„Službene novine Federacije BiH“, broj: 1/12

Na osnovu člana 9. Zakona o Agenciji za bankarstvo Federacije Bosne i Hercegovine ("Službene novine Federacije BiH", br. 9/96, 27/98, 20/00, 45/00, 58/02, 13/03, 19/03, 47/06, 59/06 i 48/08) i člana 18. Statuta Agencije za bankarstvo Federacije BiH ("Službene novine Federacije BiH", broj 42/04), Upravni odbor Agencije za bankarstvo Federacije BiH, na 36. sjednici održanoj dana 28.12.2011. godine, donosi

ODLUKU
O MINIMALNIM STANDARDIMA UPRAVLJANJA INFORMACIONIM SISTEMIMA U BANKAMA

Opće odredbe

član 1.

Odlukom o minimalnim standardima upravljanja informacionim sistemima u bankama (u daljem tekstu: odluka) utvrđuju se minimalni standardi i kriteriji koje je banka dužna da obezbijedi i provodi u procesu upravljanja informacionim sistemom.

Definicije

član 2.

Definicije koje se koriste u ovoj odluci imaju slijedeća značenja:

Autentičnost - osobina koja obezbjeđuje 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 izvornih podataka (informacijska imovina i software-ske komponente) koji su potrebni za ponovno uspostavljanje poslovnih procesa banke, te ostalih podataka za koje banka procijeni da ih je potrebno čuvati.

Dokazivost - osobina koja obezbjeđuje 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-ske komponente (hardware-ska imovina) – 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 - svaki neplanirani i neželjeni događaj koji može narušiti sigurnost i funkcionalnost resursa informacionog sistema koji podržavaju odvijanje poslovnih procesa banke.

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, interni akti i slično.

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

Integritet - osobina informacija (podataka) i procesa da nisu neovlašteno ili nepredviđeno mijenjani.

Kontrole - politike, procedure, prakse, tehnologije i organizacione strukture dizajnirane kako bi obezbijedile 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 obezbjeđuju primjenu internih akata vezanih uz informacioni sistem u cilju obezbjeđivanja funkcionalnosti i sigurnosti informacionog sistema. Logičke kontrole su kontrole implementirane na softwareskim 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 slijedećih načina:

1. pomoću nečega što samo korisnik zna (naprimjer lozinka, PIN, kriptografski ključ),
2. pomoću nečega što samo korisnik posjeduje (naprimjer 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 obezbjeđuje 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 - obezbjeđuje da samo ovlašteni korisnici (povjerljivost) imaju pristup tačnim i kompletnim informacijama (integritet) kada je potrebno (dostupnost).

Skrbnik - lice i/ili organizacioni dio, koji logički ili fizički raspolaže resursima, a koji za potrebe i interes vlasnika obavlja operativne poslove i implementaciju odgovarajućih kontrola, koji su mu dodijeljeni, u skladu sa važećim politikama, procedurama i uputstvima.

Software-ske komponente (software-ska imovina) - uključuju aplikacijski software, sistemski software, baze podataka, software-ske razvojne alate, uslužne programe te ostali sofware.

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

Vlasnik - lice i/ili organizacioni dio kojem 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, obezbjeđenja povjerljivosti, integriteta i dostupnosti informacija i cjelokupnog informacionog sistema, primjereno veličini, složenosti i obimu poslovanja banke, te kompleksnosti 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. uspostavi sistem za mjerenje, praćenje, kontrolu i upravljanje rizicima vezanim za sigurnost informacionog sistema, da prati efikasnost i unapređuje dati sistem,
5. donese i obezbijedi uspostavu adekvatne organizacione strukture i uspostavu odgovarajućih funkcija i ovlasti kako bi obezbijedila efikasno i sigurno upravljanje informacionim sistemom, sa obavezom definiranja stručnih kvalifikacija i potrebnih kompetencija,
6. obezbijedi 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. obezbijedi da su upravljačke kontrole informacionog sistema, kao i sistem internih kontrola informacionog sistema pod stalnim nadzorom interne i povremenim nadzorom eksterne revizije.

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. obezbijedi da su sve dužnosti vezane uz upravljanje informacionim sistemom jasno definirane i dodijeljene,
5. donosi plan i program za uspostavu i podizanje svijesti o sigurnosti informacionog sistema,
6. obezbijedi potrebne resurse za upravljanje informacionim sistemom,
7. usvojimetodologiju kojom će se definirati kriteriji, načini i postupci upravljanja rizicima koji proizilaze iz upotrebe informacionog sistema, te odredi odgovornosti upravljanja rizicima i prihvatljive nivoe rizika,
8. kontinuirano analizira rizike informacionog sistema, poduzima korake za smanjenje rizika na prihvatljiv nivo, te redovno, a najmanje jednom godišnje, izvještava nadzorni odbor o rezultatima procjene rizika,
9. usvoji i primjeni metodologiju upravljanja projektima kojom će se definirati 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 osnov 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.

Interni akti

član 8.

(1) Banka je dužna propisati i primijeniti detaljne procedure kojima se uređuje upravljanje informacionim sistemom, te obezbijediti 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 obezbijediti 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 Federaciji Bosne i Hercegovine.

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.

Odgovorno lice za sigurnost informacionog sistema

član 10.

Uprava banke dužna je imenovati lice odgovorno (voditelj/oficir) za funkciju sigurnosti informacionog sistema, te definirati njegova ovlaštenja, odgovornosti i obim rada. Funkcija sigurnosti informacionog sistema treba biti nezavisna od funkcije organizacijske jedinice za upravljanje informacionim sistemom. Lice odgovorno za funkciju sigurnosti informacionog sistema treba biti kompetentno lice sa dovoljno znanja i iskustva.

član 11.

Lice odgovorno za funkciju sigurnosti 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 12.

(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 definiranog 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 obezbijediti da pružalac usluga interne revizije informacionog sistema istovremeno (u toj godini) ne pruža usluge eksterne revizije informacionog sistema banci, te treba obezbijediti da ne postoji sukob interesa u skladu sa profesijom interne revizije.

Eksterna revizija

član 13.

(1) Banka je dužna Agenciji za bankarstvo Federacije BiH (u daljem tekstu: Agencija) podnijeti zahtjev za izdavanje odobrenja za imenovanje nezavisnog eksternog revizora za reviziju informacionog sistema (u daljem tekstu: eksterni revizor IS).
(2) Banka je dužna, uz zahtjev iz stava (1) ovog člana, dostaviti Agenciji slijedeće dokumente:
    1. nacrt odluke o imenovanju eksternog revizora IS,
    2. nacrt ugovora ili pisma namjere sa eksternim revizorom IS,
    3. reference eksternog revizora IS o obavljenim revizijama informacionih sistema,
    4. stručne kvalifikacije lica koja će obavljati reviziju.
(3) Agencija će rješenje po zahtjevu za izdavanje odobrenja za izbor eksternog revizora IS donijeti u roku od 30 dana od dana prijema zahtjeva sa kompletnom dokumentacijom.
(4) Nadzorni odbor banke dužan je donijeti odluku o imenovanju eksternog revizora IS za reviziju informacionog sistema, po dobijanju odobrenja od Agencije, te sa izabranim eksternim revizorom IS potpisati ugovor o izradi izvještaja o reviziji informacionog sistema. Banka je dužna Agenciji dostaviti usvojenu odluku o izboru eksternog revizora IS i potpisani ugovor sa izabranim eksternim revizorom IS, u roku od 10 dana od dana usvajanja odnosno potpisivanja.
(5) Eksterni revizor IS 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) Banka je dužna da reviziju informacionog sistema obavi u roku od godinu dana od dana stupanja na snagu ove odluke, a zatim da je obavlja periodično:
    1. jednom godišnje, u slučaju visine aktive od 500 miliona KM i iznad
    2. jednom u tri godine, u slučaju visine aktive do 500 miliona KM, izuzev u slučaju značajnih promjena u informacionom sistemu, kada je banka dužna odmah uraditi reviziju informacionog sistema.
(8) Agencija zadržava pravo nalaganja mjera propisanih

Zakonom o bankama, a koji se odnose na eksternu reviziju.

član 14.

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 15.

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

1. definiranje 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 16.

Banka je dužna, u skladu sa procjenom rizika, da obezbijedi 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 17.

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

Aplikativne kontrole

član 18.

Banka je dužna da obezbijedi da aplikativni software ima ugrađene kontrole ispravnosti, potpunosti i konzistentnosti podataka koji se unose, mijenjaju, obraduju i generišu.

Upravljanje resursima informacionog sistema

član 19.

(1) Banka je dužna da uspostavi proces upravljanja hardwareskom 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 da obuhvata postupke identifikacije, evidentiranja, određivanja vlasnika i skrbnika, načina raspolaganja, praćenja, obnavljanja i odlaganja te imovine.
(3) Banka je dužna da klasifikuje i zaštititi informacije prema njihovoj vrijednosti, pravnim zahtjevima, osjetljivosti i kritičnosti za banku.

Upravljanje promjenama

član 20.

(1) Banka je dužna uspostaviti procedure procesa upravljanja promjenama u informacionom sistemu, koje treba da uključe, kao minimum, slijedeće:
    1. iniciranje i odobravanje promjena,
    2. testiranje, odobrenje i dokumentovanje, prije uvođenja u produkcijski rad,
    3. upravljanje 'hitnim' promjenama,
    4. implementaciju promjena, uključujući i plan povratka na 'staro' stanje,
    5. praćenje i izvještavanje.
(2) Banka je dužna da utvrdi početne verzije software-skih komponenata informacionog sistema, te evidentira i dokumentuje sve promjene komponenata informacionog sistema onim slijedom kako su nastajale, zajedno sa vremenom nastanka promjene.
(3) Procedure navedene u stavu (1) ovog člana se odnose na promjene osnovnih operativnih sistema, aplikativnog software- a, konfiguracionih datoteka, hardware-a i ostalih dijelova informacionog sistema.

Dokumentacija

član 21.

Banka je dužna da definiše i implementira 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. obezbjeđenje pristupa uposlenika dokumentaciji, u skladu sa njihovim poslovnim potrebama i klasifikaciji.

Upravljanje incidentima i korisničkim zahtjevima

član 22.

(1) Banka je dužna da uspostavi proces upravljanja incidentima, koji obuhvata definiranje 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, da propiše 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, da obavijesti Agenciju o incidentu, njegovim posljedicama i poduzetim aktivnostima.

Kopije

član 23.

(1) Banka je dužna da uspostavi proces upravljanja kopijama (eng. backup) koji uključuje procedure izrade, smještaja, testiranja kopija podataka, te restauracije podataka sa kopija

podataka, kao i adekvatan transport i predaju kopija, kako bi se obezbijedila raspoloživost podataka u slučaju potrebe, te omogućio oporavak odnosno ponovna uspostava kritičnih (vitalnih) poslovnih procesa u zahtijevanom 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 24.

(1) Banka je dužna da obezbijedi stručno osposobljavanje i kontinuiranu edukaciju uposlenika zaduženih za upravljanje informacionim sistemom, kao i primjerenu, pravovremenu i kontinuiranu edukaciju korisnika informacionog sistema.

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

Upravljanje razvojem

član 25.

Banka je dužna da definiše i implementira procedure koje propisuju upravljanje razvojem i održavanjem informacionog sistema, vodeći računa o funkcionalnim i sigurnosnim aspektima, a koje uključuju, kao minimum:

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 26.

(1) Banka je dužna da uspostavi 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 da:

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

Fizičke kontrole

član 27.

(1) Banka je dužna da definiše i implementira 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 da definiše i implementira adekvatne mjere zaštite od statičkog elektriciteta, požara, poplave, zemljotresa, eksplozije i drugih oblika prirodnih katastrofa ili šteta uzrokovanih ljudskim djelovanjem.

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

Plan oporavka informacionog sistema

član 28.

(1) U cilju obezbjeđenja odvijanja kritičnih (vitalnih) poslovnih procesa u odgovarajućem vremenskom okviru, banka je dužna da donese 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 da odredi provedbom analize uticaja na poslovanje.
(3) Pri procesu planiranja kontinuiteta poslovanja, banka je dužna da uzme u obzir i eksternalizovane aktivnosti, te zavisnost o uslugama trećih lica.
(4) Na osnovu analize uticaja na poslovanje, banka je dužna da definiše i usvoji plan(ove) oporavka informacionog sistema kojim će omogućiti raspoloživost resursa, te detaljno opiše 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 da obezbijedi da je plan oporavka informacionog sistema ažuran.

član 29.

(1) Banka je dužna, u skladu sa procjenom rizika i na osnovu rezultata analize uticaja na poslovanje, da obezbijedi raspoloživost rezervnog informatičkog centra koji je na odgovarajućoj udaljenosti od primarnog informatičkog centra.
(2) Efektivna funkcionalnosti rezervnog informatičkog centra treba biti potvrđena najmanje jednom godište.

član 30.

(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 da izvrši procjenu rizika zemlje i u skladu s tim obezbijediti mogućnost odvijanja kritičnih (vitalnih) procesa.
(2) Banka je dužna obezbijediti kopije (backup) podataka ažurne na dnevnoj osnovi unutar banke, te kopije podataka, najmanje, za zadnje 3 godine.
(3) U slučaju nedostupnosti postojećeg informacionog sistema, banka je dužna, da u okviru internih akata, definiše i obezbijedi dostupnost (pristup) podataka sa kopija (backup-a), a kako bi obezbijedila raspoloživost podataka, te omogućila oporavak odnosno ponovnu uspostavu kritičnih (vitalnih) poslovnih procesa.

Prelazne i završne odredbe

član 31.

(1) Ova odluka stupa na snagu osmog dana od dana objavljivanja u "Službenim novinama Federacije BiH".
(2) Banke su dužne da usklade svoje poslovanje sa odredbama ove odluke, u dalje navedenim rokovima, počev od dana njenog stupanja na snagu:
    1. l. čl. 6., 17., i 24. - 6 mjeseci,
    2. čl. 3., 4., 5., 7., 9., 10., 11., 12., 13., 14., 18., 19. st. (l) i (2), 21., 23., 26. i 28. - 12 mjeseci.
    3. čl. 8., 15., 16., 20., 22., 25. i 27. - 18 mjeseci,
    4. čl. 19. st. (3) - 24 mjeseca,
    5. čl. 29. i 30. - 30 mjeseci.

Broj U.O.-36-5/11
28. decembra 2011. godine
Sarajevo
Predsjednik
Upravnog odbora
Mr. sc. Haris Ihtijarević, s. r.