POLITIKA SIGURNOSTI INFORMACIJSKOG SUSTAVA

PAN-PEK

Na temelju odluke Direktora na sjednici održanoj dana 05.02.2018. godine, donosi se sljedeći dokument:

POLITIKA SIGURNOSTI INFORMACIJSKOG SUSTAVA

A) Naziv politike: Politika sigurnosti informacijskog sustava
B) Datum usvajanja: 05.02.2018.
C) Pregled odgovornosti (RACI):

	Direktor	Službenik za zaštitu podataka	Administrator informacijskog sustava	Zaposlenici Društva
Iniciranje izrade	I	I, C, R	R, A	
Izrada		I, C	R, A	
Revizija		I, C	R, A	
Odobravanje	A	I	I	I

R – Provedba/Izvršenje zadatka (Responsible);
A – Donošenje odluke/Snošenje odgovornosti (Accountable);
C –Savjetodavna funkcija (Consulted);
I – Obavještavanje o aktivnosti (Informed);

D) Evidencija promjena:

Datum revizije	Oznaka verzije	Kratki opis izmjena i dopuna pravilnika
05.02.2018	V1.0	Inicijalni dokument

SADRŽAJ

I OPĆE ODREDBE

1.1 CILJEVI POLITIKE SIGURNOSTI INFORMACIJSKOG SUSTAVA

Članak 1.

Ovom Politikom sigurnosti informacijskog sustava (dalje: Politika sigurnosti) definiraju se ciljevi, temeljna načela, odgovornosti i pravila prihvatljivog ponašanja djelatnika Pan-pek d.o.o. (dalje u nastavku Društvo) koja se moraju provoditi u cilju očuvanja povjerljivosti, dostupnosti i cjelovitosti podataka i informacijskih servisa.

Članak 3.

Detaljna razrada i opis pojedinih odredbi ove Politike može biti predmet posebnih internih akata kao što su pravilnici, procedure i radne upute.

1.2 OBUHVAT POLITIKE SIGURNOSTI INFORMACIJSKOG SUSTAVA

Članak 3.

Odredbe Politike sigurnosti se primjenjuju nad svim resursima informacijskog sustava Društva, uključujući, među ostalim, podatke, računalne komponente, uređaje kojima se ostvaruje mobilna komunikacija, fizičke resurse koji su u funkciji rada informacijskog sustava, te organizacijske i operativne procese koje su vezane na rad informacijskog sustava.

2 PROCES SIGURNOSTI INFORMACIJSKOG SUSTAVA

2.1 CILJEVI

Članak 4.

Mjere za očuvanje povjerljivosti, dostupnosti i cjelovitosti moraju se provoditi u okviru unaprijed definiranog procesa, u kojem su jasno definirane nadležnosti i odgovornosti svih osoba koje sudjeluju u provedbi ovih mjera.

Rukovodstvo Društva definira glavne ciljeve mjera informacijske sigurnosti, podupire njihovu provedbu unutar svih poslovnih procesa Društva te nadzire uspješnost njihove realizacije.

Odluka o provedbi pojedinih mjera informacijske sigurnosti temelji se na visini rizika od nastupanja neprihvatljivih događaja na koje se pojedine mjere odnose.

2.2 NADLEŽNOSTI I ODGOVORNOSTI

Članak 5.

Svaki djelatnik Društva koji koristi neki od resursa informacijskog sustava sudjeluje u procesu sigurnosti informacijskog sustava kroz jednu od sljedećih uloga:

- Voditelj sigurnosti informacijskog sustava: osoba koju imenuje Rukovodstvo Društva a koje, među ostalim, definira mjere sigurnosti informacijskog sustava, daje inicijativu za njihovu provedbu ili ih provodi neposredno, te nadzire rad procesa sigurnosti informacijskog sustava. U Društvu Voditelj sigurnosti informacijskog sustava je i Direktor Sektora IKT-a.

- Davatelji informatičkih usluga: djelatnici Sektora IKT koji se skrbe o resursima informacijskog sustava, omogućuju dostupnost podataka i informacijskih servisa korisnicima informatičkih usluga, provode neposredne mjere njihove zaštite, te sudjeluju u razvoju programske podrške;
- Vlasnici podataka: rukovoditelj poslovnog procesa odgovoran za vjerodostojnost poslovnih podataka koji nastaju unutar poslovnog procesa za koji je nadležan, te za ispravnost korištenja pojedinih aplikativnih sustava unutar istog poslovnog procesa;
- Korisnici informatičkih usluga: su svi zaposlenici Društva, sve osobe koje privremeno obavljaju poslove prema ugovoru, te svi vanjski suradnici ili partneri koji dolaze u doticaj s resursima informacijskog sustava Društva.

2.3 UPRAVLJANJE INFORMACIJSKIM RIZICIMA

Članak 6.

Odluka o provedbi mjera zaštite informacijskog sustava donosi se na temelju procjene razine pojedinih prijetnji i težine prisutnih ranjivosti, a u ovisnosti od potencijalnih posljedica za poslovni proces Društva koje bi mogle nastati realizacijom ovih prijetnji.

Postupak definiran prethodnim stavkom naziva se upravljanje informacijskim rizicima, a procjena informacijskih rizika je dio ovog postupka kojim je obuhvaćena analiza prijetnji, ranjivosti i potencijalnih posljedica

2.4 ODLUČIVANJE O ODGOVARANJU NA RIZIKE

Članak 7.

Na temelju rezultata postupka procjene informacijskih rizika, rukovodstvo Društva donosi odluku o izbjegavanju, reduciranju, eliminiranju, prijenosu ili prihvaćanju utvrđenih rizika.

Uz suglasnost rukovodstva Društva, odluka o odgovaranju na rizike može se donijeti i na nižoj upravljačkoj razini.

3 PRISTUP INFORMACIJSKIM SUSTAVIMA

3.1 CILJEVI

Članak 8.

Pristup informacijskom sustavu mora biti uređen na način da korisnik informatičkih usluga ima pristup samo do onih resursa koji su neophodni za obavljanje funkcija iz djelokruga njegovog rada. Nadalje, ovlasti za korištenje informacijskog sustava moraju biti dodijeljene na način kojim će se onemogućiti potpuna ovlast ili utjecaj pojedinog korisnika nad cjelokupnim poslovnim procesom.

Registracija korisnika i otvaranje korisničkih računa korisnicima moraju biti formalno provedeni.

3.2 ODOBRENJE ZA DODJELU PRAVA PRISTUPA

Članak 9.

Pravo pristupa informacijama, informatičkim servisima i aplikacijama informacijskog sustava Društva dodjeljuje se korisnicima isključivo na temelju odobrenja nadležnog rukovoditelja i uz suglasnost vlasnika podataka.

Pristup korisniku će biti odobren tek nakon davanja pismene izjave o prihvaćanju odredbi Politike sigurnosti informacijskog sustava ili drugih internih akata kojima se uređuje upotreba informatički usluga i podataka.

3.3 IDENTIFIKACIJA I AUTENTIFIKACIJA KORISNIKA

Članak 10.

Korisnicima informatičkih usluga otvaraju se korisnički računi kroz koje će biti jednoznačno identificirani, a na način na koji se nedvojbeno može utvrditi njihov identitet tijekom korištenja resursa informacijskog sustava.

Informatički resursi moraju biti izvedeni i konfigurirani na način kojim će se omogućiti pouzdana potvrda identiteta korisnika, minimalno primjenom sustava lozinki sa strogom razinom kompleksnosti, te uz njihovu periodičku promjenu. Korisnik informatičke usluge preuzima punu odgovornost za zaštitu lozinki ili drugih mjera koje se koriste za njihovu autentifikaciju, što obuhvaća, među ostalim i brigu o izboru kompleksnih lozinki te njihovu redovitu promjenu.

3.4 PRIVILEGIRANI KORISNIČKI RAČUNI

Članak 11.

Pristup funkcijama administracije i održavanje računalnih resursa mora biti proveden korištenjem privilegiranih korisničkih računa. Korisnici kojima su dodijeljeni privilegirani korisnički računi ne smiju ove račune koristiti za redovite poslovne aktivnosti.

Ukoliko su privilegirani korisnički računi zaštićeni lozinkom, njihova se vrijednost ne smije koristiti istovremeno u drugim korisničkim računima iste osobe.

3.5 KORIŠTENJE ZAJEDNIČKIH KORISNIČKIH RAČUNA

Članak 12.

Nije dopušteno koristiti isti korisnički račun unutar grupe korisnika.

Ukoliko odredbu iz prethodnog stavka nije moguće provesti uslijed opravdanih razloga, nadležni rukovoditelj mora voditi evidenciju o pristupu informatičkim resursima korištenjem zajedničkih računa.

3.6 UDALJENI PRISTUP

Članak 13.

Udaljeni pristup resursima informacijskog sustava je krajnje ograničen, a prava pristupa se dodjeljuju isključivo uz suglasnost rukovodstva Društva.

Tehnički resursi za udaljeni pristup moraju biti konfigurirani i zaštićeni uz uvažavanje osobito strogih zahtjeva zaštite.

4 OČUVANJE POVJERLJIVOSTI PODATAKA

4.1 CILJEVI

Članak 14.

Povjerljivost podataka koji se prikupljaju, pohranjuju, obrađuju ili prosljeđuju resursima informacijskog sustava Društva mora biti zaštićena sukladno značaju ovih podataka u poslovnom procesu.

Mjere zaštite računalnih sustava, računalne mreže i drugih dijelova informacijskog sustava koji sadrže **povjerljive** podatke, moraju biti zaštićeni sukladno razini povjerljivosti podataka koji se na pojedinom sustavu nalaze.

Svi korisnici informatičkih usluga moraju postupati s podacima sukladno razini povjerljivosti ovih podataka.

4.2 KLASIFIKACIJA PODATAKA

Članak 15.

Podaci koji se prikupljaju, pohranjuju, obrađuju ili prosljeđuju resursima informacijskog sustava Društva moraju se označiti jednim sljedećih klasifikacijskih razreda:

Strogo povjerljivo – najpovjerljiviji podaci iz poslovanja Društva čije neovlašteno otkrivanje može imati kritične posljedice za poslovanje Društva,

Povjerljivo – podaci iz redovitog poslovanja Društva, namijenjeni za korištenje u poslovnim procesima Društva,

Interno – manje osjetljiviji podaci iz poslovanja Društva,

Javno – podaci o poslovanju Društva dostupni za javnost.

Za svaki klasifikacijski razred potrebno je odrediti odgovarajuće sigurnosne mjere i upute za njihovu provedbu.

4.3 KORIŠTENJE POVJERLJIVIH PODATAKA

Članak 16.

Korisnici moraju biti upoznati sa klasifikacijskim razredom podataka kojima pristupaju ili koje koriste, te moraju poznavati sigurnosne mjere koje se odnose na pojedini klasifikacijski razred.

Sigurnosne mjere za podatke koji su klasificirani razredom „Strogo povjerljivo“ i „Povjerljivo“ uključuju, minimalno, sljedeće odredbe:

- ovi podaci se ne smiju slati elektroničkom poštom u nekriptiranom, tj. čitljivom obliku
- u slučaju da se pohranjuju na prijenosnim medijima koji se iznose iz Društva, ovi podaci moraju biti kriptirani
- u slučaju ispisa, kopiranja ili slanja faksom, potrebno je osigurati neposrednu prisutnost djelatnika uz dokumente s povjerljivim podacima.

4.4 PRISTUP POVJERLJIVIM PODACIMA

Članak 17.

Pristup podacima koji su klasificirani razredom „Strogo povjerljivo" određuju se neposrednim uključivanjem korisničkog računa ovlaštene osobe u pristupnu listu, dok se pristup podataka putem korisničkih grupa dozvoljava samo u iznimnim situacijama.

5 LJUDSKI RESURSI I INFORMACIJSKA SIGURNOST

5.1 CILJEVI

Članak 18.

Društvo provodi formalne mjere kroz koje će se osigurati primjena odredbi Politike sigurnosti informacijskog sustava i drugih internih akata koji proizlaze iz ove Politike od strane djelatnika Društva.

Djelatnici Društva moraju biti upoznati sa svim formalnim zahtjevima koji se odnose na pridržavanje odredbi Politike sigurnosti informacijskog sustava.

Djelatnici Društva moraju biti pravovremeno i redovito obavještavani o svim tehničkim i proceduralnim mjerama koje provode u svom radu.

5.2 IZJAVA KORISNIKA

Članak 19.

Svi djelatnici Društva prilikom zapošljavanja potpisuju izjavu o prihvaćanju odredbi Politike sigurnosti informacijskog sustava ili drugih internih akata kojima se uređuje upotreba informatički usluga i podataka.

Takva izjava sastavni je dio Ugovora o radu.

5.3 EDUKACIJA KORISNIKA

Članak 20.

Korisnici moraju biti obaviješteni o metodama zaštite i sigurnosnim mjerama iz svog djelokruga rada. Program obuke izobrazbe mora se provoditi redovito, te mora obuhvaćati sve nove i postojeće djelatnike i poslovodstvo Društva.

Korisnici su dužni upoznati se s dokumentacijom i uputama koje opisuju mjere zaštite informacijskog sustava. Nadležne osobe moraju ovu dokumentaciju učiniti dostupnom svim korisnicima.

5.4 OBAVJEŠTAVANJE O SIGURNOSNIM NEDOSTACIMA

Članak 21.

Korisnici moraju izvijestiti nadležne osobe o svakom nedostatku u sustavu računalne sigurnosti ili na računalnim resursima koje koriste u poslovnom procesu te o svakoj zloupotrebi ili kršenju pravila za provedbu mjera informacijske sigurnosti koje primijete u svom radu.

6 SIGURNOST RAČUNALNIH RESURSA

6.1 CILJEVI

Članak 22.

Nabava, konfiguracija, operativni rad i održavanje računalnih resursa (hardverski, softverski, mrežni i komunikacijski resursi) moraju uvažavati stroge sigurnosne zahtjeve, sukladno utvrđenoj visini rizika i drugim sigurnosnim zahtjevima.

Mjere zaštite moraju biti stručno planirane i provedene na temelju stručnih zahtjeva, a njihov sadržaj i opseg usklađen sa utvrđenom visinom rizika.

6.2 UVOĐENJE RAČUNALNIH RESURSA U PRODUKCIJSKI RAD

Članak 23.

Potrebno je provesti analiza sigurnosnih svojstava i testiranje svih novih hardverskih i softverskih računalnih resursa. U produkcijski rad se mogu uvesti samo oni resursi kojima nadležne osobe prethodno odobre produkcijski rad.

6.3 KONFIGURACIJA SIGURNOSNIH PARAMETARA

Članak 24.

Sukladno zahtjevima koji proizlaze iz procjene rizika ili vanjskih sigurnosnih zahtjeva, računalni resursi moraju biti konfigurirani u skladu sa sigurnosnim konfiguracijskim standardom, a na način kojim će se spriječiti ili otežati nastup sigurnosnih prijetnji.

Potrebno je održavati usklađenost parametara računalnih resursa sa sigurnosnim konfiguracijskim standardom tijekom životnog ciklusa računalnih resursa.

6.4 INVENTURNI POPIS RAČUNALNIH RESURSA

Članak 25.

Nadležne osobe moraju voditi inventurni popis računalnih resursa, a u svrhu učinkovitog upravljanja operativnim zadacima kao što su, među ostalim, održavanje, nadzor, otkrivanje sigurnosnih propusta i otklanjanje kvarova te u svrhu upravljanja administrativnim zadacima kao što su, među ostalim, nabavke, ugovori o održavanju i reguliranje licenčnih prava.

6.5 UPRAVLJANJE PROMJENAMA NA RAČUNALNIM RESURSIMA

Članak 26.

Potrebno je pratiti operativno stanje računalnih resursa u produkcijskom redu, identificirati sve njihove manjkavosti ili nedostatke, a utvrđene manjkavosti i nedostatke otkloniti u najkraćem mogućem roku.

Svaka promjena konfiguracijskih parametara ili drugih komponenti računalnih resursa koje utječu na njihovu sigurnost mora biti testirana, a prije uvođenja u produkcijski rad odobrena i evidentirana.

6.6 ZAŠTITA OD VIRUSA I MALICIOZNIH PROGRAMA

Članak 27.

Mjere zaštite od virusa i malicioznih programa moraju se provoditi na svim računalnim resursima na kojima je utvrđen rizik od pojave takvih prijetnji. Provjera prisutnosti virusa mora se provoditi, minimalno, na svim datotekama koje se preuzimaju iz Internet okruženja. Sustav zaštite od virusa mora biti redovito ažuriran, a korisnici upoznati s dodatnim mjerama koje su u funkciji zaštite od virusa i malicioznih programa.

7 FIZIČKA ZAŠTITA RAČUNALNIH RESURSA

7.1 CILJEVI

Članak 28.

Računalni resursi moraju biti adekvatno zaštićeni od nepogoda uzrokovanih vanjskim djelovanjem tehničkih faktora, od prijetnji uzrokovanih namjernim djelovanjem ljudskog faktora te od prirodnih nepogoda.

Pristup računalnim resursima mora biti ograničen i kontroliran, sukladno značaju računalnih resursa u poslovnom procesu.

Mjere fizičke zaštite moraju biti planirane, dokumentirane i provedene za sve računalne resurse informacijskog sustava Društva

7.2 SMJEŠTAJ SREDIŠNJIH RAČUNALNIH RESURSA

Članak 29.

Središnji računalni resursi te drugi uređaji kritični za rad informacijskog sustava kojima se pružaju informacijski servisi moraju biti smješteni u odvojenim prostorima, a fizički pristup ovim prostorima mora biti ograničen i kontroliran, sukladno ulozi korisnika u radu informacijskog sustava.

Potrebno je provesti tehničke mjere kojima će se detektirati neovlašteni ulaz u prostore gdje su smješteni središnji računalni resursi.

Moraju se provesti mjere kojima će se do najveće moguće mjere reducirati utjecaj vanjskih nepogoda, kao što su destruktivno djelovanje ljudskog faktora te prirodne nepogode, na prostor u kojima su smješteni središnji računalni resursi.

7.3 PRIMJERENI UVJETI RADA ZA RAČUNALNE RESURSE

Članak 30.

Središnji računalni resursi te drugi uređaji kritični za rad informacijskog sustava moraju biti zaštićeni od prekida električnog napajanja ili drugih anomalija u električnom napajanju, a na način koji će osigurati kontinuirani rad u primjerenom razdoblju i nakon takvih anomalija.

U prostorima gdje su smješteni središnji računalni resursi te drugi uređaji kritični za rad informacijskog sustava potrebno je osigurati takve uvjete rada kojima će se spriječiti djelovanje vanjskih faktora kao što su neprimjerena temperatura i vlažnost, prodor vode i pojava onečišćenja.

Središnji računalni resursi te oprema kojom se osiguravaju primjereni uvjeti rada u prostorima gdje su ovi resursi smješteni moraju biti redovito servisirani kako bi se spriječio utjecaj tehničkih i prirodnih nepogoda na rad informacijskog sustava.

7.4 PRISTUP UREDSKIM PROSTORIMA

Članak 30.

Ulazak posjetitelja, tj. osoba koje nisu zaposlenici Društva, u uredske prostore omogućit će se isključivo nakon verifikacije poslovnih razloga za ulazak posjetitelja u Društvo te uz pratnju zaposlenika Društva.

Osobna računala i druga računalna oprema koja se koristi u uredskim prostorima mora biti zaštićena od nekontroliranog kontakta posjetitelja s ovom opremom.

7.5 OTPIS UREĐAJA

Članak 31.

Računalni uređaji i druge sklopovske komponente računalnih resursa mogu se otpisati tek nakon što podaci i instalirani softver s ovih resursa i njihovih komponenti budu nedvojbeno izbrisani.

8 PRIMJERNO KORIŠTENJE INFORMACIJSKOG SUSTAVA

8.1 CILJEVI

Članak 32.

Informacijski sustav Društva i računalni resursi koji su dio ovog sustava smiju se koristiti samo za svrhe poslovnog procesa Društva. Korisnici informacijskog sustava su odgovorni za profesionalnu, etičku i zakonitu upotrebu resursa informacijskog sustava.

Korisnici moraju pristupati informacijskom sustavu isključivo upotrebom službeno odobrenih ovlasti za pristup. Pri upotrebi informacijskog sustava Društva, korisnici moraju slijediti propisane zahtjeve koji se odnose na očuvanje povjerljivosti, dostupnosti i cjelovitosti podataka i informacijskih servisa.

8.2 PRISTUP KORISNIKA INFORMACIJSKOM SUSTAVU

Članak 33.

Korisnici smiju pristupiti resursima informacijskog sustava isključivo korištenjem podataka za prijavu koji su im osobno dodijeljeni i u svrhu za koju su podaci za prijavu dodijeljeni.

Korisnici ne smiju drugim osobama omogućiti korištenje podataka za prijavu koji su im osobno dodijeljeni.

Korisnici smiju pristupati samo onim podacima i informacijskim servisima za koje imaju dozvolu pristupa, a u okvirima radnih aktivnosti koje obavljaju u poslovnom procesu.

8.3 UPOTREBA OSOBNIH RAČUNALA

Članak 33.

Korisnici ne smiju ni na koji način mijenjati tehnička svojstva osobnih računala koja su im dodijeljena na upotrebu, a što podrazumijeva, među ostalim, da korisnici ne smiju instalirati programske i hardverske komponente, instalirati periferne uređaje te mijenjati konfiguracijske datoteke osobnih računala.

Osobna računala se moraju koristiti na način koji će spriječiti ili reducirati mogućnost pojave računalnih virusa i drugih malicioznih programa na osobnim računalima.

8.4 RAD U UREDSKIM PROSTORIMA

Članak 34.

Korisnici moraju koristiti osobna računala, podatkovne medije, dokumente i druge resurse informacijskog sustava tako da se neovlaštenim osobama onemogući pristup informacijskom sustavu i na način kojim se sprječava neovlašteni uvid u sadržaj povjerljivih informacija.

Korisnici moraju prilikom svakog izlaska iz uredskog prostora odjaviti svoj rad s osobnog računala ili privremeno zaključati pristup osobnom računalu, a podatkovne medije i povjerljive dokumente ukloniti s mjesta dostupnih drugim osobama.

8.5 KORIŠTENJE INTERNETA I SERVISA DOSTUPNIH INTERNETOM

Članak 35.

Internet i servisi dostupni Internetom smiju se koristiti isključivo u svrhu poslovnih procesa Društva, na temelju etičkih načela i na način koji nije u suprotnosti sa zakonskim zahtjevima. Servisi dostupni Internetom uključuju, među ostalim, pristup vanjskim web poslužiteljima, korištenje elektroničke pošte i sudjelovanje u radu društvenih mreža.

Prethodna odredba se odnosi na upotrebu Interneta i servisa dostupnih Internetom putem računalne mreže Društva i u svim situacijama kada se korisnici identificiraju kao djelatnici Društva.

9 RAZVOJ, PRIBAVLJANJE I ODRŽAVANJE APLIKACIJA

9.1 CILJEVI

Članak 36.

Postupku razvoja i izmjene aplikativnih komponenti informacijskog sustava mora prethoditi dubinska analiza poslovnih zahtjeva koja uključuje i procjenu rizika kojeg nove ili izmijenjene komponente mogu uvesti u poslovanje Društva.

Mjere neophodne za siguran rad sustava moraju biti predviđene već u fazi planiranja svojstava novih sustava, a provedba ovih mjera mora biti prisutna u fazama razvoja, odabira, implementacije i promjena informacijskog sustava i njegovih komponenti. U produkcijsku upotrebu se smiju uvesti isključivo oni programski sustavi koji zadovoljavaju prethodno definirane poslovne zahtjeve.

Postupak razvoja aplikacija mora biti usklađen sa formalno odobrenom metodologijom razvoja informacijskog sustava.

9.2 DUBINSKA ANALIZA POSLOVNIH ZAHTJEVA

Članak 37.

Na temelju inicijative za razvoj ili izmjenu informacijskog sustava treba provesti dubinsku analizu poslovnih zahtjeva te provesti procjenu rizika kojeg nove ili izmijenjene aplikativne komponente informacijskog sustava mogu uvesti u poslovanje Društva.

Iz dubinske analize poslovnih zahtjeva, rezultata procjene rizika i regulatornih zahtjeva, definirat će se funkcionalna specifikacija novog sustava, koja mora uključivati i sve mjere neophodne za siguran rad informacijskog sustava te za pouzdan rad poslovnog procesa podržanog ovim sustavom.

Prethodne odredbe odnose se i na slučajeve kada se aplikativna komponenta pribavlja iz vanjskih izvora, a dobavljači aplikativnih komponenti moraju uskladiti svoj rad sa zahtjevima iz ovog poglavlja Politike sigurnosti.

9.3 RAZVOJ APLIKACIJA

Članak 38.

Aplikativne komponente informacijskog sustava moraju su razvijati temeljem formalno prihvaćene metodologije razvoja informacijskog sustava. Metodologija razvoja informacijskog sustava mora, među ostalim, uključivati postupak upravljanja promjenama, upravljanja verzijama i upravljanja konfiguracijama, a čim se reducira izloženost rizicima nedokumentiranih ili neprovjerenih promjena.

Sve osobe koje sudjeluju u razvoju aplikativnih komponenti moraju uvažavati prethodno definirane mjere sigurnosti te ih implementirati sukladno svojoj ulozi u procesu razvoja.

Postupak razvoja aplikativnog koda i razvojna okolina moraju biti izvedeni na način kojim će se onemogućiti neovlaštena ili neopažena promjena programskog koda, a naročito eliminacija ili zaobilaženje definiranih mjera sigurnosti.

9.4 PRIBAVLJANJE APLIKACIJA IZ VANJSKIH IZVORA

Članak 39.

Svojstva aplikacija koja se pribavljaju iz vanjskih izvora moraju biti usklađena sa funkcionalnim zahtjevima definiranim sukladno odredbama pasusa 9.2. U slučaju da aplikacija koja se pribavlja iz vanjskih izvora ne sadrži zahtijevanu funkcionalnost, a dobavljač nije u mogućnosti ovu funkcionalnost dopuniti, nadležne osobe Društva donose ocjenu o eventualnom prilagođavanju poslovnog procesa i prihvaćanju aplikacije. Nadležne osobe moraju u takvim situacijama obrazložiti svoju odluku te predložiti izmjene u poslovnom procesu.

Ugovor o pribavljanju aplikacije mora uključivati odredbe prema kojima dobavljač jamči cjelovitost isporučene aplikacije, a što podrazumijeva izostanak bilo kakvih nedokumentiranih funkcija, a naročito onih funkcija koje bi uključivale mogućnost neovlaštenog ulaza na sustav.

Ugovor o pribavljanju aplikacije mora sadržavati jasne odredbe kojom se Društvu odobrava pristup izvornom aplikativnom kodu u slučaju prestanka potpore aplikativnom kodu uslijed trajnog prestanka rada dobavljača aplikacije i prestanka potpore.

9.5 APLIKACIJSKE KONTROLNE MJERE

Članak 40.

Informacijski sustavi i njihove aplikativne komponente moraju uključivati aplikacijske kontrolne mjere kojima je cilj validacija ulaznih i izlaznih vrijednosti, očuvanje cjelovitosti podatka te provedba autorizacije kod promjene ili čitanja osjetljivih podataka te pokretanja osjetljivih aplikativnih funkcija.

Aplikativne komponente moraju bilježiti u evidencijske datoteke sve relevantne podate o provedenim transakcijama, a u svrhu naknadnog dokazivanja tijeka upotrebe aplikacije.

9.6 TESTIRANJE APLIKATIVNOG KODA

Članak 41.

Svaka nova ili izmijenjena aplikativna komponenta razvijena unutar Društva ili pribavljena od vanjskih dobavljača mora, prije početka produkcijskog korištenja, proći postupak testiranja kojim će se verificirati funkcionalna svojstva i sigurnosne kontrolne mjere ove komponente.

Testiranje aplikativnih komponenti mora biti provedeno izvan produkcijske okoline i na podacima koji simuliraju produkcijske uvjete. Podaci koji se koriste u testiranju ne smiju sadržavati povjerljiv sadržaj.

Postupak testiranja mora biti dokumentiran, a osobe nadležne za testiranje moraju potvrditi ispravnost testirane aplikativne komponente.

U produkcijski rad može biti uvedena samo ona aplikacija koja je prethodno uspješno testirana i za koju su sastavljena cjelovita korisnička dokumentacija.

9.7 UPRAVLJANJE PROMJENAMA U APLIKACIJAMA

Članak 42.

Postupak uvođenja aplikativnih promjena provodi se na temelju formalno definirane procedure. Odredbe ove procedure mogu biti usklađene s kompleksnošću i potencijalnim utjecajem predloženih promjena, pri čemu je nužno pridržavati se svih zahtjeva za očuvanjem sigurnosnih svojstava u aplikacijama.

Postupak uvođenja aplikativnih promjena mora biti dokumentiran, a evidencija o verzijama aplikativnog koda mora biti točna i ažurna.

10 SIGURNOST KOMUNIKACIJSKO-OPERATIVNIH PROCESA

10.1 CILJEVI

Članak 43.

Procesi kojima se provode redovite operativno-komunikacijske aktivnosti u informacijskom sustavu Društva moraju biti izvedeni na način kojim će se realizirati minimalno sljedeći ciljevi:

- izvedba informacijskih servisa u okruženju koje jamči održive performanse rada
- zaštita povjerljivosti i cjelovitosti podataka tijekom prijenosa informacijskim sustavom
- prepoznavanje i sprječavanje neovlaštenog pristupa na resurse informacijskog sustava
- odgovaranje na sigurnosne incidente

10.2 ADMINISTRACIJA SUSTAVA

Članak 44.

Administracija informacijskog sustava i njegovih komponenti može se povjeriti isključivo osobi kompetentnoj za obavljanje ovih poslova.

Obaveze administratora sustava uključuju, među ostalim, skrb o primjernoj konfiguraciji tehničkih postavki sustava, praćenje rada sustava i otklanjanje uočenih nepravilnosti u radu.

Operativne procedure koje se odnose na administraciju informacijskog sustava i njegovih komponenti moraju biti dokumentirane i ažurne.

10.3 PLANIRANJE I KAPACITIRANJE SUSTAVA

Članak 45.

Informacijski sustav i njegove komponente moraju biti izvedene na način koji će spriječiti ispade sustava i neodgovarajuće performanse rada sustava.

Rad informacijskog sustava i upotreba njegovih resursa moraju biti redovito nadzirani u cilju utvrđivanja razine iskorištenosti te planiranja budućih kapaciteta koji će omogućiti njihov primjeren rad.

10.4 SIGURNOST RAČUNALNE MREŽE

Članak 46.

Infrastruktura računalne mreže Društva i sve komponente ove infrastrukture moraju biti implementirane na način kojim će se zaštiti sigurnost priključenih računalnih resursa i podataka koji se prenose ovom mrežom.

Na računalnoj mreži Društva smiju se koristiti samo oni mrežni servisi za koje postoji poslovna opravdanost.

Pojedine komponente računalne mreže moraju biti izvedene i konfigurirane na način kojim će se spriječiti kompromitacija ovih komponenti, a pristup ovim resursima biti kontroliran sukladno poslovnim zahtjevima i uz restrikciju prava pristupa. Komponente računalne mreže moraju biti segmentirane kako bi se povjerljivi resursi izolirali od pokušaja neovlaštenog pristupa.

Udaljeni pristup na računalnu mrežu dozvoljava se isključivo na temelju poslovno opravdanih razloga te uz restrikciju pristupnih prava sukladno zahtjevima poslovnih procesa. Udaljeni pristup na računalnu mrežu bit će omogućen nakon nedvojbene autentifikacije korisnika i uz kriptiranje mrežnog prometa.

Provođenje promjena u infrastrukturi računalne mreže i u konfiguraciji mrežnih resursa mora se provoditi na kontrolirani način, a same promjene moraju biti dokumentirane.

10.5 NADZOR NAD RADOM SUSTAVA

Članak 47.

Sve komponente informacijskog sustava koje imaju značajnu ulogu u njegovom radu moraju biti konfigurirane na način kojim će se omogućiti bilježenje evidencijskih podataka. U evidencijskim podacima moraju se zabilježiti svi relevantni događaji koji se odnose na pristup korisnika, pogreške u radu sustava te podaci o sigurnosno uvjetovanim događajima.

Evidencijski podaci moraju biti redovito nadzirani te na odgovarajuću način obrađeni.

Evidencijski podaci moraju biti zaštićeni od neovlaštene modifikacije te pohranjeni na primjeren način i kroz primjereno razdoblje pohrane.

10.6 IZRADA PRIČUVNIH KOPIJA

Članak 48.

Podaci pohranjeni u informacijskom sustavu Društva moraju biti redovito arhivirani u svrhu obnove kod izvanrednih situacija.

Dinamika izrade pričuvnih kopija, njihov sadržaj i mjere zaštite ovih kopija moraju biti usklađeni s zahtjevima poslovnog procesa u kojem se pojedina kategorija podataka koristi.

Obnova podataka iz pričuvnih kopija mora biti periodički provjeravana kako bi se verificirala njihova ispravnost i primjenjivost.

11 PLANIRANJE KONTINUITETA POSLOVANJA

11.1 CILJEVI

Članak 49.

Planom kontinuiteta poslovanja predviđa se postupak za očuvanje neprekinutosti rada informacijskog sustava Društva u slučajevima nastupanja kritičnih nepogoda koje značajno narušavaju dostupnost informacijskih servisa.

Plan kontinuiteta poslovanja treba se temeljiti na procjeni rizika od nastupanja kritičnih nepogoda, a elementi ovog plana trebaju biti usklađeni s poslovnim zahtjevima.

Plan kontinuiteta poslovanja mora biti dokumentiran, redovito provjeravan i prema potrebi ažuriran, a njegovo provođenje uvježbano.

11.2 NADLEŽNOST ZA PLAN KONTINUITETA POSLOVANJA

Članak 50.

Za izradu i upravljanje planom kontinuiteta poslovanja je nadležno radno tijelo koje imenuje rukovodstvo Društva, a koje uključuje, među ostalim, davatelja informatičkih usluga i vlasnike podataka.

U provedbu plana kontinuiteta moraju biti uključene svi zaposlenici Društva čije je uloga definirana ovim planom.

11.3 PROCJENA RIZIKA

Članak 51.

Postupak procjene rizika uključuje analizu izglednosti nastupanja kritičnih nepogoda te procjenu utjecaja ovih nepogoda na poslovanje Društva. Procjena utjecaja mora sadržavati procjenu očekivanih gubitaka u poslovnom procesu, pri čemu treba uzeti u obzir razmjer i trajanje nepogode.

Na temelju rezultata procjene rizika donosi se strategija za postupanje u slučaju kritičnih nepogoda.

11.4 AKCIJSKI PLANOVI ZA KRITIČNE NEPOGODE

Članak 52.

Postupak obnove rada računalnih resursa i informacijskih resursa u slučajevima kritičnih nepogoda definirani su akcijskim planovima, koji su sastavni dio plana kontinuiteta poslovanja.

Akcijski planovi moraju biti usklađeni sa strategijom za postupanje u slučaju kritičnih nepogoda te moraju reflektirati tehničke uvjete koji su raspoloživi za postupak obnove informacijskih servisa

11.5 PROVJERA I ODRŽAVANJE PLANA KONTINUITETA POSLOVANJA

Članak 53.

Svaki element plana kontinuiteta poslovanja mora biti dokumentiran, a njegov sadržaj redovito ažuriran sukladno promjenama u informacijskom sustavu, poslovnim zahtjevima ili regulatornim uvjetima. Sudionici u provedbi plana kontinuiteta poslovanja moraju uvježbati sve faze provedbe ovog plana, a svako odstupanje treba biti obrađeno na odgovarajući način.

12 SIGURNOSNI INCIDENTI

12.1 CILJEVI

Članak 55.

Korisnici informacijskog sustava moraju dojaviti nadležnim osobama svaki događaj koji predstavlja prijetnju povjerljivosti, cjelovitosti i dostupnosti resursa informacijskog sustava Društva. Nad svakim događajem koji ima elemente sigurnosnog incidenta mora biti pokrenuta obrada u najkraćem mogućem roku. Obrada takvih događaja mora biti učinkovita te uzeti u obzir zakonske uvjete tijekom postupka obrade.

12.2 PRIJAVA SIGURNOSNIH INCIDENATA

Članak 56.

Korisnici informacijskog sustava moraju biti upoznati s načinom prepoznavanja sigurnosnih incidenata te takve incidente dojaviti nadležnim osobama. Informacijski sustav mora sadržavati mjere za detekciju i dojavu incidenata iz evidencijskih podataka i drugih sistemskih resursa, a plan odgovaranja na sigurnosne incidente mora uključiti i postupke za rješavanje ovih incidenata.

12.3 PLAN ODGOVARANJA NA SIGURNOSNE INCIDENTE

Članak 57.

Postupak odgovaranja na sigurnosne incidente definiran mora se provoditi temeljem formalno prihvaćenog plana odgovaranja na sigurnosne incidente, a tijek odgovaranja mora biti dokumentirani. Rukovodstvo Društva mora biti redovito izvještavana o tijeku odgovaranja na sigurnosne incidente.

12.4 PRIKUPLJANJE DOKAZA

Članak 58.

Postupak odgovaranja na sigurnosne incidente za koje se pretpostavlja da bi mogli rezultirati pravnim postupkom mora uvažavati obvezu pravne valjanosti prikupljenih dokaza.

Podaci koji se koriste u postupku odgovaranja na sigurnosne incidente za koje se pretpostavlja da bi mogli rezultirati pravnim postupkom moraju biti pribavljeni i pohranjeni na pravno valjan način.

13 NADZOR I SUKLADNOST

13.1 CILJEVI

Članak 59.

Sigurnosne mjere u informacijskom sustavu Društva te radne postavke pojedinih komponenti informacijskog sustava moraju biti usklađene sa zahtjevima Politike sigurnosti, sigurnosnim standardima koji se mogu izvesti iz Politike sigurnosti i procesa upravljanja rizicima te sa odgovarajućim regulatornim zahtjevima, ako su takvi zahtjevi doneseni.

Stupanj usklađenosti sigurnosnih mjera i radnih postavki sa zahtjevima navedenim u prethodnom poglavlju, moraju biti predmet redovite provjere.

13.2 USKLAĐENOST S REGULATORNIM ZAHTJEVIMA

Članak 60.

Ukoliko se zakonskim aktima ili odvojenim regulatornim zahtjevima propisuju mjere sigurnosti informacijskog sustava, nadležne osobe moraju napraviti plan primjene ovih zahtjeva te ih implementirati u najkraćem mogućem roku.

13.3 USKLAĐENOST ZA ZAHTJEVIMA KOJI PROIZLAZE IZ POLITIKE SIGURNOSTI

Članak 61.

Nadležne osobe moraju primjenjivati mjere sigurnosti informacijskog sustava koje su propisane Politikom sigurnosti ili drugim aktima koji proizlaze iz Politike sigurnosti.

Mjere iz prethodnog stavka moraju biti na odgovarajući način dokumentirane kroz konfiguracijske standarde ili radne upute.

13.4 PROVJERA USKLAĐENOSTI

Članak 62.

Stvarna usklađenost sigurnosnih mjera i radnih postavki implementiranih u informacijskom sustavu i njegovim resursima s vrijednostima ovih mjera kako su izvorno definirane u Politici sigurnosti, regulatornim zahtjevima ili odgovarajućim konfiguracijskim standardima, mora biti predmet redovite provjere. Svaka neusklađenost mora biti analizirana, a plan otklanjanja definiran. Nadležne osobe moraju izvjesiti rukovodstvo Društva o rezultatima provjere usklađenosti i planiranim korektivnim akcijama.

14 ZAVRŠNE ODREDBE

Članak 63.

Ova Politika stupa na snagu i primjenjuje se danom donošenja.

DIREKTOR PAN-PE... Zagreb, Planin...

Ivan Parać, dipl. ing.