BOSNA I HERCEGOVINA
FEDERACIJA BOSNE I HERCEGOVINE
AGENCIJA ZA BANKARSTVO FEDERACIJE BOSNE I HERCEGOVINE

Sarajevo, 15.08.2011. godine

Predmet: Nacrt Odluke iz oblasti upravljanja informacionim sistemima u bankama

Agencija za bankarstvo FBiH je izradila nacrt Odluke o minimalnim standardima upravljanja informacionim sistemima u bankama.

Svoje komentare i sugestije možete dostaviti na email agencija@fba.ba najkasnije do 04.09.2011. godine

Ured FBA za informisanje

71000 Sarajevo, Koševo br.3, Bosna i Hercegovina
Tel: ++387 33 72 14 00, Fax: ++387 33 66 88 11
E-mail: agencija@fba.ba
Web site: www.fba.ba

Na osnovu člana 4., 9. i 25. Zakona o Agenciji za bankarstvo Federacije Bosne i Hercegovine („Službene novine Federacije BiH“, broj 9/96, 27/98, 20/00, 45/00, 58/02, 13/03, 19/03, 47/06, 59/06 i 48/08), člana 38. stav 1. i člana 69. stav 3. Zakona o bankama („Službene novine Federacije BiH“, broj 39/98, 32/00, 48/01, 27/02, 41/02, 58/02, 13/03, 19/03 i 28/03) i člana 18. Statuta Agencije za bankarstvo Federacije Bosne i Hercegovine („Službene novine Federacije BiH“, broj 42/04), Upravni odbor Agencije za bankarstvo Federacije Bosne i Hercegovine na sjednici održanoj dana _____ donosi

O D L U K U
O MINIMALNIM STANDARDIMA
UPRAVLJANJA INFORMACIONIM SISTEMIMA U BANKAMA

Opće odredbe

Član 1.

Ovom Odlukom utvrđuju se minimalni standardi i kriteriji koje je banka dužna da osigura i provodi u procesu upravljanja informacionim sistemima u bankama.

Definicije

Član 2.

Definicije koje se koriste u ovoj Odluci imaju slijedeća značenja:

Autentičnost – osobina koja osigurava da je identitet lica zaista onaj za koji se tvrdi da jeste.

Autentifikacija – proces potvrde identiteta korisnika/procesa od strane sistema.

Autorizacija – proces dodjele prava pristupa ili drugih prava korisniku, programu ili procesu.

Backup – kopija originalnih podataka (informacijska imovina i software-ske komponente) koji su potrebni za ponovno uspostavljanje poslovnih procesa banke, te ostalih podataka za koje banka procjeni da ih je potrebno čuvati.

Dokazivost – osobina koja osigurava da aktivnosti lica mogu biti praćene jedinstveno do samog lica.

Dostupnost – osobina da informacija bude dostupna i iskoristiva na zahtjev od strane ovlaštenog lica.

Elektronsko bankarstvo – sistem koji omogućava klijentima banke obavljanje bankarskih poslova sa udaljene lokacije putem javnih komunikacionih mreža ili sl.

Evidentiranje korisničkih prava pristupa – proces dodjele prava pristupa korisnicima informacionog sistema.

Hardware – fizičke komponente informacionog sistema koje uključuju: računare i računarsku opremu, komunikacijsku opremu, medije za čuvanje podataka, te ostalu tehničku opremu koja podržava rad informacionog sistema.

Identifikacija i autentifikacija – procesi identifikacije korisnika informacionog sistema i potvrde njegova identiteta prilikom prijave i tokom provođenja radnji na informacionom sistemu.

Incident – neželjeni odnosno neočekivani događaj koji ugrožava povjerljivost, integritet, dokazivost ili dostupnost informacija i informacionog sistema.

Informacioni sistem – sveobuhvatan skup resursa organizovan u svrhu prikupljanja, spremanja, obrade, održavanja, korištenja, distribucije i raspolaganja informacijama.

Informacijska imovina – podaci u bazama podataka, datoteke sa podacima, programski kod, sistemska i aplikacijska dokumentacija, korisnička dokumentacija, planovi i slično.

Informacijska tehnologija – hardware, software, komunikacije i drugi uređaji koji se koriste za unos, spremanje, procesiranje (obradu), prenos i izlaz podataka, u bilo kojem obliku.

Integritet – osobina zaštite tačnosti i kompletnosti (cjelovitosti) imovine.

Interna kontrola – proces uspostavljen sa svrhom sticanja razumnog uvjerenja o pouzdanosti informacionog sistema, usklađenosti sa zakonima i regulativom, efektivnosti i efikasnosti operacija i zaštite imovine.

Kontrole – politike, procedure, prakse, tehnologije i organizacione strukture dizajnirane kako bi obezbjedile razumno uvjerenje da će poslovni ciljevi biti dostignuti i da će neželjeni događaji biti spriječeni ili detektovani. Kontrole se dijele na upravljačke, logičke i fizičke. **Upravljačke kontrole** uključuju donošenje internih akata vezanih uz informacioni sistem i uspostavljanje odgovarajuće organizacijske strukture, te osiguravaju primjenu internih akata vezanih uz informacioni sistem u cilju osiguravanja funkcionalnosti i sigurnosti informacionog sistema. **Logičke kontrole** su kontrole implementirane na software-skim komponentama. **Fizičke kontrole** su kontrole koje štite resurse informacionog sistema od neovlaštenog fizičkog pristupa, krađe, fizičkog oštećenja ili uništenja.

Korisnici informacionog sistema – sva lica koja koriste informacioni sistem (uposlenici banke, uposlenici pružaoca usluga, korisnici elektronskog bankarstva, uposlenici pravnih lica koji koriste informacioni sistem banke i dr).

Korisnički identitet – identitet koji je moguće potvrditi korištenjem jednoga ili kombinacijom sljedećih načina:

1. pomoću nečega što samo korisnik zna (na primjer lozinka, PIN, kriptografski ključ)
2. pomoću nečega što samo korisnik posjeduje (na primjer magnetna kartica, čip kartica, token)

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

Kritični/vitalni procesi – poslovne aktivnosti ili informacije koje ne mogu biti prekinute ili nedostupne, a da značajno ne ugroze poslovanje banke.

Maliciozni kod – bilo koji oblik programskog koda dizajniran sa namjerom da se pristupi, uništi ili prikupi informacija iz informacionog sistema, bez znanja i odobrenja vlasnika.

Nadzor korisničkih prava pristupa – proces koji uključuje praćenje, izmjenu i reviziju prava pristupa korisnika informacijskog sistema**.**

Neporecivost – osobina koja osigurava nemogućnost poricanja izvršene aktivnosti ili primanja informacija (podataka).

Operativni i sistemski zapisi – hronološki zapisi o aktivnostima na resursima informacionog sistema (zapisi operativnih sistema, aplikacijskog software-a, baza podataka, mrežnih uređaja i sl).

Pouzdanost – osobina dosljednosti, očekivanog ponašanja i rezultata.

Povjerljivost – osobina da informacija nije dostupna ili otkrivena neovlaštenim licima ili procesima.

Povlašteni pristup – pristup resursima informacionog sistema koji omogućava korisnicima znatno veća prava te zaobilaženje ugrađenih logičkih kontrola (administrator mrežne opreme, baze podataka, sistemskog software-a, aplikativnog software-a i sl.)

Raspoloživost – svojstvo imovine da je dostupna i upotrebljiva na zahtjev ovlaštenog lica.

Resursi informacionog sistema – resursi koji uključuju informacijsku imovinu, software-ske i hardware-ske komponente, ljude i procese.

Rizik informacionog sistema – rizik koji proizilazi iz korištenja informacijske tehnologije odnosno informacionog sistema.

Sigurnost informacija – osigurava da samo ovlašteni korisnici (povjerljivost) imaju pristup tačnim i kompletnim informacijama (integritet) kada je potrebno (dostupnost).

Skrbnik – lica i/ili odjeli odgovorni za skladištenje i zaštitu podataka, kao i implementaciju odgovarajućih kontrola.

Software – programi i prateća dokumentacija koja omogućava i olakšava korištenje računara, uključujući aplikacijski software, sistemski software, baze podataka i slično.

Udaljeni pristup – omogućava pristup resursima informacionog sistema sa udaljene lokacije putem telekomunikacionih linija nad kojima banka nema potpunu kontrolu odnosno nadzor.

Vlasnik – lica i/ili odjeli kojoj je odobrena upravljačka odgovornost za produkciju, razvoj, održavanje, korištenje i zaštitu imovine.

Okvir za upravljanje informacionim sistemom

Član 3.

Banka je dužna uspostaviti, implementirati, nadzirati, održavati, redovno revidirati i poboljšavati proces upravljanja informacionim sistemom u cilju smanjenja izloženosti rizicima, osiguranja povjerljivosti, integriteta i dostupnosti informacija i cjelokupnog informacionog sistema, primjereno veličini, složenošću i obimu poslovanja banke te kompleksnošću informacionog sistema.

Nadzorni odbor

Član 4.

Nadzorni odbor banke je dužan i odgovoran, kao minimum, da:

1. na osnovu prijedloga uprave, donosi strategiju informacionog sistema, koja treba biti sastavni dio ukupne poslovne strategije banke
2. na osnovu prijedloga uprave, donosi politike za upravljanje informacionim sistemom, a posebno politiku sigurnosti informacionog sistema i nadzire njihovu implementaciju
3. aktuelizira usvojene politike u skladu sa promjenama ekonomskih, tržišnih, tehnoloških i drugih uslova
4. donosi odluke (odluku) o uspostavi, praćenju efikasnosti i unaprijeđivanju sistema za mjerenje, praćenje, kontrolu i upravljanje rizicima vezanim za sigurnost informacionog sistema
5. donese i osigura uspostavu adekvatne organizacione strukture i uspostavu odgovarajućih funkcija i ovlasti kako bi obezbjedila efikasno i sigurno upravljanje informacionim sistemom
6. obezbjedi selekciju i imenovanje kvalifikovanog i kompetentnog člana uprave koji će biti nadležan za uspostavu i nadzor procesa upravljanja informacionim sistemom
7. na osnovu prijedloga uprave, propiše sadržaj i periodičnost izvještavanja uprave i nadzornog odbora banke o relevantnim činjenicama vezanim uz upravljanje informacionim sistemom
8. osigura da su upravljačke kontrole informacionog sistema, kao i sistem internih kontrola informacionog sistema pod stalnim nadzorom interne i povremenim nadzorom eksterne revizije
9. obezbjedi jasne i vidljive potpore inicijativama vezanim uz upravljanje informacionim sistemom.

Uprava banke

Član 5.

Uprava banke je dužna i odgovorna, kao minimum, da:

1. imenuje odbor za upravljanje informacionim sistemom, sastavljen od predstavnika različitih poslovnih funkcija, koji će se sastajati periodično i izvještavati upravu o svojim aktivnostima, a čija uloga treba biti koordinacija inicijativa i praćenje razvojnih aktivnosti informacionog sistema, kao i usklađenosti ciljeva informacionog sistema sa poslovnim ciljevima i poslovnom strategijom banke
2. uspostavi i implementira politike i procedure upravljanja informacionim sistemom u skladu sa poslovnim ciljevima i poslovnom strategijom banke

3. implementira sistem za mjerenje, praćenje, kontrolu i upravljanje rizicima vezanim za informacioni sistem
4. osigura da su sve dužnosti vezane uz upravljanje informacionim sistemom jasno definisane i dodijeljene
5. inicira plan i program za uspostavu i podizanje svijesti o sigurnosti informacionog sistema
6. obezbjedi potrebne resurse za upravljanje informacionim sistemom
7. usvoji metodologiju kojom će se definisati kriteriji, načini i postupci upravljanja rizicima koji proizilaze iz upotrebe informacionog sistema, te odredi odgovornosti upravljanja rizicima i prihvatljive nivoe rizika
8. identificira i procjeni rizike, poduzme korake za smanjenje rizika na prihvatljiv nivo, te donese odluku o prihvatanju preostalih rizika
9. kontinuirano analizira rizike informacionog sistema, te najmanje jednom godišnje, dostavlja pisani izvještaj o rezultatima procjene rizika
10. usvoji i primjeni metodologiju upravljanja projektima kojom će se definisati kriteriji, načini i postupci upravljanja projektima vezanim uz informacioni sistem.

Strategija informacionog sistema

Član 6.

Banka je dužna razviti i nadzirati implementaciju strategije informacionog sistema koja, kao minimum, treba da:

1. obuhvati dugoročne i kratkoročne inicijative vezane za informacioni sistem
2. definiše povezanost i usklađenost ciljeva informacionog sistema sa poslovnim ciljevima banke
3. se detaljnije razradi kroz donošenje strateških i operativnih planova.

Politika sigurnosti informacionog sistema

Član 7.

Banka je dužna usvojiti i implementirati politiku sigurnosti informacionog sistema, koja predstavlja temelj za upravljanje sigurnošću informacionog sistema banke, i koja kao minimum treba da:

1. sadrži načela i principe upravljanja sigurnošću resursa informacionog sistema
2. definiše odgovornosti koje se odnose na područje upravljanja sigurnošću informacionog sistema
3. obuhvati područja upravljačke, logičke i fizičke zaštite resursa informacionog sistema, u skladu sa veličinom i kompleksnošću informacionog sistema.

Interna akta

Član 8.

(1) Banka je dužna propisati i primjeniti detaljne procedure kojima se uređuje upravljanje informacionim sistemom, te osigurati provođenje tih procedura.

(2) Interni akti trebaju, kao minimum, biti:
   1. usklađeni sa propisima, standardima i pravilima struke
   2. redovno pregledani i ažurirani
   3. potpuni, detaljni i primjenjivi.

(3) Potrebno je osigurati da su svi korisnici informacionog sistema upoznati sa sadržajem internih akata, vezanih uz informacioni sistem, u skladu sa potrebama svakog korisnika.

(4) Ugovori, nalazi revizije, uputstva i ostali dokumenti trebaju biti sačinjeni odnosno prevedeni na jedan od jezika u zvaničnoj upotrebi u Bosni i Hercegovini.

Upravljanje rizicima iz ugovornih odnosa

Član 9.

Banka je dužna kontinuirano procjenjivati i adekvatno upravljati rizicima koji proizilaze iz ugovornih odnosa sa pravnim i fizičkim licima, a čije su aktivnosti vezane uz informacioni sistem banke.

Organizacija funkcije upravljanja informacionim sistemom

Član 10.

(1) Banka je dužna adekvatno pozicionirati funkciju upravljanja informacionim sistemom u svojoj organizacionoj strukturi, te uspostaviti njenu odgovarajuću strukturu i veličinu.

(2) Banka je dužna u okviru specifikacije svake radne pozicije detaljno navesti opis posla, stručne kvalifikacije, odgovornosti i potrebne kompetencije.

Odgovorno lice za sigurnost informacionog sistema

Član 11.

Uprava banke dužna je imenovati odgovorno lice (voditelj/oficir) za funkciju sigurnosti informacionog sistema, te definisati njegova ovlaštenja, odgovornosti i obim rada. Funkcija sigurnosti informacionog sistema treba biti neovisna o funkciji organizacijske jedinice za upravljanje informacionim sistemom. Lice odgovorno za sigurnost informacionog sistema treba biti kompetentna osoba sa dovoljno znanja i iskustva.

Član 12.

Odgovorno lice za sigurnost informacionog sistema treba, kao minimum, da nadzire i koordinira aktivnosti vezane uz sigurnost informacionog sistema, te da redovno izvještava upravu banke o stanju i aktivnostima vezanim uz sigurnost informacionog sistema.

Interna revizija

Član 13.

(1) Banka je dužna sprovoditi internu reviziju informacionog sistema u skladu sa Odlukom o minimalnim standardima interne i eksterne revizije u bankama, a na osnovu definisanog programa rada interne revizije.

(2) Lica koja obavljaju internu reviziju informacionog sistema banke trebaju posjedovati stručna znanja i vještine o informacionim sistemima.

(3) U slučaju eksternalizacije aktivnosti interne revizije informacionog sistema, banka treba osigurati da pružalac usluga interne revizije informacionog sistema istovremeno ne pruža usluge eksterne revizije informacionog sistema banci, te treba osigurati da ne postoji sukob interesa u skladu sa profesijom interne revizije.

Eksterna revizija

Član 14.

(1) Banka je dužna Agenciji podnijeti zahtjev za izdavanje odobrenja za imenovanje nezavisnog eksternog revizora za reviziju informacionog sistema.

(2) Banka je dužna, uz zahtjev iz st. (1) ovog člana, dostaviti Agenciji slijedeće dokumente:
1. nacrt odluke o imenovanju nezavisnog eksternog revizora informacionog sistema
2. nacrt ugovora ili pisma namjere sa eksternim revizorom
3. reference eksternog revizora o obavljenim revizijama informacionih sistema
4. stručne kvalifikacije lica koja će obavljati reviziju.

(3) Agencija će rješenje po zahtjevu za izdavanje odobrenja za izbor nezavisnog eksternog revizora donijeti u roku od 30 dana od dana prijema zahtjeva sa kompletnom dokumentacijom.

(4) Nadzorni odbor banke dužan je donijeti odluku o imenovanju nezavisnog eksternog revizora za reviziju informacionog sistema, po dobijanju odobrenja od Agencije, te sa izabranim revizorom potpisati ugovor o izradi izvještaja o reviziji informacionog sistema. Banka je dužna Agenciji dostaviti usvojenu odluku o izboru nezavisnog eksternog revizora i potpisani ugovor sa izabranim nezavisnim eksternim revizorom, u roku od 10 dana od dana usvajanja odnosno potpisivanja.

(5) Eksterni revizor je dužan sačiniti revizorski izvještaj o obavljenoj reviziji informacionog sistema i pismo upravi.

(6) Izvještaj o obavljenoj reviziji informacionog sistema je poseban izvještaj koji usvaja nadzorni odbor banke i dostavlja Agenciji odmah po usvajanju istog.

(7) Reviziju informacionog sistema treba obavljati periodično:
1. obavezno jednom u roku od godinu dana od dana stupanja na snagu ove odluke
2. jednom godišnje, u slučaju visine aktive 500 miliona KM i iznad
3. jednom u tri godine, u slučaju visine aktive ispod 500 miliona KM, izuzev u slučaju značajnih promjena u informacionom sistemu, kada je banka dužna obavezno uraditi reviziju informacionog sistema.

(8) Agencija zadržava pravo nalaganja mjera propisanih Zakonom o bankama, a koji se odnose na eksternu reviziju.

Član 15.

Prilikom obavljanja eksterne revizije informacionog sistema, eksterni revizor je dužan uzeti u obzir eksternalizovane usluge i njihovu značajnost i uticaj na informacioni sistem, te u skladu s tim razviti plan revizije i efikasni pristup reviziji.

Upravljanje kontrolama pristupa

Član 16.

Banka je dužna uspostaviti adekvatan sistem upravljanja pristupom resursima informacionog sistema koji će, kao minimum, obuhvatiti:

1. definisanje odgovarajućih upravljačkih, logičkih i fizičkih kontrola
2. upravljanje korisničkim pravima pristupa koji obuhvata procese evidentiranja, autorizacije, identifikacije i autentifikacije, te nadzora prava pristupa
3. upravljanje povlaštenim i udaljenim pristupima.

Član 17.

Banka je dužna, u skladu sa procjenom rizika, osigurati izradu, redovno praćenje i čuvanje operativnih i sistemskih zapisa u svrhu otkrivanja neovlaštenih pristupa i radnji u informacionom sistemu, identificiranja problema, rekonstruisanja događaja, te utvrđivanja odgovornosti.

Maliciozni kod

Član 18.

Banka je dužna uspostaviti kontrole prevencije, detekcije i oporavka informacionog sistema, sa ciljem zaštite resursa od malicioznog programskog koda, te podići svijest korisnika kroz program edukacije.

Aplikativne kontrole

Član 19.

Banka je dužna osigurati da aplikativni software ima ugrađene kontrole ispravnosti, potpunosti i konzistentnosti podataka koji se unose, mijenjaju, obrađuju i generišu.
Upravljanje resursima

Član 20.

(1) Banka je dužna uspostaviti proces upravljanja hardware-skom i software-skom imovinom, koja je neophodna za obavljanje kritičnih (vitalnih) procesa, tokom njenog životnog ciklusa.

(2) Proces upravljanja hardware-skom i software-skom imovinom treba obuhvatiti postupke identifikacije, evidentiranja, određivanja vlasnika i skrbnika, načina raspolaganja, praćenja, obnavljanja i odlaganja imovine.

(3) Banka je dužna klasifikovati i zaštititi informacije prema njihovoj vrijednosti, pravnim zahtjevima, osjetljivosti i kritičnosti za banku.

Upravljanje promjenama

Član 21.

(1) Banka je dužna uspostaviti proces upravljanja promjenama u informacionom sistemu, koji treba da uključi, kao minimum, slijedeće:
1. procedure iniciranja i odobravanja promjena,
2. procedure testiranja, odobrenja i dokumentovanja, prije uvođenja u produkcijski rad
3. procedure za upravljanje 'hitnim' promjenama
4. procedure implementacije promjena, uključujući i plan povratka na 'staro' stanje
5. proces praćenja i izvještavanja.

(2) Banka je dužna utvrditi početne verzije software-skih komponenata informacionog sistema, te evidentirati i dokumentovati sve promjene komponenata informacionog sistema onim slijedom kako su nastajale, zajedno sa vremenom nastanka promjene.

(3) Procedure navedene u st. (1) ovog člana se odnose na promjene osnovnih operativnih sistema, aplikativnog software-a, konfiguracionih datoteka, hardware-a i ostalih dijelova informacionog sistema.

Dokumentacija

Član 22.

Banka je dužna definisati i implementirati procedure upravljanja dokumentacijom (tehničkom, funkcionalnom, korisničkom i dr.) koja se odnosi na informacioni sistem, a koja, kao minimum, treba da uključi slijedeće:

1. obezbjeđenje tačne, potpune i ažurne dokumentacije
2. osiguranje pristupa uposlenika dokumentaciji, u skladu sa njihovim poslovnim potrebama i klasifikaciji.

Upravljanje incidentima i korisničkim zahtjevima

Član 23.

(1) Banka je dužna uspostaviti proces upravljanja incidentima, koji obuhvata definisanje odgovornosti i procedura, a koji treba omogućiti brz, efektivan i propisan odgovor u slučaju narušavanja sigurnosti i funkcionalnosti informacionog sistema.

(2) Banka je dužna, kao minimum, propisati slijedeće:

1. procedure za prijavljivanje, klasificiranje, praćenje i izvještavanje o incidentima
2. procedure za upravljanje korisničkim zahtjevima.

(3) Banka je dužna, u slučaju težih incidenata, obavijestiti Agenciju o incidentu, njegovim posljedicama i poduzetim aktivnostima.

Kopije

Član 24.

(1) Banka je dužna uspostaviti proces upravljanja kopijama (eng. back up) koji uključuje procedure izrade, smještaja, testiranja kopija podataka, te restauracije podataka, kao i adekvatan transport i predaju kopija, kako bi se osigurala raspoloživost podataka u slučaju potrebe, te omogućio oporavak odnosno ponovna uspostava kritičnih (vitalnih) poslovnih procesa u zahtjevanom vremenu.

(2) Kopije trebaju biti ažurne i čuvane na primjeren način, na jednoj ili više sekundarnih lokacija od kojih najmanje jedna mora biti dovoljno udaljena od primarne lokacije na kojoj se nalaze izvorni podaci, a na osnovu urađene analize rizika.

Edukacija

Član 25.

(1) Banka je dužna osigurati stručno osposobljavanje i kontinuiranu edukaciju IT uposlenika, kao i primjerenu, pravovremenu i kontinuiranu edukaciju korisnika informacionog sistema.

(2) Banka je dužna provoditi programe podizanja svijesti korisnika informacionog sistema, vezane za sigurnost informacionog sistema u banci.

Upravljanje razvojem

Član 26.

Banka je dužna definisati i implementirati procedure koje propisuju upravljanje razvojem i održavanjem informacionog sistema, vodeći računa o funkcionalnim i sigurnosnim aspektima, a koje uključuju, kao minimum, slijedeća područja:

1. način iniciranja i odobravanja zahtjeva
2. planiranje i formalnu organizaciju projekta, u skladu sa usvojenom metodologijom
3. uspostavu i dokumentovanje procesa programskog razvoja i isporuke informacionog sistema, koji obuhvata postupke analize i projektovanja, programiranja, adekvatnog testiranja, uvođenja u produkcijski rad i plana povratka na 'staro' stanje
4. razdvajanje razvojnog, testnog i produkcijskog okruženja
5. način upravljanja 'hitnim' promjenama u informacionom sistemu.

Elektronsko bankarstvo

Član 27.

(1) Banka je dužna uspostaviti proces upravljanja rizikom elektronskog bankarstva, koji treba biti sastavni dio cjelokupnog upravljanja rizicima kojima je banka izložena.

(2) U sklopu upravljanja rizicima elektronskog bankarstva, banka je, kao minimum, dužna uraditi slijedeće:

1. uspostaviti, redovno pregledati i testirati sigurnosne mjere i kontrole
2. primjeniti sigurne i efikasne metode autentifikacije za potvrdu identiteta i ovlasti lica, procesa i sistema
3. osigurati da autentifikacija korisnika uključuje kombinaciju najmanje dva načina potvrđivanja korisničkog identiteta, gdje god je moguće to primjeniti
4. osigurati odgovarajuću potvrdu svog identiteta na distribucijskom kanalu elektronskog bankarstva, kako bi korisnici elektronskog bankarstva mogli provjeriti identitet i autentičnost banke
5. obezbjediti postojanje odgovarajućih operativnih i sistemskih zapisa kako bi osigurala neporecivost i dokazivost radnji povezanih sa elektronskim bankarstvom.

Fizičke kontrole

Član 28.

(1) Banka je dužna definisati i implementirati procedure kojim se definišu mjere zaštite i kontrole pristupa prostorijama u kojima su smješteni resursi informacionog sistema (prostorije sa serverima, prostorije sa komunikacijskom opremom i sl.), kao i prostorijama u kojima se nalaze sistemi za podršku funkcionisanju informacionog sistema, u cilju zaštite od neovlaštenog fizičkog pristupa, krađe, fizičkog oštećenja ili uništenja resursa informacionog sistema.

(2) Banka je dužna definisati i implementirati adekvatne mjere zaštite od statičkog elektriciteta, požara, poplave, zemljotresa, eksplozije i drugih oblika prirodnih katastrofa ili šteta uzrokovanih ljudskim djelovanjem.

(3) Banka je dužna periodično kontrolisati ispravnost implementiranih mjera zaštite.

Plan oporavka informacionog sistema

Član 29.

(1) U cilju osiguranja odvijanja kritičnih (vitalnih) poslovnih procesa u odgovarajućem vremenskom okviru, banka je dužna donijeti plan oporavka informacionog sistema koji je sastavni dio plana za vanredne situacije, a u skladu sa Odlukom o minimalnim standardima za upravljanje operativnim rizikom u bankama.

(2) Odgovarajući vremenski okvir oporavka banka mora odrediti provedbom analize uticaja na poslovanje.

(3) Pri procesu planiranja kontinuiteta poslovanja, banka je dužna uzeti u obzir i eksternalizovane aktivnosti, te ovisnost o uslugama trećih lica.

(4) Na osnovu analize uticaja na poslovanje, banka je dužna definisati i usvojiti plan(ove) oporavka informacionog sistema kojim će omogućiti raspoloživost resursa, te detaljno opisati postupke koje je potrebno slijediti kako bi se u zahtijevanom vremenskom roku i sa zahtijevanim funkcionalnostima oporavili kritični (vitalni) poslovni procesi i podaci.

(5) Uprava banke treba osigurati da je plan oporavka informacionog sistema ažuran.

Član 30.

Banka je dužna, u skladu sa procjenom rizika i na osnovu rezultata analize uticaja na poslovanje, osigurati raspoloživost rezervnog informatičkog centra koji je na odgovarajućoj udaljenosti od primarnog informatičkog centra.

Član 31.

(1) U planu oporavka informacionog sistema, u slučaju eksternalizacije informacionog sistema izvan teritorije Bosne i Hercegovine (kada se i primarni i sekundardni informacioni sistem nalaze izvan Bosne i Hercegovine), banka je dužna izvršiti procjenu rizika zemlje i u skladu s tim obezbjediti mogućnost odvijanja kritičnih (vitalnih) procesa.

(2) Banka je dužna osigurati kopije (backup) podataka ažurne na dnevnoj osnovi unutar banke, te kopije podataka, najmanje, za zadnje 3 godine.

Prelazne i završne odredbe

Član 32.

(1) Ova Odluka stupa na snagu 8. dana od dana objavljivanja u „Službenim novinama Federacije Bosne i Hercegovine“.

(2) Banke su dužne da usklade svoje poslovanje sa odredbama ove Odluke, u dalje navedenim rokovima, počev od dana stupanja na snagu ove Odluke:

1. čl. 6., 18. i 25. – 6 mjeseci,
2. čl. 3., 4., 5., 7., 9., 11., 13., 14., 19., 20. st. (1) i (2), 22., 24., 27. i 29. – 12 mjeseci,
3. čl 8., 16., 17., 21., 23., 26. i 28. – 18 mjeseci,
4. čl. 20. st. (3) – 24 mjeseca,
5. čl. 30. i 31. – 30 mjeseci.

Broj: U.O. - _____/11

Sarajevo, _____2011. godine

PREDSJEDNIK

UPRAVNOG ODBORA

Mr.sc. Haris Ihtijarević, dipl. ecc.