HNB

Trg hrvatskih velikana 3, 10002 Zagreb
tel.: 01 45 64 555 / faks: 01 46 10 551, 45 50 726, 46 10 591
teleks: 22 569 / www.hnb.hr / mb 3269817

ODLUKA

O PRIMJERENOM UPRAVLJANJU INFORMACIJSKIM SUSTAVOM

("Narodne novine", br. 37/2010.)

Na temelju članka 161. stavka 1. pod 3. Zakona o kreditnim institucijama (»Narodne novine«, br. 117/2008., 74/2009. i 153/2009.) te članka 43. stavka 2. pod 9. Zakona o Hrvatskoj narodnoj banci (»Narodne novine«, br. 75/2008.) guverner Hrvatske narodne banke donosi

ODLUKU

O PRIMJERENOM UPRAVLJANJU INFORMACIJSKIM SUSTAVOM

I. OPĆE ODREDBE

Članak 1.

(1) Ovom se Odlukom uređuju obveze kreditne institucije koje se odnose na upravljanje informacijskim sustavom.

(2) Ova se Odluka primjenjuje:

1) na kreditne institucije sa sjedištem u Republici Hrvatskoj koje su od Hrvatske narodne banke dobile odobrenje za rad i

2) na podružnice kreditnih institucija iz trećih država koje su od Hrvatske narodne banke dobile odobrenje za pružanje usluga.

(3) Iznimno od stavka 2. ovog članka ova se Odluka ne primjenjuje na institucije za elektronički novac.

II. ZNAČENJE POJMOVA

Članak 2.

1) *Softverske komponente* (softverska imovina) uključuju aplikacijski softver, sistemski softver, baze podataka, softverske razvojne alate, uslužne programe te ostali softver.

2) *Hardverske komponente* (hardverska imovina) uključuju računala i računalnu opremu (stacionarna i prijenosna osobna računala, poslužitelje, monitore, tipkovnice, pisače i slično), komunikacijsku opremu (usmjernike, preklopnike, vatrozide i slično), medije za pohranu podataka (magnetne diskove, magnetne trake, optičke diskove i slično) te ostalu tehničku opremu koja podržava rad informacijskog sustava (uređaje za neprekidno napajanje električnom strujom, klimatizacijske uređaje i slično).

3) *Informacijska imovina* uključuje podatke u bazama podataka, datoteke s podacima, programski kôd, sistemsku i aplikacijsku dokumentaciju, korisničke priručnike, planove, interne akte i slično.

4) *Informacijska tehnologija* omogućuje automatizirano prikupljanje, obradu, generiranje, pohranu, prijenos, prikaz te distribuciju informacija kao i raspolaganje njima. Informacijska se tehnologija sastoji od softverskih i hardverskih komponenata.

5) *Informacijski sustav* je sveobuhvatnost tehnološke infrastrukture, organizacije, ljudi i postupaka za prikupljanje, obradu, generiranje, pohranu, prijenos, prikaz te distribuciju informacija kao i raspolaganje njima. Informacijski sustav moguće je definirati i kao međudjelovanje informacijske tehnologije, podataka i postupaka za procesiranje podataka te ljudi koji prikupljaju navedene podatke i njima se koriste.

6) *Korisnici informacijskog sustava* su sve osobe koje se koriste informacijskim sustavom (zaposlenici kreditne institucije, zaposlenici pružatelja usluga, korisnici elektroničkog bankarstva, zaposlenici pravnih osoba koji se koriste informacijskim sustavom kreditne institucije itd.).

7) *Rizik informacijskog sustava* jest rizik koji proizlazi iz korištenja informacijske tehnologije odnosno informacijskog sustava.

8) *Resursi informacijskog sustava* uključuju informacijsku imovinu, softverske komponente i hardverske komponente.

9) *Svojstva informacija i procesa* uključuju povjerljivost, integritet, raspoloživost, autentičnost, neporecivost, dokazivost i pouzdanost.

10) *Povjerljivost* je svojstvo informacija (podataka) da nisu dostupne ili otkrivene neovlaštenim subjektima.

11) *Integritet* je svojstvo informacija (podataka) i procesa da nisu neovlašteno ili nepredviđeno mijenjani.

12) *Raspoloživost* je svojstvo informacija i procesa koje omogućuje pristup tim informacijama i procesima te njihovu upotrebljivost, tj. njihovu dostupnost na zahtjev ovlaštenog subjekta.

13) *Autentičnost* je svojstvo koje osigurava da je identitet subjekta zaista onaj za koji se tvrdi da jest.

14) *Neporecivost* je svojstvo koje osigurava nemogućnost poricanja izvršene aktivnosti ili primitka informacije (podatka).

15) *Dokazivost* je svojstvo koje osigurava da aktivnosti subjekta mogu biti praćene jedinstveno do samog subjekta.

16) *Pouzdanost* je svojstvo dosljednoga, očekivanog ponašanja i rezultata.

17) *Kontrole* uključuju upravljačke, logičke i fizičke kontrole.

18) *Upravljačke kontrole* uključuju donošenje internih akata vezanih uz informacijski sustav i uspostavljanje odgovarajuće organizacijske strukture te osiguravaju primjenu internih akata vezanih uz informacijski sustav radi osiguravanja funkcionalnosti i sigurnosti informacijskog sustava.

19) *Logičke kontrole* su kontrole implementirane na softverskim komponentama informacijskog sustava.

20) *Fizičke kontrole* su kontrole koje štite resurse informacijskog sustava od neovlaštenoga fizičkog pristupa, krađe, fizičkog oštećenja ili uništenja.

21) *Upravljanje korisničkim pravima pristupa* uključuje evidentiranje, autorizaciju, identifikaciju i autentifikaciju te nadzor korisničkih prava pristupa.

22) *Evidentiranje* je proces definiranja novih korisnika informacijskog sustava.

23) *Autorizacija* je proces dodjele prava pristupa korisnicima informacijskog sustava.

24) *Identifikacija i autentifikacija* procesi su identifikacije korisnika informacijskog sustava i potvrde njegova identiteta prilikom prijave i tijekom provođenja radnja na informacijskom sustavu.

25) *Nadzor korisničkih prava pristupa* je proces koji uključuje praćenje, izmjenu i revidiranje prava pristupa korisnika informacijskog sustava.

26) *Korisnički identitet* moguće je potvrditi korištenjem jednoga ili kombinacijom sljedećih načina:

a) pomoću nečega što samo korisnik zna (primjerice zaporka, PIN ili kriptografski ključ),

b) pomoću nečega što samo korisnik posjeduje (primjerice magnetska kartica, čip kartica ili »token») i

c) pomoću nečega što korisnik jest (korištenjem biometrijskih metoda kao što su provjera otiska prsta ili karakteristika šarenice oka, prepoznavanje glasa ili rukopisa i slično).

27) *Povlašteni pristup informacijskom sustavu* (engl. *administrative access*) onaj je pristup resursima informacijskog sustava koji je omogućen korisnicima informacijskog sustava s velikim ovlastima te povlaštenim pravima pristupa koja im omogućuju zaobilaženje ugrađenih logičkih kontrola, a to su, među ostalim, administratori baza podataka, administratori mrežne opreme, administratori sistemskog softvera i administratori aplikacijskog softvera.

28) *Udaljeni pristup resursima informacijskog sustava* kreditne institucije je pristup tim resursima s udaljene lokacije pomoću telekomunikacijske infrastrukture nad kojom kreditna institucija nema potpunu kontrolu ili nadzor.

29) *Operativni i sistemski zapisi* jesu bilješke o aktivnostima na resursima informacijskog sustava nastale onim slijedom kako su se te aktivnosti ostvarivale (zapisi operacijskih sustava, vatrozida, usmjernika, sustava za otkrivanje neovlaštenog pristupa i radnja na informacijskom sustavu, zapisi aplikacijskog softvera, baza podataka i slično).

30) Operativni i sistemski zapisi trebali bi omogućiti sljedeće:

a) rekonstrukciju događaja,

b) utvrđivanje odgovornosti za aktivnosti ostvarene na informacijskom sustavu,

c) otkrivanje neovlaštenog pristupa i radnji provedenih na informacijskom sustavu i

d) identifikaciju problema.

31) *Maliciozni programski kôd* je bilo koji oblik programskoga kôda stvoren da bi djelovao neočekivano i na potencijalno štetan način, odnosno na način koji može narušiti povjerljivost, integritet i raspoloživost resursa informacijskog sustava. Primjeri su malicioznoga programskog kôda računalni crvi i virusi te »trojanski konji«.

32) *Elektroničko bankarstvo* je neposredna ponuda novih i tradicionalnih proizvoda i usluga klijentima putem elektroničkih interaktivnih komunikacijskih kanala.

33) *Elektroničko bankarstvo* uključuje sustave koji klijentima kreditne institucije pružaju bankarske proizvode i usluge (primjerice pristup financijskim informacijama, informiranje o proizvodima i uslugama te elektroničko plaćanje).

34) *Incident* je svaki neplanirani i neželjeni događaj koji može narušiti sigurnost i funkcionalnost resursa informacijskog sustava koji podržavaju odvijanje poslovnih procesa kreditne institucije.

35) *Zahtijevano vrijeme oporavka* (engl. *recovery time objective*) je prihvatljivo vrijeme neraspoloživosti poslovnih procesa kreditne institucije i resursa informacijskog sustava potrebnih za njihovo odvijanje, odnosno vrijeme tijekom kojega je potrebno obnoviti (oporaviti) poslovne procese.

36) *Kritični i/ili ključni poslovni procesi* oni su poslovni procesi koje je kreditna institucija identificirala kao takve te čija nedostupnost može ozbiljnije ugroziti odnosno narušiti poslovanje kreditne institucije.

37) *Pričuvne kopije podataka* su pričuvne inačice podataka (informacijska imovina i softverske komponente) koje su potrebne za ponovno uspostavljanje (oporavak)

poslovnih procesa kreditne institucije te ostalih podataka za koje kreditna institucija procijeni da ih je potrebno pričuvno pohraniti.

III. OKVIR ZA UPRAVLJANJE INFORMACIJSKIM SUSTAVOM

Članak 3.

Uprava kreditne institucije dužna je odrediti člana uprave koji će biti nadležan za uspostavu i nadzor procesa upravljanja informacijskim sustavom.

Članak 4.

Uprava kreditne institucije dužna je uspostaviti adekvatnu organizacijsku strukturu, odgovarajuće funkcije i odbore te u skladu s tim prenijeti ovlasti kako bi se osiguralo primjereno upravljanje informacijskim sustavom kreditne institucije.

Članak 5.

(1) Uprava kreditne institucije dužna je donijeti strategiju informacijskog sustava koja mora biti u skladu s poslovnom strategijom kreditne institucije.

(2) Strategiju informacijskog sustava kreditne institucije potrebno je razraditi donošenjem strateških i operativnih planova.

Članak 6.

Uprava kreditne institucije dužna je donijeti interne akte kojima se uređuje upravljanje informacijskim sustavom te osigurati provođenje tih akata.

Članak 7.

Uprava kreditne institucije dužna je osigurati da svi korisnici informacijskog sustava budu upoznati sa sadržajem internih akata vezanih uz informacijski sustav u skladu s dodijeljenim ovlastima te potrebama korisnika informacijskog sustava.

Članak 8.

Kreditna institucija je dužna definirati kriterije, načine i postupke izvješćivanja uprave i nadzornog odbora kreditne institucije o relevantnim činjenicama vezanima uz funkcionalnost i sigurnost informacijskog sustava.

Članak 9.

Uprava kreditne institucije dužna je uspostaviti funkciju voditelja sigurnosti informacijskog sustava neovisnu o funkciji voditelja organizacijske jedinice za informacijsku tehnologiju te definirati njegove ovlasti, odgovornosti i djelokrug rada.

Članak 10.

Uprava kreditne institucije dužna je imenovati odbor za upravljanje informacijskim sustavom ili druge odbore čija uloga treba biti praćenje i nadziranje informacijskog sustava i njegovih aktivnosti te koordinacija inicijativa vezanih uz informacijski sustav, a koje se tiču usklađenosti s poslovnim ciljevima i poslovnom strategijom kreditne institucije.

Članak 11.

Uprava kreditne institucije dužna je donijeti metodologiju upravljanja projektima kojom će se definirati kriteriji, načini i postupci upravljanja projektima vezanima uz informacijski sustav.

IV. UPRAVLJANJE RIZIKOM INFORMACIJSKOG SUSTAVA

Članak 12.

Opća pravila za primjenu i uspostavu sustava upravljanja rizicima u smislu Zakona o kreditnim institucijama i propisa donesenih na temelju tog Zakona moraju se primijeniti i na upravljanje rizikom informacijskog sustava.

V. UPRAVLJANJE UGOVORNIM ODNOSIMA

Članak 13.

Kreditna institucija je dužna procijeniti i svesti na prihvatljivu razinu rizike koji proizlaze iz ugovornih odnosa s pravnim i fizičkim osobama čije su aktivnosti vezane uz informacijski sustav kreditne institucije.

Članak 14.

Kreditna institucija je dužna kontinuirano nadzirati način i kvalitetu pružanja ugovorenih usluga vezanih uz informacijski sustav kreditne institucije.

VI. UNUTARNJA REVIZIJA

Članak 15.

(1) Metodologija koju je kreditna institucija dužna donijeti u skladu s člankom 187. stavkom 5. Zakona o kreditnim institucijama mora sadržavati kriterije, načine i postupke revizije informacijskog sustava kreditne institucije zasnovane na procjeni rizika.

(2) Na unutarnju reviziju informacijskog sustava primjenjuju se odredbe Odluke o sustavu unutarnjih kontrola (»Narodne novine«, br. 1/2009., 75/2009. i 2/2010.).

VII. SIGURNOST INFORMACIJSKOG SUSTAVA

Članak 16.

Kreditna je institucija dužna donijeti interni akt koji će biti okvir za upravljanje sigurnošću informacijskog sustava (u nastavku teksta: politika sigurnosti informacijskog sustava) te definirati odgovornosti koje se odnose na područje sigurnosti informacijskog sustava.

Članak 17.

Kreditna je institucija dužna klasificirati i zaštititi informacije prema stupnju njihove osjetljivosti s obzirom na moguće posljedice narušavanja povjerljivosti, integriteta i raspoloživosti informacija.

Članak 18.

Kreditna institucija je dužna kontrolirati pristup resursima informacijskog sustava, prostorijama s resursima informacijskog sustava kao i sustavima koji su podrška funkcioniranju informacijskog sustava te primijeniti odgovarajuće upravljačke, logičke i fizičke kontrole pristupa. Posebnu pozornost potrebno je posvetiti povlaštenom i udaljenom pristupu resursima informacijskog sustava.

Članak 19.

Kreditna institucija je dužna uspostaviti sustav upravljanja korisničkim pravima pristupa koji obuhvaća procese evidentiranja, autorizacije, identifikacije i autentifikacije te nadzora korisničkih prava pristupa.

Članak 20.

Kreditna institucija je dužna u skladu s procjenom rizika osigurati izradu i odrediti vrijeme čuvanja operativnih i sistemskih zapisa koji će omogućiti rekonstruiranje događaja, otkrivanje neovlaštenih pristupa i radnji na informacijskom sustavu, identificiranje problema te utvrđivanje odgovornosti.

Članak 21.

Kreditna institucija je dužna zaštititi resurse informacijskog sustava od malicioznoga programskog kôda primjenom odgovarajućih upravljačkih, logičkih i fizičkih kontrola.

VIII. ODRŽAVANJE INFORMACIJSKOG SUSTAVA

Članak 22.

(1) Kreditna je institucija dužna uspostaviti proces upravljanja hardverskom imovinom informacijskog sustava tijekom njezina životnog ciklusa.

(2) Proces upravljanja hardverskom imovinom mora obuhvatiti postupke detektiranja, evidentiranja, raspolaganja, praćenja, obnavljanja i odlaganja te imovine.

Članak 23.

(1) Kreditna je institucija dužna uspostaviti proces upravljanja promjenama softverskih komponenata informacijskog sustava koji obuhvaća barem sljedeće postupke:

a) utvrđivanje početnih inačica softverskih komponenata informacijskog sustava,

b) identifikacija i praćenje svih programskih promjena aplikacijskog softvera koji podržava pružanje bankovnih i financijskih usluga,

c) identifikacija i praćenje svih promjena arhitekture baza podataka koje podržavaju pružanje bankovnih i financijskih usluga i

d) identifikacija i praćenje promjena svih ostalih softverskih komponenata informacijskog sustava koje utječu ili mogu utjecati na funkcionalnost i/ili sigurnost informacijskog sustava.

(2) Promjene softverskih komponenata informacijskog sustava moraju biti evidentirane i dokumentirane onim slijedom kako su nastajale zajedno s vremenom nastanka promjene.

(3) Sve promjene softverskih komponenata informacijskog sustava prije uvođenja u produkcijski rad potrebno je na odgovarajući način testirati i odobriti.

Članak 24.

Kreditna je institucija dužna definirati postupke izrade, pohrane, održavanja i čuvanja dokumentacije koja se odnosi na informacijski sustav te osigurati da je dokumentacija točna, potpuna i ažurna.

Članak 25.

Kreditna institucija je dužna osigurati primjereno i kontinuirano stručno obrazovanje i osposobljavanje svih zaposlenika kreditne institucije koji se koriste informacijskim sustavom.

IX. UPRAVLJANJE KONTINUITETOM POSLOVANJA

Članak 26.

Na proces upravljanja kontinuitetom poslovanja primjenjuju se odredbe Odluke o upravljanju rizicima (»Narodne novine«, br. 1/2009., 41/2009., 75/2009. i 2/2010.) osim ako ovom Odlukom nije drugačije propisano.

Članak 27.

Osim obveza propisanih Odlukom o upravljanju rizicima u okviru upravljanja kontinuitetom poslovanja kreditna institucija dužna je:

a) donijeti plan(ove) oporavka informacijskog sustava koji će omogućiti oporavak i raspoloživost resursa informacijskog sustava potrebnih za odvijanje kritičnih i/ili ključnih poslovnih procesa u zahtijevanom vremenu te

b) periodično i nakon značajnih promjena u poslovnim procesima ili na informacijskom sustavu na odgovarajući način testirati plan(ove) oporavka informacijskog sustava te sastaviti pisana izvješća o rezultatima testiranja.

Članak 28.

Kreditna institucija je dužna uspostaviti proces upravljanja incidentima koji će omogućiti pravodoban i učinkovit odgovor u slučaju narušavanja sigurnosti i funkcionalnosti resursa informacijskog sustava koji podržavaju odvijanje poslovnih procesa.

Članak 29.

Kreditna institucija je dužna u slučaju težih incidenata u primjerenom roku od nastanka incidenta obavijestiti Hrvatsku narodnu banku o incidentu, njegovu učinku i poduzetim radnjama.

Članak 30.

(1) Kreditna institucija je dužna uspostaviti proces upravljanja pričuvnom pohranom koji obuhvaća postupke izrade, pohrane i testiranja pričuvnih kopija podataka te restauracije podataka s pričuvnih kopija podataka kako bi se osigurala raspoloživost podataka u slučaju potrebe te omogućio oporavak odnosno ponovna uspostava kritičnih i/ili ključnih poslovnih procesa u zahtijevanom vremenu.

(2) Pričuvne kopije podataka moraju biti ažurne i pohranjene na primjeren način na jednoj ili više lokacija, od kojih najmanje jedna mora biti, u skladu s procjenom rizika, dovoljno udaljena od lokacije na kojoj se nalaze izvorni podaci (od kojih su izrađene pričuvne kopije podataka).

Članak 31.

Kreditna institucija je dužna, u skladu s procjenom rizika i procijenjenim utjecajem neraspoloživosti pojedinih procesa odnosno resursa informacijskog sustava potrebnih za odvijanje tih procesa na poslovanje kreditne institucije, osigurati raspoloživost pričuvnoga računalnog centra s odgovarajućom opremljenošću, funkcionalnošću i razinom sigurnosti koji je na odgovarajućoj udaljenosti od primarnoga računalnog centra.

X. RAZVOJ INFORMACIJSKOG SUSTAVA

Članak 32.

Kreditna institucija je dužna definirati načine, kriterije i postupke razvoja informacijskog sustava, pri čemu treba uzeti u obzir funkcionalne i sigurnosne aspekte.

Članak 33.

Kreditna institucija je dužna uspostaviti proces razvoja informacijskog sustava u skladu s donesenom metodologijom upravljanja projektima.

Članak 34.

Kreditna institucija je dužna, u sklopu procesa razvoja informacijskog sustava unutar kreditne institucije, uspostaviti i dokumentirati proces programskog razvoja i isporuke informacijskog sustava koji obuhvaća postupke analize i projektiranja, programiranja, testiranja te uvođenja u produkcijski rad.

Članak 35.

Kreditna institucija je dužna osigurati da sve razvijene softverske komponente informacijskog sustava kao i nove hardverske komponente informacijskog sustava prije uvođenja u produkcijski rad budu na odgovarajući način testirane i odobrene.

Članak 36.

Kreditna institucija je dužna na odgovarajući način razdvojiti razvojnu, testnu i produkcijsku okolinu.

XI. ELEKTRONIČKO BANKARSTVO

Članak 37.

(1) Kreditna institucija je dužna primijeniti sigurne i učinkovite autentifikacijske metode za potvrdu identiteta i ovlasti osoba, procesa i sustava.

(2) Autentifikacija osoba mora uključivati kombinaciju najmanje dvaju načina potvrđivanja korisničkog identiteta, gdje je god to moguće primijeniti.

Članak 38.

Kreditna institucija je dužna osigurati odgovarajuću potvrdu svog identiteta na distribucijskom kanalu elektroničkog bankarstva kako bi korisnici elektroničkog bankarstva mogli provjeriti identitet i izvornost kreditne institucije.

Članak 39.

Kreditna institucija je dužna osigurati postojanje odgovarajućih operativnih i sistemskih zapisa kako bi se osigurale neporecivost i dokazivost radnji povezanih s elektroničkim bankarstvom.

XII. PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 40.

Na dan stupanja na snagu ove Odluke prestaje važiti Odluka o primjerenom upravljanju informacijskim sustavom (»Narodne novine«, br. 80/2007.).

Članak 41.

Ova Odluka objavljuje se u »Narodnim novinama« i stupa na snagu 31. ožujka 2010., osim članka 23. stavka 1., članka 26., članka 27., članka 30. stavka 1. i članka 31., koji stupaju na snagu 1. srpnja 2010.

O. br.: 139-020/03-10/ŽR

Zagreb, 17. ožujka 2010.

Guverner

Hrvatske narodne banke

dr. sc. ŽeljkoRohatinski, v. r.