SIGURNOSNA POLITIKA

INFORMACIJSKOG SUSTAVA VELEUČILIŠTA U RIJECI

studeni 2021.

Sukladno Odluci o prihvatljivom korištenju CARNet mreže (CDA0035), KLASA: 500-200/12/95, URBROJ: I10082-650-109-12-1 od 15. lipnja 2012. (verzija 4.0) i odredbi članka 41. Statuta Veleučilišta u Rijeci od 16. ožujka 2015., KLASA:003-05/15-01/07, URBROJ:2170-57-01-15-4 (Potpuni tekst od 31. listopada 2017.), dekan Veleučilišta u Rijeci, donosi

Sigurnosnu politiku

informacijskog sustava Veleučilišta u Rijeci

Opće odredbe

Članak 1.

Ovom politikom reguliraju se mjere sigurnosne zaštite informacijskog sustava Veleučilišta u Rijeci (u daljnjem tekstu: Veleučilište), organizacija upravljanja, način postupanja korisnika i davatelja usluga, način provođenja mjera, praktična primjena mjera, način postupanja, odgovornosti te mjere u slučaju nepridržavanja pravila.

Dokumenti u elektroničkom obliku smatraju se službenim dokumentima za koje treba osigurati čuvanje i pristup dopustiti samo ovlaštenim osobama.

Pojam sigurnosne politike i organizacije upravljanja sigurnošću

Članak 2.

Sigurnosna politika je skup svih mjera, pravila rada, postupanja i odgovornosti svakog pojedinca za uporabu računalne opreme na Veleučilištu.

Pojam pojedinca iz stavka 1. ovoga članka uključuje korisnike računalne opreme na Veleučilištu i davatelje informatičkih usluga Veleučilištu.

Obuhvat sigurnosne politike

Članak 3.

Pravila rada i ponašanja koja definira sigurnosna politika vrijede za:

- administratore informacijskih sustava,
- korisnike, u koje spadaju: radnici, vanjski suradnici, studenti, polaznici cjeloživotnog učenja i drugi
- vanjske tvrtke koje po ugovoru rade na održavanju opreme ili softvera

na svoj računalnoj opremi koja se nalazi u prostorima Veleučilišta i pripadajućim programima.

Korisnici informatičkih usluga

Članak 4.

Korisnici su osobe koje se u svom radu ili učenju služe računalima, proizvode dokumente ili unose podatke, ali nisu odgovorni za instalaciju i konfiguraciju softvera, niti za ispravan i neprekidan rad računala i mreže.

Svaki korisnik informacijskog sustava mora biti upoznat sa svojim pravima, dužnostima i obvezama te ulogom u poboljšanju sigurnosti ukupnog sustava i pridržavati se istih.

Upoznavanje u smislu stavka 2. ovoga članka vrši se neposredno (usmeno, pisano) te većem broju korisnika putem pisanih obavijesti, naputaka i pravila.

Članak 5.

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.

Korisnici koji unose podatke odgovorni su za njihovu vjerodostojnost.

Davatelji usluga osiguravaju automatsku pohranu (backup) važnih informacija, dok za vlastite podatke i dokumente korisnici sami izrađuju sigurnosne kopije i odgovorni su za iste.

Voditelj Odjeljka za informatičke poslove

Članak 6.

Voditelj Odjeljka za informatičke poslove dostavlja dekanu prijedlog Sigurnosne politike iz stavka 1. ovoga članka.

Voditelj Odjeljka za informatičke poslove odgovaran je za ispravnost podataka, za provjeru ispravnosti i sigurnosti aplikacije, za dodjelu dozvola za pristup podacima i za mjere sprječavanja izmjene podataka od neautoriziranih osoba.

Voditelj Odjeljka za informatičke poslove kontaktira proizvođača aplikacije i dogovara isporuku novih verzija, traži ugradnju sigurnosnih mehanizama i obavlja sve druge potrebne radnje i postupke.

Ako se ukaže potreba, dekan Veleučilišta može imenovati i zamjenike glavnih korisnika za pojedine aplikacije, na prijedlog Voditelja informatičko tehničke službe.

Davatelji informatičkih usluga

Članak 7.

Davateljima usluga u smislu ove politike smatraju se zaposlenici u Odjeljku za informatičke poslove koji brinu o radu računala, mreže, informacijskih sustava te su zaduženi za osiguranje neprekidnosti rada sustava.

Specijalisti za sigurnost

Članak 8.

Veleučilište će, ukoliko okolnosti nalažu, pri rješavanju sigurnosnih incidenata koristiti pomoć CARNeta.

Članak 9.

Voditelj Odjeljka za informatičke poslove dužan je brinuti se o ukupnoj sigurnosti informacijskih sustava.

Ukupna sigurnost informacijskih sustava uključuje i fizičku sigurnost sustava, pa će voditelj surađivati i sa svim ostalim radnicima.

Članak 10.

Obveze Voditelj Odjeljka za informatičke poslove vezane za sigurnost su:

- surađuje u pisanju provedbenih akata,
- nadziranje rada mreže i servisa,
- predlaže obrazovanje korisnika i administratora,
- komuniciranje s upravom,
- sudjelovanje u donošenju odluka o nabavi računala i softvera, te
- sudjelovanje u razvoju softvera, kako bi osigurao da se poštuju pravila iz sigurnosne politike.

Članak 11.

Voditelj Odjeljka za informatičke poslove razradit će procedure za postupanje u incidentnim situacijama, te izvršiti istragu i što prije vratiti informacijski sustav u redovno stanje.

Veleučilište će izraditi i održavati kontakt listu s imenima, brojevima telefona, e-mail adresama osoba kojima se prijavljuju incidenti: kvarovi opreme, sporost ili nedostupnost mrežnih usluga i podataka, povreda pravila sigurnosne politike ili zakonskih odredbi, na prijedlog Voditelja Odjeljka za informatičke poslove.

Administriranje računala

Članak 12.

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

Članak 13.

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.

Članak 14.

Administratori računala svakodnevno prate rad sustava, čitaju dnevničke zapise i provjeravaju rad servisa. Pored toga administratori nadgledaju i rad korisnika, kako bi otkrili i spriječili nedopuštene aktivnosti.

U slučajevima kad administrator(i) 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 Informatičko tehničke službe, 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, prijavljuje se CERT-u (Computer Emergency Response Team).

Članak 15.

Davatelji usluga dužni su u svome radu poštivati privatnost korisnika i povjerljivost informacija s kojima pri obavljanju posla dolaze u dodir. Na poštivanje tih pravila obvezuju se Veleučilištu potpisivanjem *Izjave o čuvanju povjerljivih informacija,* čiji je predložak dan kao prilog i sastavni dio ove politike.

Upravljanje mrežom

Članak 16.

Veleučilište će propisati i postupke za priključivanje računala u mrežu, odrediti obrasce kojima se izdaje odobrenje za priključenje računala na mrežu i dodjelu adrese na prijedlog Voditelja Odjeljka za informatičke poslove.

Voditelj Odjeljka za informatičke poslove zadužen za upravljanje mrežom mora u svakom trenutku imati točan popis svih mrežnih priključaka i umreženih uređaja, uključujući i prijenosna računala.

Članak 17.

U slučaju podržavanja rada na daljinu (primjerice: kada se radnicima dopušta da sa kućnog računala ažuriraju podatke) zbog mogućnosti da ga koriste neautorizirane osobe (članovi obitelji i slično), morat će se osigurati da udaljeno računalo ne ugrozi sigurnost mreže ustanove te povjerljivi podaci na udaljenom računalu moraju biti jednako sigurni kao da se računalo nalazi u zgradi ustanove.

Članak 18.

Veleučilište će razraditi pravila za spajanje na mrežu gostujućih računala, koja donose sa sobom vanjski suradnici, predavači, studenti, poslovni partneri, serviseri i dr.

Zbog opasnosti od širenja virusa ili namjernih nedopuštenih radnji (poput presretanja mrežnog prometa, prikupljanja informacija itd.) ne dozvoljava se da osobe iz prethodnog stavka, po svom nahođenju priključuju računala na mrežu Veleučilišta.

Veleučilište će odrediti mjesta gdje je dopušteno priključiti gostujuća računala, te konfiguracijom mreže spriječiti da se sa toga segmenta mreže dopre do ostalih računala u ustanovi.

Članak 19.

Dijelovi Veleučilišta koji koriste bežičnu mrežu, osigurani su od mogućnosti priključivanja na privatnu mrežu i snimanja prometa metodama enkripcije i autentifikacije uređaja i korisnika.

Radi zaštite povjerljivih informacija pri prijenosu mrežom, poželjno je da takav promet bude kriptiran.

Instalacija i licenciranje softvera

Članak 20.

Korištenje ilegalnog softvera predstavlja povredu autorskog prava i intelektualnog vlasništva.

Da bi se zaštitila povreda autorskog prava i intelektualnog vlasništva od moralne i materijalne štete koja time može nastati, Veleučilište zadužuje Voditelja Odjeljka za informatičke poslove 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.

Sve korisnike treba obavezati na poštivanje autorskih prava, između ostalog i potpisivanjem izjave o tome da su upoznati s ***Politikom prihvatljivog korištenja*** i da će je se pridržavati. Na taj način Veleučilište odgovornost za eventualno kršenje zakona prebacuje na nesavjesnog korisnika.

Video nadzor

Članak 21.

U vezi sa legitimnim interesom Veleučilišta da zaštiti imovinu i prostore, Veleučilište može koristiti videonadzor.

Fizička sigurnost

Članak 22.

Prostor u Veleučilištu dijeli se na dio koji je otvoren za javnost, prostor u koji imaju pristup samo radnici, te prostore u koje pristup imaju samo grupe radnika, ovisno o vrsti posla koji obavljaju.

Veleučilište će sastaviti popis osoba koje imaju pristup u zaštićene prostore, a domar mora imati popis osoba koje mogu dobiti ključeve određenih prostorija.

Sigurne zone

Članak 23.

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.

Veleučilište je dužno održavati popis ovlaštenih osoba koje imaju pristup u sigurne zone.

U smislu iz stavka 2. isključivo su radnici koji administriraju mrežnu, komunikacijsku opremu i poslužitelje ključnih servisa. Oni ulaze u sigurne zone samo kada treba ukloniti zastoje, obaviti servisiranje opreme, te se istima treba osigurati radni prostor odvojeno od prostorija u kojima je smještena oprema koja sadrži najvažnije informacije.

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.

Veleučilište će 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

Članak 24.

Povremeno se osobama iz vanjskih poduzeća ili ustanova, odnosno iz ostalih pravnih osoba, uključujući ovlaštene osobe iz ministarstva, županije, različitih inspekcijskih nadzora, serviserima i sl. mora dopustiti pristup opremi, radi servisiranja, održavanja, podrške, obuke, zajedničkog poslovanja, konzultacija itd.

Veleučilište 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.

Članak 25.

Ukoliko se vanjskoj pravnoj osobi prepušta održavanje opreme i aplikacija s povjerljivim podacima, Veleučilište može od te pravne osobe zatražiti popis osoba koje će dolaziti u prostorije Veleučilišta radi obavljanja posla. U slučaju zamjene izvršitelja, vanjska pravna osoba dužna je na vrijeme obavijestiti Veleučilište.

Veleučilište zadržava diskrecijsko pravo da osobama koje se predstavljaju kao radnici vanjskih pravnih osoba uskrati pristup u svoje prostorije, ukoliko nisu na popisu ovlaštenih radnika dostavljenom Veleučilištu.

Sigurnost opreme i klasifikacija računalne opreme

Članak 26.

Veleučilište dijeli svu opremu u grupe prema zadaćama:

- Zona javnih servisa (tzv. demilitarizirana zona) - oprema koja obavlja javne servise (DNS poslužitelj, HTTP poslužitelj, poslužitelj elektroničke pošte itd.).
- Intranet je privatna mreža Veleučilišta, sačinjavaju je poslužitelji internih servisa, osobna računala zaposlenih, te komunikacijska oprema lokalne mreže.
- Extranet je proširenje privatne mreže otvoreno mobilnim korisnicima, poslovnim partnerima ili povezivanje izdvojenih lokacija. U ovu grupu se ubrajaju veze lokalnih baza podataka s centralnim poslužiteljima, interni modemski ulazi, VPN i sl.
- Wi-Fi- mreža otvorena je za djelatnike i studente uz nadzor isključivo administratora i osoba za održavanje opreme.

Podjela opreme prema vlasništvu

Članak 27.

U prostorijama Veleučilišta može se nalaziti i oprema drugih ustanova kao npr. Ministarstva obrazovanja, sindikata ili hot spotovi ISP-a (Internet Service provider).

Veleučilište je obavezno održavati popis sve računalne opreme, s opisom ugrađenih komponenti, inventarnim brojevima i slično.

Veleučilište jednako brine o svoj opremi kojom raspolaže, bez obzira na to tko je njezin vlasnik.

Sva oprema se čuva od oštećenja i otuđenja.

Odgovornost za računalnu opremu

Članak 28.

Za fizičku sigurnost opreme odgovoran je dekan Veleučilišta.

Odgovornost dekana iz prethodnog stavka za grupe uređaja ili pojedine uređaje može se prenijeti na druge radnike, koji pri tome potpisuju dokument kojim potvrđuju da su preuzeli

opremu.

Veleučilište je dužno razraditi procedure kojima se nastoji spriječiti otuđenje i oštećenje računalne opreme.

Osiguranje neprekidnosti poslovanja

Članak 29.

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 softvera. 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 radnike za izradu i čuvanje kopija informacija, te ih obavezati na čuvanje povjerljivosti informacija.

Radi osiguranja neprekinutosti poslovanja, potrebno je razraditi i procedure za oporavak kritičnih sustava. Čuva ih se u pisanom obliku, kako bi se u slučaju nesreće, a kada je došlo do zamjene izvršitelja novozaposlenim radnikom, moglo brzo reagirati.

Povremeno se provjerava upotrebljivost rezervnih kopija podataka, te izvode vježbe oporavka sustava.

Vježbe iz prethodnog stavka ne izvode se na produkcijskim računalima, već na rezervnoj opremi (koju bi trebalo osigurati radnicima zaduženim za te poslove), u laboratorijskim uvjetima.

Nadzor nad informacijskim sustavima

Članak 30.

Veleučilište zadržava pravo nadzora nad instaliranim softverom 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, te
- provjere da li su informacijski sustavi i njihovo korištenje usklađeni sa zahtjevima sigurnosne politike.

Članak 31.

Nadzor nad informacijskim sustavom smiju obavljati samo osobe koje je Veleučilište za to ovlastilo.

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

Članak 32.

Odredbe ove politike odnose se na svu računalnu opremu koja se nalazi u prostorijama Veleučilišta, posebno na onu koja je priključena na mrežu CARNet, na sav instalirani softver, te na sve mrežne servise.

Ovu politiku su dužni poštivati i provoditi svi radnici, studenti, polaznici cjeloživotnog učenja i vanjski suradnici koji po ugovoru obavljaju određene poslove.

Provođenje

Članak 33.

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.

Navedeno u stavku 1. ovoga članka, vrijedi i za administratore računala i pojedinih servisa, koji su dužni specijalistima za sigurnost pomagati pri istrazi.

Članak 34.

Pristup iz članka 33. ove politike 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 Veleučilišta, ili oprema Veleučilišta služi za njezin prijenos,
- pristup radnom prostoru (uredu, laboratoriju, sigurnoj zoni itd.),
- pravo na interaktivno nadgledanje i bilježenje prometa na mreži Veleučilišta.

Nepridržavanje

Članak 35.

Radnika koji se ogluši na pravila o nadzoru može se stegovno kazniti sukladno općim aktima Veleučilišta, ili mu se mogu uskratiti prava korištenja mreže i njezinih servisa.

Praktična primjena sigurnosne politike

Članak 36.

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 Veleučilištu, 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.

Veleučilište u svakom trenutku treba imati ažurirani popis softvera koji se koristi u LAN-u, kako bi mogla brinuti o licenciranju.

U svrhu iz prethodnih stavaka ovih članaka, potrebno je organizirati stručni tim koji će izvršiti detaljan popis sve informatičke opreme, softvera, podataka i mrežnih instalacija.

Prateći dokumenti

Članak 37.

S nabavom nove informatičke opreme i razvojem informacijskih sustava u Veleučilištu, kao i s porastom ovisnosti o njihovom ispravnom funkcioniranju, javlja se potreba da se sigurnosna politika dopuni pratećim dokumentima, u kojima se definiraju pravila za pojedina područja rada.

Prateći dokumenti su razna pravila, pravilnici, upute i/ili naputci za rješavanje konkretnih problema i mogu se češće mijenjati.

Prateći dokumenti sastavni su dio sigurnosne politike Veleučilišta.

Članak 38.

Prilog i sastavni dio ove Sigurnosne politike su:

1. Pravila o rukovanju zaporkama
2. Pravila o korištenju elektroničke pošte
3. Pravila o antivirusnoj zaštiti
4. Pravila o zaštiti od sparna
5. Pravila o zaštiti od *špijunskih* i *nametnik* programa
6. Pravila o izradi kopija podataka
7. Pravila o rješavanju sigurnosnih incidenata
8. Pravila o rukovanju povjerljivim informacijama
9. Pravila o korištenju javnih računala
10. Pravila o dodjeljivanju AAI@Edu.hr elektroničkih identiteta

Prijelazne i završne odredbe

Članak 39.

Tumačenje odredbi ove politike daje dekan Veleučilišta u Rijeci.

Članak 40.

U slučaju izmjene pojedinih zakonskih propisa i podzakonskih akata, u svezi s dotičnom materijom, neposredno će se primjenjivati nove zakonske odredbe, bez obzira da li je došlo do izmjene ove politike.

Članak 41.

Ova Sigurnosna politika informacijskog sustava Veleučilišta u Rijeci stupa na snagu dan nakon dana objave na oglasnoj ploči Veleučilišta.

KLASA: 650-03/21-01/01
URBROJ: 2170-57-01-21-2
Rijeka, 02. studenoga 2021.

Veleučilište u Rijeci
Dekan:

dr. sc. Saša Hirnig, prof. v. š.

Sigurnosna politika informacijskih sustava Veleučilišta u Rijeci objavljena je na oglasnoj ploči u sjedištu Veleučilišta u Rijeci dana 03. studenoga 2021., a stupila je na snagu 04. studenoga 2021.

Veleučilište u Rijeci
Rukovoditelj odjela u područnoj službi: tajnik

Đurđica Pajalić Karajković, mag. iur.

Pravila o rukovanju zaporkama

Svrha

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 probio obrambenu liniju i otvorio prolaz za napade na važnije sustave i informacije. Lanac puca na najslabijoj karici. 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 korisnici (radnici, suradnici i članovi, studenti) Veleučilišta 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 (8) znakova od kojih je minimalno dva (2) broja, preporučuje se korištenje još dužih zaporki i specijalnih znakova.

2. Riječi iz rječnika

Ne koristiti ih, 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. Neki korisnici naizmjence koriste dvije standardne zaporke, lako su dvije zaporke bolje nego jedna, ipak se ovakvim trikovima izigrava osnovna svrha promjene zaporki. Preporuka je mijenjati zaporku barem jednom godišnje.

6. Tajnost zaporke

Korisnici su odgovorni za svoju zaporku i ni u kom je slučaju ne smiju otkriti, čak ni administratorima sustava. **Administrator sustava NIKADA neće tražiti korisnikovu zaporku. 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. Ukoliko korisnik zaboravi zaporku, administrator će mu omogućiti da unese novu.

Korisnik ne smije zloupotrebljavati mogućnosti da mu se od strane administratora unese nove zaporka, nego je dužan voditi računa o sigurnosti dodijeljene zaporke!

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.

Prilikom provjere sustava, sigurnosni tim može ispitati jesu li korisničke zaporke u skladu s navedenim pravilima.

Nepridržavanje

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

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

Pravila o korištenju elektroničke pošte

Elektronička pošta dio je svakodnevne komunikacije, poslovne i privatne. S obzirom na moguće posljedice treba razmotriti sve aspekte elektroničke komunikacije.

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

Problemi koji mogu nastati 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. U ovome uvelike može pomoći administrator sustava konfigurirajući e-mail poslužitelj da koristi kriptirane protokole.

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 (Odgovori) pritisne Reply All (Odgovori svima), poruka će umjesto jednom primatelju otići na više adresa, a povjerljive informacije dospjeti do neželjenih primatelja.
- Česta je pogreška i preuzimanje pogrešne adrese iz adresara.
- Neki mail klijenti sami dovršavaju e-mail adresu koju tipkate. U žurbi se može prihvatiti pogrešna adresa, slična onoj koju zapravo želite.

3. **Nesporazumi**

- Ljudi su skloni pisati e-mail poruke 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 e-mail adresi nalazi se ime ustanove. Pišući, budite svjesni da netko može shvatiti vašu privatnu prepisku kao službeni dopis, vaše privatno mišljenje kao službeni stav ustanove. Stoga u raspravi uvijek jasno naznačite kada je izneseni stav vaše privatno uvjerenje.

4. **Otkrivanje informacija**

- Poruke namijenjene jednoj osobi, začas se mogu proslijediti drugima, npr. na mailing listu. To se može dogoditi:
    - (zlo)namjerno, s ciljem da se naškodi drugoj osobi ili tvrtki,
    - nemarom sudionika, koji ne traži dozvolu za prosljeđivanje poruke,
    - slučajnom omaškom, na primjer nehotičnim klikom mišem na pogrešnu ikonu - Reply All (Odgovori svima) umjesto Reply (Odgovori).
- Stoga poslovne dopise koji sadrže osjetljive informacije treba označiti kao povjerljive, kako bismo primatelja obavezali na diskreciju.
- U slučaju sigurnosnog incidenta, istraga može dovesti do otkrivanja sadržaja poruka koje su zamišljene kao privatna komunikacija. Veleučilište se obavezuje čuvati povjerljivost takvih poruka, ali to neće moći garantirati budu li poruke tretirane kao dokazni materijal u istrazi ili u mogućem sudskom procesu.

5. **Radna etika**

- Veliki broj poruka koje treba svakodnevno pročitati može vam oduzeti znatan dio radnog vremena. Stoga ograničite broj privatnih 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).*
- Spam, slanje neželjenih komercijalnih poruka, sve više opterećuje promet na Internetu, te oduzima vrijeme, čak i ako brišete takve poruka bez čitanja. Veleučilište će filtrirati spam na poslužitelju elektroničke pošte. Obaveza je 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 Veleučilište.

Zbog svega nabrojanog korištenje elektroničke pošte smatra se rizičnom djelatnošću, te su korisnici obvezni pridržavati se sljedećih pravila:

- Radnicima se otvara korisnički račun radi obavljanja posla.
- Privatne poruke dozvoljene su u umjerenoj količini, ukoliko to ne ometa redoviti rad.

- Pišući poruke, budite svjesni da ne predstavljate samo sebe, već i ustanovu za koju radite.
- Pridržavajte se 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 (osim službenih mail lista).
- 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 sadrži virus, neće biti isporučena.
- Veleučilište 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.
- Protokol elektroničke pošte nije zamišljen za slanje velikih količina podataka, stoga priloge treba slati umjereno, provjeriti mogućnosti za smanjivanje ili kompresiju priloga, a ukoliko je zaista potrebno poslati veliku količinu podataka, za to se predlažu drugi servisi poput dijeljenja privitaka putem Office 365 sustava u oblaku (cloud) i slični.

Procedura za dodjelu e-mail adrese

Pri zapošljavanju novog radnika, rukovoditelj zatraži od administratora poslužitelja elektroničke pošte otvaranje korisničkog računa uz prethodno pridržavanje procesne procedure.

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

Studenti imaju pravo besplatnog korištenja e-maila za vrijeme trajanja studija. Studentima se e-mail korisnički račun otvara automatskom procedurom. Nakon odlaska s Veleučilišta, njihov se korisnički račun zatvara.

Na koga se odnose pravila korištenja e-maila

Pravila za korištenje e-maila odnose se na sve zaposlene, vanjske suradnike i studente koji imaju otvoren korisnički račun na poslužitelju Veleučilišta.

Nepridržavanje

Protiv korisnika koji ne poštuju ova pravila Veleučilište može pokrenuti postupak za povrede obveza iz radnog odnosa ili u svezi s radnim odnosom. U slučaju ponovljenih težih prekršaja, korisniku se može zatvoriti korisnički račun i uskratiti pravo korištenja servisa elektroničke pošte.

Pravila o antivirusnoj zaštiti

Svrha

Virusi i crvi predstavljaju opasnost za informacijske sustave jer ugrožavaju funkcioniranje mreže i povjerljivost podataka.

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

Stoga je zaštita od virusa obaveza Veleučilišta, administratora računala i svakog korisnika.

Pravila

Veleučilište 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.

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

Nepridržavanje

Za korisnika koji samovoljno isključi protuvirusnu zaštitu na svom računalu, te na taj način izazove štetu, bit će pokrenut postupak za povrede obveza iz radnog odnosa ili u svezi s radnim odnosom i te biti isključen sa mreže na određeni period.

Pravila o zaštiti od *spama*

Svrha

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

Dio neželjenih poruka nastoji uvući primatelja u kriminalne aktivnosti, na primjer otvaranje računa za pranje novca, nastoje pobuditi samilost kako bi se izvukao novac (eng. hoax).

Pravila za administratore

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.

Pravila za korisnike

Korisnici 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 Veleučilištu.

Nepridržavanje

Protiv korisnika koji se ne pridržavaju pravila prihvatljivog korištenja i šalju masovne neželjene poruke biti će pokrenut postupak za povrede obveza iz radnog odnosa ili u svezi s radnim odnosom.

Pravila o zaštiti od špijunskih i nametnik programa (spyware)

Svrha

Internetom se širi sve više neželjenih, skrivenih, tzv. špijunskih programa (spyware) koji mogu biti veoma opasni. To su programi koji se često instaliraju na računalo bez znanja korisnika te na računalu čine razne, štetne radnje. Posljedice mogu biti: usporeni rad računala, promijenjena početna web stranica, neprekidna aktivnost na Internetu bez obzira što je modem isključen, otvaranje drugog prozora iz čista mira,... Najčešće dolaze potiho uz neki besplatan software.

Pravila za administratore

Administratori osobnih računala dužni su na računalo instalirati odgovarajući *anti špijunski* program koji omogućava uklanjanje špijunskih programa s računala. Program je potrebno konfigurirati tako da ga može pokrenuti i tzv. obični korisnik računala.

Pravila za korisnike

Ako instaliraju besplatni softvere, korisnici su dužni obratiti pozornost da uz njega ne instaliraju i neki od skrivenih programa.

Korisnici su dužni povremeno pokrenuti *anti špijunski* program kako bi uklonili ove maliciozne programe.

Nepridržavanje

Korisnici su dužni obratiti pozornost da na računalo ne instaliraju skriveni programi, a protiv onih koji namjerno instaliraju špijunske programe bit će pokrenut postupak za povrede obveza iz radnog odnosa ili u svezi s radnim odnosom.

Pravila o izradi kopija podataka

Voditelj Odjeljka za informatičke poslove u dogovoru sa sistem inženjerom, određuje tko je od radnika zadužen za izradu kopija pojedine vrste podataka. Veću pozornost treba obratiti na spremanje važnijih podataka (baza podataka, mail, web...).

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

Osnovna strategija izrade kopija:

- Kopije podataka iz baze podataka glavnog servera se izrađuje svakodnevno, na drugoj particiji diska.
- Također, više puta godišnje radi se potpuni backup. Za navedeno zadužen je sistem inženjer ili osoba kojoj on povjeri obavljanje tog zadatka.
- Kopija podataka ključnih servisa (mail, web...), kao i osobnih podataka sa poslužitelja se izrađuju s većom učestalošću.
- Kopije podataka sa osobnih računala se izrađuje prema potrebi.

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

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

.

Pravila o rješavanju sigurnosnih incidenata

Svrha

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

Prijava incidenta

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

Veleučilište 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 web stranicama.

Svaki sigurnosni incident se dokumentira na odgovarajući način.

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 sprečavanja, ali isto tako i kao dokazni materijal u eventualnim stegovnim ili sudskim procesima.

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

Procedure za rješavanje incidenata

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

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, CD...), 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.

- U 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.

Veleučilište može objavljivati statističke podatke o sigurnosnim incidentima, bez otkrivanja povjerljivih i osobnih informacija.

Sankcije

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

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

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

Pravila o rukovanju povjerljivim informacijama

Klasifikacija informacija

Klasificiranje povjerljivih informacija uređeno je Zakonom za zaštiti tajnosti podataka – glave 8. i 9. (NN br. 108/96), Zakonom o tajnosti podataka (NN br. 79/07, 86/12), Uredbom (EU) 2016/679 o zaštiti pojedinaca u vezi s obradom podatka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ te Zakonom o provedbi Opće uredbe o zaštiti podataka (NN 42/18).

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

Prema stupnju tajnosti, informacije mogu biti povjerljive, tajne ili vrlo tajne. Kategorije službene, državne i vojne tajne pripadaju tijelima državne uprave.

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

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

Dokumenti koji ulaze u Veleučilište s nekom od oznaka povjerljivosti određuju stupanj povjerljivosti svih dokumenata i informacija koje će Veleučilište proizvesti kao odgovor. U tom slučaju može se koristiti neka od kategorija tajnosti koje su rezervirane za tijela državne uprave.

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

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

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

Raspodjela odgovornosti

Za klasificiranje povjerljivih informacija zadužen je dekan Veleučilišta, 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 radnike Veleučilišta i vanjske suradnike koji dolaze u doticaj s osjetljivim podacima. Obaveza čuvanja povjerljivosti ne prestaje s prestankom radnog odnosa.

Čuvanje povjerljivih informacija

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

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

Informacije o radnicima

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

Veleučilište može informacije o zaposlenima koje se smatraju javnima objaviti na svojim web stranicama u skladu sa GDPR uredbom. Javnim informacijama smatraju se:

- ime i prezime
- posao koji radnik obavlja
- broj telefona na poslu
- službena e-mail adresa
- lokacija, odnosno kabinet ili soba u kojoj radnik obavlja posao.

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

Povjerljive informacije u načelu se ne daju putem telefona 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 radnik Veleučilišta će se posavjetovati s upravom i ukoliko dobije odobrenje nazvati službenu osobu i odgovoriti na pitanja.

Prenošenje povjerljivih informacija

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

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

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

Kopiranje povjerljivih informacija

Za kopiranje povjerljivih informacija treba zatražiti dozvolu vlasnika informacije.

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

Dokumenti koji pripadaju Veleučilištu 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.

Uništavanje povjerljivih informacija

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

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

Ne pridržavanje

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

Protiv radnika koji ne poštuju pravila o čuvanju povjerljivih informacija bit će pokrenut postupak za povrede obveza iz radnog odnosa ili u svezi s radnim odnosom, 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. Stoga Veleučilište treba već u ugovor unijeti stavke po kojima je povreda povjerljivosti podataka dovoljan razlog za prekid ugovora.

Sastavni dio *Pravila o upravljanju povjerljivim informacijama* je / *Izjava o čuvanju povjerljivih informacija*

Pravila o korištenju javnih računala

Svrha

Veleučilište u Rijeci osiguralo je studentima određeni broj računala na kojima se može pristupiti na internet, raditi seminarske i druge radove te poslužiti se u neku drugu obrazovnu ili akademsku svrhu. Računala se nalaze u knjižnici ili računalnim kabinetima, kada nisu zauzeti nastavom.

Pravila

1. Pravo korištenja javnih računala imaju djelatnici i studenti Veleučilišta (u daljnjem tekstu: korisnici).

2. Javna računala trebaju se koristiti savjesno i pažljivo, kako bi se osigurala njihova ispravnost, a time i mogućnost korištenja. S obzirom na ograničena sredstva, Veleučilište nije u mogućnosti svako malo kupovati nova računala. Zabranjuje se korisnicima da narušavaju fizički integritet računala na bilo koji način (lupanje, udaranje, trganje kablova, itd.). Također, zabranjuje se korisnicima da samovoljno premještaju pojedine periferne uređaje (tipkovnice, miševe, monitore, itd.) ili da samovoljno vrše „popravak“ neispravnih računala. Ukoliko neko računalo (ili neki njegov dio) ne radi ispravno, korisnici su dužni to prijaviti administratoru.

3. Korisnici su dužni pridržavati se etičkih i moralnih pravila prilikom korištenja javnih računala, kao i važećih zakona. Zabranjuje se pristup pornografskim, pedofilskim i sličnim sadržajima na internetu; zabranjuje se korištenje i širenje takvih materijala na javnim računalima. Zabranjuje se nelegalno preuzimanje (download), korištenje i širenje zakonom zaštićenih materijala – softwarea, glazbe, e-knjiga, e-časopisa, dokumenata, filmova, itd. Zabranjuje se postavljanje, pokretanje i širenje malicioznih programa, kodova, virusa, trojanaca, spywarea, malwarea, spama, itd.

4. Zbog velikog negativnog utjecaja na throughput, brzinu i performanse pristupa internetu, te zbog nekoliko slučajeva zlouporabe, ograničava se korištenje bittorent ili sličnih P2P protokola.

Nepridržavanje

Protiv korisnika koji ne poštuju ova pravila, Veleri može pokrenuti postupak za povrede obveza iz radnog odnosa ili u svezi s radnim odnosom. U slučaju ponovljenih težih prekršaja, korisniku se može uskratiti pravo korištenja javnih računala na Veleučilištu, kao i naplatiti eventualna učinjena šteta.

Pravila o dodjeljivanju AAI@Edu.hr elektroničkih identiteta

Što je elektronički identitet?

Elektronički identitet je skup podataka o pojedincu, koji se koristi za potrebe autentikacije (provjere identiteta) i autorizacije (provjere prava pristupa) nekom resursu (npr. web stranici, aplikaciji, računalnoj mreži, sustavu, itd.).

Elektronički identitet je skup podataka o pojedincu čije su sastavnice (atributi):

- ime i prezime
- brojčani identifikator osobe (JMBG, OIB)
- korisnička oznaka
- identifikator korisnika u ustanovi
- zaporka
- elektronička adresa
- poštanska adresa
- naziv i oznaka matične ustanove
- itd.

AAI@Edu.hr

AAI@EduHr je autentikacijska i autorizacijska infrastruktura sustava znanosti i visokog obrazovanja u Republici Hrvatskoj. Sustav AAI@EduHr tehnički je realiziran uporabom distribuiranih LDAP imenika. Svaka matična ustanova iz sustava MZO ima vlastiti LDAP imenik u kojemu su pohranjeni elektronički identiteti korisnika iz te ustanove.

Sustav AAI@EduHR korisnicima (pojedincima) nudi jednostavno, sigurno i pouzdano korištenje svih resursa u sustavu AAI@EduHr uz pomoć jedinstvenog elektroničkog identiteta dobivenog na matičnoj ustanovi.

AAI@Edu.hr e-identitet

Elektronički identitet u sustavu AAI@EduHr je virtualni identitet na CARNet mreži kojega dobivaju pojedinačni korisnici iz ustanova članica CARNeta (učenici, nastavnici, studenti, profesori) i koji im omogućuje korištenje CARNetovih usluga.

Elektronički identitet služi pri autentikaciji i autorizaciji za razne CARNetove usluge, te je nužan za ostvarivanje prava na CARNetove usluge.

Oblik: korisnik@ustanova.hr

Dodjeljivanje e-identiteta

Elektronički identitet otvaraju nadležne matične ustanove i to ovisno o statusu osobe koja traži otvaranje elektroničkog identiteta.

Sve škole članice CARNeta imaju svog administratora imenika zaduženog za otvaranje elektroničkih identiteta u HUSO (Hosting usluga za srednje i osnovne škole) sustavu svim učenicima i nastavnicima.

Elektronički identitet u sustavu AAI@EduHr mogu dobiti pripadnici akademske i istraživačke zajednice u RH i to isključivo u nadležnoj matičnoj ustanovi. Pojedinci čija matična ustanova nije u sustavu AAI@EduHr mogu dobiti elektronički identitet na Javnom poslužitelju CARNeta (public.carnet.hr) slanjem pristupnice u CARNet.

Dodjeljivanje AAI@Edu.hr e-identiteta na Veleučilištu u Rijeci

Dodjeljivanje AAI@Edu.hr e-identiteta vrši administrator.

Studentima se e-indetiteti dodjeljuju automatski preko ISVU sustava prilikom upisa na studij i ostaju otvoreni sve do odlaska s ustanove, bilo završetkom ili prekidom studija. Regulacija i produživanje trajanja e-identiteta vrši se redovito jednom godišnje, a također i vanredno u određenim prilikama.

Profesorima, nastavnicima i asistentima se e-indetiteti dodjeljuju prilikom zapošljavanja i ostaju otvoreni sve do odlaska s ustanove, bilo završetkom radnog odnosa ili nekim drugim razlogom. Regulacija i produživanje trajanja e-identiteta vrši se redovito jednom godišnje, a također i vanredno u određenim prilikama.

Ostalim djelatnicima ustanove se e-identiteti dodjeljuju ili na osobni zahtjev ili ukoliko je za vršenje službe nužno posjedovanje e-identiteta, i ostaju otvoreni sve do odlaska s ustanove, bilo završetkom radnog odnosa ili nekim drugim razlogom. Regulacija i produživanje trajanja e-identiteta vrši se redovito jednom godišnje, a također i vanredno u određenim prilikama.