zatvara po završetku angažmana. (Ako bi Institut u budućnosti uključivao studente pripravnike, njima se može otvoriti besplatni privremeni e-račun za vrijeme trajanja prakse, a po odlasku se račun zatvara.)

Primjena pravila: Pravila korištenja e-pošte odnose se na sve zaposlenike, vanjske suradnike (i druge osobe) koji imaju otvoren korisnički račun na e-poslužitelju Instituta. Svi navedeni dužni su pročitati ovaj Pravilnik te ga se pridržavati prilikom slanja i primanja elektroničke pošte putem službene adrese.

Nepridržavanje: Kršenje ovih pravila smatra se povredom radne discipline. Protiv korisnika koji ne poštuje pravila korištenja e-pošte Institut može pokrenuti stegovni postupak. U slučaju ponovljenih ili težih prekršaja (npr. slanja uvredljivih sadržaja, odavanja poslovnih tajni putem e-pošte, slanja spam poruka i sl.) korisniku se može privremeno ili trajno zatvoriti korisnički račun e-pošte te uskratiti pravo korištenja institutske elektroničke pošte. O svim mjerama odlučuje ravnatelj, uz prethodno pribavljeno očitovanje neposredno nadređenog i (ako postoji) voditelja sigurnosti.

PRAVILNIK O ANTIVIRUSNOJ ZAŠTITI

Uvod: Računalni virusi, crvi i ostali zlonamjerni programi predstavljaju stalnu opasnost za informacijske sustave – mogu ugroziti rad mreže, oštetiti podatke te narušiti povjerljivost informacija.

Moderni virusi iznimno su složeni: mnogi se znaju vješto prikriti u sustavu i bilježiti unos s tipkovnice, krasti lozinke ili dokumente i slati ih napadaču preko interneta, pa čak uspostaviti skriveni kanal kojim napadač preuzima daljinsku kontrolu nad računalom. Zbog svega toga zaštita od zlonamjernih programa (malware) više nije stvar izbora pojedinca, nego obvezna odgovornost i Instituta kao cjeline i svakog administratora i korisnika ponaosob.

Opća obveza zaštite: Institut propisuje da je antivirusna zaštita obvezna na svim računalnim sustavima i provodi se na više razina istovremeno:

- na ulaznim točkama mreže – ponajprije na poslužiteljima elektroničke pošte, gdje će se skenirati dolazne i odlazne poruke
- na poslužiteljima datoteka i ostalim internim serverima, gdje će biti postavljena centralizirana antivirusna aplikacija koja štiti zajedničke resurse
- na svakom osobnom računalu (radnoj stanici) u mreži administratori su dužni instalirati antivirusni program na svako računalo korisnika i konfigurirati tzv. centralnu administraciju AV sustava. To znači da se na jednom centralnom poslužitelju održava aktualna baza definicija virusa i postavke zaštite, a sva se korisnička računala automatski povezuju i ažuriraju s tog poslužitelja bez potrebe za djelovanjem korisnika. Time se osigurava jedinstvena i uvijek aktualna zaštita na cijeloj mreži.

Obveze korisnika: Korisnicima se zabranjuje samovoljno isključivanje ili zaobilazanje antivirusne zaštite na službenim računalima. Antivirusni program (skener) mora biti aktivan u memoriji i redovito pregledavati datoteke (u realnom vremenu ili prema rasporedu). Ako korisnik iz nekog opravdanog razloga mora privremeno isključiti antivirus (npr. zbog instalacije softvera koji to zahtijeva), dužan je o tome obavijestiti administratore i čim prije ponovo uključiti zaštitu. Nije dopušteno deinstalirati antivirusni program, mijenjati njegove postavke (npr. isključiti automatsko ažuriranje) ili ignorirati upozorenja koja program javlja.

Reakcija na incident s malwareom: Ako antivirusni program detektira zarazu na nekom računalu, korisnik ili administrator mora nastojati ukloniti zlonamjerni program. Svaki takav slučaj – posebno ako je virus napravio štetu na podacima ili se proširio dalje – smatra se sigurnosnim incidentom i treba biti prijavljen prema proceduri (pogledati Pravilnik o rješavanju sigurnosnih incidenata). Administratori će utvrditi izvor zaraze (npr. USB uređaj, prilog e-poruke) i poduzeti korake da se spriječi ponavljanje (npr. ažurirati filtre, upozoriti korisnika na oprez).

Nepridržavanje: Korisnik koji svjesno isključi ili onemogućí antivirusnu zaštitu na svojem računalu i time uzrokuje štetu ili ugroženost sustava bit će podvrgnut stegovnim sankcijama.

To može uključivati i materijalnu odgovornost ako je nastala veća šteta zbog njegove nebrige. Također, ako korisnik uporno ignorira upozorenja o virusima (npr. stalno unosi zaražene USB stickove i sl.), odgovorna osoba može mu privremeno ograničiti ovlasti korištenja tog medija ili računala.

Administratori koji propuste implementirati propisanu antivirusnu zaštitu na sustavima pod svojom kontrolom također će odgovarati za propust u radu. Institut će povremeno provesti neovisnu provjeru antivirusne zaštite (audit) kako bi se uvjerio da su sva računala pokrivena i da su definicije virusa ažurne.

PRAVILNIK O ZAŠTITI OD SPAMA

Svrha: Neželjene komercijalne poruke (spam) postale su globalni problem internetske komunikacije. Većina spam poruka je reklamnog sadržaja, masovno poslanog na tisuće adresa gotovo bez troška za pošiljatelja – trošak snose primatelji i sustavi koji ih moraju obraditi. Čitanje i brisanje spama troši dragocjeno radno vrijeme i smanjuje produktivnost. Dio neželjenih poruka ima i opasniji karakter: pokušava uvući primatelja u kriminalne aktivnosti ili prijevare – npr. lažno se obećava novčana nagrada u zamjenu za podatke o bankovnom računu, ili se putem e-pošte pokuša iznuditi novac predstavljajući se kao poznanik u nevolji. Takve pokusne prevare (hoax) šire se internetom i cilj im je obmanuti lakovjerne. Korisnici bi trebali znati prepoznati ovakve poruke.

Mjere filtriranja (administratori): Administratori institutske e-infrastrukture dužni su podesiti sustave da bi se maksimalno smanjio ulaz spama.

Preporučuje se višeslojna zaštita:

- prva razina: Primjena tzv. blacklist filtara – prilikom uspostave SMTP veze za dolaznu poštu poslužitelj provjerava IP adresu pošiljatelja u bazama poznatih izvora spama (DNSBL liste otvorenih releja, kompromitiranih izvora itd.). Ako je adresa na „crnoj listi”, poslužitelj će poruku odbiti još na ulazu, čime se sprječava zaprimanje očitog spama.
- druga razina: Automatska provjera sadržaja poruke – poslužitelj može pomoću antispam alata (npr. SpamAssassin) analizirati sadržaj svake pristigle poruke i dodijeliti joj ocjenu (score) koja označava vjerojatnost da je spam. Ako je ocjena iznad određenog praga, poslužitelj može tu poruku automatski označiti kao spam u naslovu, premjestiti ju u posebnu mapu ili privremeno pohraniti u karantenu. Primatelj takve poruke može po potrebi zatražiti da mu se isporuči iz karantene (ako smatra da nije spam). Nakon određenog roka (npr. 30 dana) poruke u karanteni trajno se brišu.
- treća razina: Individualne korisničke postavke – moderni antispam sustavi omogućuju da svaki korisnik dodatno prilagodi filtre za svoju poštu. Npr., korisnik može uključiti da mu se sumnjive poruke automatski preusmjere u lokalnu „Junk” mapu ili da se određeni pošiljatelji uvijek tretiraju kao spam. Kako nije moguće 100 % točno strojno odrediti što je spam, a što legitimna pošta, krajnjem korisniku ostavlja se mogućnost finog podešavanja filtra (tzv. podešavanje praga bodova, kreiranje osobnih „bijelih” i „crnih” lista adresa itd.). Informatičar zadužen za sigurnost dužan je obučiti korisnike kako koristiti te mogućnosti i pomoći im u podešavanju filtara za označavanje, odvajanje ili uništavanje neželjenih poruka.

Pravila za korisnike:

- Korisnicima se zabranjuje slanje masovnih e-poruka putem institutske pošte, bez obzira na sadržaj, osim ako za to postoji izričito odobrenje uprave (npr. službene newsletter poruke). Masovno prosljeđivanje bilo kakvih „forvardiranih” poruka (šala, peticija, lanaca sreće) smatra se kršenjem ovog pravila. Razne uzbune o virusima i dramatična upozorenja koja stižu e-poštom često su lažna i šire nepotrebnu paniku. Korisnici ne bi trebali nekritično prosljeđivati takva upozorenja – uglavnom se radi o hoax porukama koje treba ignorirati ili provjeriti preko službenih izvora. IT služba povremeno će obavijestiti korisnike o poznatim prevarama da bi ih educirala.
- Korisnici ne smiju koristiti računala i mrežu Instituta za slanje propagandnih ili reklamnih poruka u svrhu stjecanja osobne koristi. To uključuje slanje ponuda, marketinških proizvoda, lančane sheme i slične aktivnosti koje nisu dio službenog posla. Korištenje institutske opreme za privatne poslovne aktivnosti (npr. vlastiti biznis) nije dopušteno bez suglasnosti Instituta.

Nepridržavanje: Svako oglašivanje korisnika o ova pravila (i općenito o Politiku prihvatljivog korištenja) – posebno slanje masovnih neželjenih poruka – smatrat će se teškom povredom i protiv takva korisnika bit će pokrenut stegovni postupak. Sankcije mogu uključivati i momentalno zatvaranje e-računa te isključenje s mreže ako je to nužno da se zaustavi daljnje širenje spama.

PRAVILNIK O RJEŠAVANJU SIGURNOSNIH INCIDENATA

Svrha: Ovaj Pravilnik propisuje obvezu prijavljivanja svakog sigurnosnog incidenta te definira postupke kako se incidenti istražuju i rješavaju. Cilj je osigurati da se svi incidenti evidentiraju, da se poduzmu odgovarajuće mjere za sanaciju te da se iz njih izvuku pouke radi sprječavanja budućih incidenata.

Definicija incidenta: Sigurnosni incident je svaki događaj koji ugrožava povjerljivost, integritet ili dostupnost informacija i sustava Instituta. To uključuje (ali nije ograničeno na): neovlašteni pristup sustavu ili podacima, namjerno ili slučajno otkrivanje povjerljivih podataka, gubitak podataka, zarazu računalnim virusom ili drugim malwareom, DoS napad na mrežne servise, krađu ili oštećenje opreme, ozbiljno kršenje ove Politike od strane korisnika, i slične događaje.

Prijava incidenta: Svaki djelatnik ili vanjski suradnik Instituta dužan je odmah prijaviti svaki sigurnosni incident ili sumnju na incident. Konkretni primjeri: primijećeni usporen rad servera ili mreže, nemogućnost pristupa nekom resursu koji je prije radio (moguća indikacija napada ili kvara), gubitak važnih datoteka, sumnja da su podaci neovlašteno izmijenjeni ili obrisani, pojava neobičnog programa ili poruke (mogući virus), kompromitacija lozinke, fizički proboj u zaštićeni prostor i dr.

Institut će izraditi i održavati kontaktnu listu osoba kojima se prijavljuju problemi i incidenti. Ta lista sadržava barem dva telefonska broja za kontakt (npr. administrator i voditelj sigurnosti) i e-adrese, a bit će dostavljena svim zaposlenicima i objavljena na internom webu. Uz to, bit će dostupan i standardni obrazac za prijavu incidenta, koji prijavitelj (ili osoba koja zaprimi usmenu prijavu) ispunjava osnovnim podacima: datum/vrijeme, tko je uočio događaj, kratak opis događaja.

Evidencija incidenata: Svaki prijavljeni incident mora se dokumentirati. Dokumentacija incidenta sastoji se od: popunjenog obrasca prijave, zapisa o poduzetim koracima u rješavanju te konačnog izvješća. Sva se dokumentacija čuva u sigurnosnoj arhivi Instituta. Izvještaji o incidentima smatraju se povjerljivim dokumentima te se spremaju na sigurno mjesto kojem mogu pristupiti samo ovlaštene osobe. Čuvaju se najmanje 10 godina, radi mogućih kasnijih analiza i kao dokazni materijal u potencijalnim stegovnim ili sudskim postupcima. Institut može objavljivati anonimizirane statističke podatke o sigurnosnim incidentima (npr. broj incidenata mjesečno, vrste napada i sl.), ali bez otkrivanja povjerljivih detalja ili osobnih podataka.

Vanjsko prijavljivanje: Ozbiljnije incidente (primjerice, one koji ugrožavaju širu računalnu mrežu ili imaju obilježja kaznenog djela) Institut će prijaviti i nadležnim tijelima. Prijava se vrši ispunjavanjem propisanim putem, što je odgovornost voditelja sigurnosti. Prema potrebi će se incident prijaviti i policiji (odjelu MUP-a za visokotehnološki kriminal) ako postoji sumnja na kazneno djelo.

Postupanje i istraga: Nakon što je incident prijavljen, odgovorne osobe (administrator, voditelj sigurnosti, povjerenstvo – ovisno o težini) započinju istragu i sanaciju:

Hitne mjere ograničavanja štete: Prvo se poduzimaju koraci da se spriječi širenje ili pogoršanje incidenta. Npr., ako je u tijeku računalni napad izvana, može se privremeno odspojiti poslužitelj iz mreže; ako je otkriven virus, izolirat će se zaraženo računalo iz mreže; ako je kompromitiran korisnički račun, odmah ga se blokira; ako su procurili podaci, ograničit će se pristup kompromitiranom sustavu.

Forenzička pravila: Tijekom istrage potrebno je očuvati zatečeno stanje sustava koliko je god moguće. To znači da administratori ne bi smjeli brzopleto ponovno pokrenuti stroj ili brisati tragove – prvo se nastoji sve dokumentirati i napraviti kopije dokaznog materijala. Konkretno, važno je napraviti kopiju svih relevantnih podataka – npr. snimiti sadržaj diska, memorije, konfiguraciju datoteka – prije bilo kakvih promjena. Idealno je napraviti bit-by-bit kopiju (imaging) diska na drugi medij da bi datoteke imale neizmijenjene vremenske oznake (npr. na Linuxu korištenjem naredbe dd). Svaki korak istrage

mora se dokumentirati (što je napravljeno, u koliko sati, tko je napravio) da bi se poslije mogao rekonstruirati cijeli proces. Istragu provodi po mogućnosti jedna osoba uz prisutnost svjedoka da bi se osigurala vjerodostojnost i objektivnost (svjedok može potvrditi poduzete radnje).

Opseg interne istrage: Administratori smiju pratiti korisničke procese na sustavu i provjeriti osnovne indikacije u korisničkim direktorijima (popis datoteka, veličine, datume) ako sumnjaju da se računalo zlorabljiva. Međutim, ne smiju pregledavati sadržaj privatnih korisničkih datoteka (dokumente, e-poruke) bez odobrenja nadređenih i pokretanja službene istrage preko povjerenstva.

Dakle, daljnja detaljna istraga podataka moguća je tek nakon što povjerenstvo za sigurnost (ili ravnatelj) formalno odobri takvu istragu, uz primjenu navedenih forenzičkih pravila.

Izrada izvještaja: Po dovršetku istrage, odgovorna osoba sastavit će službeni izvještaj o incidentu. U njemu se opisuju sve relevantne činjenice: što se dogodilo, kada i kako je otkriveno, koji su podaci bili pogođeni, što je učinjeno, koji je ishod. Izvještaj također sadržava preporuke kako spriječiti da se sličan incident ubuduće ponovi. Izvještaj (ili njegov sažetak) bit će predstavljen upravi Instituta, a čuva se zajedno s incidentnom dokumentacijom u arhivi.

Saniranje i zaključivanje: Kad je incident riješen ili eliminiran, provode se mjere za povratak sustava u normalno stanje – npr. vraćanje oštećenih podataka iz backupa, ponovno podizanje servisa, reset kompromitiranih lozinki, obnova oštećene opreme i slično. Provjerava se je li sustav siguran (clean) prije ponovnog spajanja na mrežu. Voditelj sigurnosti osigurava da su iz incidenta naučene sve lekcije: identificira korijenski uzrok i predlaže trajne mjere (tehničke ili organizacijske) da se takav incident ne bi ponovio. Ako je uzrok bio ljudski faktor (nemar ili zlonamjernost), razmatra se primjena sankcija prema odgovornim osobama.

Sankcije: Osobama koje su svojim djelovanjem ili propustom uzrokovale sigurnosni incident mogu se izreći sankcije, u skladu s težinom incidenta i pravilima Instituta. Institut može odgovornoj osobi zabraniti pristup pojedinim resursima, privremeno ili trajno. Zaposleniku se, ovisno o slučaju, može izreći opomena, smanjenje ovlasti, premještanje ili otkaz ugovora o radu ako se radi o teškoj povredi obveza. Ako je incident prouzročio zaposlenik vanjske tvrtke (npr. konzultant, serviser), Institut može zatražiti od te tvrtke da ga ukloni s liste ovlaštenih osoba za rad u Institutu. U slučaju ozbiljne ili namjerne povrede pravila Institut će razmotriti i raskid ugovora s dotičnom vanjskom tvrtkom, uz moguće pravne korake za nadoknadu štete.

PRAVILNIK O UPRAVLJANJU POVJERLJIVIM INFORMACIJAMA

Klasifikacija informacija: Institut u redovitom poslovanju posjeduje i obrađuje određene povjerljive informacije, ali ne radi se o podacima koji su klasificirani državnom tajnošću. Klasifikacija tajnih podataka u RH uređena je Zakonom o zaštiti tajnosti podataka (*Narodne novine* 64/07 i dr.). Taj zakon definira vrste tajni (vojna, državna, službena, poslovna, profesionalna) i stupnjeve tajnosti (interno, povjerljivo, tajno, vrlo tajno).

Vojna, državna i službena tajna odnose se na državna tijela i u pravilu se ne primjenjuju na rad Instituta (kao znanstvene ustanove).

Međutim, Institut može posjedovati poslovne tajne – informacije komercijalne ili istraživačke vrijednosti čije bi neovlašteno otkrivanje moglo naštetiti interesima Instituta ili njegovih partnera.

To mogu biti, primjerice, povjerljivi ugovori i sporazumi, interni financijski izvještaji, planovi istraživanja, rezultati još neobjavljenih znanstvenih studija, nacrti projekata i sl. Također, djelatnici Instituta mogu doći u posjed osobnih podataka drugih ljudi (npr. podaci o zaposlenicima, suradnicima, sudionicima istraživanja). Po hrvatskim propisima i GDPR-u, osobni podaci uvijek se tretiraju kao povjerljivi (čak i ako formalno nisu označeni tim stupnjem).

Ovaj Pravilnik fokusira se na poslovnu tajnu i povjerljive informacije u širem smislu (uključujući osobne podatke). Svaka informacija koju Institut označi kao povjerljivu ili koja po svojoj prirodi zahtijeva ograničeno raspačavanje mora biti primjereno zaštićena. Dokumenti pristigli izvana s određenom oznakom tajnosti (npr. „povjerljivo“) zadržavaju tu razinu tajnosti u Institutu; ako Institut izradi odgovor ili vlastiti dokument na temelju takva dokumenta, može upotrijebiti istu oznaku tajnosti radi konzistentnosti.

Označavanje i dostupnost: Svi dokumenti i datoteke koji se smatraju povjerljivima moraju biti jasno označeni, po mogućnosti vidljivom naznakom „POVJERLJIVO“ na vrhu, te eventualno navedenim stupnjem povjerljivosti (ako se koristi više razina). Informacije koje nisu tako označene smatraju se javnima (osim osobnih podataka, koji su povjerljivi bez obzira na oznaku). Pravila čuvanja povjerljivosti vrijede neovisno o obliku informacije – bila ona na papiru, u elektroničkom zapisu, izgovorena usmeno ili prikazana vizualno (makete, slike itd.).

Raspodjela odgovornosti: Za formalno proglašavanje određene informacije tajnom/povjerljivom odgovoran je ravnatelj Instituta (ili osoba koju on ovlasti). Ravnatelj donosi popis osoba koje imaju pravo klasificirati podatke kao tajne, kao i popis onih koji mogu pristupiti takvim podacima.

Po inicijalnoj procjeni, gotovo svi zaposlenici imaju pristup barem nekim povjerljivim informacijama (npr. vlastiti ugovor o radu sadržava osobne podatke, što je povjerljivo). No, pristup osjetljivijim poslovnim tajnama imat će uži krug ovlaštenih (npr. samo vodstvo i odgovorni istraživači za pojedini projekt). Obveza čuvanja povjerljivosti ugrađena je u ugovore o radu i ugovore sa suradnicima, a nastavlja vrijediti i nakon prestanka radnog odnosa ili suradnje. Svaka osoba koja prestaje raditi u Institutu i dalje je dužna čuvati u tajnosti povjerljive podatke do kojih je došla za vrijeme suradnje.

Čuvanje povjerljivih dokumenata: Svi povjerljivi materijali – tiskani dokumenti, elektronički zapisi na disku, sigurnosne kopije na medijima i sl. – moraju se čuvati pod fizičkom zaštitom. To znači da trebaju biti u zaključanim metalnim ormarima ili sefovima, po mogućnosti vatrootpornim, smještenim u prostorijama s kontroliranim pristupom. Institut će odrediti osobe zadužene za čuvanje određenih povjerljivih zbirki (npr. tajništvo za ugovore i akte, voditelj projekta za projektne podatke, kadrovska služba za osobne dosjee). Pristup povjerljivim dokumentima regulira se sistemom evidencije: vodi se

lista zaposlenika s ovlastima pristupa i knjiga evidencije u kojoj se bilježi svako izdavanje ili vraćanje povjerljivog dokumenta (datum, ime osobe, dokument).

Tako se u svakom trenutku zna tko raspolaže određenim povjerljivim spisom. Elektroničke povjerljive dokumente treba držati na zaštićenim poslužiteljima s kontrolom pristupa (npr. ograničiti pristup određenim mrežnim mapama samo ovlaštenim korisnicima uz lozinku).

Informacije o zaposlenicima: Podaci o zaposlenicima (i vanjskim suradnicima) smatraju se osjetljivima zbog mogućih zloporaba socijalnog inženjeringa. Socijalni inženjering je tehnika kojom napadači pokušavaju manipulirati ljudima da bi otkrili povjerljive informacije (npr. telefonskim pozivom predstave se kao neka službena osoba i zatraže određene podatke). Radi zaštite privatnosti osoblja, Institut će javno objavljivati samo one podatke o zaposlenicima koji se smatraju javnima: ime i prezime, titulu i radno mjesto, službeni telefonski broj u uredu i službenu e-adresu. Te informacije mogu stajati na web stranici Instituta (kontakti). Na sve druge upite o zaposlenicima (bilo telefonom, e-porukom ili osobno) davat će se samo osnovni podaci već objavljeni na webu ili eventualno u internom imeniku. Osobni podaci zaposlenika (poput kućne adrese, JMBG-a/OIB-a, datuma rođenja, bračnog statusa, plaće, poreznih olakšica, zdravstvenog statusa, privatnog telefona itd.) ne smiju se davati trećim osobama bez izričitog odobrenja dotičnog zaposlenika, osim ovlaštenim državnim tijelima u okviru zakonskih ovlasti (npr. porezna uprava, mirovinsko osiguranje i sl.). Interno su takve osobne informacije dostupne samo ovlaštenim djelatnicima (npr. kadrovskoj i računovodstvenoj službi).

Postupanje s upitima: Ako netko npr. telefonom traži osjetljive podatke o zaposleniku, osoba koja prima poziv treba biti oprezna. Pravilo je da se telefonom načelno ne odaju povjerljivi podaci. Ako se pozivatelj predstavlja kao službena osoba koja „ima pravo“ znati određene podatke (npr. istražitelj, revizor, IT administrator s više razine), treba zapisati njegove podatke: ime, prezime, instituciju i telefon za kontakt. Potom se taj poziv provjerava – kontaktira se nadređeni (npr. ravnatelj ili voditelj sigurnosti) i zajedno odlučuje je li zahtjev legitiman. Tek nakon neovisne provjere autentičnosti i uz odobrenje uprave nazvat će se natrag tu službenu osobu i odgovoriti na pitanja.

Ako se posumnja da je riječ o prevari, traženi podaci se ne daju i incident se prijavljuje voditelju sigurnosti. Zaposlenicima se savjetuje: „budite sumnjičavi prema neobičnim zahtjevima za informacije o kolegama i uvijek provjerite identitet i pravo na te informacije prije otkrivanja bilo čega.”

Prijenos povjerljivih informacija: Za prijenos (dostavu) podataka koji su klasificirani kao povjerljivi vrijede posebne mjere:

- tiskani dokumenti koji su povjerljivi ne smiju se slati običnom poštom u omotnici – preporučuje se koristiti kurirsku dostavu uz potpis primatelja
- npr. za interne povjerljive dopise između ustanova koristiti DHL Secure ili osobno uručivanje uz potpis primitka.

Elektronička dostava: Povjerljive informacije ne šalju se nezaštićenim kanalima. Ako se šalju putem elektroničke pošte ili pohrane u oblaku, moraju biti kriptirane (šifrirane) primjerenom metodom. To može biti enkripcija privitka lozinkom (poslati lozinku drugim kanalom), korištenje PKI certifikata za šifriranje e-poruke ili sigurne end-to-end enkripcije ako je dostupna.

Telefonom/faksom: Izbjegavati prenošenje povjerljivih informacija telefonom ili faksom. Ako je neophodno, prethodno dogovoriti kodne riječi ili identifikaciju. Faksirati povjerljive dokumente samo uz prethodni dogovor da je ovlaštena osoba kraj faks uređaja na strani primatelja.

Interni prijenos: Ako se povjerljivi dokumenti nose unutar zgrade (npr. iz jednog ureda u drugi), treba ih nositi tako da sadržaj nije vidljiv (u fasciklu ili zatvorenoj omotnici). Ne smije se ostavljati takve dokumente bez nadzora na stolovima ili u zajedničkim prostorijama.

Umnožavanje povjerljivih dokumenata: Nije dopušteno kopirati ili umnožavati povjerljive dokumente osim ako je to nužno za posao i uz odobrenje vlasnika informacije (osobe ili tijela koje je dokument označilo povjerljivim).

Svaka kopija postaje povjerljiv dokument koji podliježe istom režimu zaštite. Broj kopija treba svesti na minimum. Posebno, dokumenti pristigli izvana s oznakom tajnosti ne smiju se kopirati bez izričitog dopuštenja pošiljatelja. Ako je potrebno više osoba upoznati s takvim sadržajem, poželjno je zatražiti od pošiljatelja dodatne primjerke ili dozvolu za umnožavanje uz evidenciju.

Uništavanje povjerljivih podataka: Povjerljivi dokumenti koji više nisu potrebni moraju se uništiti na siguran način. Papirnati dokumenti uništavaju se rezanjem u sitne čestice (minimalno razina 3 unakrsne rezalice ili usluga arhivskog uništavanja). Elektronički mediji (CD, USB) s povjerljivim podacima fizički se uništavaju ili barem nepovratno brišu (npr. višestrukim prepisivanjem, degausserom za magnetne medije). Za uništavanje većeg opsega dokumenata Institut može angažirati ovlaštenu tvrtku, uz potpis ugovora o povjerljivosti i dobivanje certifikata o uništenju.

Nepridržavanje: Svako neovlašteno otkrivanje povjerljivih informacija smatra se teškom povredom obveza. Zaposlenik koji namjerno ili iz krajnje nepažnje odaje poslovnu tajnu ili osobne podatke neovlaštenim osobama podliježe stegovnom postupku i mogućem izvanrednom otkazu ugovora o radu, a može snositi i kaznenu odgovornost prema Kaznenom zakonu i prekršajnu prema Zakonu o GDPR-u. Vanjski suradnik koji prekrši povjerljivost bit će odmah isključen iz svih poslova i odgovarat će prema uvjetima ugovora o suradnji (ugovorna kazna, naknada štete). Institut će u svakom takvu slučaju poduzeti potrebne pravne radnje da bi zaštitio svoje interese i podatke svojih djelatnika/klijenata.

Zaključak: Upravljanje povjerljivim informacijama ključno je za ugled i pravnu sigurnost Instituta. Poštovanjem ovog Pravilnika svaki zaposlenik doprinosi zaštiti podataka i povjerenju koje javnost ima u Hrvatski institut za povijest. Svi zaposlenici i suradnici potpisom ugovora o radu ili Izjave o čuvanju povjerljivih informacija (NDA) potvrđuju da su upoznati i suglasni s ovdje navedenim obvezama čuvanja tajnosti.

Politika informacijske sigurnosti objavljena je na mrežnim stranicama Instituta i primjenjuje se od dana objave na mrežnim stranicama Instituta.

KLASA: 119-01/26-03/05

URBROJ: 251-849-02-01-26-5

U Zagrebu 18. 2. 2026.



dr. sc. Miroslav Akmadža