Institut za
javne financije

Temeljem čl. 1. Odluke o prihvatljivom korištenju CARNet mreže; Klasa: 500-200/12/95, Ur.br.: 110082-650-109-12-1 od 15 lipnja 2012. i članka 12. Statuta Instituta za javne financije, Upravno vijeće Instituta za javne financije (u daljnjem tekstu: Institut) na sjednici održanoj 20. prosinca 2019. godine donosi

Sigurnosnu politiku informacijskih sustava Instituta za javne financije

Pravila rada i ponašanja koja definira sigurnosna politika vrijede za:

- svu računalnu opremu koja se nalazi u prostorima Instituta;
- administratore informacijskih sustava te pripadajuću tehničku službu;
- korisnike, među koje spadaju zaposlenici, vanjski suradnici, volonteri i studenti;
- vanjske pravne i/ili fizičke osobe tvrtke koje po ugovoru rade na održavanju opreme ili softvera.

Organizacija upravljanja sigurnošću

Ključna stvar pri provođenju sigurnosne politike informacijskoga sustava jest da se u svakome trenutku točno zna tko je zadužen za obavljanje određenoga zadatka te tko odgovara za određeni segment opreme, odnosno računalnoga programa. Potrebno je, stoga, raspodijeliti zaduženja, obrazovati korisnike te oformiti povjerenstvo za sigurnost.

Ljudi koji se u radu koriste računalima dijele se na korisnike i davatelje informatičkih usluga.

Korisnici informatičkih usluga

Korisnici su osobe koje se u svom radu ili učenju služe računalima, proizvode dokumente ili unose podatke. Svaki korisnik informacijskog sustava mora znati koja je njegova uloga u poboljšanju sigurnosti ukupnog sustava.

Dužnosti korisnika su:

- pridržavanje pravila prihvatljivoga korištenja, što znači da ne smiju koristiti računala za djelatnosti koje nisu u skladu s važećim zakonima, etičkim normama i pravilima lokalne sigurnosne politike
- čuvanje zaporke
- prijavljivanje sigurnosnih incidenata kako bi se što prije riješili problemi.

Korisnici koji proizvode podatke i dokumente odgovorni su za njihovo čuvanje. To podrazumijeva da, čak i kada postoji automatski sustav stvaranja sigurnosnih kopija, sami moraju izrađivati sigurnosne kopije.

Dokumenti u elektroničkom obliku smatraju se službenim dokumentima na isti način kao i dokumenti na papiru, pa treba osigurati njihovo čuvanje i ograničiti pristup samo ovlaštenim osobama.

Glavni korisnik

Institut koristi aplikacije za obradu podataka i to računovodstveno-knjigovodstvene programe kao module centralne aplikacije/blagajna, glavna knjiga i saldo konti, osnovna sredstva, sitni inventar, obračun ugovora o djelu, obračun plaća...) i web aplikacije. Kada postoji više korisnika

koji rabe određenu aplikaciju za obradu podataka, primjerice računovodstveni program, radi poboljšanja sigurnosti jedna osoba imenuje se glavnim korisnikom. U navedenome primjeru voditelj računovodstva bio bi glavni korisnik.

Glavni korisnik kontaktira proizvođača aplikacije i dogovara isporuku novih inačica, traži ugradnju sigurnosnih mehanizama itd.

Zaposlenici koji unose podatke odgovaraju za njihovu vjerodostojnost, dok je glavni korisnik odgovaran za ispravnost podataka, provjeru ispravnosti i sigurnosti aplikacije, za dodjelu dozvola za pristup podatcima i za mjere sprečavanja izmjene podataka od strane neautoriziranih osoba.

Davatelji informatičkih usluga

Davateljima usluga smatraju se profesionalci koji se brinu o radu računala, mreže i informacijskih sustava. Ugovoreni davatelj informacijskih usluga za Institut za javne financije je Obrt za informatičku djelatnost "WEB-DATA" - vl. Petar Turtula, Zagreb, Ilica 114/1. On odgovara za ispravnost i neprekidnost rada informacijskog sustava, sukladno ugovoru o održavanju.

Ugovorenog davatelja informacijskih usluga Institut može promijeniti odlukom Ravnatelja.

Davatelji usluga dužni su u svome radu poštivati privatnost ostalih korisnika i povjerljivost informacija s kojima dolaze u dodir pri obavljanju posla. Kako bi ih Institut obvezao na poštivanje tih pravila, davatelji usluga potpisuju Izjavu o čuvanju povjerljivih informacija, čiji je predložak dan među pratećim dokumentima.

Specijalisti za sigurnost

Institut će pri rješavanju sigurnosnih incidenata koristiti pomoć CARNeta.

Pored toga, Institut će obrazovati i imenovati djelatnika čija će zadaća biti briga za organizaciju i provođenje sigurnosnih mjera navedenih u Sigurnosnoj politici.

Ravnatelj Instituta imenuje voditelja sigurnosti čija je prvenstvena briga sigurnost informacijskih sustava. Poželjno je da voditelj sigurnosti bude stručna osoba, a i da posjeduje sposobnost vođenja ljudi te da je komunikativan. U pravilu je to CARNet koordinator ustanove.

Njegova je briga ukupna sigurnost informacijskih sustava. To uključuje i fizičku sigurnost sustava, pa će voditelj surađivati i s ostalim zaposlenicima. Voditelj sigurnosti piše upute, nadzire rad mreže i servisa, organizira obrazovanje korisnika i administratora, komunicira s upravom, sudjeluje u donošenju odluka o nabavi računala i softvera te sudjeluje u razvoju softvera, kako bi osigurao da se poštuju pravila iz sigurnosne politike.

U radu koristi pomoć vanjskih suradnika, stručnjaka za pojedina područja sigurnosti informacijskih sustava kao i pomoć CARNeta .

Postupci za rješavanje incidenata dani su u pratećem dokumentu pod nazivom Protokol o rješavanju sigurnosnih incidenata.

Institut treba izraditi i održavati kontakt listu s imenima, brojevima telefona, e-mail adresama osoba kojima se prijavljuju incidenti: kvarovi opreme, sporost ili nedostupnost mrežnih usluga i podataka, povreda pravila sigurnosne politike ili zakonskih odredbi.

Administriranje računala

Davatelji usluga dužni su administrirati računala i mrežnu opremu u skladu s pravilima struke, brinući se istodobno o funkcionalnosti i sigurnosti.

Za svako računalo se imenuje administrator, koji odgovara za instalaciju i konfiguraciju softvera. U pravilu to je CARNet koordinator ili davatelj informatičkih usluga. Samo iznimno, ukoliko se, po procjeni ravnatelja, ukaže potreba da korisnici sami administriraju osobno računalo na kojem rade, uz posebno dopuštenje i odluku ravnatelja, a uz suglasnost voditelja sigurnosti, potpisuju izjavu o tome, nakon čega za njih vrijede sva pravila za administriranje računala.

Računala se moraju konfigurirati na način da budu zaštićena od napada izvana i iznutra, što se osigurava instaliranjem softverskih zakrpa prema preporukama proizvođača, listama pristupa, filtriranjem prometa i drugim sredstvima.

Posebnu pozornost administratori su dužni posvetiti opremi koja obavlja ključne funkcije ili sadrži vrijedne i povjerljive informacije koje treba štititi od neovlaštena pristupa.

Administratori računala svakodnevno prate rad sustava, čitaju dnevničke zapise i provjeravaju rad servisa. Zadaća je administratora i nadgledanje rada korisnika, kako bi se otkrile nedopuštene aktivnosti.

Administratori su dužni prijaviti incidente ravnatelju Instituta pismenim putem te pomoći pri istrazi i uklanjanju problema. Incidenti se dokumentiraju kako bi se pomoglo u nastojanju da se izbjegnu slične situacije u budućnosti. Ako je incident ozbiljan i uključuje kršenje zakona, prijavljuju se CARNet-ovu CERT-u.

Upravljanje mrežom

Ravnatelj Instituta imenuje osobu koji je zadužen za upravljanje mrežom, konfiguriranje mrežnih uređaja, dodjeljivanje adresa, kreiranje virtualnih LAN-ova itd.

Ne dopušta se priključivanje računala vanjskih korisnika i suradnika na mrežu Instituta. Načini spajanja propisani su Protokolom o korištenju informacijskih sustava Instituta za vanjske suradnike, studente i korisnike Instituta.

Osoba zadužena za upravljanjem mrežom mora u svakom trenutku imati točan popis svih mrežnih priključaka i umreženih uređaja, uključujući i prijenosna računala.

Ako je podržan rad na daljinu, kada se primjerice djelatnicima dopušta spajanje s kućnoga računala na mrežu Instituta, mora se osigurati da udaljeno računalo ne ugrozi sigurnost mreže ustanove, s obzirom na mogućnost da ga koriste neautorizirane osobe, članovi obitelji i slično. Povjerljivi podatci na udaljenom računalu moraju biti jednako sigurni kao da se računalo nalazi u zgradi ustanove.

Spajanje gostujućih računala na mrežu, koja donose sa sobom vanjski suradnici, predavači, poslovni partneri i serviseri podrazumijeva poštivanje institutskih pravila koja se odnose na sigurnost i zaštitu podataka. Ne dopušta se da oni po svom nahođenju priključuju računala na mrežu ustanove zbog opasnosti od širenja virusa ili namjernih agresivnih radnji, poput presretanja mrežnoga prometa, prikupljanja informacija itd. Institut može odrediti priključna mjesta, primjerice u određenim uredima, gdje je dopušteno priključiti gostujuća računala, te konfiguracijom mreže spriječiti da se s tog segmenta mreže dopre do ostalih računala u ustanovi.

Institutska bežična mreža zaštićena je na način da se ne može bilo tko priključiti i služiti se njome te snimati promet. To se postiže metodama enkripcije i autentifikacije uređaja i korisnika.

Instalacija i licenciranje softvera

Korištenje ilegalnoga softvera predstavlja povredu autorskog prava i intelektualnoga vlasništva. Da bi se zaštitila od moralne i materijalne štete koja time može nastati, Institut zadužuje administratore za instaliranje softvera i njegovo licenciranje. Korisnik koji ima potrebu za nekim programom mora se obratiti ovlaštenoj osobi i zatražiti, uz obrazloženje, nabavu i instalaciju.

Korisnici su obvezni poštivati autorska prava, između ostalog i potpisivanjem Izjave o prihvaćanju odredbi sigurnosne politike Instituta i da će je se pridržavati. Povjerenstvo za sigurnost informacijskih sustava

Kako bi osigurao upravljanje sigurnošću, Institut će oformiti Povjerenstvo za sigurnost. Povjerenstvo sačinjavaju Ravnatelj, voditelj sigurnosti i davatelj informatičkih usluga.

Povjerenstvo prima izvještaje o sigurnosnoj situaciji i predlaže mjere za njezino poboljšanje, uključujući nabavu opreme, organizaciju obrazovanja korisnika i specijalista. Povjerenstvo daje odobrenje za provođenje istrage u slučajevima incidenata, podnosi izvještaj o stanju sigurnosti upravi Instituta, te se zalaže za donošenje konkretnih mjera, nabavu potrebne opreme, ulaganje u obrazovanje specijalista, ali i običnih korisnika.

Fizička sigurnost

Prostor u Institutu dijeli se na dio koji je otvoren za javnost, prostor u koji imaju pristup samo zaposleni te prostor u koji pristup imaju samo skupine zaposlenih, ovisno o vrsti posla koji obavljaju.

Ključeve Instituta smiju imati samo zaposlenici Instituta, a osoba ovlaštena za izdavanje ključeva je ravnatelj Instituta. Iznimno, odlukom ravnatelja, ključevi se mogu dodijeliti vanjskim suradnicima i o tome se treba voditi uredna dokumentacija. Popis osoba koje imaju ključ Instituta mora biti ažuran, a prijem ključa i/ili njegov povrat vlastoručno potpisan.

U skupinu prostora s ograničenim pristupom spadaju server soba, računalna ostava 2, računovodstvo i arhiva. Institut je dužan sastaviti popis osoba koje imaju pristup u zaštićene prostore, a ravnatelj i osoba za sigurnost moraju imati popis osoba koje mogu dobiti ključeve određenih prostorija.

Sigurne zone

Računalna oprema koja obavlja kritične funkcije, neophodne za funkcioniranje informacijskoga sustava ili sadrži povjerljive informacije, fizički se odvaja u prostor u koji je ulaz dopušten samo ovlaštenim osobama.

Institut je dužan održavati popis ovlaštenih osoba koje imaju pristup u sigurne zone.

U pravilu su to zaposlenici koji administriraju mrežnu i komunikacijsku opremu i poslužitelje ključnih servisa. Oni ulaze u sigurne zone samo kada treba ukloniti zastoje, obaviti servisiranje opreme. Stoga je poželjno administratorima osigurati radni prostor odvojeno od prostorija u kojima je smještena oprema koja sadrži najvažnije informacije .

Kritična oprema treba biti zaštićena od problema s napajanjem električnom energijom, što znači da električne instalacije moraju biti izvedene kvalitetno, da se koriste uređaji za neprekidno napajanje, a po potrebi i generatori električne energije.

Treba predvidjeti i druge moguće probleme, poput poplava, požara i slično te poduzeti mjere da se oprema i informacije zaštite te da se osigura njihov što brži oporavak. U sigurnim zonama i u njihovoj blizini ne smiju se držati zapaljive i eksplozivne tvari.

Vanjske tvrtke

Ugovorom se regulira pristup vanjskim tvrtkama, čime se podrazumijeva pristup prostorijama, pristup opremi ili logički pristup povjerljivim informacijama. Treću stranu treba obvezati na čuvanje povjerljivih informacija s kojima dođu u dodir pri obavljanju posla.

Vanjske tvrtke svoj redovni dolazak radi servisiranja opreme trebaju najaviti voditelju sigurnosti najmanje 24 sata ranije kako bi im se omogućio ulazak u prostorije koje su proglašene sigurnim zonama.

Institut može zahtijevati da svaka osoba koja pristupa povjerljivoj opremi, sigurnoj zoni ili osjetljivim informacijama potpiše Izjavu o čuvanju povjerljivih informacija.

Ako u sigurnu zonu radi potrebe posla ulaze osobe koje nemaju ovlasti, mora im se osigurati pratnja. Strana osoba može se ostaviti da obavi posao u zaštićenom prostoru samo ako je osiguran video-nadzor.

Ako se vanjskoj tvrtki prepušta održavanje opreme i aplikacija s povjerljivim podatcima, Institut može od vanjske tvrtke zatražiti popis osoba koje će dolaziti u prostorije Instituta radi obavljanja posla. U slučaju zamjene izvršitelja, vanjska tvrtka dužna je na vrijeme obavijestiti Institut.

Institut zadržava pravo da osobama koje se predstavljaju kao djelatnici vanjskih tvrtki uskrati pristup ako nisu na popisu ovlaštenih djelatnika.

Sigurnost opreme

Klasifikacija računalne opreme

Institut dijeli svu opremu u grupe prema zadaćama:

- Zona javnih servisa (tzv. demilitarizirana zona) – oprema koja obavlja javne servise (DNS poslužitelj, HTTP poslužitelj, poslužitelj elektroničke pošte itd.).
- Intranet je privatna mreža Instituta, a čine je poslužitelji internih servisa, osobna računala zaposlenih, računalne učionice te komunikacijska oprema lokalne mreže.

Podjela opreme prema vlasništvu

U prostorijama Instituta nalazi se i oprema CARNeta i/ili Ministarstva znanosti i obrazovanja, koja je dana na korištenje Ustanovi.

Institut održava popis sve računalne opreme, s opisom ugrađenih komponenata, inventarnim brojevima itd.

Institut se brine jednako o svoj opremi kojom raspolaže, bez obzira na to tko je njezin vlasnik. Oprema se čuva od oštećivanja i otuđenja.

Institut je dužan osoblju CARNeta i/ili Srca dozvoliti pristup opremi u vlasništvu CARNeta/MZO-a/ministarstva koja se nalazi u Institutu.

Odgovornost za računalnu opremu

Za fizičku sigurnost opreme odgovoran je ravnatelj Instituta. On odgovornost za grupe uređaja ili pojedine uređaje prenosi na druge zaposlene, koji potpisuju dokument kojim potvrđuju da su preuzeli opremu.

Preporuka je da Institut razradi procedure kojima se nastoji spriječiti otuđenje i oštećenje računalne opreme. Osoba zadužena za sigurnost provjerava je li oprema koja se iznosi ima potrebne prateće dokumente, izdatnice, radne naloge za popravak itd.

Osiguranje neprekidnosti poslovanja

Kako bi se sačuvali podatci u slučaju nezgoda, poput kvarova na sklopovlju, požara ili ljudskih pogrešaka, potrebno je redovito izrađivati pričuvne kopije svih vrijednih informacija, uključujući i konfiguraciju softvera. Preporuča se izrada više kopija koje se čuvaju na različitim mjestima, po mogućnosti u vatrootpornim ormarima. Procedura za izradu rezervnih kopija razrađena je u Protokolu o izradi sigurnosnih kopija.

Radi osiguranja neprekinutosti poslovanja, preporuka je razraditi i procedure za oporavak kritičnih sustava te ih čuvati u pismenom obliku, kako bi u slučaju zamjene izvršitelja novozaposleni djelatnici mogli brzo reagirati u slučaju nezgoda.

Povremeno se provjerava upotrebljivost pričuvnih kopija podataka te se izvode vježbe oporavka sustava. Vježbe se ne izvode na produkcijskim računalima, već na pričuvnoj opremi.

Nadzor nad informacijskim sustavima

Institut zadržava pravo nadzora nad instaliranim softverom i podatcima koji su pohranjeni na umreženim računalima te nad načinom korištenja računala.

Nadzor se smije provoditi radi:

- osiguranja integriteta, povjerljivosti i dostupnosti informacija i resursa
- provođenja istrage u slučaju sumnje da se dogodio sigurnosni incident
- provjere jesu li informacijski sustavi i njihovo korištenje usklađeni sa zahtjevima sigurnosne politike.

Nadzor smiju obavljati samo osobe koje je Institut za to ovlastio. Pri provođenju nadzora ovlaštene osobe dužne su poštivati privatnost i osobnost korisnika i njihovih podataka. No, u slučaju da je korisnik prekršio pravila sigurnosne politike, ne može se više osigurati povjerljivost informacija otkrivenih u istrazi te se one mogu koristiti u stegovnom ili sudskom postupku.

Doseg

Ova se pravila odnose na svu računalnu opremu koja se nalazi u prostorijama Instituta i priključena je na mrežu CARNet, na sav instalirani softver te na sve mrežne servise, kao i na prijenosna računala u vlasništvu Instituta.

Pravila su dužni poštivati i provoditi svi zaposleni, studenti i vanjski suradnici koji po ugovoru obavljaju određene poslove.

Provođenje

Svi korisnici su dužni pomoći osobama zaduženima za nadzor informacijskih sustava tako što će im pružiti sve potrebne informacije i omogućiti im pristup prostorijama i opremi radi provođenja nadzora.

Isto vrijedi i za administratore računala i pojedinih servisa, koji su dužni osobama za sigurnost pomagati pri istrazi.

Pristup uključuje:

- pristup na razini korisnika ili sustava svoj računalnoj opremi
- pristup svakoj informaciji, u elektroničkom ili tiskanom obliku, koja je proizvedena ili spremljena na opremi Instituta, ili oprema Instituta služi za njezin prijenos
- pristup radnom prostoru (uredu, sigurnoj zoni itd.)
- pravo na interaktivno nadgledanje i bilježenje prometa na mreži Instituta.

Nepridržavanje

Zaposlenika koji se ogluši na pravila o nadzoru može se disciplinski kazniti ili mu se mogu uskratiti prava korištenja mreže i njezinih servisa. Ostali korisnici Instituta koji se ogluše na pravila o nadzoru mogu podlijegati ugovornim sankcijama uz uskraćivanje prava korištenja mreže i njezinih servisa.

Uz pravila nadvedena u Općoj sigurnosnoj politici po potrebi i u posebnim slučajevima primjenjuju se posebna pravila definirana pratećim dokumentima. Prateći protokoli pisani su kao upute za rješavanje konkretnih problema i mogu se mijenjati prema potrebi. To su:

- Protokol o rukovanju zaporkama
- Protokol o korištenju elektroničke pošte
- Protokol o rješavanju sigurnosnih incidenata
- Protokol o izradi kopija podataka
- Protokol o korištenju informacijskih sustava Instituta za vanjske suradnike i korisnike
- Protokol o korištenju prijenosnih računala Instituta
- Protokol o antivirusnoj zaštiti
- Protokol o zaštiti od *spama*
- Protokol o obrazovanju osoba zaduženih za sigurnost računalnog sustava
- Protokol o upravljanju povjerljivim informacijama
- Izjava o čuvanju povjerljivih informacija
- Izjava o prihvaćanju odredbi sigurnosne politike

Sigurnosna politika informacijskih sustava Instituta za javne financije temelji se na dokumentu Sigurnosna politika informacijskih sustava za clanice CARNeta (prijedlog)

Za Institut:

prof. dr. sc. Ivan Pavić
Predsjednik Upravnog vijeća

U Zagrebu, 20. prosinca 2019.
Ur.broj:

Sigurnosna politika informacijskih sustava objavljena je na oglasnoj ploči Instituta dana 23. prosinca 2019., a stupa na snagu dana 1. siječnja 2020.

Protokol o rukovanju zaporkama

Svrha

Prosječan korisnik nerijetko smatra kako se ne mora brinuti o sigurnosti jer njegovo računalo ne sadrži vrijedne informacije. No, kompromitiranjem jednoga osobnog računala u lokalnoj mreži ili jednoga korisničkog računa na poslužitelju napadač je probio obrambenu liniju i otvorio prolaz za napade na važnije sustave i informacije. Stoga je svaki korisnik dužan čuvati zaporke i time doprinositi zaštiti cijeloga sustava.

Dok snaga računala neprestano raste, ljudske sposobnosti stagniraju. Današnja računala mogu brzo dekriptirati jednostavne zaporke, dok u isto vrijeme većina ljudi ne može pamtiti složene zaporke od osam i više znakova.

Doseg

Svi korisnici Instituta za javne financije kao i suradnici koji se u svome radu služe računalima dužni su pridržavati se ovih pravila korištenja zaporki, dok su ih administratori dužni tehnički ugraditi u sve sustave koji to omogućuju.

Pravila za korištenje zaporki

1. Minimalna dužina zaporke

Kratku zaporku lakše je probiti. Stoga je minimalna dužina zaporke šest znakova, ali se preporučuje korištenje još dužih zaporki i zaporki koje uključuju barem jedno veliko slovo i jednu brojku, odnosno jedan poseban znak.

2. Ne služiti se riječima iz rječnika

Ne preporučuje se služenje riječima iz standardnojezičnih rječnika. Hakeri posjeduju zbirke rječnika, što im olakšava probijanje ovakvih zaporki (tzv. *dictionary attack*).

3. Izmiješati mala i velika slova s brojevima

Npr. h0bo3niCa. Na prvi pogled besmislena i teška za pamćenje, ova je zaporka izvedena iz riječi hobotnica. Polazište je pojam koji lako pamtimo, ali po nekom algoritmu provodimo zamjenu znakova.

4. Imena bliskih osoba, ljubimaca, datume

Ne treba koristiti takve zaporke jer se lako otkriju socijalnim inženjeringom.

5. Tajnost zaporke

Korisnici su odgovorni za svoju zaporku i ni u kom je slučaju ne smiju otkriti nikome, pogotovo je ne smije slati e-mailom, čak ni administratorima sustava. Hakeri nastoje izmamiti zaporke lažno se predstavljajući kao administratori (*phishing*).

6. Čuvanje zaporke

Zaporke se ne ostavljaju na papirićima koji su zalijepljeni na ekran ili ostavljeni na stolovima, u nezaključanim ladicama itd. Korisnik je odgovoran za tajnost svoje zaporke te mora naći način da je sakrije. Ako korisnik zaboravi zaporku, administrator će mu omogućiti da unese novu.

Nepridržavanje

Korisnici koji se ne pridržavaju navedenih pravila ugrožavaju sigurnost informacijskoga sustava. Institut je obavezan djelovati i obrazovati korisnike u kreiranju sigurnih zaporki.

U slučaju ignoriranja ovih pravila Institut može stegovno djelovati ili postaviti zaposlenika na radno mjesto na kojem je manja mogućnost ugrožavanja integriteta i sigurnosti sustava i podataka, a u u skladu s općim radnopravnim pravilima.

Protokol o korištenju elektroničke pošte

Elektronička pošta (e-mail) postala je dio svakodnevne komunikacije, poslovne i privatne, slijedom toga sa sobom nosi i izvjesne rizike, poput otkrivanja povjerljivih podataka, lažnog predstavljanja, širenja virusa i sl. Stoga zaposlenici i suradnici moraju komunicirati na način da se izbjegne nanošenje štete Institutu. Pravila korištenja elektroničke pošte odnose se na sve zaposlenike Instituta i vanjske suradnike kojima radi obavljanja posla Institut daje identitet s e-mail adresom u domeni ijf.hr.

Protokol koji se koristi za prijenos elektroničke pošte, SMTP ili Simple Mail Transport Protocol, nije od samog početka dizajniran da bude siguran. Dodatne probleme ponekad izazivaju i korisnici, koji nisu posve svjesni zamki pri korištenju e-maila.

Problemi koji mogu nastati korištenjem elektroničke pošte su sljedeći:

1. Nesigurnost protokola
   - Poruke putuju kao običan tekst, te ih je lako presresti i pročitati, ili čak izmijeniti sadržaj.
   - Lako je krivotvoriti adresu pošiljatelja, tako da nikada niste sigurni tko vam je zapravo poslao poruku.
   - Protokoli za čitanje elektroničke pošte, POP i IMAP, u svom osnovnom obliku šalju korisničko ime i zaporku kao običan tekst, pa ih je moguće presresti i pročitati. Stoga je potrebno, kad god je to moguće, koristiti kriptografiju, na primjer SSL za prijenos i PGP za skrivanje sadržaja.

2. Nepažnja korisnika
   - U žurbi se lako pritisne pogrešna tipka ili se klikne na susjednu ikonu. Time može nastati nepopravljiva šteta - ne možete zaustaviti poruku koja je već otišla. Na primjer, ako se umjesto *Odgovori* pritisne *Odgovori svima* (engl. *Reply, Reply All*) , poruka može otići primateljima kojima nije namijenjena.
   - Česta je pogreška i preuzimanje pogrešne adrese iz adresara.
   - Neki mail klijenti sami dovršavaju e-mail adresu koju tipkate. Nepažnjom se može prihvatiti adresa slična onoj koju zapravo tražite.

3. Nesporazumi
   - Elektroničku poštu smo skloni pisati leženo i neobavezno. Primatelj ne mora doživjeti poruku na isti način, stoga službene dopise pišite pažljivo i odmjereno.
   - Iza Vašeg imena u adresi elektroničke pošte nalazi se naziv ustanove. Pišući, budite svjesni da netko može shvatiti vašu privatnu prepisku kao službeni dopis, vaše privatno mišljenje kao službeni stav ustanove. Stoga u raspravi uvijek jasno naznačite kada je izneseni stav vaše privatno uvjerenje.

4. Otkrivanje informacija
   - Poruke koje ste uputili jednoj osobi začas se mogu proslijediti dalje. To se može dogoditi
     - (zlo)namjerno, s ciljem da se naškodi drugoj osobi ili tvrtki
     - nemarom sudionika, koji ne traži dozvolu za prosljeđivanje poruke
     - slučajno, na primjer nehotičnim klikom mišem na pogrešnu ikonu (Odgovori svima umjesto Odgovori)

- Stoga poslovne dopise koji sadrže osjetljive informacije treba označiti kao povjerljive, kako bismo primatelja obavezali na diskreciju.
- U slučaju sigurnosnog incidenta, istraga može dovesti do otkrivanja sadržaja poruka koje su zamišljene kao privatna komunikacija. Institut se obavezuje čuvati povjerljivost takvih poruka, ali to neće moći garantirati budu li poruke tretirane kao dokazni materijal u istrazi ili u mogućem sudskom procesu.

5. Radna etika

- Veliki broj poruka koje treba svakodnevno pročitati može vam oduzeti znatan dio radnog vremena. Stoga ograničite broj privatnih poruka.
- Lančane poruke koje ljudi šalju poznanicima mogu sadržavati lažne informacije ili biti dio prijevare, s namjerom da se ljudima izvuče novac (pomozite nesretniku kojem treba operacija, otvorite račun kako bi svrgnuti diktator mogao izvuci novac iz nestabilne afričke države...). Za provjeru ovakvih poruka (engl. hoax) može se koristiti servis CARNet CERT-a Hoax recognizer
- *Spam*, slanje neželjenih komercijalnih poruka, sve više opterećuje promet na Internetu, te oduzima vrijeme, cak i ako brišete takve poruka bez čitanja. Institut će filtrirati *spam* na poslužitelju elektroničke pošte . Obaveza je korisnika da sami ne šalju takve poruke.

6. Povrede autorskih prava

- Svaka poruka elektroničke pošte može se, kao dovršen dokument, smatrati autorskim djelom. Prosljeđivanje poruke trećoj strani bez dozvole autora odnosno vlasnika smatra se povredom autorskog prava. Prosljeđivanjem poruke koja je pisana za vas trećoj strani, autora poruke možete dovesti u neugodnu situaciju, jer bi poruku, da je znao da će je čitati i ljudi kojima nije namijenjena, drugačije sročio.
- Prilozi koji se šalju uz elektroničke poruke mogu sadržavati autorski zaštićene informacije, npr. glazbu, članke itd.

Zbog svega navedenog korištenje elektroničke pošte smatra se rizičnom djelatnošću, te se zaposlenici obvezuju na pridržavanje sljedećih pravila:

- Institut daje zaposlenima e-mail adresu radi službene komunikacije.
- Poslovne poruke elektroničke pošte smatraju se službenim dokumentima.
- Privatne poruke dozvoljene su u mjeri u kojoj ne ometaju obavljanje posla. Za privatne potrebe mogu se koristiti za to namijenjene HR-F domene.
- Svaki dopis ili poruka s adrese koja završava s @ijf.hr može se shvatiti kao službeni dopis ili poruka, a osobni stav pošiljatelja kao službeni stav IJF-a. Zato prilikom iznošenja osobnih uvjerenja treba jasno istaknuti da su to samo osobna uvjerenja.
- Nije dozvoljeno slanje neželjenih masovnih poruka, jer se primateljima oduzima dragocjeno vrijeme i neracionalno troše mrežni i računalni resursi.
- Zabranjeno je slanje poruka s adrese koja završava s @ijf.hr u slučaju da se poruka odnosi na privatnu aktivnost koja je slična ili može izgledati zbunjujuće slična poslovnoj aktivnosti IJF-a ili aktivnosti za koju primatelj može smatrati da je aktivnost IJF-a.
- Svaka napisana poruka smatra se dokumentom, te na taj način podliježe propisima o autorskom pravu i intelektualnom vlasništvu. Nemate pravo poruke koju su poslane Vama osobno proslijediti dalje bez dozvole autora, odnosno pošiljatelja.
- Ukoliko poruka sadrži povjerljive informacije, treba je kriptirati i potpisati, a u sadržaju poruke jasno naznačiti da se radi o povjerljivim informacijama.

- Pri autentikaciji radi pristupa porukama potrebno je u IMAP/POP protokolu uključiti enkripciju, kako bi se spriječila mogućnost otkrivanja korisničkih lozinki.
- Korisnici su dužni oprezno rukovati s prispjelim porukama sumnjiva sadržaja, ne otvarati sumnjive priloge, ne klikati na sumnjive linkove itd. U slučaju sumnje, treba zatražiti pomoć administratora ustanove.
- Sve poruke pregledati će automatski aplikacija koja otkriva viruse. Ako poruka zadrži virus, neće biti isporučena.
- Institut zadržava pravo konfiguriranja sustava na način da ne obavještava pošiljatelja i primatelja o otkrivenom virusu u poruci, a naročito ukoliko se ustanovi da se radi o tzv. virusima koji lažiraju adresu.
- Institut zadržava pravo pregledavanja dolaznih i odlaznih poruka specijaliziranim programima radi zaustavljanja virusa i *spama*.
- Institut će poštivati privatnost korisnika i neće provjeravati sadržaj poruka. No, u slučaju sigurnosnog incidenta, Povjerenstvo za sigurnost ovlašten je pregledati kompletan sadržaj diska, a poruke elektroničke pošte mogu poslužiti kao dokazni materijal u stegovnom ili sudskom procesu.

Procedura za dodjelu e-mail adrese

Pri zapošljavanju novog djelatnika ravnatelj zatraži od administratora ustanove otvaranje korisničkog računa. Djelatniku se dodjeljuje elektronički identitet, koji uključuje e-mail adresu u domeni IJF-a, u skladu s važećim Pravilnikom o dodjeljivanju AAI@EduHr elektroničkih identiteta i informacijskom održavanju imenika AAI@EduHr elektroničkih identiteta u Institutu za javne financije.

Pri prestanku radnoga odnosa, ravnatelj je dužan najkasnije u roku od osam dana zatražiti zatvaranje korisničkoga računa i elektroničkog identiteta.

Ako zaposlenik nakon odlaska u mirovinu zatraži nastavak korištenja korisničkog računa to mu se, uz suglasnost CARNet-ove službe za članice i odluke ravnatelja, može odobriti.

Vanjskim suradnicima po potrebi se dodjeljuje elektronički identitet, s tim da za njih vrijede ista pravila korištenja kao i za zaposlene.

Protiv korisnika koji ne poštuju ova pravila Institut može pokrenuti stegovni postupak, a u skladu s odgovarajućim internim pravilnikom Instituta. U slučaju ponovljenih težih prekršaja korisniku se može zatvoriti korisnički račun i uskratiti pravo korištenja servisa elektroničke pošte.

Protokol o rješavanju sigurnosnih incidenata

Svrha

Svrha je ovog dokumenta da ustanovi obvezu prijavljivanja sigurnosnih incidenata te da razradi procedure za provođenje istrage.

Prijava incidenta

Svaki zaposlenik, korisnik ili suradnik Instituta dužan je odmah po uočavanju problema u radu servisa pismenim putem (e-mailom) prijavljivati probleme poput usporenog rada servisa, nemogućnosti pristupa, gubitka ili neovlaštene izmjene podataka, pojave virusa itd. Incident se prijavljuje voditelju sigurnosti koji je dužan svaki prijavljeni incident i dokumentirati.

Izvještaji o incidentima smatraju se povjerljivim dokumentima, za njihovo dokumentiranje odgovara voditelj sigurnosti te se spremaju na sigurno mjesto i čuvaju 10 godina kako bi mogli poslužiti za statističke obrade kojima je cilj ustanoviti najčešće propuste radi njihova sprečavanja, ali isto tako i kao dokazni materijal u eventualnim stegovnim ili sudskim procesima.

Ozbiljniji incidenti prijavljuju se CARNet-ovom CERT-u, preko obrasca na web stranici www.cert.hr.

Procedure za rješavanje incidenata

Administratori smiju pratiti korisničke procese. Ako sumnjaju da se računalo koristi na nedopušten način, mogu izlistati sadržaj korisničke mape, ali ne smiju provjeravati sadržaj korisničkih podatkovnih datoteka (npr. dokumenata ili poruka e-pošte). Provjera sadržaja korisničkih podataka je moguća jedino na zahtjev i uz odobrenje korisnika.

Daljnja istraga može se provesti samo ako je prijavljena Povjerenstvu za sigurnost koje je uspostavljeno sigurnosnom politikom ustanove, uz poštivanje sljedećih pravila:

- Istragu provodi jedna osoba, ali uz nazočnost svjedoka kako bi se omogućilo svjedočenje o poduzetim radnjama.
- Prvo pravilo forenzičke istrage jest da se informacijski sustav sačuva u zatečenom stanju, odnosno da se ne načine izmjene koje bi otežale ili onemogućile dijagnosticiranje.
- Najprije se napravi kopija zatečenog stanja (npr. na vanjsku memoriju, CD…), po mogućnosti na takav način da se ne izmijene atributi datoteka.
- Dokumentira se svaka radnja tako da se ponavljanjem zabilježenih akcija može rekonstruirati tijek istrage.
- O istrazi se napiše izvještaj kako bi u slučaju potrebe mogao poslužiti kao dokaz u eventualnim stegovnim ili sudskim procesima.
- Izvještaji o incidentu smatraju se povjerljivim dokumentima i čuvaju se tako da im pristup imaju samo ovlaštene osobe.
- Institut može objavljivati statističke podatke o sigurnosnim incidentima, bez otkrivanja povjerljivih i osobnih informacija.

Sankcije

Svrha je istrage da se odredi uzrok nastanka problema te da se iz toga izvuku zaključci o tome kako spriječiti ponavljanje incidenta ili se barem bolje pripremiti za slične situacije. Ako je uzrok sigurnosnom incidentu bio ljudski čimbenik, protiv odgovornih se mogu poduzeti sankcije.

Institut može osobama odgovornim za sigurnosni incident zabraniti fizički pristup prostorijama ili pristup podatcima.

Ako je incident izazvao zaposlenik vanjske tvrtke, Institut može zatražiti od vanjske tvrtke da ga ukloni s popisa osoba ovlaštenih za obavljanje posla na Institutu. U slučaju teže povrede pravila sigurnosne politike Institut može raskinuti ugovor s vanjskom tvrtkom.

Protokol o izradi kopija podataka

Izradu kopija podataka treba prilagoditi postojećoj tehnološkoj osnovi kojom raspolaže Institut.

Ravnatelj Instituta određuje tko je od zaposlenika zadužen za izradu kopija pojedine vrste podataka. Veću pozornost treba obratiti na spremanje važnijih podataka (baza podataka, mail, web, dns, …).

Osnovna strategija izrade kopija:

- kopija podataka iz baze podataka informacijskog sustava se izrađuje svakodnevno na *storage* serveru automatskim backupom;
- kopija podataka ključnih servisa (mail, web, dns,…), kao i osobnih podataka s poslužitelja, se izrađuje jednom tjedno ili najkasnije mjesečno;
- kopija konfiguracije firewalla se izrađuje jednom tjedno ili najkasnije mjesečno;
- kopije podataka s osobnih računala se izrađuju prema potrebi.

Podatke s osobnih računala mogu spremati korisnici (zaposlenici) pojedinačno na *storage* server. Ukoliko im je u tome potrebna pomoć, pomaže im administrator informatičkog sustava .

Zaposlenici Instituta, kao i vanjski suradnici, ne mogu koristiti vlastite medije za pohranu podataka (USB disk, disketa, CD, DVD,…) bez prethodnog odobrenja odgovorne osobe u Institutu (u pravilu ravnatelj ili rukovoditelj odjela)

Protokol o korištenju informacijskih sustava Instituta za vanjske suradnike, studente i korisnike Instituta

Informacijski sustav Instituta

Vanjskim suradnicima i korisnicima ograničeno je korištenje informacijskih sustava Instituta. Korištenje pojedinih vrsta resursa dopušteno im je ograničeno i uz nadzor.

Mrežu treba segmentirati tako da računala na mreži iz ovih grupa, ovisno o namjeni, imaju pristup Internetu, poslužiteljima ustanove u demilitariziranoj zoni, te internim poslužiteljima ustanove ukoliko je to potrebno. Segmentu mreže u kojemu su računala za vanjske korisnike i korisnike Instituta neće se dozvoliti pristup osobnim računalima zaposlenika.

Vanjskim suradnicima ili korisnicima Instituta nije dozvoljen rad na nekom od računala kojim se koriste zaposlenici Instituta. Ravnatelj iznimno može odlukom odrediti osobe kojima se odobrava rad na računalima Instituta, ali će za rad koristiti posebno namijenjena računala za korisnike.

Ispis i kopiranje podataka

Djelatnici Instituta i vanjski suradnici ne mogu koristiti vlastite medije za pohranu podataka (disketa, CD, DVD, USB uređaje…) bez prethodnog odobrenja odgovorne osobe u Instituta.

Nepridržavanje

U slučajevima kada se studenti, korisnici Instituta ili vanjski suradnici ne pridržavaju mjera sigurnosne politike najprije ih se upozori na prekršaj, a kod težih povreda mjera može im se i uskratiti daljnje korištenje usluga Instituta u skladu s odgovarajućim internim pravilnikom Instituta. Kod vanjskih suradnika mogu se razmatrati i aktivirati ugovorom predviđene i/ili zakonske sankcije.

Protokol o korištenju prijenosnih računala Instituta

Svrha

Institut je osigurao je određeni broj prijenosnih računala za korištenje .

Pravila

1. Računala su prvenstveno namijenjena znanstvenicima , ali ih uz odobrenje ravnatelja mogu koristiti i drugi djelatnici.

2. Računala trebaju se koristiti savjesno i pažljivo, kako bi se osigurala njihova ispravnost, a time i mogućnost korištenja. S obzirom na ograničena sredstva, Institut nije u mogućnosti svako malo kupovati nova računala. Zabranjuje se korisnicima da narušavaju fizički integritet računala na bilo koji način (lupanje, udaranje, trganje, itd.). Također, zabranjuje se korisnicima da samovoljno vrše „popravak" neispravnih računala. Ukoliko neko računalo (ili neki njegov dio) ne radi ispravno, korisnici su dužni pismeni (e-mailom) to prijaviti administratoru ustanove.

3. S obzirom na mogućnost neželjenih problema s računalima, bilo da se radi o softverskim ili hardverskim problemima, na mogućnost gubljenja, nestanka, odnosno otuđivanja računala ili pojedinih dijelova, vodit će se stroga evidencija o korištenju pojedinog računala. U tu svrhu u Institutu će se voditi uredna evidencija osoba koje su zadužile prijenosna računala

4. U slučaju potrebe instalacije dodatnih aplikacija, potrebno je na vrijeme javiti se administratoru ustanove.

Nepridržavanje

Protiv korisnika koji ne poštuju ova pravila, Institut može pokrenuti odgovarajući postupak u skladu s odgovarajućim internim pravilnikom Instituta. U slučaju težih prekršaja, korisniku se može uskratiti pravo korištenja prijenosnih računala Instituta, kao i naplatiti eventualna učinjena šteta.

Protokol o antivirusnoj zaštiti

Virusi i crvi predstavljaju opasnost za informacijske sustave, ugrožavajući funkcioniranje mreže i povjerljivost podataka.

Nove generacije virusa izuzetno su složene i opasne, sposobne da prikriju svoju nazočnost, presreću unos podataka na tipkovnici. Informacije poput zaporki ili povjerljivih dokumenata mogu slati svome tvorcu nekamo na internet te otvoriti kriptiran kanal do čijeg računala kako bi hakeri preuzeli kontrolu nad njim.

Stoga zaštita od virusa više nije stvar osobnog izbora, već obveza Instituta, administratora računala i svakog korisnika.

Institut za javne financije propisuje da je zaštita od virusa obvezna i da se provodi na nekoliko razina:

- na poslužiteljima elektroničke pošte
- na internim poslužiteljima, gdje se stavlja centralna instalacija
- na svakom osobnom računalu korisnika.

Administratori su dužni instalirati protuvirusne programe na sva korisnička računala i konfigurirati ih tako da se izmjene u bazi virusa i u konfiguraciji automatski propagiraju s centralne instalacije na korisnička računala u lokalnoj mreži, bez aktivnog sudjelovanja korisnika.

Korisnici ne smiju samovoljno isključiti protuvirusnu zaštitu na svome računalu. Ako iz nekog razloga moraju privremeno zaustaviti protuvirusni program, korisnici moraju obavijestiti voditelja sigurnosti ili administratora ustanove.

Korisnik koji samovoljno isključi protuvirusnu zaštitu na svom računalu bit će stegovno kažnjen.

Protokol o zaštitit od spama

Svrha

Internetom putuje sve više neželjenih komercijalnih poruka, tzv. *spam*. Masovne poruke elektroničke pošte najjeftiniji su način reklamiranja. Cijenu plaćaju korisnici i tvrtke, jer čitanje i brisanje neželjenih poruka troši njihovo radno vrijeme i umanjuje produktivnost.

Dio neželjenih poruka nastoji uvuci primatelja u kriminalne aktivnosti, na primjer otvaranje računa za pranje novca, nastoje pobuditi samilost kako bi se izvukao novac (engl. *hoax*). Za prepoznavanje ovakvih poruka korisnici mogu koristiti uslugu CARNet CERT-a Hoax recognizer.

Pravila za administratore

Davatelj informatičkih usluga dužan je konfigurirati računala na taj način da se što više neželjenih poruka zaustavi.

Prva je mogućnost da se definira ulazni filter koji će prilikom primanja poruke konzultirati baze podataka koje sadrže popise poslužitelja koji su otvoreni za odašiljanje (open relay), te baza s adresama poznatih *spamera*. Pošta koja dolazi s tako pronađenih adresa neće se primati.

Druga razina zaštite je automatska provjera sadržaja. Poslužitelj može poruke koje su obilježene kao *spam* spremati na određeno vrijeme u karantenu.

Treću razinu zaštite mogu određivati sami korisnici. Poruke dobivaju bodove koji ukazuju na vjerojatnost da se radi o *spamu*. Kako nije uvijek moguće pouzdano definirati što je *spam*, ovakva zaštita mora biti uvjetna, odnosno krajnjem korisniku se prepušta uključivanje bodovanja i konfiguriranje preusmjeravanja označenih poruka.

Administrator ustanove će pomagati korisnicima pri kreiranju filtera za obilježavanje, odvajanje ili uništavanje neželjenih poruka.

Pravila za korisnike

Korisnici ne smiju slati masovne poruke, bez obzira na njihov sadržaj.

Upozorenja na viruse su često lažna i šire zablude pa su korisnici dužni striktno se držati Protokola o rukovanju zaporkama.

Korisnici ne smiju radi stjecanja dobiti odašiljati propagandne poruke koristeći računalnu opremu koja pripada ustanovi.

Nepridržavanje

Korisnici koji se ne pridržavaju pravila prihvatljivog korištenja i šalju masovne neželjene poruke mogu podlijegati odgovarajućim sankcijama u skladu sa odgovarajućim internim pravilnikom Instituta.

Protokol o obrazovanju osoba zaduženih za sigurnost računalnog sustava

Svrha

Bez kontinuiranog obrazovanja i praćenja najnovijih postignuća u zaštiti računalnih i informacijskih sustava nema učinkovite zaštite.

Pravila

Osobe zadužene za sigurnost računalnog sustava obvezne su pratiti najnovija postignuća u zaštiti računalnih i informacijskih sustava putem obrazovanja, praćenja literature i informiranja iz raznih izvora. Također su obavezne pohađati seminare o sigurnosti računalnih sustava koji se održavaju u organizaciji CARNeta. Isto tako preporučuje se praćenje i ostalih seminara, kojima CARNet usavršava sistem inženjere. O obukama se obavezno vode odgovarajući zapisi koji su u skladu sa sustavom kvalitete Instituta.

Resursi

Ravnatelj je dužan u okviru mogućnosti Instituta planirati i osigurati resurse i omogućiti osobama zadužim za sigurnost računalnog sustava da prate najnovija postignuća u zaštiti računalnih i informacijskih sustava.

Protokol o upravljanju povjerljivim informacijama

Klasifikacija informacija

Klasificiranje povjerljivih informacija uređeno je Zakonom o tajnosti podataka objavljenim u Narodnim novinama br. 79/07, 86/12 i Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) SL EU L119 na snazi od 25. svibnja 2018.

Prema vrsti tajnosti, informacije se dijele na vojnu, državnu, službenu, poslovnu i profesionalnu tajnu.

Prema stupnju tajnosti, informacije mogu biti povjerljive, tajne ili vrlo tajne.

Kategorije službene, državne i vojne tajne pripadaju tijelima državne uprave.

Poslovna tajna su informacije koje imaju komercijalnu vrijednost i čije bi otkrivanje moglo nanijeti štetne posljedice Institutu ili njenim poslovnim partnerima (ugovori, financijski izvještaji, planovi, rezultati istraživanja itd.).

Profesionalna tajna odnosi na zanimanja poput liječnika, svećenika i odvjetnika, no može se primijeniti i na zaposlene koji u svom radu dolaze u dodir s podacima o drugim ljudima, poput zaposlenih u posebnim odjelima Instituta, osoba koje unose podatke u baze podataka o korisnicima ili sistem administratora poslužitelja, koji u nekim situacijama može doci u dodir s podacima koji pripadaju korisnicima računala.

Dokumenti koji ulaze u Institut s nekom od oznaka povjerljivosti određuju stupanj povjerljivosti svih dokumenata i informacija koje će Institut proizvesti kao odgovor. U tom slučaju može se koristiti neka od kategorija tajnosti koje su rezervirane za tijela državne uprave (službena, državna ili vojna tajna).

Dokumenti koji se smatraju povjerljivima moraju biti jasno označeni isticanjem vrste i stupnja tajnosti.

Javnima se smatraju sve informacije koje nisu označene kao povjerljive. Izuzetak su osobne informacije, za koje se podrazumijeva da su povjerljive i ne treba ih posebno označavati.

Pravila za čuvanje povjerljivosti odnose se na informacije bez obzira na to u kom su obliku: na papiru, u elektroničkom obliku, zabilježene ili usmeno prenesene, ili su objekti poput maketa, slika itd.

Raspodjela odgovornosti

Za klasificiranje povjerljivih informacija zadužen je ravnatelj Instituta, koji će izraditi listu osoba koje imaju pravo proglasiti podatke tajnima, te listu osoba koje imaju pristup povjerljivim podacima.

Pravila za čuvanje povjerljivih informacija odnose se na sve zaposlenike Instituta i vanjske suradnike koji dolaze u doticaj s osjetljivim podacima. Obaveza čuvanja povjerljivosti ne prestaje s prestankom radnog odnosa.

Čuvanje povjerljivih informacija

Povjerljive informacije, tiskane na papiru ili u elektroničkom obliku, snimljene na neki medij za pohranu podataka, čuvaju se u zaključanim metalnim, vatrootpornim ormarima, u prostorijama u koje je ograničen pristup.

Pristup povjerljivim informacijama regulira se izradom liste zaposlenika koji imaju ovlasti, te bilježenjem vremena izdavanja i vraćanja dokumenata, kako bi se u svakom trenutku znalo gdje se oni nalaze.

Informacije o zaposlenicima

Socijalni inženjering je metoda koju primjenjuju hakeri kako bi prikupili informacije potrebne za provalu na računala.

Institut može informacije o zaposlenima koje se smatraju javnima objaviti na svojim mrežnim stranicama. Javnim informacijama smatraju se:

- ime i prezime
- posao koji zaposlenik obavlja
- broj telefona na poslu
- službena e-mail adresa.

Na upite o zaposlenicima davati će se samo informacije objavljene na internim web stranicama. Daljnje informacije o zaposlenima ne smiju se davati bez suglasnosti osobe kojoj podaci pripadaju (npr. adresa stana, broj privatnog telefona ili mobitela, podaci o primanjima, porezu, osiguranju i sl.)

Povjerljive informacije u načelu se ne daju telefonom jer se sugovornik može lažno predstaviti. Ukoliko se sugovornik predstavlja kao službena osoba koja ima pravo pristupa povjerljivim podacima, zapisuje se ime i prezime te osobe, naziv institucije kojoj pripada i broj telefona s kojeg zove. Nakon provjere istinitosti tih podataka zaposlenik Instituta će se posavjetovati s upravom i ukoliko dobije odobrenje nazvati službenu osobu i odgovoriti na pitanja.

Prenošenje povjerljivih informacija

Informacije koje su klasificirane kao povjerljive zahtijevaju posebne procedure pri njihovu slanju i prenošenju.

Povjerljive informacije ne šalju se običnom već kurirskom poštom. Na odredištu se predaju u ruke osobi kojoj su upućeni, što se potvrđuje potpisom.

Ako se povjerljive informacije šalju elektronički (npr. kao poruke elektroničke pošte), tada se moraju slati kriptirane.

Kopiranje povjerljivih informacija

Za kopiranje povjerljivih informacija treba zatražiti dozvolu vlasnika informacije.

Povjerljivi dokumenti koji izvana dođu u Institut ne smiju se kopirati bez izričite dozvole pošiljatelja.

Dokumenti koji pripadaju Institutu smiju se kopirati samo uz dozvolu osobe koja ih je proglasila povjerljivim, odnosno uprave (ravnatelja). Kopija se numerira i o njenom izdavanju vodi se evidencija kao i za original s kojeg je proizvedena.

Osoblje koje poslužuje uređaje za kopiranje/tiskanje/skeniranje treba obučiti i obavezati da odbiju kopiranje povjerljivih dokumenata ukoliko nije ispoštovana propisana procedura.

Uništavanje povjerljivih informacija

Mediji koji sadrže povjerljive informacije ne bacaju se, već se uništavaju metodom koja osigurava da se trajno i pouzdano uništi njihov sadržaj (spaljivanjem, usitnjavanjem, prešanjem).

Ukoliko se zastarjela i rashodovana računalna oprema daje na korištenje trećoj strani, obavezno je uništavanje podataka sa diskova posebnim programom koji nepovratno briše sadržaj diska.

Nepridržavanje

Zaposlenici i suradnici koji dolaze u dodir s povjerljivim informacijama potpisuju Izjavu o čuvanju povjerljivosti informacija.

Protiv zaposlenika koji ne poštuju pravila o čuvanju povjerljivih informacija bit će pokrenut stegovni postupak, u skladu sa odgovarajućim internim pravilnikom Instituta.

Institut treba već u ugovor unijeti stavke po kojima je povreda povjerljivosti podataka dovoljan razlog za prekid ugovora.

Sastavni dio Protokola o upravljanju povjerljivim informacijama je i Izjava o čuvanju povjerljivih informacija.

Institut za
javne financije

Izjava o prihvaćanju odredbi sigurnosne politike

Institut posvećuje značajnu pažnju pitanjima informacijske sigurnosti i dužnost je svakog korisnika pridržavati se svih pravilnika i uputa koje reguliraju pitanja zaštite informacijske imovine Instituta.

Korisnik, ovime prima na znanje i prihvaća sljedeće odredbe:

- Korisnik je odgovoran za sigurno, etično i zakonito korištenje informacijskog sustava i imovine Instituta.
- Od korisnika se očekuje korištenje informacijskog sustava na način koji neće onemogućavati ili umanjivati učinkovitost poslovnih procesa.
- Korisniku je dozvoljeno korištenje isključivo programskih rješenja dobavljenih od strane Instituta ili programskih rješenja otvorenog koda.
- Korisniku je zabranjeno korištenje plug-in-ova koja nisu preporučena od strane informatičke podrške.
- Korisniku kojemu je istekao radni odnos u Institutu u roku od 10 dana briše se elektronski identitet iz sustava AAI@EduHR te se ukida korisnički račun iz domene: @ijf.hr
- Korisnici ne smiju namjerno sudjelovati u širenju zlonamjernih programa.
- Korisnici ·ne smiju na vidljivom i lako dostupnom mjestu držati lozinke u pisanom obliku.
- Prilikom napuštanja prostorije korisnik mora adekvatno zbrinuti službene dokumente za koje je odgovoran i zaključati računalo. Ako osoba posljednja odlazi, dužna je ugasiti svjetlo u prostoriji, zatvoriti prozore, zatvoriti i zaključati vrata, a ako je to moguće, ugasiti klime, grijalice, električna i druga kuhala.
- Mogućnost korisnika da pristupa, koristi ili utječe na rad resursa za koji je odgovorna druga osoba ne podrazumijeva i dozvolu za takvu akciju.
- Korisnik će se pridržavati svih sigurnosnih odredbi sigurnosne politike i mjera koje iz nje proizlaze.
- Korisnik je upoznat s Politikom sigurnosti i prihvaća njegove odredbe.
- Vlastoručnim potpisom korisnik izjavljuje da je·suglasan sa svim gore navedenim.

Ime i prezime korisnika	Datum	Potpis korisnika
_____	_____	_____