SVEUČILIŠTE U RIJECI
SVEUČILIŠNA KNJIŽNICA RIJEKA
Dolac 1, 51000 Rijeka

Sigurnosna politika informacijskih sustava u Sveučilišnoj knjižnici Rijeka

Sigurnosna politika u Sveučilišnoj knjižnici Rijeka (dalje u tekstu: Sigurnosna politika) dio je sustava upravljanja sigurnošću informacijskih sustava. Njezina je svrha definirati prihvatljive i neprihvatljive načine ponašanja, jasno raspodijeliti zadatke i odgovornosti te propisati sankcije u slučaju njihova nepridržavanja.

Osnovni dokument o sigurnosti, koji postavlja opće principe, prate drugi dokumenti koji definiraju pravila za specifična područja (npr. pravila o rukovanju zaporkama, o uporabi elektroničke pošte, pohrani podataka i slično). Ta pravila su ovisna o promjenama u tehnologiji i organizaciji te će se češće mijenjati i dorađivati.

Prilikom zapošljavanja, nove zaposlenike treba upoznati s pravilima propisanim Sigurnosnom politikom, a nove članove prilikom učlanjenja u Sveučilišnu knjižnicu Rijeka (dalje u tekstu: Knjižnica). Nakon usvajanja, dokument o Sigurnosnoj politici bit će objavljen na javnim mrežnim stranicama Knjižnice te svi korisnici trebaju biti upoznati i sa svim dodatnim dokumentima koji su u prilogu ovog dokumenta.

Sigurnosne politike u poslovnom svijetu iznimno su restriktivne. Pojednostavljeno rečeno, sve je zabranjeno, osim onog što je izričito dopušteno. A dopušteno je samo ono što je neophodno za obavljanje posla.

Akademska zajednica pripada otvorenoj kulturi, okrenuta je komuniciranju, istraživanju, samorazvoju i učenju. Sveučilište brani svoje slobode i nezavisnost, ne trpi restrikcije te će stoga i ova Sigurnosna politika biti liberalnija.

Tako je i Knjižnica doradila i prilagodila pravila kako bi Sigurnosna politika bila primjenjiva i u njezinim, specifičnim uvjetima.

Sigurnosna politika informacijskih sustava u Knjižnici temelji se na dokumentu Sigurnosna politika informacijskih sustava za članice CARNeta.

Na koga se odnosi Sigurnosna politika?

Pravila rada i ponašanja koja definira Sigurnosna politika vrijede za:

- ✓ Svu računalnu opremu (kao i pripadajuće programe) koja se nalazi u prostorima Knjižnice
- ✓ Administratore informacijskih sustava
- ✓ Korisnike, u koje spadaju: zaposlenici, vanjski suradnici i članovi Knjižnice
- ✓ Vanjske tvrtke koje po ugovoru rade na održavanju opreme ili *softwarea*

Organizacija upravljanja sigurnošću

Osobe koje se u radu koriste računalima dijele se na *korisnike i davatelje informacijskih usluga*.

Korisnici informatičkih usluga

Korisnici su osobe koje se u svom radu ili učenju služe računalima, proizvode dokumente ili unose podatke, ali nisu odgovorni za instalaciju i konfiguraciju *softwarea*, niti za ispravan i neprekidan rad računala i mreže.
Svaki korisnik informacijskog sustava mora znati koja je njegova uloga u poboljšanju sigurnosti ukupnog sustava.

Korisnici su dužni:
- ✓ Pridržavati se pravila prihvatljivog korištenja, što znači da ne smiju koristiti računala za djelatnosti koje nisu u skladu s važećim zakonima, etičkim normama i pravilima lokalne Sigurnosne politike
- ✓ Izabrati kvalitetne zaporke i povremeno ih mijenjati
- ✓ Prijavljivati sigurnosne incidente kako bi problemi što prije nestali
- ✓ Korisnici koji proizvode podatke i dokumente odgovorni su i za njihovo čuvanje. Davatelji usluga osiguravaju automatsku pohranu (*backup*) važnih informacija, dok za vlastite podatke i dokumente korisnici sami izrađuju sigurnosne kopije.

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

Glavni korisnik

Knjižnica koristi aplikacije za obradu podataka: računovodstvene programe i programe za obradu knjižnične građe. Radi poboljšanja sigurnosti za svaki od tih programa imenuje se glavni korisnik. Voditelj računovodstva je glavni korisnik za računovodstvene programe, a administrator baze podataka je glavni korisnik programa za obradu knjižne građe.

Zaposlenici koji unose podatke odgovorni su za njihovu vjerodostojnost, dok je glavni korisnik odgovaran za ispravnost podataka, za provjeru ispravnosti i sigurnosti aplikacije, za dodjelu dozvola za pristup podacima i za mjere sprečavanja izmjene podataka od neautoriziranih osoba.
Glavni korisnik kontaktira proizvođača aplikacije i dogovara isporuku novih verzija, traži ugradnju sigurnosnih mehanizama itd.
Ako se ukaže potreba, ravnatelj Knjižnice može imenovati i zamjenike glavnih korisnika za pojedine aplikacije.

Davatelji informatičkih usluga

Davateljima usluga smatraju se profesionalci koji brinu o radu računala i mreže te informacijskih sustava. U Knjižniciji je to Služba primjene IT (dalje u tekstu: Služba). Služba je zadužena za ispravnost i neprekidnost rada informacijskih sustava.

Specijalisti za sigurnost

Knjižnica će pri rješavanju sigurnosnih incidenata koristiti pomoć CARNeta.
Pored toga, Knjižnica će obrazovati i imenovati pojedince čija će zadaća biti briga za organizaciju i provođenje sigurnosnih mjera navedenih u Sigurnosnoj politici.

Ravnatelj Knjižnice 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.
Njegova je briga ukupna sigurnost informacijskih sustava.

Voditelj sigurnosti piše pravilnike, nadzire rad mreže i servisa, organizira obrazovanje korisnika i administratora, komunicira s upravom, sudjeluje u donošenju odluka o nabavi računala i *softwarea* te sudjeluje u razvoju *softwarea* kako bi osigurao da se poštuju pravila iz Sigurnosne politike.

Administriranje računala

Davatelji usluga dužni su administrirati računala i mrežnu opremu u skladu s pravilima struke, brinući istovremeno o funkcionalnosti i sigurnosti.
Za svako računalo se imenuje administrator koji odgovara za instalaciju i konfiguraciju *softwarea*.
Računala se moraju konfigurirati na taj način da budu zaštićena od napada izvana i iznutra, što se osigurava instaliranjem dodataka programima po preporukama proizvođača, listama pristupa, filtriranjem prometa i drugim sredstvima.

Posebnu pažnju administratori su dužni posvetiti onoj opremi preko koje se obavljaju ključne funkcije ili koja sadrži vrijedne i povjerljive informacije koje treba štiti od neovlaštenog pristupa.

Administratori računala svakodnevno prate rad sustava.
Isto tako, administratori nadgledaju i rad korisnika kako bi otkrili i spriječili nedopuštene aktivnosti. U slučajevima kad administrator treba na sustavu obaviti više poslova istovremeno, prioritet određuje samostalno u skladu s pravilima struke, brinući istovremeno o funkcionalnosti i sigurnosti.

Administratori su dužni prijaviti incidente voditelju sigurnosti te pomoći pri istrazi i uklanjanju problema.

Incidenti se dokumentiraju kako bi se pomoglo u nastojanju da se izbjegnu slične situacije u budućnosti. Ukoliko je incident ozbiljan i uključuje kršenje zakona, prijavljuju se CARNet-ovu CERT-u.
Davatelji usluga dužni su u svome radu poštivati privatnost korisnika i povjerljivost informacija s kojima pri obavljanju posla dolaze u dodir.

Upravljanje mrežom

Ravnatelj Knjižnice imenuje zaposlenika/e koji su zaduženi za upravljanje mrežom, konfiguriranje mrežnih uređaja, dodjeljivanje adresa, kreiranje virtualnih LAN-ova itd.

Knjižnica treba propisati i postupke za priključivanje računala u mrežu, odrediti obrasce kojima se izdaje odobrenje za priključenje računala na mrežu i dodjelu adrese.

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

Ukoliko će se podržavati rad na daljinu (npr. kada se zaposlenicima dopušta da s kućnog računala ažuriraju podatke), bit će potreban poseban pravilnik kojeg će morati poznavati i pridržavati ga se svi koji tako rade. Obzirom na mogućnost da ga koriste neautorizirane osobe (članovi obitelji i slično), morat će se osigurati da udaljeno računalo ne ugrozi sigurnost mreže ustanove. Stoga povjerljivi podaci na udaljenom računalu moraju biti jednako sigurni kao da se računalo nalazi u zgradi ustanove.

Knjižnica će razraditi pravila za spajanje na mrežu gostujućih računala koja donose sa sobom vanjski suradnici, predavači, poslovni partneri, serviseri. Zbog opasnosti od širenja virusa ili namjernih nedopuštenih radnji (poput presretanja mrežnog prometa, prikupljanja informacija itd.), ne smije se dozvoliti da oni po svom nahođenju priključuju računala na mrežu Knjižnice.

Knjižnica će odrediti mjesta gdje je dopušteno priključiti gostujuća računala te konfiguracijom mreže spriječiti da se s tog segmenta mreže dolazi do ostalih računala u ustanovi.
Dijelovi Knjižnice koji koriste bežičnu mrežu su osigurani od mogućnosti priključivanja na privatnu mrežu i snimanja prometa. To je postignuto metodama enkripcije i autentifikacije uređaja i korisnika.

Instalacija i licenciranje softwarea

Korištenje ilegalnog *softwarea* predstavlja povredu autorskog prava i intelektualnog vlasništva. Da bi se zaštitila od moralne i materijalne štete koja time može nastati, Knjižnica zadužuje jednu ili više odgovornih osoba za instaliranje *softwarea* i njegovo licenciranje. Korisnik koji ima potrebu za nekim programom mora se obratiti ovlaštenoj osobi i zatražiti, uz obrazloženje, nabavu i instalaciju.
Sve korisnike treba obavezati na poštivanje autorskih prava, između ostalog i potpisivanjem Izjave da su upoznati s Politikom prihvatljivog korištenja i da će je se pridržavati. Na taj način Knjižnica odgovornost za eventualno kršenje zakona prebacuje na nesavjesnog korisnika.

Povjerenstvo za sigurnost informacijskih sustava

Kako bi se osiguralo upravljanje sigurnošću, poželjno je ustrojiti Povjerenstvo za sigurnost (dalje u tekstu: Povjerenstvo), a koje bi bilo sastavljeno od predstavnika uprave i specijalista tehničara (npr. voditelj sigurnosti, ravnatelj, CARNet koordinator, glavni korisnik baze podataka koja sadrži povjerljive informacije itd.).
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.
Povjerenstvo podnosi izvještaj o stanju sigurnosti upravi Knjižnice te se zalaže za donošenje konkretnih mjera, nabavu potrebne opreme, ulaganje u obrazovanje specijalista, ali i običnih korisnika.

Fizička sigurnost

Prostor u Knjižnici 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.
Knjižnica je dužna sastaviti popis osoba koje imaju pristup u zaštićene prostore.

Sigurne zone

Računalna oprema koja obavlja najvažnije funkcije neophodne za funkcioniranje informacijskog sustava ili sadrži povjerljive informacije, fizički se odvaja u prostor u koji je ulaz dozvoljen samo ovlaštenim osobama.
Knjižnica je dužna 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. Ta 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 incidente, poput poplava, požara i slično, te poduzeti mjere da se oprema i informacije zaštite i da se osigura što brži oporavak sustava.
U sigurnim zonama i u njihovoj blizini ne smiju se držati zapaljive i eksplozivne tvari.

Vanjske tvrtke

Povremeno se osobama iz vanjskih tvrtki ili ustanova mora dopustiti pristup opremi, radi servisiranja,

održavanja, podrške, obuke, zajedničkog poslovanja, konzultacija itd.
Knjižnica u ugovore s vanjskim tvrtkama ugrađuje odredbe kojima obavezuje poslovne partnere na poštivanje sigurnosnih pravila.
Ugovorom će se regulirati pristup prostorijama, pristup opremi ili logički pristup povjerljivim informacijama.

Treću stranu treba obavezati na čuvanje povjerljivih informacija s kojima dođu u dodir pri obavljanju posla. Knjižnica 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 za to nemaju ovlasti, mora im se osigurati pratnja. Strana osoba može se ostaviti da obavi posao u zaštićenom prostoru samo ako je prostor osiguran video nadzorom.

Ukoliko se vanjskoj tvrtki prepušta održavanje opreme i aplikacija s povjerljivim podacima, Knjižnica može od te tvrtke zatražiti popis osoba koje će dolaziti u prostorije Knjižnice radi obavljanja posla.
U slučaju zamjene izvršitelja, vanjska tvrtka dužna je na vrijeme obavijestiti Knjižnicu.
Knjižnica zadržava diskreciono pravo da osobama koje se predstavljaju kao zaposlenici vanjskih tvrtki uskrati pristup u svoje prostorije ukoliko nisu na popisu ovlaštenih zaposlenika dostavljenom Knjižnici.

Sigurnost opreme

Klasifikacija računalne opreme

Knjižnica dijeli svu opremu u grupe prema zadaćama:
- ✓ Zona javnih servisa (tzv. demilitarizirana zona) – oprema koja obavlja javne servise (CROLIST-kooperativna katalogizacija – lokal i dr.)
- ✓ Intranet je privatna mreža Knjižnice, sačinjavaju je poslužitelji internih servisa, osobna računala zaposlenih, računalne učionice, video nadzor te komunikacijska oprema lokalne mreže
- ✓ Extranet je proširenje privatne mreže otvoreno mobilnim korisnicima, poslovnim partnerima ili povezivanje izdvojenih lokacija. U ovu grupu, za sada, mogu se ubrojiti veze lokalnih baza podataka s centralnim poslužiteljima (LDAP, CROLIST-kooperativna katalogizacija – korisnici, office365, web server, poslužitelj elektroničke pošte).

Podjela opreme prema vlasništvu

U prostorijama Knjižnice nalazi se i oprema CARNeta koja je dana na korištenje Knjižnici.
Knjižnica je obavezna održavati popis sve računalne opreme s opisom ugrađenih komponenti, inventarnim brojevima i slično.
Knjižnica jednako brine o svoj opremi kojom raspolaže, bez obzira na to tko je njezin vlasnik. Oprema se čuva od oštećenja i otuđenja.

Odgovornost za računalnu opremu

Za fizičku sigurnost opreme odgovoran je rukovoditelj ustanove, ravnatelj. On odgovornost za grupe uređaja ili pojedine uređaje prenosi na druge zaposlene koji potpisuju dokument kojim potvrđuju da su preuzeli opremu.
Knjižnica je dužna razraditi procedure kojima se nastoji spriječiti otuđenje i oštećenje računalne opreme.

Osiguranje neprekidnosti poslovanja

Kako bi se u slučaju nezgoda (poput kvarova na sklopovlju, požara, ili ljudskih grešaka) podaci sačuvali, potrebno je redovito izrađivati rezervne kopije svih vrijednih informacija, uključujući i konfiguraciju *softwarea*.
Preporučuje se izraditi više kopija i čuvati ih na različitim mjestima, po mogućnosti u vatrootpornim ormarima.

Procedura za izradu rezervnih kopija razrađena je u zasebnom dokumentu. Potrebno je zadužiti konkretne zaposlenike za izradu i čuvanje kopija informacija te ih obavezati na čuvanje povjerljivosti informacija.

Povremeno se provjerava upotrebljivost rezervnih kopija podataka te izvode vježbe oporavka sustava. Vježbe se ne izvode na produkcijskim računalima već na rezervnoj opremi (koju bi trebalo osigurati zaposlenicima zaduženim za te poslove) u laboratorijskim uvjetima.

Nadzor nad informacijskim sustavima

Knjižnica zadržava pravo nadzora nad instaliranim *softwareom* i podacima 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 da li su informacijski sustavi i njihovo korištenje usklađeni sa zahtjevima Sigurnosne politike.

Nadzor smiju obavljati samo osobe koje je Knjižnica za to ovlastila.
Pri provođenju nadzora, ovlaštene osobe dužne su poštivati privatnost i osobnost korisnika i njihovih podataka. U slučajevima kada je korisnik prekršio pravila Sigurnosne politike, ne može se više osigurati povjerljivost informacija otkrivenih u istrazi pa se one mogu koristiti u stegovnom ili sudskom postupku.

Doseg

Ova se pravila odnose na svu računalnu opremu koja se nalazi u prostorijama Knjižnice i priključena je u mrežu Knjižnice, na sav instalirani *software* te na sve mrežne servise.

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

Provođenje

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. Isto vrijedi i za administratore računala i pojedinih servisa koji su dužni specijalistima 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 Knjižnice, ili oprema Knjižnice služi za njezin prijenos

- ✓ Pristup radnom prostoru (uredu, laboratoriju, sigurnoj zoni itd.)
- ✓ Pravo na interaktivno nadgledanje i bilježenje prometa na mreži Knjižnice.

Nepridržavanje

Zaposlenika koji se ogluši na pravila o nadzoru može se disciplinski kazniti ili mu se mogu uskratiti prava korištenja mreže i njezinih servisa.

Praktična primjena Sigurnosne politike

Kako bi se Sigurnosna politika mogla što uspješnije primijeniti, nužno je:
- ✓ Obnoviti postojeći popis računala, pisača i drugih informatičkih uređaja
- ✓ Postojeću skicu mreže provjeriti i ažurirati novim priključcima. Sve mrežne priključke numerirati na razumljiv i jedinstven način u Knjižnici tako da se svaki priključak može brzo pronaći.

Nakon usvajanja Sigurnosne politike, treba napraviti inventuru kompletne računalne opreme, uključujući mrežne i komunikacijske uređaje. Za svako računalo potrebno je evidentirati koji se operacijski sustav na njemu koristi te popisati aplikacije koje su na njemu instalirane. Knjižnica u svakom trenutku treba imati ažurirani popis *softwarea* koji se koristi u LAN-u kako bi mogla brinuti o licenciranju.

Uz ovu Sigurnosnu politiku prilažu se i pravilnici.
Pisani su kao upute za rješavanje konkretnih problema i mogu se češće mijenjati.
Pravilnici su sastavni dio Sigurnosne politike Sveučilišne knjižnice Rijeka.

KLASA: 012-03/22-02
URBROJ: 2170-04-01-22-7
Rijeka, 12. rujna 2022.

SVEUČILIŠTE U RIJECI
SVEUČILIŠNA KNJIŽNICA RIJEKA

RAVNATELJICA:

Lea Lazzarich, knjiž. savjetnica

MOBITEL +385 (0)91 245 0007 E-MAIL ravnatelj@svkri.hr
WEB STRANICA: https://www.svkri.uniri.hr,
MATIČNI BROJ: 3328686 OIB: 84122581314 IBAN HR7524020061100996596 (ERSTE BANK)

Prilog 1

Pravilnik o rukovanju zaporkama

Članak 1.

Svi korisnici (zaposlenici, suradnici i članovi) Knjižnice koji u svome radu koriste računala dužni su pridržavati se pravila o korištenju zaporki, dok su ih administratori dužni tehnički ugraditi u sve sustave koji to omogućavaju.

Članak 2.

1. Minimalna dužina zaporke
Minimalna dužina zaporke bi se trebala sastojati od šest znakova, ali preporučuje se korištenje još dužih zaporki.

2. Riječi iz rječnika
Ne ih koristiti jer hackeri posjeduju zbirke rječnika, što im olakšava probijanje ovakvih zaporki (tzv. dictionary attack).

3. Izmiješati mala i velika slova s brojevima
Polazište je pojam koji lako pamtimo, ali onda po nekom algoritmu vršimo zamjenu znakova. Koristiti i specijalne znakove ako su dopušteni u sustavu (npr. £).

4. Imena bliskih osoba, ljubimaca, datumi
Ne treba koristiti takve zaporke jer se lako otkriju socijalnim inženjeringom.

5. Trajanje zaporke
Promjena zaporke smanjuje vjerojatnost njezina otkrivanja.

6. Tajnost zaporke
Potpisom na obrascu za preuzimanje zaporke korisnici preuzimaju odgovornost za svoju zaporku i ni u kom je slučaju ne smiju otkriti.

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. Ukoliko korisnik zaboravi zaporku, administrator će mu omogućiti da unese novu.

8. Administriranje zaporki
Ukoliko sustav dopušta 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 bi trebali konfigurirati autentifikaciju tako da zaporke zastare nakon 90 dana te onemogućiti korištenje zaporki koje su već potrošene, ako sustav to dopušta.
Prilikom provjere sustava, sigurnosni tim može ispitati jesu li korisničke zaporke u skladu s navedenim pravilima.

Članak 3.

Korisnici koji se ne pridržavaju navedenih pravila ugrožavaju sigurnost informacijskog sustava.
Knjižnica je obavezna odgojno djelovati i obrazovati korisnike prilikom kreiranja sigurnih zaporki.

Prilog 2

Pravilnik o korištenju elektroničke pošte

Članak 1.

Pravilnikom o korištenju elektroničke pošte (dalje u tekstu: Pravilnik) uređuje se elektronička pošta kao dio svakodnevne komunikacije, poslovne i privatne u Sveučilišnoj knjižnici Rijeka.

Članak 2.

Problemi koji mogu nastati pri korištenju elektroničke pošte:

1. Nesigurnost protokola
2. Nezgode
3. Nesporazumi
4. Otkrivanje informacija
5. Radna etika
6. Povreda autorskih prava

Članak 3.

Korištenje elektroničke pošte smatra se rizičnom djelatnošću te su korisnici obvezni pridržavati se sljedećih pravila:

- Zaposlenicima se otvara korisnički račun radi obavljanja posla
- Privatne poruke dozvoljene su u umjerenoj količini, ukoliko to ne ometa redoviti rad. Za privatne potrebe mogu se koristiti za to namijenjene HR-F domene
- Pišući poruke, budite svjesni da ne predstavljate samo sebe, već i ustanovu za koju radite
- Pridržavajte se netiquete, pravila pristojnog ponašanja na internetu, službenu e-mail adresu nemojte koristiti za slanje uvredljivih, omalovažavajućih poruka, za seksualno ili bilo koje drugo uznemiravanje.
- Nije dozvoljeno slanje lančanih poruka kojima se opterećuju mrežni resursi, a 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
- Sve poruke pregledat će automatski aplikacija koja otkriva viruse. Ako poruka zadrži virus, neće biti isporučena, a pošiljatelj i primatelj će biti o tome obaviješteni. Poruka će provesti određeno vrijeme u karanteni, odakle ju je moguće na zahtjev primatelja izvući. Nakon određenog vremena, obično mjesec dana, poruka se briše iz karantene kako bi se oslobodio prostor na disku
- Knjižnica zadržava pravo konfiguriranja sustava na način da ne obavještava pošiljatelja i primatelja o otkrivenom virusu u poruci ukoliko se ustanovi da se radi o tzv. virusima koji lažiraju adresu
- Knjižnica zadržava pravo filtriranja poruka s namjerom da se zaustavi spam
- U slučaju istrage uzrokovane mogućim sigurnosnim incidentom, sigurnosni tim može pregledavati kompletan sadržaj diska, pa time i e-mail poruke
- Poruke koje su dio poslovnog procesa treba arhivirati i čuvati propisani vremenski period kao i dokumente na papiru.

Članak 4.

Pri zapošljavanju novog zaposlenika, ravnatelj će zatražiti od administratora poslužitelja elektroničke pošte otvaranje korisničkog računa.

Pri prestanku radnog odnosa, ravnatelj je dužan najkasnije u roku od sedam dana zatražiti zatvaranje korisničkog računa.

Članak 5.

Pravila za korištenje e-maila odnose se na sve zaposlene, vanjske suradnike i ostale korisnike koji imaju otvoren korisnički račun na poslužitelju Knjižnice i Sveučilišta.

Članak 6.

Protiv korisnika koji ne poštuju ova pravila, Knjižnica može pokrenuti stegovni postupak. U slučaju ponovljenih težih prekršaja, korisniku se može zatvoriti korisnički račun i uskratiti pravo korištenja servisa elektroničke pošte.

Prilog 3

Pravilnik o antivirusnoj zaštiti

Članak 1.

Pravilnikom o antivirusnoj zaštiti (dalje u tekstu: Pravilnik) uređuje se zaštita od virusa u Sveučilišnoj knjižnici Rijeka, a koji potencijalno predstavljaju opasnost za informacijske sustave jer ugrožavaju funkcioniranje mreže i povjerljivost podataka.

Članak 2.

Zaštita od virusa je osnovna obaveza Knjižnice, administratora računala i svakog korisnika.
Knjižnica propisuje da je zaštita od virusa obavezna i da se provodi na nekoliko razina:

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

Članak 3.

Administratori su dužni instalirati protuvirusne programe na sva korisnička računala i konfigurirati ih.

Članak 4.

Korisnici ne smiju samovoljno isključiti protuvirusnu zaštitu na svome računalu. Ukoliko iz nekog razloga moraju privremeno zaustaviti protuvirusni program, korisnici prethodno obavijestiti sistem inženjera.

Članak 5.

Korisnik koji samovoljno isključi protuvirusnu zaštitu na svom računalu te na taj način izazove štetu, bit će stegovno kažnjen.

Prilog 4

Pravilnik o zaštiti od spama

Članak 1.

Pravilnikom o zaštiti od spama (dalje u tekstu: Pravilnik) uređuje se zaštita od sve više neželjenih komercijalnih poruka, tzv. spama u Sveučilišnoj knjižnici Rijeka.

Članak 2.

Administratori poslužitelja elektroničke pošte dužni su 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.

Članak 3.

Informatičar zadužen za sigurnost će pomagati korisnicima pri kreiranju filtera za obilježavanje, odvajanje ili uništavanje neželjenih poruka.

Članak 4.

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

Članak 5.

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

Članak 6.

Protiv korisnika koji se ne pridržavaju pravila prihvatljivog korištenja i šalju masovne neželjene poruke bit će pokrenut stegovni postupak.

Prilog 5

Pravilnik o izradi kopija podataka

Članak 1.

Ravnatelj Knjižnice određuje tko je od zaposlenika zadužen za izradu kopija pojedine vrste podataka. Izradu kopija podataka treba prilagoditi postojećoj tehnološkoj osnovi kojom raspolaže Knjižnica.

Članak 2.

Osnovna strategija izrade kopija:

- Kopije podataka iz baze podataka knjižnično-informacijskog sustava izrađuje vanjska tvrtka s kojom je Knjižnica sklopila ugovor o pružanju *cloud backup* usluga. Ona osigurava sigurnosnu pohranu kopija podataka na udaljenu lokaciju u svrhu zaštite podataka od nepredviđenih, katastrofalnih događaja.
- Kopija podataka ključnih servisa (mail, web), kao i osobnih podataka s poslužitelja, izrađuje se jednom tjedno za servise Knjižnica, a za office365 je zadužen SIC sa Sveučilišta
- Kopije podataka s osobnih računala se izrađuju prema potrebi.

Članak 3.

Podatke s osobnih računala spremaju korisnici (zaposlenici) pojedinačno. Ukoliko im je u tome potrebna pomoć, pomaže im Služba za primjenu IT u Knjižnici.

Članak 4.

Članovi knjižnice, kao i vanjski suradnici, ne mogu koristiti vlastite medije za pohranu podataka (CD, DVD, USB) bez prethodnog odobrenja odgovorne osobe u Knjižnici.

Prilog 6

Pravilnik o rješavanju sigurnosnih incidenata

Članak 1.

Pravilnikom o rješavanju sigurnosnih incidenata (dalje u tekstu: Pravilnik) uređuje se u Sveučilišnoj knjižnici Rijeka obaveza prijavljivanja sigurnosnih incidenata, razrada procedure za provođenje istrage.

Članak 2.

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

Knjižnica treba izraditi i održavati listu kontakt osoba kojima se prijavljuju problemi u radu računala i servisa te obrazac za prijavu incidenta. Listu treba podijeliti svim zaposlenima i objaviti je na internim mrežnim stranicama.

Svaki incident se dokumentira. Uz obrazac za prijavu incidenta, dokumentacija sadrži i obrazac s opisom incidenta i poduzetih mjera pri rješavanju problema.

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

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

Članak 3.

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 (npr. dokumenata ili e-mail poruka).

Članak 4.

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 učine izmjene koje bi otežale ili onemogućile dijagnosticiranje
- Najprije se napravi kopija zatečenog stanja (npr. na traku, CDI), po mogućnosti na takav način da se ne izmijene atributi datoteka (na Unixu naredbom dd)
- Dokumentira se svaka radnja, tako da se ponavljanjem zabilježenih akcija može rekonstruirati tijek istrage
- O istrazi se napiše izvještaj, kako bi u slučaju potrebe mogli poslužili kao dokaz u eventualnim stegovnim ili sudskim procesima
- Izvještaji o incidentu smatraju se povjerljivim dokumentima i čuvaju se na taj način da im pristup imaju samo ovlaštene osobe.

Članak 5.

Dok ne bude formirano Povjerenstvo za sigurnost, Knjižnica će koristiti pomoć CARNeta za rješavanje sigurnosnih problema.

Članak 6.

Knjižnica može objavljivati statističke podatke o sigurnosnim incidentima, bez otkrivanja povjerljivih i

osobnih informacija.

Članak 7.

Svrha istrage je 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 bila pogreška čovjeka, protiv odgovornih se mogu poduzeti sankcije.

Članak 8.

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

Ukoliko je incident izazvao zaposlenik vanjske tvrke, Knjižnica može zatražiti od vanjske tvrtke da ga ukloni s liste osoba ovlaštenih za obavljanje posla na ustanovi. U slučaju teže povrede pravila Sigurnosne politike, Knjižnica može raskinuti ugovor s vanjskom tvrtkom.

Prilog 7

Pravilnik o upravljanju povjerljivim informacijama

Članak 1.

Prema stupnju tajnosti, informacije mogu biti povjerljive, tajne ili vrlo tajne.
Poslovna tajna su informacije koje imaju komercijalnu vrijednost i čije bi otkrivanje moglo nanijeti štetne posljedice Knjižnici ili njenim poslovnim partnerima (ugovori, financijski izvještaji, planovi, rezultati istraživanja itd.).

Članak 2.

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.

Članak 3.

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

Članak 4.

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

Članak 5.

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.

Članak 6.

Knjižnica 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

Članak 7.

Na upite o zaposlenicima davat će se samo informacije objavljene na mrežnim stranicama Knjižnice.
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 itd.).
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 Knjižnice će se posavjetovati s upravom i ukoliko dobije odobrenje nazvati službenu osobu i odgovoriti na pitanja.

Članak 8.

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.

Članak 9.

Za kopiranje povjerljivih informacija treba zatražiti dozvolu vlasnika informacije.

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

Dokumenti koji pripadaju Knjižnici 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 ukoliko nije ispoštovana propisana procedura.

Članak 10.

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, na kojima su bili povjerljivi podaci, daje na korištenje trećoj strani, obavezno je uništavanje podataka s diskova posebnim programom koji nepovratno briše sadržaj diska.

Članak 11.

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, a može ih se 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. Knjižnica treba u ugovor unijeti stavke po kojima je povreda povjerljivosti podataka dovoljan razlog za prekid ugovora.