Na temelju članaka 20. stavak (5) točka 1. Statuta Sveučilišta u Zagrebu Prehrambeno-biotehnološkog fakulteta, Fakultetsko vijeće Sveučilišta u Zagrebu Prehrambeno-biotehnološkog fakulteta na 9. redovitoj sjednici za akademsku godinu 2017./2018. održanoj dana 14. lipnja 2018. godine donosi

Pravilnik o sigurnosnoj politici informacijskog sustava

I. OPĆE ODREDBE

Članak 1.

(1) Pravilnik o sigurnosnoj politici informacijskog sustava Sveučilišta u Zagrebu Prehrambeno-biotehnološkog fakulteta (u daljnjem tekstu: Pravilnik) je skup pravila koji propisuju mjere koje moraju biti sadržane u organizacijskom i tehničkom dijelu upravljanja informacijskim sustavom.

(2) Pravilnik je dio sustava upravljanja sigurnošću informacijskih sustava. Njegova je svrha definirati prihvatljive i neprihvatljive načine ponašanja te jasno raspodijeliti zadatke i odgovornosti. Planira se i provodi na način da omogućava sigurno obavljanje posla, a da pritom ne ometa poslovne procese.

(3) Informacijski sustav mora omogućiti neometano odvijanje poslovnih procesa kroz uporabu informacija. Obavljanje poslovnih procesa Sveučilišta u Zagrebu Prehrambeno-biotehnološkog fakulteta (u daljnjem tekstu: PBF) ovisi o radu informacijskog sustava PBF-a.

II. POJMOVI I TERMINI

Članak 2.

(1) *Informacijski sustav* (u daljnjem tekstu: IS) podrazumijeva usklađeno djelovanje svojih sastavnica:

- računalne i komunikacijske tehnologije
- sistemskog i aplikativnog softvera
- podataka / informacija
- metoda i postupaka za obradu podataka
- osoba koje održavaju IS, obrađuju podatke i koriste ih
- poslovnih partnera i suradnika.

(2) *Informacijsku imovinu* čini svaki resurs IS koji služi za prikupljanje, obradu, spremanje i distribuciju podataka, na primjer:

- opipljiva (materijalna) imovina (zgrade, računala i komunikacijska oprema, infrastruktura)
- neopipljiva (nematerijalna) imovina (ugled, tehnologija, metodologija, zaštitni znak)
- podatci (dokumenti, ugovori, osobni podatci itd.)
- softver (sistemski i aplikativni programski paketi)
- ljudi koji održavaju i koriste IS

(3) *Sigurnost informacijskog sustava* definira se kao skup mjera i postupaka na tehničkoj i organizacijskoj razini, čijom se primjenom postiže i održava prihvatljiva razina rizika IS.

(4) *Temeljna načela sigurnosti informacijskog sustava* su:

- Povjerljivost – osiguravanje da su informacije dostupne samo ovlaštenim osobama i organizacijama
- Cjelovitost – zaštita točnosti i cjelovitosti informacija i metoda njihove obrade
- Dostupnost – osiguravanje da su podatci na raspolaganju ovlaštenim korisnicima u trenutku kada je to potrebno

(5) *Procjena rizika* je postupak kojim se identificiraju prijetnje i ranjivosti koje mogu ugroziti rad IS-a. Osnovne odrednice procjene rizika su:

- za svaku prijetnju određuje se vjerojatnost ostvarenja i potencijalna šteta, kako bi se odredili prioriteti i odabrale mjere koje smanjuju rizik na prihvatljivu razinu.
- procjena rizika provodi se periodički kako bi se ustanovile promjene u prijetnjama, ranjivostima i poslovnim prioritetima.
- troškovi primjene sigurnosnih mjera moraju biti razmjeni s osjetljivošću i vrijednošću informacija koje se takvim mjerama štite i prilagođeni materijalnim i ljudskim mogućnostima.

(6) *Sigurnosni događaj* je svaki događaj koji ukazuje na probleme koji ne ugrožavaju rad samog IS-a niti povjerljivost podataka (primjerice, zaboravljanje zaporke).

(7) *Sigurnosni incident* je događaj koji ugrožava povjerljivost, integritet i dostupnost podataka, integritet sistemskog softvera i poslovnih aplikacija ili ukazuje na neovlašten pristup informacijskim resursima. Incidentom se smatraju i događaji koji onemogućavaju neprekidnost poslovanja, poput nestanka električne energije, poplave, požara itd.

Članak 3.

Izrazi koji se koriste u ovom Pravilniku, a imaju rodno značenje, koriste se neutralno i odnose se jednako na muški i ženski rod.

III. OPSEG

Članak 4.

Pravila rada i ponašanja koja definira ovaj Pravilnik vrijede za:

- svu računalnu i elektroničku opremu koja se nalazi u prostorima PBF-a
- administratore informacijskih sustava – davatelje informatičkih usluga
- korisnike, među koje spadaju: zaposlenici, vanjski suradnici, studenti, gosti
- vanjske organizacije koje po ugovoru rade na održavanju opreme ili softvera

IV. ORGANIZACIJA UPRAVLJANJA SIGURNOŠĆU

Članak 5.

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

Članak 6.

(1) Korisnici su osobe koje se u svom radu ili učenju služe računalima, proizvode dokumente ili unose podatke. Oni ne odgovaraju za instalaciju i konfiguraciju softvera, niti za ispravan i neprekidan rad računala i mreže osim kada se ne pridržavaju pravila propisanih ovim dokumentom.

(2) Dužnosti korisnika su:

- pridržavanje pravila prihvatljivog korištenja, što znači da ne smiju koristiti računala za djelatnosti koje nisu u skladu sa važećim zakonima, etičkim normama i pravilima lokalne sigurnosne politike.
- pridržavati se odredbi ovoga Pravilnika
- pridržavati se odredbi Pravilnika o politici zaštite podataka Sveučilišta u Zagrebu Prehrambeno-biotehnološkog fakulteta
- Korisnici koji proizvode podatke i dokumente odgovorni su za njihovo čuvanje. To između ostaloga znači da moraju od davatelja usluga zatražiti da uspostave automatsku pohranu (*backup*) važnih informacija, ili u protivnom moraju sami izrađivati sigurnosne kopije.

(3) 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.

Članak 7.

(1) Radi poboljšanja sigurnosti, za svaku aplikaciju za obradu podataka imenuje se glavni korisnik.

(2) Dok zaposlenici koji unose podatke odgovaraju za vjerodostojnost tih podataka, glavni je korisnik odgovaran za provjeru ispravnosti podataka, za provjeru ispravnosti i sigurnosti aplikacije, za dodjelu

dozvola za pristup podacima (kada je primjenjivo) i za mjere sprečavanja izmjene podataka od strane neautoriziranih osoba.

(3) Glavni korisnik kontaktira proizvođača aplikacije i dogovara isporuku novih verzija, traži ugradnju sigurnosnih mehanizama, izmjene ili dopune općih podataka o organizaciji.

Članak 8.

Davateljima usluga smatraju se profesionalci koji brinu o radu računala, mreže i informacijskih sustava. Na ustanovama članicama CARNeta, uključujući i PBF, to su sistem inženjer i članovi njegova tima (ako je primjenjivo). Oni odgovaraju za ispravnost i neprekidnost rada informacijskog sustava.

Članak 9.

(1) Za brigu o sigurnosti i pomoć pri rješavanju incidenata PBF može koristiti pomoć CARNeta.

(2) Osoba čije je prvenstvena briga sigurnost informacijskih sustava PBF-a je Voditelj sigurnosti (engl. *CSO, Chief Security Officer*).

(3) Njegova je briga ukupna sigurnost informacijskih sustava. To uključuje i fizičku sigurnost, pri čemu surađuje sa zaposlenicima poput portira, čuvara i slično.

(4) Voditelj sigurnosti piše pravilnike, nadzire rad mreže i servisa, organizira obrazovanje svih 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.

Članak 10.

(1) Pri PBF-u djeluje Povjerenstvo za informacijsku usklađenost i sigurnost informacijskog sustava (u daljnjem tekstu: Povjerenstvo), čija je zadaća osiguravanje usklađenosti s odredbama Pravilnika o politici zaštite podataka Sveučilišta u Zagrebu, Prehrambeno-biotehnološkog fakulteta, kao i ovoga Pravilnika.

(2) Povjerenstvo prati sigurnosnu situaciju i predlaže mjere za njeno poboljšanje, uključujući nabavu opreme i organizaciju obrazovanja korisnika. O navedenome minimalno jednom godišnje izvješćuje dekana.

(3) Povjerenstvo je zaduženo za postupanje u incidentnim situacijama (npr. povrede osobnih podataka) te su korisnici obvezni prijaviti članovima Povjerenstva.

Članak 11.

(1) Davatelji usluga dužni su administrirati računala i mrežnu opremu u skladu s pravilima struke, brinući istovremeno o funkcionalnosti i sigurnosti.

(2) Svako računalo mora imati imenovanog administratora, koji odgovara za instalaciju i konfiguraciju softvera. Ako napredni korisnici žele sami administrirati svoje osobno računalo, obvezni su potpisati izjavu o tome, nakon čega za njih vrijede sva pravila za administriranje računala. Naziv ove vrste administratora je administrator lokalnoga računala.

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

(4) Posebnu pažnju administratori su dužni posvetiti opremi koja obavlja ključne funkcije ili sadrži vrijedne i povjerljive informacije koje treba štiti od neovlaštenog pristupa (npr. osobni podatci).

(5) 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.

(6) Administratori su dužni prijaviti incidente Voditelju sigurnosti, a radi li se o povredi osobnih podataka i Službeniku za zaštitu osobnih podataka 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 CARNetovu CERT-u i nadležnim institucijama.

(7) Davatelji usluga dužni su u svome radu poštivati privatnost ostalih korisnika i povjerljivost informacija s kojima dolaze u dodir pri obavljanju posla.

Članak 12.

(1) PBF razrađuje pravila koja određuju tko upravlja mrežom, konfigurira mrežne uređaje, dodjeljuje adrese, kreira virtualne LAN-ove i slično.

(2) Osim što se odgovornost za rad mreže dodjeljuje određenim ljudima, mogu se propisati i protokoli za priključivanje računala u mrežu, odrediti obrasci kojima se izdaje odobrenje za priključenje računala na mrežu i dodjeljivanje adresa.

(3) Djelatnik zadužen za upravljanjem mrežom mora u svakom trenutku imati točan popis svih mrežnih priključaka i umreženih uređaja, uključujući i prenosiva računala.

(4) PBF razrađuje pravila za spajanje na mrežu gostujućih računala, koja donose sa sobom vanjski suradnici, predavači, poslovni partneri, serviseri i druge osobe.

V. FIZIČKA SIGURNOST

Članak 13.

(1) Prostor na PBF-u dijeli se na dio koji je otvoren za javnost, prostor u koji imaju pristup samo zaposleni, te prostore u koje pristup imaju samo grupe zaposlenih, ovisno o vrsti posla koji obavljaju.

(2) Pristup zaštićenim područjima ima Voditelj sigurnosti i od njega ovlaštene osobe. Voditelj sigurnosti održava popis ovlaštenih osoba.

(3) Općenite smjernice vezane za fizičku sigurnost:

1. Zaključavanje ureda i ormara s dokumentima je jednostavna, ali učinkovita prva prepreka koja smanjuje rizik neovlaštenog pristupa. Čak i ako podatci nisu osjetljivi, njihovo uništavanje ili neovlašteno mijenjanje može uzrokovati neželjene posljedice za zaposlenike ili studente te gubitak vremena i novca. Uredi i ormari koji sadrže osjetljive informacije te oprema koja omogućuje pristup takvim informacijama mora se uvijek zaključavati kada je prostorija prazna.
2. Računalni sustavi koji se koriste za pristup osjetljivim podatcima moraju se instalirati samo ondje gdje su dostupni ovlaštenim zaposlenicima. Zasloni i printeri moraju se pozicionirati na način da se izbjegne slučajno otkrivanje.
3. Svi korisnici moraju poduzeti primjerene mjere opreza da bi osigurali da drugi korisnici ne mogu neovlašteno pristupati podatcima koristeći njihovu opremu. Posebice, oprema se ne smije puštati bez nadzora osim ako ima zaporkom zaštićeni zaslon ili ako se ugasi ili iz nje odjavi. Također ne smiju pristupati opremi koristeći tuđe korisničko ime.
4. Pristup informacijama mora odobriti za to ovlašteni zaposlenik PBF-a. Potrebna je potpuna autorizacija prije no što se informacije otkriju drugom korisniku ili vanjskoj organizaciji.
5. Sva oprema i mediji za otpis moraju se razdužiti na propisani način. Osjetljivi podatci i softver koji ima neprenosivu licencu mora se potpuno izbrisati s diska (npr. koristeći *low-level reformatting*).
6. Svi osjetljivi i povjerljivi tiskani zapisi moraju se isjeckati prije odlaganja.
7. Svi dokumenti koji sadrže povjerljive informacije ne smiju se puštati u pisačima i fotokopirnim uređajima.
8. Oprema, podatci i softver u vlasništvu PBF-a ne smije se iznositi iz službenih prostora bez službenog odobrenja.
9. Ako se oprema koristi izvan prostora PBF-a za obradu osjetljivih podataka, na nju se odnose iste mjere opreza kao i za opremu korištenu unutar prostora.
10. Mobilni uređaji za pohranu podataka (USB, CD, DVD, vanjski tvrdi disk) koriste se samo u situacijama kada mrežno priključivanje nije dostupno ili ne postoji druga sigurna metoda prijenosa podataka.
11. Oprema i mediji koji sadrže osjetljive informacije ne smiju se ostavljati bez nadzora na javnim mjestima niti na vidljivom mjestu unutar automobila. Prenosiva računala nosite kao ručnu prtljagu. Zaštite opremu barem zaporkom, a gdje je to moguće i enkripcijom.
12. Korisnici ne smiju izrađivati neovlaštene kopije softvera u vlasništvu PBF-a osim u slučajevima kada je navedeno zakonom dopušteno ili kada to odobri vlasnik. Regulacijom intelektualnog vlasništva propisane su posljedice kopiranje originalnih podataka i softvera te će za njih

odgovarati korisnik.

Članak 14.

(1) Računalna oprema koja obavlja kritične funkcije, neophodne za funkcioniranje informacijskog sustava, ili sadrži povjerljive informacije, fizički se odvaja u prostor u koji je ulaz dozvoljen samo ovlaštenim osobama.

(2) Pristup u sigurne zone u pravilu imaju samo zaposlenici koji administriraju mrežnu i komunikacijsku opremu i poslužitelje ključnih servisa. Oni ulaze u sigurne zone samo kada treba ukloniti zastoje i obaviti servisiranje opreme. Stoga je poželjno je administratorima osigurati radni prostor odvojeno od prostorija u kojima je smještena kritična oprema.

(3) 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.

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

Članak 15.

(1) Povremeno se mora dopustiti pristup osobama iz vanjskih organizacija, radi servisiranja, održavanja, podrške, obuke, zajedničkog poslovanja, konzultacija itd.

(2) PBF će u ugovore s vanjskim organizacijama ugraditi odredbe kojima obavezuje poslovne partnere na poštivanje ovog Pravilnika.

(3) Ugovorom će se regulirati pristup, čime se podrazumijeva pristup prostorijama, pristup opremi ili logički pristup povjerljivim informacijama. Treću stranu će se obavezati na čuvanje povjerljivih informacija s kojima dođu u dodir pri obavljanju posla.

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

(5) Ako u sigurnu zonu radi potrebe posla ulaze osobe koje nemaju ovlasti, mora im se osigurati pratnja.

(6) Ako se vanjskoj organizaciji bude prepuštalo održavanje opreme i aplikacija s povjerljivim podacima, PBF može od vanjske organizacije zatražiti popis osoba koje će dolaziti u prostorije PBF-a radi obavljanja posla. U slučaju zamjene izvršitelja, vanjska organizacija dužna je na vrijeme obavijestiti PBF.

(7) PBF zadržava pravo da osobama koje se predstavljaju kao djelatnici vanjskih organizacija uskrati pristup ukoliko nisu na popisu ovlaštenih djelatnika.

VI. SIGURNOST OPREME

Članak 16.

PBF 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 - privatna mreža PBF-a, sačinjavaju je poslužitelji internih servisa, osobna računala zaposlenih, računalne učionice te komunikacijska oprema lokalne mreže.
- Ekstranet - proširenje privatne mreže otvoreno mobilnim korisnicima, poslovnim partnerima ili povezuje izdvojene lokacije. U ovu grupu spadaju na primjer interni modemski ulazi ili veza lokalnih baza podataka s centralnim poslužiteljima (LDAP, ISVU, X-ice).

Članak 17.

(1) U prostorijama PBF-a nalazi se i oprema CARNeta ili nadležnog ministarstva koja je dana na korištenje PBF-u.

(2) PBF je obavezan održavati popis sve računalne opreme, s opisom ugrađenih komponenti, inventarskim brojevima itd.

(3) PBF brine jednako o svoj opremi kojom raspolaže, bez obzira na to tko je njezin vlasnik. Pažnjom dobrog gospodara oprema se čuva od oštećivanja i otuđenja.

(4) PBF je dužan osoblju CARNeta dozvoliti pristup opremi u vlasništvu CARNeta koja se nalazi u PBF-u.

Članak 18.

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

(2) PBF razrađuje procedure kojima se nastoji spriječiti otuđenje i oštećenje računalne opreme.

VII. OSIGURANJE NEPREKIDNOSTI POSLOVANJA

Članak 19.

(1) Kako bi se sačuvali podaci u slučaju nezgoda, poput kvarova na sklopovlju, požara, ili ljudskih grešaka, potrebno je redovito izrađivati rezervne kopije svih vrijednih informacija, uključujući i konfiguraciju softvera. Preporučuje se izrada više kopija, koje se čuvaju na različitim mjestima, po mogućnosti u vatrootpornim ormarima. Pravila o izradi kopija podataka sastavni je dio ovog Pravilnika.

(2) Radi osiguranja neprekinutosti poslovanja, razrađuju se i procedure (npr. procedura upravljanja rizicima unutar Priručnika kvalitete).

VIII. NADZOR NAD INFORMACIJSKIM SUSTAVIMA

Članak 20.

(1) PBF zadržava pravo nadzora nad instaliranim softverom i podacima koji su pohranjeni na umreženim računalima, te nad načinom korištenja računala.

(2) Nadzor se smije provoditi radi:

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

(3) Nadzor smiju obavljati samo osobe koje je PBF za to ovlastio.

(4) Pri provođenju nadzora ovlaštene osobe dužne su poštivati privatnost i osobnost korisnika i njihovih podataka. No u slučaju da je korisnik prekršio odredbe ovog Pravilnika, ne može se više osigurati povjerljivost informacija otkrivenih u istrazi, te se one mogu koristiti u stegovnom ili sudskom postupku.

Članak 21.

(1) Odredbe iz članka 20. ovog Pravilnika odnose se na svu računalnu opremu koja se nalazi u prostorijama PBF-a i priključena je u mrežu CARNet, na sav instalirani softver, te na sve mrežne servise.

(2) Odredbe su dužni poštivati i provoditi svi zaposleni, studenti i vanjski suradnici koji po ugovoru obavljaju određene poslove.

Članak 22.

(1) Korisnici su dužni pomoći osobama zaduženim za nadzor informacijskih sustava, na taj način što će im pružiti sve potrebne informacije i omogućiti im pristup prostorijama i opremi radi provođenja nadzora.

(2) Isto vrijedi i za administratore računala i pojedinih servisa, koji su dužni Povjerenstvu iz članka 10. ovog Pravilnika pomagati pri istrazi.

(3) 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 PBF-a, ili oprema PBF-a služi za njezin prijenos
- pristup radnom prostoru (uredu, laboratoriju, sigurnoj zoni itd.)
- pravo na interaktivno nadgledanje i bilježenje prometa na mreži PBF-a.

Članak 23.

Zaposleniku koji se ogluši na pravila o nadzoru može se uskratiti pravo korištenja CARNetove mreže i njezinih servisa.

IX. DODATNA PRAVILA

Članak 24.

(1) Korisnici su se dužni pridržavati akata vezanih za prihvatljivo korištenje CARNet mreže.

(2) Za pojedina područja rada PBF definira pravila koja čine sastavni dio ovoga Pravilnika. Nepridržavanje pravilima smatra se težom povredom radnog odnosa.

Članak 25.

Ovaj Pravilnik stupa na snagu osmog dana od njegova donošenja na Fakultetskom vijeću i objavljuje se na mrežnim stranicama Fakulteta.

KLASA: 004-01/18-01/01
URBROJ: 251-69-01-18-3

Dekan

prof. dr. sc. Damir Ježek

Pravila o uporabi lokalne mreže i Interneta

Svrha

Svrha je odrediti smjernice, postupke i zahtjeve za osiguranje prihvatljivih načina uporabe lokalne računalne mreže PBF-a kao i javne računalne mreže - Interneta, te zaštitu informacija i opreme PBF-a od zlouporaba korištenjem lokane mreže i Interneta

Doseg

Pravila se odnose na zaposlenike, studente, vanjske suradnike i sve druge osobe kojima se dopušta uporaba računalnog informacijskog sustava PBF-a korištenjem lokalne mreže i Interneta.

Odgovornosti

Odgovornost za primjenu ovih pravila imaju svi korisnici.

Od svih korisnika se očekuje da budu upoznati i da se pridržavaju ovih pravila u svakodnevnom radu.

Odgovornost i obveze Službe za informatičku potporu ogleda se u:

- uspostavljanju i održavanju sigurnosnih pravila i standarda te davanju korisnicima tehničku potporu pri uporabi lokalne mreže i Interneta,
- organiziranju i provođenju reakcije na moguće krizne situacije u računalnom sustavu (zaraza računalnim virusom, napad hakera i sl.),
- provođenju periodičke procjene sigurnosnih rizika na svim produkcijskim sustavima koji su u njegovoj odgovornosti,

- provjeri sigurnosnih mjera implementiranih na tim sustavima i utvrđivanju da li odgovaraju razini osjetljivosti u njima pohranjenih informacija,

- osiguranju pristupna prava pojedinih korisnika na najmanjoj razini potrebnoj za njihov rad,
- nadziranju uporabe Interneta, detektiranju mogućih kršenja odredbi ovih pravila, te izvještavanja Povjerenstva o tim pojavama

Čelnici ustrojbenih jedinica moraju osigurati da svi korisnici u njihovim ustrojbenim jedinicama budu upoznati i da se pridržavaju ovim pravilima.

Korisnici računalnog sustava moraju:

- poznavati i primjenjivati ova pravila,
- ne dozvoliti neovlaštenim pojedincima pristup u lokalnu mrežu PBF-a i odatle javnu računalnu mrežu Internet,

- održavati tajnost uporabe svojih pristupnih zaporki za mrežne usluge i zaštititi ih od nenamjernog otkrivanja drugim osobama,
- Službi za informatičku potporu prijaviti svaku pojavu za koju se čini da narušava sigurnost informacijskog sustava pri korištenju lokalne mreže ili Interneta (virusne zaraze, neobjašnjive transakcije, nedostajuće podatke, neovlašteno ili zabranjeno skidanje programa i audio/video sadržaja i slično),
- pristupati samo podacima i funkcijama za koje su slijedom redovnih poslovnih aktivnosti ovlašteni,
- tražiti ovlaštenje od nadležnih osoba za sve aktivnosti koje izlaze iz okvira korisnikovih redovnih poslovnih aktivnosti, posebno aktivnosti razmjene podataka s osobama i sustavima izvan PBF-a.

Pravila o rukovanju zaporkama

Svrha

Svrha je osigurati sigurno korištenje i čuvanje zaporki na svim razinama i za sve informacijske sustave u uporabi na PBF-u.

Uvod

Prosječan korisnik nerijetko smatra kako ne mora brinuti o sigurnosti jer njegovo računalo ne sadrži vrijedne informacije. No kompromitiranjem jednog osobnog računala u lokalnoj mreži ili jednog korisničkog računa na poslužitelju napadač je otvorio prolaz za napade na važnije sustave i informacije. Stoga je svaki korisnik dužan izborom zaporke i njezinom povremenom promjenom doprinositi zaštiti ukupnog 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 dugačke osam znakova.

Doseg

Svi zaposlenici PBF-a koji u svome radu koriste računala dužni su pridržavati se ovih pravila korištenja zaporki, dok su ih administratori dužni tehnički ugraditi u sve sustave koji to omogućavaju.

Pravila za korištenje zaporki

1. Minimalna dužina zaporke

Kratku zaporku lakše je probiti. Stoga neka minimalna dužina zaporke bude osam znakova.

2. Ne koristiti riječi iz rječnika

Hakeri posjeduju zbirke rječnika, što im olakšava probijanje ovakvih zaporki (tzv. d*ictionary, brute force attack*).

3. Izmiješati mala i velika slova s brojevima

Na primjer: h0bo7niCa. Na prvi pogled besmislena i teška za pamćenje, ova je zaporka izvedena iz riječi hobotnica. Polazište je pojam koji lako pamtimo, ali onda po nekom algoritmu vršimo zamjenu znakova. Preporučamo da zaporku sačinjava kombinacija velikih i malih slova, brojeva i simbola.

4. Ne koristiti imena bliskih osoba, ljubimaca, datume

Takve se zaporke lako otkriju socijalnim inženjeringom.

5. Trajanje zaporke

Promjena zaporke smanjuje vjerojatnost njezina otkrivanja. Neki korisnici naizmjence koriste dvije standardne zaporke. Iako su dvije zaporke bolje nego jedna, ipak se ovakvim trikovima izigrava osnovna svrha promjene zaporki. Preporučamo da zaporku mijenjate minimalno dvaput godišnje.

6. Tajnost zaporke

Korisnici su odgovorni za svoju zaporku i ni u kom je slučaju ne smiju otkriti, čak ni administratorima sustava.

Hakeri nastoje izmamiti zaporke lažno se predstavljajući kao administratori. Pravi administratori imaju mogućnost rješavanja problema i bez poznavanja korisničkih zaporki.

7. 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.

8. Administriranje zaporki

Na računalima koja spadaju u zonu visokog rizika administratori su dužni konfigurirati sustav na taj način da se korisnički račun zaključa nakon tri neuspjela pokušaja prijave.

Administratori su dužni konfigurirati autentikaciju tako da zaporke zastare nakon 180 dana te onemogućiti korištenje zaporki koje su već potrošene, ako sustav to dozvoljava.

Nepridržavanje

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

U slučaju ponovljenog ignoriranja ovih pravila, PBF može stegovno djelovati ili postaviti zaposlenika na radno mjesto na kojem je manja mogućnost ugrožavanja integriteta i sigurnosti sustava i podataka.

Pravila o korištenju elektroničke pošte

Svrha

Svrha je davanje smjernice poslovanja, postupke i zahtjeve za osiguranje prihvatljivih načina uporabe sustava elektroničke pošte PBF, te zaštitu informacija i resursa PBF-a od zlouporaba korištenjem elektroničke pošte.

Uvod

Elektronička pošta dio je svakodnevne komunikacije, poslovne. Komuniciranje e-poštom na PBF-u zahtijeva da se razmotre svi aspekti elektroničke komunikacije s obzirom na moguće posljedice.

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-pošte.

U nastavku su neki problemi koji mogu nastati pri korištenju elektroničke pošte.

1. Nesigurnost protokola

- Poruke putuju kao običan tekst, otvorene kao na razglednici, 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. Nezgode

- Uvijek je moguće pritisnuti pogrešnu tipku ili kliknuti mišem na susjednu ikonu.
- Time može nastati nepopravljiva šteta – ne možete zaustaviti poruku koja je već otišla. Ako se umjesto *Reply* pritisne *Reply All*, poruka će umjesto jednom primatelju otići na više adresa, a povjerljive informacije dospjeti do neželjenih primatelja.
- Česta je pogreška i kada se pokupi pogrešna adresa iz adresara.
- Neki mail klijenti sami dovršavaju adresu e-pošte koju tipkate. U žurbi se može prihvatiti pogrešna adresa, slična onoj koju zapravo želite.

3. Nesporazumi

- Ljudi su skloni pisati e-poštu na ležerniji, opušteniji način. To može dovesti do nesporazuma ako druga strana ne shvaća poruku na isti način. Stoga službene dopise pišite u službenom tonu.
- Iza vašeg imena u potpisu se nalazi ime PBF-a. Pišući, budite svjesni da netko može shvatiti vašu privatnu prepisku kao službeni dopis, vaše privatno mišljenje kao službeni stav PBF-a. Stoga u raspravi uvijek jasno naznačite kada je izneseni stav vaše privatno uvjerenje.

4. Otkrivanje informacija

- Poruke namijenjene jednoj osobi, začas se mogu proslijediti drugima, na primjer na *mailing* listu. To se može dogoditi
    - (zlo)namjerno, s ciljem da se naškodi drugoj osobi ili organizaciji
    - nemarom sudionika, koji ne traži dozvolu za prosljeđivanje poruke
    - omaškom, na primjer nehotičnim klikom mišem na pogrešnu ikonu (*Reply All* umjesto *Reply*)
- 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. PBF se obavezuje čuvati povjerljivost takvih poruka, ali to ne može garantirati ako poruke budu tretirane kao dokazni materijal u istrazi ili u mogućem sudskom procesu.

5. Radna etika

- Velika količina poruka koje treba svakodnevno pročitati može vam oduzeti znatan dio radnog vremena. Stoga ograničite broj privatnih i zabavnih 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 izvući 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, čak i ako brišete takve poruke bez čitanja. PBF će filtrirati *spam* na poslužitelju elektroničke pošte, ali je obaveza korisnika da sami ne šalju takve poruke.

6. Povreda autorskih prava

- Svaka poruka elektroničke pošte može se smatrati autorskim djelom, stoga ona pripada osobi koja ju je poslala. Stoga za prosljeđivanje tuđe poruke morate tražiti dozvolu njezina autora.
- Prilozi koji se šalju uz elektroničke poruke mogu sadržavati autorski zaštićene informacije, na primjer glazbu, filmove, članke itd. Primajući i šaljući takve sadržaje možete izložiti tužbi ne samo sebe, već i PBF.

7. Zadržavanje e-pošte koja sadržava osobne podatke

- E-pošta koja sadrži osobne podatke, a čija svrha obrade je završena, predstavlja sigurnosni rizik koji netko može zloupotrijebiti, nanijeti štetu PBF-u i ispitaniku.

Pravila

Zbog svega nabrojanog korištenje elektroničke pošte smatra se rizičnom djelatnošću, te se korisnici obavezuju na pridržavanje određenih pravila:

- Zaposlenicima se otvara korisnički račun radi obavljanja posla.
- Privatne poruke dozvoljene su u umjerenoj količini, ukoliko to ne ometa rad. Za privatne potrebe mogu se koristiti za to namijenjeni davatelji usluga e-pošte.
- Pišući poruke, budite svjesni da ne predstavljate samo sebe, već i organizaciju za koju radite.
- Pridržavajte se netikete, pravila pristojnog ponašanja na Internetu, službenu adresu e-pošte nemojte koristiti za slanje uvredljivih, omalovažavajućih poruka, ili za seksualno i drugo uznemiravanje.
- Nije dozvoljeno slanje lančanih poruka kojima se opterećuju mrežni resursi i ljudima oduzima radno vrijeme.
- 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.
- PBF zadržava pravo filtriranja poruka s namjerom da se zaustavi *spam*.
- U slučaju istrage uzrokovane mogućim sigurnosnim incidentom, Povjerenstvo može pregledavati kompletan sadržaj diska, pa time i e-poštu.
- Poruke koje su dio poslovnog procesa treba arhivirati i čuvati propisani vremenski period kao i dokumente na papiru.
- E-pošta koja sadrži osobne podatke, a čija svrha obrade je završena, obvezno se uklanja.
- Kod slanja e-pošte većoj skupini primatelja, obvezno je korištenje bcc polja.

Doseg

Ova pravila odnose se na sve zaposlenike, vanjske suradnike, studente, gostujuće profesore i studente i sve druge osobe kojima je dopuštena uporaba računalnog informacijskog sustava PBF-a.

Pravila obuhvaćaju sustav elektroničke pošte i sve poruke elektroničke pošte smještene na svim elektroničkim uređajima koji koriste informacijski sustav PBF-a.

Pravila se odnose i na sva elektroničke uređaje u vlasništvu PBF-a, priključena u računalnu mrežu ili samostalna elektroničke uređaje priključena u Internet pomoću drugih veza.

Odgovornosti

Odgovornost za primjenu ovih pravila imaju svi korisnici.

Administrator sustava mora:

- uspostaviti i održavati sigurnosna pravila i standarde te korisnicima PBF-a davati tehničku podršku pri uporabi sustava elektroničke pošte,
- nadzirati rad i uporabu sustava elektroničke pošte, detektirati moguća kršenja ovih pravila, te o tim pojavama izvijestiti Povjerenstvo.

Voditelji svih ustrojbenih jedinica moraju osigurati da svi njihovi korisnici elektroničke pošte budu upoznati i da se pridržavaju ovim pravilima.

Procedura za dodjelu adrese e-pošte

Pri zapošljavanju novog djelatnika dodijeli će mu se elektronički identitet i adresa e-pošte.

Pri prestanku radnog odnosa zatvara se korisničke račun.

Studenti imaju mogućnost besplatnog korištenja e-pošte za vrijeme trajanja studija. Nakon prestanka studiranja njihov se korisnički račun zatvara.

Nepridržavanje

Protiv korisnika koji ne poštuju ova pravila PBF može poduzeti odgovarajuće mjere (na primjer ograničiti korištenje korisničkog računa). U slučaju ponovljenih težih prekršaja, korisniku se može zatvoriti korisnički račun i uskratiti mogućnost korištenja servisa elektroničke pošte.

Pravila o zaštiti od neželjenih elektroničkih poruka (*spam*-a)

Svrha

Svrha je osigurati i provoditi sustavnu zaštitu od neželjenih elektroničkih poruka (*spam*-a).

Uvod

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 radno vrijeme i umanjuje produktivnost.

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

Pravila za administratore

Administratori poslužitelja elektroničke pošte dužni su konfigurirati računala na taj način da se što više neželjenih poruka zaustavi.

Prva mogućnost jest 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 određuju 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.

Službu za informatičku potporu će obučiti korisnike i pomagati im pri kreiranju filtera za obilježavanje, odvajanje ili uništavanje neželjenih poruka.

Pravila za korisnike

Korisnici (osim onih s odobrenjem) ne smiju slati masovne poruke, bez obzira na njihov sadržaj. Upozorenja na viruse su često lažna i šire zablude.

Korisnici ne smiju radi stjecanja dobiti odašiljati propagandne poruke koristeći računalnu opremu koja pripada PBF-u.

Nepridržavanje

Protiv korisnika koji se oglušuju o pravila prihvatljivog korištenja i šalju masovne neželjene poruke postupit će se sukladno odredbama vezanim za teže povrede radnih obveza iz Pravilnika o radu.

Pravila o antivirusnoj zaštiti

Svrha

Svrha je osigurati i provoditi sustavnu zaštitu od zloćudnih programa.

Uvod

Zloćudni programi predstavljaju opasnost za informacijske sustave, ugrožavajući funkcioniranje mreže i povjerljivost podataka.

Nove generacije zloćudnih programa su izuzetno složene i opasne, sposobne da prikriju svoje prisustvo, presreću unos podataka na tipkovnici. Informacije poput zaporki ili povjerljivih dokumenata mogu slati svome tvorcu nekamo na Internet, te otvoriti kriptiran kanal do vašeg računala, kako bi hakeri preuzeli kontrolu nad njim.

Stoga zaštita od virusa ne smije više biti stvar osobnog izbora, već obaveza organizacije, administratora računala i svakog korisnika.

Odgovornosti

Zaštita od virusa je obavezna i provodi se na nekoliko razina:

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

Administratori su dužni instalirati antivirusne programe na sva korisnička računala i konfigurirati ih tako da se izmjene u bazi virusa i u konfiguraciji automatski ažuriranju na korisnička računala u lokalnoj mreži.

Korisnici ne smiju samovoljno isključiti antivirusnu zaštitu na svome računalu. Ukoliko iz nekog razloga moraju privremeno zaustaviti antivirusni program, korisnici moraju obavijestiti Službu za informatičku potporu.

Nepridržavanje

Prema korisniku koji samovoljno isključi antivirusnu zaštitu na svom računalu te na taj način izazove štetu, postupit će se sukladno odredbama vezanim za teže povrede radnih obveza iz Pravilnika o radu.

Pravila o klasifikaciji i upravljanju povjerljivim informacijama

Svrha

Svrha je zaštiti povjerljive podatke kojima raspolaže bilo koji segment PBF-a od neovlaštenog pristupa trećih osoba.

Doseg

Ova pravila odnosi se na sve čelnike ustrojbenih jedinica i na sve korisnike koji na bilo koji način raspolažu ili dolaze u kontakt s povjerljivim informacijama.

Klasifikacija informacija

PBF dijeli informacije na:

1. Povjerljive – informacije čije bi otkrivanje moglo nanijeti ozbiljne štetne posljedice PBF-u ili njenim poslovnim partnerima. Uključuju podatke koji su definirani kao poslovna tajna sukladno Statutu Sveučilišta u Zagrebu Prehrambeno-biotehnološkog fakulteta. PBF će uskratiti obavijesti o podacima koji su poslovna tajna, te u uvid u dokumentaciju neovlaštenim osobama. Poslovne tajne može drugim osobama priopćavati samo dekan, odnosno osoba koju dekan za to ovlasti. Također uključuju podatke koji se prema Općoj odredbi o zaštiti podataka smatraju osjetljivima.

2. Ograničene - otkrivanje i dijeljenje ovih informacija može nanijeti negativni publicitet, ali vjerojatno neće uzrokovati ozbiljne financijske posljedice ili posljedice narušavanja ugleda. Ovaj tip informacija može se poistovjetiti s profesionalnom tajnom u smislu pristupa informacijama drugih ljudi od strane djelatnika PBF-a (npr. djelatnici Ureda za studente, Službe za informatičku potporu, Ureda za upravljanje kvalitetom i slično). U ovu skupinu podataka spadaju osobni podatci sukladno Općoj uredbi o zaštiti podataka (koji nisu osjetljivi).

3. Za unutarnju uporabu – informacije koje vlasnik može otkriti i dijeliti sa zaposlenicima i drugim pojedincima bez ograničenja o sadržaju i vremenu objave.

4. Javne – sve informacije koje nemaju neki od stupnjeva povjerljivosti (1 – 3). Mogu se otkrivati ili dijeliti bez ikakvih ograničenja vezanih za sadržaj i vrijeme objave. Ipak, dijeljenje i objava ovih informacija ne smije kršiti primjenjivu regulaciju. Izmjena se mora ograničiti na pojedince koji za to imaju ovlast od vlasnika informacija i koji su se uspješno autentificirali putem računalnog sustava.

Dokumenti koji izvana dolaze u PBF s nekom od oznaka povjerljivosti određuju stupanj povjerljivosti svih dokumenata i informacija koje će PBF proizvesti kao odgovor.

Dokumenti koji se smatraju povjerljivima (svi koji nisu javni) moraju biti jasno označeni isticanjem vrste i stupnja tajnosti.

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.

Odgovornosti

Za klasificiranje povjerljivih informacija zadužen je u Dekan, 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 PBF-a i vanjske suradnike koji dolaze u doticaj sa osjetljivim podacima. Obaveza čuvanja povjerljivosti ne prestaje s prestankom radnog odnosa.

Čelnici ustrojbenih jedinica obvezni su voditi brigu o ograničenoj dostupnosti povjerljivih informacija i podataka za to nadležnim korisnicima u njihovoj ustrojbenoj jedinici, a posebno da:

- korisnici brišu osjetljive (povjerljive) informacije sa svojih diskova i drugih vanjskih memorijskih komponenti kad im ti podaci više nisu potrebni za rad,
- korisnici snimaju i pohranjuju svoje zaštitne kopije važnih informacija u skladu s razinom važnosti informacija,
- korisnici kojima prestaje radni odnos prođu postupak razduživanja informatičke opreme i pohranjenih povjerljivih i važnih podataka prije napuštanja PBF-a
- osiguraju da podaci pod korisnikovom kontrolom budu pravilno zaštićeni, u skladu s razinom osjetljivosti informacija
- korisnici snimaju zaštitne kopije važnih podataka onoliko često koliko sami smatraju razumnim za razinu važnosti informacija.

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.

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

- ime i prezime
- naziv radnog mjesta
- broj telefona na poslu
- službena adresa e-pošte
- predmete i projekte u čijoj izvedbi sudjeluje

Na upite o zaposlenicima davati će se samo informacije objavljene na mrežnim stranicama PBF-a. Daljnje informacije o zaposlenima ne smiju se davati bez suglasnosti osobe kojoj podatci pripadaju (na primjer adresa stana, broj privatnog telefona, podaci o primanjima, porezu, osiguranju itd.).

Povjerljive informacije ne daju se telefonom jer se sugovornik može lažno predstaviti. Ako 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 PBF-a će se posavjetovati s dekanom i ako dobije odobrenje nazvati službenu osobu i odgovoriti na pitanja ili ih dostaviti poštom.

Prenošenje povjerljivih informacija

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

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

Ako se povjerljive informacije šalju elektronički, na primjer 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 PBF ne smiju se kopirati bez izričite dozvole pošiljatelja.

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

Osoblje koje poslužuje uređaje za kopiranje treba obučiti i obavezati da odbiju kopiranje povjerljivih dokumenata ako 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 sadržaj (spaljivanjem, usitnjavanjem, prešanjem).

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

Nepridržavanje

Nepoštivanje pravila o čuvanju povjerljivih informacija smatra se težom povredom o radu te se takve korisnike može premjestiti na drugo radno mjesto na kojem neće dolaziti u dodir s povjerljivim podacima.

S vanjskim suradnicima za koje se ustanovi da otkrivaju povjerljive informacije razvrgnuti će se ugovor. U ugovor će se unijeti stavke po kojima je povreda povjerljivosti podataka dovoljan razlog za raskid ugovora.

Napomena:

Za dio o osobnim podatcima obvezno konzultirajte PBF-ove akte vezane za zaštitu osobnih podataka.

Pravilo čistog stola i čistog ekrana

Svrha

Svrha je definirati minimalne zahtjeve za održavanje „čistog stola i ekrana“, čime PBF štiti osjetljive informacije o zaposlenicima, intelektualnom vlasništvu, studentima ili drugim osobama/organizacijama s kojima surađujemo.

Doseg

Pravila se odnose na sve zaposlenike i studente.

Pravila

- Zaposlenici moraju osigurati da su svi osjetljivi/povjerljivi tiskani ili elektronički podatci zaštićeni na kraju dana i kada očekuju dulje izbivanje.
- Računala moraju biti zaključana kada se s njih izbiva.
- Računala se moraju ugasiti na kraju radnog dana.
- Sve povjerljive i osjetljive informacije moraju se ukloniti sa stola i zaključati kada se stol pušta bez nadzora i na kraju radnog dana.
- Ladičari/Ormari koji sadrže povjerljive i osjetljive informacije moraju se zatvoriti i zaključati kada nisu u uporabi ili su bez nadzora.
- Ključevi koji se koriste za pristup povjerljivim i osjetljivim informacijama ne smiju se puštati na stolu koji nije pod nadzorom.
- Prijenosna računala i svi prijenosni uređaji za pohranu podataka moraju se zaključati (u ladičar, ormar ili drugo).
- Zaporke se ne smiju puštati na samoljepljivim listićima na ili ispod računala odnosno na pristupačnom mjestu.
- Tiskani materijali koji sadrže povjerljive ili osjetljive informacije moraju se smjesta preuzeti s pisača.
- Nakon isteka roka zadanoga Pravilnikom o zaštiti arhivskoga i registraturnoga gradiva dokumente koji sadrže osjetljive ili povjerljive podatke treba izlučiti i/ili uništiti pomoću uništavača dokumenata.
- Ploče koje sadrže osjetljive ili povjerljive podatke valja brisati.

Odgovornosti

Šteta nastala nepoštivanjem ovih pravila odgovornost je zaposlenika odnosno studenta.

Pravila o izradi kopija podataka

Svrha

Svrha je ovih pravila:

- zaštititi informacije PBF-a
- spriječiti gubitak podataka u situacijama slučajnog brisanja ili oštećenja podataka, kvara sustava ili nepogode
- omogućiti blagovremeni oporavak informacija i poslovnih procesa

Odgovornosti

Dekan, u dogovoru sa Službom za informatičku potporu, 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, itd.).

Svaki korisnik javnih računala (info kabinet, knjižnica) sam je zadužen i odgovoran za sigurnost i pohranu osobnih podataka na javna računala. PBF, odnosno osobe zadužene za brigu o javnim računalima na PBF-u, ne izrađuju sigurnosne kopije privatnih podataka korisnika javnih računala te nisu odgovorni za njihov eventualni gubitak.

Podatke s osobnih računala spremaju korisnici (zaposlenici) pojedinačno. Ukoliko im je u tome potrebna pomoć, obraćaju se Službi za informatičku potporu.

Pravila

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

Osnovna strategija izrade kopija:

- Kopija podataka iz baze podataka glavnog servera se izrađuju svakodnevno, na drugoj particiji diska, te u određenim vremenskim intervalima i na traci ručnim backupom. Također, tri ili četiri puta godišnje radi se potpuni backup. Za navedeno je zadužena Službom za informatičku potporu.
- Kopija podataka ključnih servisa (mail, web, dns, itd.), kao i osobnih podataka s poslužitelja, se izrađuje nekoliko puta mjesečno, najčešće jednom tjedno ili dvotjedno.
- Kopije podataka s osobnih računala se izrađuju prema potrebi.

Zaposlenici i vanjski suradnici za izradu sigurnosnih kopija i pohranu podataka mogu koristiti ili medije dobivene od strane PBF-a ili vlastite medije. U bilo kojem slučaju, svaki pojedinac je sam odgovoran za sigurnost dotičnih.

Pravila o enkripciji podataka

Svrha

Povećanje sigurnosti u rukovanju podacima kroz enkripciju podataka, kako bi se osigurala povjerljivost osobnih te službenih podataka. Enkripcija nije obavezna, ali se preporuča.

Rizik

Rizik ne-enkriptiranih datoteka je da ako se potencijalno uređaji na kojima se podaci prenose zagube, treća strana može zlouporabiti podatke.

Preporuka

Preporuka je da se koristi enkripcija na datotekama protokol AES-256 ili RSA-4096 koji potpuno kriptiraju datoteke, te je vrlo teško dekriptirati datoteke potencijalnom hakeru ili trećoj strani.

Doseg

Ova pravila odnose se na sve zaposlenike PBF-a, odnosno na sva računala u vlasništvu PBF-a, priključena u računalnu mrežu ili samostalna računala priključena u Internet pomoću drugih veza.

Odgovornosti

Odgovornost za primjenu ovih pravila imaju sistem administratori sustava (zaposleni ili vanjski po ugovoru), čelnici ustrojbenih jedinica, te svi korisnici.

Administrator sustava mora:

- Pružiti tehničku podršku kod implementacije softvera za enkripciju te uputa za enkripciju

Pomoć kod dekripcije

U slučaju da se korisnik enkripcije nađe u problemima glede dekripcije svojih podataka, zbog zaboravljene lozinke enkriptiranih datoteka, isti će se obratiti Informatičkoj službi, kako bi pokušali otkloniti problem. Ako se problem ne može otkloniti, podaci se moraju spasiti a sustav reinstalirati.

Pravila o instalaciji softvera

Uvod

Korištenje ilegalnog softvera predstavlja povredu autorskog prava i intelektualnog vlasništva. Dopustiti bilo kojem korisniku instalaciju softvera na opremu PBF-a predstavljalo bi nepotreban rizik zbog mogućnosti posljedičnog nefunkcioniranja postojećih programa, instalacije zlonamjernog (eng. *malware*) ili nelicenciranog softvera.

Svrha

Svrha je definirati zahtjeve za instaliranje softvera na opremu PBF-a radi smanjenja rizika gubitka funkcionalnosti programa, otkrivanja osjetljivih informacija unutar računalne mreže PBF-a i rizika instalacije zlonamjernog softvera.

Doseg

Pravila se odnose na sve korisnike i cjelokupnu računalnu i elektroničku opremu PBF-a.

Pravila

Da bi se zaštitio od moralne i materijalne štete koja time može nastati, PBF zadužuje jednu ili više osoba iz Službe za informatičku potporu 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.

Iznimka su administratori lokalnih računala koji mogu samostalno instalirati softvere. Njima se preporuča konzultirati se s djelatnicima Službe za informatičku potporu prije instalacije.

Odgovornosti

Osobe koje instaliraju softver zadužene su za praćenje licenci i testiranje novih softvera (konflikti i kompatibilnost).

Nepoštivanje ovih pravila smatra se težom povredom radnih odnosa te se takve korisnike može premjestiti na drugo radno mjesto na kojem neće dolaziti u dodir s povjerljivim podacima.

Pravila za objavljivanje informacija

Svrha

Svrha je davanje smjernica za poslovanje, postupke i zahtjeve za osiguranjem prihvatljivih načina uporabe računalne mreže i Interneta za interno i javno objavljivanje informacija na mrežnim stranicama (uključujući i one na društvenim mrežama), uključujući procedure za administriranje mrežnih stranica intraneta i Interneta i mrežnih stranica na društvenim mrežama, te zaštitu informacija i resursa PBF-a od zlouporaba.

Doseg

Ova pravila odnose se na zaposlenike, studente, vanjske suradnike, gostujuće studente i sve druge osobe kojima je dopuštena uporaba računalnog informacijskog sustava PBF-a za objavljivanje informacija na mrežnim stranicama PBF-a (u daljnjem tekstu: Sustav).

Pravila obuhvaćaju sustav za administriranje mrežnih stranica primoran pohađati edukaciju na temu antivirusne zaštite koju će održati ono tijelo, te sve poslužitelje koji su dio ovog sustava, a u administrativnoj su domeni ili vlasništvu PBF-a.

Uredništvo

Uredništvo čine glavni urednik, administrator mrežnih stranica i druge osobe imenovane od Uprave.

Odgovornosti

Uredništvo mrežnih stranica:

- definira i objavljuje upute za objavu informacija na mrežnim stranicama
- određuje strukturu informacija na mrežnim stranicama te definira stupnjeve ovlasti za rad sa Sustavom
- predlaže i nadzire vizualnu i sadržajnu ujednačenost objavljenih informacija
- nadzire korektnost objavljenih informacija te korektnost uporabe Sustava od strane korisnika
- objavljuje informacije po zahtjevima i odobrenju Uprave, odnosno, po zahtjevima ovlaštenih čelnika ustrojbenih jedinica,
- prati posjećenost mrežnim stranicama s ciljem unapređenja kvalitete rada.

Pravila o prijenosu podataka

Svrha

Utvrditi minimalne sigurnosne zahtjeve vezane za prijenos podataka.

Doseg

Ova pravila odnose se na sve zaposlenike PBF-a, odnosno na sva računala u vlasništvu PBF-a, priključena u računalnu mrežu ili samostalna računala priključena u Internet pomoću drugih veza.

Pravila

Prijenosi podataka ne bi se smjeli odvijati putem prijenosnih memorija.

Ako se prijenosi ipak prenose na taj način, podatci se moraju enkriptirati koristeći najjaču moguću enkripcijsku metodu. Koristite jake zaporke (pogledajte pravila o zaporkama).

Ako se prijenosi ipak prenose na taj način, dostavu mora obaviti zaposlenik i mora se dostaviti izravno primatelju koji potpisuje primitak.

Zaporke za enkripciju ne smiju se slati s podatcima koje treba zaštititi. Moraju se poslati izravno primatelju i ne otkrivati drugim osobama.

Standardna e-pošta nikada se ne bi trebala koristiti za prijenos osobnih ili osjetljivih podataka. Ako je drugi način prijenosa nemoguć, mora se osigurati enkripcija (pogledajte pravila o enkripciji).

Kada je potreban prijenos s trećom stranom, potrebno je utvrditi zakonsku osnovu ili dobiti privolu ispitanika te unaprijed pripremiti ugovor kojim će se definirati:

- Koji će se podatci prenijeti
- Kontakti osoba koje su odgovorne za podatke u svakoj organizaciji
- Učestalost prijenosa
- Razlog prijenosa
- Metoda prijenosa koja će se koristiti
- Metoda enkripcije koja će se koristiti
- Kako će se dokazati primitak podataka
- Koliko će treća strana zadržati podatke
- Potvrda treće strane da će se podatcima rukovati na istoj razini kontrola kao i na PBF-u
- U kojem trenutku treća strana preuzima odgovornost za zaštitu podatka
- Vrijeme čuvanja i metoda uništenja podataka
- Postupanje vezano za povrede podataka

Odgovornosti

Svi korisnici odgovorni su za eventualnu štetu koja nastane zbog nepridržavanja ovim pravilima.

Djelatnici Službe za informatičku potporu odgovorni su za pomoć kod enkripcije.

PBF je odgovoran za podatke kao voditelj obrade prema Općoj uredbi o zaštiti podataka.

Pravila za postupanje pri sigurnosnim incidentima

Svrha

Svrha je utvrditi korake koje je potrebno poduzeti pri pojavi sigurnosnih incidenata, s posebnim naglaskom na povrede osobnih podataka.

Uzroci

Sigurnosni incident može se dogoditi zbog raznih razloga, uključujući:

- gubitak ili krađa podataka ili opreme na kojoj su pohranjeni podatci (uključujući provale)
- neprimjerene kontrole pristupa koje omogućuju neovlašteno korištenje
- kvar opreme
- ljudska pogreška
- nepredviđene okolnosti kao što su poplava ili požar
- hakerski napad
- pristup koji je rezultat prevare

Tipični koraci

Tipični koraci za rješavanje sigurnosnih incidenata su:

1. prijava
2. istraživanje i oporavak
3. izvještavanje/obavještavanje
4. procjena/poboljšanja

Prijava

Svaki zaposlenik, student ili suradnik PBF-a dužan je prijavljivati sigurnosne incidente, poput usporenog rada servisa, nemogućnosti pristupa, gubitka ili neovlaštene izmjene podataka, pojave virusa itd.

Incidenti se prijavljuju djelatnicima Službe za informatičku potporu, a u slučaju povrede osobnih podataka i Službeniku za zaštitu osobnih podataka. Za prijavu se koristi zadani obrazac.

Istraživanje i oporavak

Ovaj se korak sastoji u ograničavanju utjecaja incidenta.

Administratori smiju pratiti korisničke procese. Ako sumnjaju da se računalo koristi na nedozvoljen način, mogu izlistati sadržaj korisničkog direktorija, ali ne smiju provjeravati sadržaj korisničkih podatkovnih datoteka (na pr. dokumenata ili e-mail poruka).

Čim se otkrije incident, moraju se poduzeti radnje za njegovo ograničavanje.

Daljnja istraga može se provesti samo ako je prijavljena Povjerenstvu, uz poštivanje sljedećih pravila:

- Istragu provodi Povjerenstvo.
- Prvo pravilo forenzičke istrage jest da se informacijski sustav sačuva u zatečenom stanju, odnosno da se ne učine izmjene koje bi otežale ili onemogućile dijagnosticiranje.
- Najprije se napravi kopija zatečenog stanja (na pr. na traku, 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.

Posebice se istražuju rizici vezani za incident:

- koji je tip podataka uključen i koliko su podatci osjetljivi
- na koga incident ima utjecaj
- što može otkriti o poslovanju PBF-a ili o ispitanicima
- može li se incident klasificirati kao kršenje prava i sloboda ispitanika
- količina podataka (posebice osobnih) na koju incident ima utjecaj
- kako se informacije mogu iskoristiti (koje su moguće štete za ispitanike i PBF)
- je li bilo drugih incidenata koji mogu imati kumulativni učinak
- postoji li rizik ponavljajućih incidenata i daljnjeg otkrivanja podataka
- postoje li dokazi o krađi
- jesu li korištene neke mjere zaštite (npr. enkripcija, anonimizacija...)
- koji je uzrok incidenta (i je li namjeran ili slučajan)
- koje su mjere poduzete
- radi li se o sustavnom problemu ili izoliranom incidentu

Opravak podataka vrši se sukladno pravilima struke te sukladno ozbiljnosti sigurnosnih incidenata, uzimajući u obzir:

- pravila o izradi kopija podataka
- kritične sustave i prioritete
- mjere oporavka za povratak u normalno stanje
- odgovornosti i ovlasti uključenih

Obavještavanje/Izvještavanje

Općenito, ako incident predstavlja rizik ozbiljne štete ispitanika, oni se moraju obavijestiti.

Osnovni parametar je hoće li obavještavanje u konačnici rezultirati manjom štetom za ispitanike.

Potrebno je uzeti u obzir:

- koji su rizici identificirani pri istraživanju incidenta
- može li ispitanik, poduzimajući određene radnje, izbjeći ili umanjiti moguću štetu ako ga se obavijesti o incidentu (uz mjere koje će poduzeti PBF)
- ako ispitanik ne može poduzeti neke mjere, odnosi li se povreda na podatke koji su osjetljivi ili mogu uzrokovati poniženje
- koje su zakonske ili ugovorne obveze vezane za obavještavanje/izvještavanje o incidentu

Ovisno o stupnju rizika za prava i slobode pojedinaca, o povredama osobnih podataka obavještavaju se i Agencija za zaštitu osobnih podataka i ispitanici u što kraćem roku, a najkasnije u roku od 72 sata.

Obavještavanje ispitanika mora biti izravno (telefonom, e-poštom, osobno), osim kada to nije moguće (npr. u slučajevima kada ne postoji kontakt ili gdje takvo obavještavanje može rezultirati dodatnom štetom). U tim iznimnim slučajevima koriste se mrežne stranice ili mediji.

Ozbiljniji incidenti prijavljuju se CARNetovom CERT-u, preko obrasca na mrežnoj stranici www.cert.hr

Obavještavanje/Izvještavanje

Cjelokupno postupanje se dokumentira, a krajnja je forma zadana obrascem Izvješće o sigurnosnom incidentu.

Izvještaji se klasificiraju kao ograničene informacije te se na odgovarajući način njima upravlja (pogledajte predmetna pravila), čuvaju se sukladno Pravilniku o zaštiti arhivskoga i registraturnoga gradiva PBF-a.

Procjena/Poboljšanja

Sve informacije prikupljene tijekom rješavanja sigurnosnih incidenata moraju se koristiti za otkrivanje uzroka i poboljšanje mjera sigurnosti u budućem razdoblju, uključujući:

- ažuriranje ovog Pravilnika o svih njegovih sastavnih dijelova
- provođenje unutarnjeg vrjednovanja
- plan edukacija zaposlenika

Nepridržavanje

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 faktor, protiv odgovornih se mogu poduzeti odgovarajuće mjere.

PBF može osobama odgovornim za sigurnosni incident zabraniti fizički pristup prostorijama ili logički pristup podacima.

Ako je incident izazvao zaposlenik vanjske organizacije, PBF može zatražiti od vanjske organizacije da ga ukloni s liste osoba ovlaštenih za obavljanje posla na PBF-u. U slučaju teže povrede pravila sigurnosne politike, PBF može raskinuti ugovor s vanjskom organizacijom.

Napomena: za povrede osobnih podataka pročitajte dodatnu dokumentaciju.