Na temelju članka 68. stavka 3. Zakona o bankama ("Narodne novine", br. 84/2002. i 141/2006.) i članka 39. stavka 2. pod i) Zakona o Hrvatskoj narodnoj banci ("Narodne novine", br. 36/2001. i 135/2006.) guverner Hrvatske narodne banke donio je

ODLUKU
O PRIMJERENOM UPRAVLJANJU INFORMACIJSKIM SUSTAVOM

I. Opće odredbe

Članak 1.

Ovom se Odlukom uređuju zahtjevi Hrvatske narodne banke koji se odnose na upravljanje informacijskim sustavom banaka (uključujući i stambene štedionice).

II. Značenje pojmova

Članak 2.

U smislu ove odluke:

Softverske komponente (softverska imovina)

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

Hardverske komponente (hardverska imovina)

(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).

Informacijska imovina

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

Informacijska tehnologija

(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.

Informacijski sustav

(5) Informacijski je sustav 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.

Korisnici informacijskog sustava

(6) Korisnici informacijskog sustava jesu sve osobe koje se koriste informacijskim sustavom (zaposlenici banke ili stambene štedionice, zaposlenici pružatelja usluga, korisnici elektroničkog bankarstva, zaposlenici pravnih osoba koji se koriste informacijskim sustavom banke ili stambene štedionice itd.).

Rizik informacijskog sustava

(7) Rizik informacijskog sustava je rizik koji proizlazi iz korištenja informacijske tehnologije odnosno informacijskog sustava.

Resursi informacijskog sustava

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

Svojstva informacija i procesa

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

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

(11) Raspoloživost je svojstvo informacija i procesa koje omogućuje pristup i upotrebljivost tih informacija i procesa, tj. njihovu dostupnost na zahtjev ovlaštenog subjekta.

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

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

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

(15) Pouzdanost je svojstvo dosljednoga, očekivanog ponašanja i rezultata.

Kontrole

(16) Kontrole se dijele na upravljačke, logičke i fizičke.

(17) Upravljačke kontrole uključuju donošenje internih akata vezanih uz informacijski sustav i uspostavljanje odgovarajuće organizacijske strukture te osiguravaju primjenu internih akata vezanih uz informacijski sustav u cilju osiguravanja funkcionalnosti i sigurnosti informacijskog sustava.

(18) Logičke kontrole su kontrole implementirane na softverskim komponentama informacijskog sustava.

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

Upravljanje korisničkim pravima pristupa

(20) Evidentiranje je proces definiranja novih korisnika informacijskog sustava.

(21) Autorizacija je proces dodjele prava pristupa korisnicima informacijskog sustava.

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

(23) Nadzor korisničkih prava pristupa jest proces koji uključuje praćenje, izmjenu i revidiranje prava pristupa korisnika informacijskog sustava.

Načini potvrđivanja korisničkog identiteta

(24) Korisnički identitet moguće je potvrditi korištenjem jednoga ili kombinacijom sljedećih načina:

a) pomoću nečega što samo korisnik zna (primjerice zaporka, PIN, kriptografski ključ)
b) pomoću nečega što samo korisnik posjeduje (primjerice magnetska kartica, čip kartica, "token")
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).

Povlašteni pristup informacijskom sustavu

(25) Povlašteni pristup resursima informacijskog sustava (engl. *administrative access*) jest onaj pristup resursima informacijskog sustava koji je omogućen korisnicima informacijskog sustava koji imaju velike ovlasti koje im omogućuju zaobilaženje ugrađenih logičkih kontrola.

(26) Korisnici informacijskog sustava s pravima povlaštenog pristupa, među ostalim, jesu administratori baza podataka, administratori mrežne opreme, administratori sistemskog softvera i administratori aplikacijskog softvera.

Udaljeni pristup informacijskom sustavu

(27) Udaljeni pristup resursima informacijskog sustava banke je pristup tim resursima s udaljene lokacije pomoću telekomunikacijske infrastrukture nad kojom banka nema potpunu kontrolu ili nadzor.

Operativni i sistemski zapisi

(28) 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).

(29) 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 radnja provedenih na informacijskom sustavu
d) identifikaciju problema.

Maliciozni programski kôd

(30) 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 malicioznoga programskog kôda su računalni crvi i virusi te "trojanski konji".

Elektroničko bankarstvo

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

(32) Elektroničko bankarstvo uključuje sustave koji klijentima banke pružaju bankarske proizvode i usluge (primjerice pristup financijskim informacijama, informiranje o proizvodima i uslugama, elektroničko plaćanje i elektronički novac).

Eksternalizacija

(33) Eksternalizacija (odnosno izdvajanje dijela poslovanja) jest korištenje usluga koje čine sastavni dio poslovnih procesa banke, a koje na temelju ugovora banci pružaju pružatelji usluga na kontinuiranoj osnovi i kojima se podržava pružanje bankovnih, financijskih i/ili pomoćnih bankovnih usluga od strane same banke.

(34) Eksternalizacija aktivnosti vezanih uz informacijski sustav banke smatra se eksternalizacijom (dijela) informacijskog sustava.

(35) Postupak nabave robe i ugovor(i) o nabavi robe (primjerice o nabavi informacijske imovine te hardverskih i softverskih komponenata) ne smatraju se eksternalizacijom.

Incident

(36) Incident je svaki neplanirani i neželjeni događaj koji može narušiti sigurnost i funkcionalnost resursa informacijskog sustava koji podržavaju odvijanje poslovnih procesa banke.

Zahtijevano vrijeme oporavka

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

Kritični i/ili vitalni poslovni procesi

(38) Kritični i/ili vitalni poslovni procesi su oni poslovni procesi koje je banka identificirala kao takve te čija nedostupnost može ozbiljnije ugroziti odnosno narušiti poslovanje banke.

Pričuvne kopije podataka

(39) Pričuvne kopije podataka su pričuvne inačice podataka (informacijska imovina i softverske komponente) koje su potrebne za ponovno uspostavljanje (oporavak) poslovnih procesa banke te ostalih podataka za koje banka procijeni da ih je potrebno pričuvno pohraniti**.**

III. Okvir za upravljanje informacijskim sustavom

Članak 3.

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

Članak 4.

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

Članak 5.

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

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

Članak 6.

Uprava banke dužna je donijeti interne akte kojima se uređuje upravljanje informacijskim sustavom te definirati odgovornosti za nadzor nad provođenjem tih akata.

Članak 7.

Uprava banke dužna je osigurati da svi korisnici informacijskog sustava budu upoznati s internim aktima vezanima uz informacijski sustav ili njihovim sadržajem u skladu s dodijeljenim ovlaštenjima te potrebama korisnika informacijskog sustava.

Članak 8.

Banka je dužna definirati kriterije, načine i postupke izvješćivanja uprave i nadzornog odbora banke o relevantnim činjenicama vezanima uz funkcionalnost i sigurnost informacijskog sustava.

Članak 9.

Uprava banke 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 banke 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 banke.

Članak 11.

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

IV. Upravljanje rizikom informacijskog sustava

Članak 12.

(1) Banka je dužna uspostaviti proces upravljanja rizikom informacijskog sustava koji obuhvaća procjenu rizika, ovladavanje rizikom (poduzimanje radnja za svođenje rizika na prihvatljivu razinu) te kontinuirano praćenje i održavanje prihvatljive razine rizika.

(2) Banka je dužna usvojiti metodologiju upravljanja rizikom informacijskog sustava kojom će se definirati kriteriji, načini i postupci upravljanja rizikom informacijskog sustava.

(3) Banka je dužna dokumentirati rezultate procjene rizika informacijskog sustava u obliku formalnog izvješća.

Članak 13.

Uprava banke odgovorna je za određivanje prihvatljive razine rizika kojemu je izložen informacijski sustav.

Članak 14.

Banka 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 banke.

Članak 15.

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

V. Unutarnja revizija

Članak 16.

Unutarnja revizija dužna je obavljati reviziju informacijskog sustava banke.

Članak 17.

Banka je dužna usvojiti metodologiju za provođenje revizije informacijskog sustava zasnovanu na procjeni rizika, a kojom se definiraju kriteriji, načini i postupci revizije informacijskog sustava banke.

VI. Sigurnost informacijskog sustava

Članak 18.

Banka je dužna usvojiti interni akt koji će biti okvir za upravljanje sigurnošću informacijskog sustava (u daljnjem tekstu: politika sigurnosti informacijskog sustava) te definirati odgovornosti koje se odnose na područje sigurnosti informacijskog sustava.

Članak 19.

Banka 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 20.

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

Članak 21.

Banka 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 radnja na informacijskom sustavu, identificiranje problema te utvrđivanje odgovornosti.

Članak 22.

Banka je dužna zaštiti resurse informacijskog sustava od malicioznoga programskog kôda primjenom odgovarajućih upravljačkih, logičkih i fizičkih kontrola.

VII. Održavanje informacijskog sustava

Članak 23.

(1) Banka je 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 24.

(1) Banka je 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 koje podržavaju pružanje bankovnih, financijskih i/ili pomoćnih bankovnih usluga
c) identifikacija i praćenje svih promjena arhitekture baza podataka koje podržavaju pružanje bankovnih, financijskih i/ili pomoćnih bankovnih usluga
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 25.

Banka je 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 26.

Banka je dužna osigurati primjerenu i kontinuiranu izobrazbu svih zaposlenika banke koji se koriste informacijskim sustavom.

VIII. Upravljanje kontinuitetom poslovanja

Članak 27.

Banka je dužna uspostaviti proces planiranja kontinuiteta poslovanja kako bi osigurala postojanost kritičnih i/ili vitalnih poslovnih procesa. U sklopu procesa planiranja kontinuiteta poslovanja banka je dužna:

a) izraditi i dokumentirati analizu utjecaja na poslovanje koja će odrediti utjecaj neraspoloživosti pojedinih poslovnih procesa odnosno resursa informacijskog sustava potrebnih za odvijanje tih procesa na poslovanje banke
b) usvojiti plan(ove) kontinuiteta poslovanja koji će omogućiti ponovnu uspostavu kritičnih i/ili vitalnih poslovnih procesa u zahtijevanom vremenu oporavka te ograničiti i smanjiti gubitke koji mogu nastati kao posljedica narušavanja ili prekida poslovnih procesa
c) usvojiti plan(ove) oporavka informacijskog sustava koji će omogućiti oporavak i raspoloživost resursa informacijskog sustava potrebnih za odvijanje kritičnih i/ili vitalnih poslovnih procesa u zahtijevanom vremenu
d) periodično i nakon značajnih promjena u poslovnim procesima ili na informacijskom sustavu na odgovarajući način testirati plan(ove) kontinuiteta poslovanja i plan(ove) oporavka informacijskog sustava te sastaviti pisana izvješća o rezultatima testiranja.

Članak 28.

Banka 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.

Banka 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) Banka 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 vitalnih 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.

Banka je dužna, u skladu s procjenom rizika i na osnovi rezultata analize utjecaja na poslovanje, osigurati raspoloživost pričuvnoga računalnog centra s odgovarajućom opremljenošću, funkcionalnošću i razinom sigurnosti koji je na odgovarajućoj udaljenosti od primarnoga računalnog centra.

IX. Razvoj informacijskog sustava i eksternalizacija

Članak 32.

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

Članak 33.

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

Članak 34.

Banka je dužna, u sklopu procesa razvoja informacijskog sustava unutar banke, 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.

Banka 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.

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

Članak 37.

Prije donošenja odluke o eksternalizaciji banka je dužna utvrditi omogućuje li zakonodavstvo odnosno propisi države u kojima pružatelj usluga posluje Hrvatskoj narodnoj banci da ostvari cjelovit i neograničen pristup djelatnostima i poslovima u svezi s kojima Hrvatska narodna banka obavlja nadzor.

Članak 38.

Izravni nadzor od strane Hrvatske narodne banke u odnosu na pružanje usluga na teritoriju Republike Hrvatske i izvan njega od strane pružatelja usluga rezidenata ili nerezidenata ne smije ni na koji način i ni u kojem trenutku biti onemogućen, ograničen ili otežan.

Članak 39.

Prije donošenja odluke o eksternalizaciji (dijela) informacijskog sustava banka je dužna procijeniti rizik eksternalizacije.

Članak 40.

Banka je dužna kontinuirano nadzirati način i kvalitetu pružanja ugovorenih usluga.

X. Elektroničko bankarstvo

Članak 41.

(1) Banka 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 42.

Banka je dužna osigurati odgovarajuću potvrdu svog identiteta na distribucijskom kanalu elektroničkog bankarstva kako bi korisnici elektroničkog bankarstva mogli provjeriti identitet i izvornost banke.

Članak 43.

Banka je dužna osigurati postojanje odgovarajućih operativnih i sistemskih zapisa kako bi se osigurala neporecivost i dokazivost radnja povezanih s elektroničkim bankarstvom.

XI. Prijelazne i završne odredbe

Članak 44.

Ova odluka stupa na snagu **1. siječnja 2008.,** osim odredbi sljedećih članaka:

(1) Odredbe čl. 4., čl. 5. stavka 1., čl. 10., čl. 22., čl. 24. stavka 3., čl. 25., čl. 26., čl. 29. te čl. 30. stavka 2. stupaju na snagu **1. srpnja 2008.**

(2) Odredbe čl. 5. stavka 2., čl. 6., čl. 7., čl. 9, čl. 11., čl. 12. stavka 1. i 2., čl. 13., čl. 16., čl. 17., čl. 18., čl. 20., čl. 23., čl. 24. stavka 2., čl. 35., čl. 36., čl. 40., čl. 41., čl. 42. te čl. 43. stupaju na snagu **1. siječnja 2009.**

(3) Odredbe čl. 12. stavka 3., čl. 14., čl. 19., čl. 28., čl. 32., čl. 33. i čl. 34. stupaju na snagu **1. srpnja 2009.**

(4) Odredbe čl. 15. i čl. 21. stupaju na snagu **1. siječnja 2010.**

(5) Odredbe čl. 24. stavka 1., čl. 27., čl. 30. stavka 1. i čl. 31. stupaju na snagu **1. srpnja 2010.**

O. br. 502-020/07-07/ŽR

Zagreb, 17. srpnja 2007.

Guverner
Hrvatske narodne banke

dr. sc. Željko Rohatinski