BANKA QENDRORE E REPUBLIKËS SË KOSOVËS
CENTRALNA BANKA REPUBLIKE KOSOVA
CENTRAL BANK OF THE REPUBLIC OF KOSOVO

Na osnovu člana 35, stav 1, podstav 1.1 Zakona br. 03/L-209 o Centralnoj banci Republike Kosova (Službeni list Republike Kosovo, br. 77/16. avgust 2010.) kao i člana 85, stav 1, Zakona br. 04/L-093 o bankama, mikrofinansijskim institucijama i nebankarskim finansijskim institucijama (Službeni list Republike Kosovo, br. 11/11. maj 2012.) Odbor Centralne banke na sastanku održanom 26. marta 2020. godine, usvojio je:

# UREDBA O INFORMACIONOJ TEHNOLOGIJI ZA BANKE

## Član 1
## Cilj i delokrug

1. Cilj ove uredbe je da utvrdi kriterijume i uslove koje banke treba da ispune za organizaciju i rad svojih sistema informacione tehnologije (u sledećem tekstu IT) koji omogućavaju smanjenje operativnog rizika koji može biti izazvan zbog zloupotreba IT sistema i da sačuva pouzdanost tih sistema u podršci aktivnostima banaka.
2. Ova uredba se sprovodi na sve banke i ogranke stranih banaka koje je CBK licencirao za rad u Republici Kosovo kojima se referišemo u nastavku kao banke.

## Član 2
## Definicije

1. Svi izrazi koji se koriste u ovoj Uredbiimaju isto značenje kao i izrazi koji su određeni u članu 3 Zakona br.04/L-093 o bankama, mikrofinansijskim institucijama i nebankarskim finansijskim institucijama (u nastavku: Zakon o bankama) ili/i sledećim definicijama u svrhu ove uredbe:

   1.1. **Informacioni sistem** – označava kompletnu tehnološku grupu koja se sastoji od infrastrukture (softverske i hardverske komponente), organizacije, ljudi i postupaka za prikupljanje, čuvanje, obradu, prenošenje, prikazivanje i korišćenje podataka i informacija;

   1.2. **Softverske komponente** - označavaju sve vrste operativnog sistema, aplikativnog softvera, alat za razvoj softvera i drugih softverskih sistema;

   1.3. **Hardverske komponente** - označavaju računarsku opremu, opremu mreža, medij za čuvanje podataka i drugu tehničku opremu koja služi kao podrška za funkcionisanje informacionih sistema;

1.4. **Korisnici informacionog sistema -** podrazumevaju sva lica koja su ovlašćena za korišćenje informacionih sistema (zaposleni u instituciji, zaposleni u drugim kompanijama koji imaju pristup informacijama o sistemu i klijentima banke);

1.5. **Spoljni pružalac usluga -** znači fizičko ili pravno lice koje na osnovu pismenog ugovora pruža uslugu bankama za delegirane bankarske funkcije;

1.6. **Sredstva -** označava informacije (kao što su baze podataka, ugovori i sporazumi, dokumentovanje sistema, informacije o istraživanju, priručnici korisnika, materijale za obuku, procedure rada ili podrške, planove kontinuiteta poslovanja, evidenciju revizije i arhivirane informacije), softverska sredstva (softverske aplikacije, softverski sistemi, alat za razvoj itd.), fizička sredstva (računarska oprema, komunikacioni uređaji, prenosiva oprema (eng. Removable media) i drugi uređaji), usluge (računarske usluge i za komunikaciju, opšte usluge), osoblje (zajedno sa kvalifikacijama, veštinama i iskustvom), nedodirljive (kao što je ugled banke);

1.7. **Čist sto -** znači uklanjanje svih dokumenata i drugih poverljivih sredstava sa radne površine tokom perioda bez nadzora i na kraju radnog vremena.

## Član 3
## Upravljanje informacionom tehnologijom

1. Upravljanje informacionom tehnologijom treba da sadrži sledeće zahteve:

   1.1. Da ima funkcionalnost, kapacitet i učinak koji pruža podršku koja se traži od poslovnih procesa;

   1.2. Pruža odgovarajuću kontrolu validacije podataka tokom procesa obrade i tokom dobijanja podataka kako bi se sprečila netačnost i neusklađenost podataka i informacija;

   1.3. Pruža pravovremene, tačne i potpune informacije o donošenju poslovnih odluka i upravljanju rizikom kako bi se omogućila sigurnost i održivo poslovanje banke;

2. Banka će vršiti nadgledanje, regulisanje i stalno poboljšanje procesa upravljanja IT-om kako bi se smanjila izloženost riziku i održavala njegovu bezbednost i funkcionalnost.

## Član 4
## Organizaciona struktura za upravljanje IT-om

1. Banka treba da uspostavi organizacionu strukturu IT jedinice sa dovoljnim brojem i odgovarajućim osobljem kako bi se obezbedilo efikasno upravljanje oblastima IT-a. Raspodela zadataka treba da se vrši u skladu sa standardom ISO 27000 sa jasno definisanim odgovornostima i nadležnostima za proces upravljanja IT-om. Ova jedinica mora dokumentovati redovne informativne izveštaje najmanje na tromesečnoj osnovi za viši menadžment banke.

2. U slučaju delegiranja IT funkcija na spoljnog pružaoca usluga (eng. outsource), banka bi trebalo da odredi najmanje jednog unutrašnjeg zaposlenog specijalizovanog za oblast informacionih tehnologija, kao odgovornog za koordinaciju i napredak IT funkcija IT-a.

3. Banka treba da odredi odgovorno lice za bezbednost informacija koje treba da upravlja bezbednošću informacionog sistema i koordinira politike i procese bezbednosti informacija u vezi sa tehnološkim funkcijama i platformama. Odgovorno lice podnosi izveštaj glavnom izvršnom načelniku i mora biti nezavisno od ostalih organizacionih jedinica. Odgovorno lice mora najmanje jednom godišnje da podnosi izveštaj preko izvršnog načelnika, a po potrebi i Odboru direktora koji mora biti informisan o radu i funkcijama vezanim za bezbednost informacija.

**Član 5**
**Politike i procedure upravljanja IT-om**

1. Odbor direktora odgovoran je za odobravanje politika tehnologija i bezbednosti informacija i na godišnjem nivou treba da proceni pogodnost ovih politika i izvrši njihov pregled.
2. Banka određuje ciljeve, strategije i zahteve bezbednostu za rad IT sistema, određuje politike ta tehnologiju i bezbednost informacije kao i procedure za procese u oblasti. Ove postupke mora odobriti viši menadžment.
3. Banka u skladu sa poslovnom strategijom usvaja strategije za razvoj IT sistema.
4. U slučaju da banka obezbedi celokupni ili deo svoje IT aktivnosti (ili sistema) od spoljnih pružaoca usluga, onda banka odobrava unutrašnju proceduru za delegiranje funkcija da bi se obezbedila usklađenost sa zahtevima ove uredbe za bezbednost i pravilno funkcionisanje ovih sistema.
5. Unutrašnji postupak za delegiranje funkcija prena stavu 4. ovog člana mora da sadrži najmanje sledeće elemente:
   5.1. Identifikaciju funkcija koje će biti delegirane i procenu uticaja koji će delegiranje tih funkcija imati;
   5.2. Postupci delegiranja funkcija, uključujući kriterijume za izbor primaoca delegiranih funkcija;
   5.3. Rokovi i metode izveštavanja primaoca delegiranih funkcija banci;
   5.4. Načini praćenja primaoca delegiranih funkcija od strane banke;
6. Politike i procedure za upravljanje IT-om treba da odrede najmanje sledeće elemente:
   6.1. Upravljanje i rad sistema IT-a;
   6.2. Organizaciona struktura za upravljanje IT-om;
   6.3. Hardverska infrastruktura oblasti IT-a (dijagrami konfiguracija);
   6.4. Klasifikacija dokumentacije i zaštita sistema i podataka;
   6.5. Backup podataka sistema;
   6.6. Upravljanje promenama sistema (eng. change management);
   6.7. Upravljanje incidentima;

6.8. Upravljanje rizikom sistema IT-a;

6.9. Utvrđivanje mehanizama zaštite sistema IT-a;

6.10. Upravljanje trećim stranama.

**Član 6**
**Razvoj i nabavka sistema IT-a**

1. Da bi smanjio rizik, banka bi trebalo da sledi trend razvoja softvera vodeći računa da koristi samo ažurirane verzije i podržane od strane njihovih pružaoca.
2. Banka usvaja unutrašnje procedure o načinu na koji realizuje razvoj, promene i testiranja u svojim IT sistemima. Sistemi IT se postavljaju u rad uživo, tek nakon što specijalizirani službenik koji vrši proveru primenjivosti postupaka i ispravnog funkcionisanja sistema da svoju dokumentiranu saglasnost..
3. Spoljni pružalac usluga tokom sprovoženja i rada sistema ni na koji način ne bi trebao imati pristup verzijama sistema koji su u produkciji (live), osim pristupa samo za čitanje (read only) uz posebnu saglasnost i uz nadzor banke. Izvođači i ostale spoljne strane moraju da testiraju sve promene u testnom okruženju.

**Član 7**
**Delegiranje funkcija IT-a spoljnim pružaocima usluga**

1. Banka je odgovorna da obezbedi da se aktivnost IT sprovodi u skladu sa svim zahtevima koji su utvrđeni u ovoj uredbi i u slučajevima kada se celokupni ili deo aktivnosti IT-a obezbeđuje od strane spoljnog pružaoca usluga IT..
2. Pre izbora spoljnog pružaoca usluga IT-a, Banka mora da preduzme sledeće aktivnosti:
   2.1. Sprovede procenu rizika poslovanja banke koji može nastati korišćenjem spoljne usluge koja se pruža tokom obrade aktivnosti banke;
   2.2. Odredi minimalne standarde koje spoljni pružalac IT usluga treba da ispuni i koji moraju biti usklađeni sa planom kontinuiteta poslovanja;
   2.3. Odredi neophodne mere za izbegavanje sukoba interesa;
   2.4. Odredi način praćenja usluge i kvaliteta poslovanja kompanije, finansijske situacije i profila rizika putem periodičnog testiranja usklađenosti sa politikom bezbednosti informacionog sistema;
   2.5. Izvrši odgovarajuću procenu aktivnosti spoljnog pružaoca usluga IT sa pravnog i finansijskog stanovišta, kao i sa stanovišta načina koji se upravlja bezbednošću informacionog sistema utvrđenog ovom uredbom;
   2.6. Odredi koordinisano upravljanje bezbednosnim incidentima.
3. Sporazum između banke i spoljnog pružaoca IT usluga mora biti određen pisanim ugovorom koji, između ostalog, treba da uključi:

3.1. Podatke povezanih strana (banka i spoljni pružalac usluga IT);

3.2. Prava i obaveze povezanih strana;

3.3. Opis delegiranih funkcija;

3.4. Vremenske rokove za pružanje usluga;

3.5. Nivo pružanja usluga (eng. Service level agreement);

3.6. Angažovanje pružaoca usluga IT da obavlja svoju delatnost u skladu sa važećim zakonodavstvom, zahtevima, regulatorima i politikama koje je usvojila banka i da sarađuje sa CBK-om u pogledu delegiranih funkcija;

3.7. Period obaveštenja o završetku ugovora koji je dovoljan da se pronađu alternativna rešenja;

3.8. Tretman i čuvanje poverljivosti podataka;

3.9. Odredba koja određuje da spoljni pružalac usluga IT treba da bude podvrgnut nadzoru od strane CBK-a u vezi sa delegiranim aktivnostima IT-a;

3.10. Obaveza spoljnog pružaoca usluga IT da odmah obavesti banku o bilo kojoj činjenici koja može značajno uticati na njenu sposobnost da efikasno i efektivno obavlja svoju delatnost u skladu sa važećim zakonskim zahtevima;

3.11. Pravo banke da bude obaveštena o toku funkcija koje je delegirao spoljni pružalac usluga IT, kao i pravo banke da pruži opšta ili posebna uputstva u vezi sa obavljanjem delegiranih funkcija;

3.12. Pravo banke da izvrši inspekciju i kontrolu aktivnosti spoljnog pružaoca usluga IT u vezi sa delegiranim aktivnostima IT.

4. Spoljni pružalac usluga ne može da podugovara usluge osim ako to nije određeno osnovnim ugovorom sklopljenim između banke i pružaoca usluga.

5. Banka je dužna da upravlja rizicima koji proizilaze iz ugovornih odnosa sa spoljnim pružaocima usluga, a čije su aktivnosti povezane sa informacionim sistemom koji banka koristi. Banka je obavezna da stalno prati način i kvalitet aktivnosti ugovorenih od strane spoljnog pružaoca.

## Član 8
## Upravljanje rizikom informacionih sistema

1. Banka određuje kriterijume za dozvoljeni rizik u vezi sa korišćenjem svojih sistema IT u skladu sa standardima ISO 27005.

2. Najmanje jednom godišnje ili u slučaju značajnih promena u zahtevima za bezbednost IT-a, banka vrši analizu rizika sistema IT-a kako bi obezbedila da se taj rizik održi u prihvatljivim granicama u pogledu delatnosti banka. Rezultati analize rizika se dokumentuju.

3. Banka mora pismeno da obavesti CBK u slučaju identifikacije incidenata u oblasti IT-a i promena u ključnim funkcijama važnih IT procesa koji mogu ometati ili ugroziti biznis, najkasnije jedan radni dan nakon incidenta.
4. Upravljanje rizikom informacionog sistema trebalo bi da uključi celokupan informacioni sistem integrisane banke u svim fazama svog razvoja.
5. Upravljanje rizikom informacionog sistema treba da uključi godišnji plan podizanja svesti zaposlenih u banci o adekvatnoj upotrebi usluga pruženih putem informacionog sistema banke.

## Član 9
## Bezbednost informacionih sistema

1. Bezbednost sistema IT zasnivaće se na utvrđivanju ispunjenosti sledećih kriterijuma:

   1.1. Poverljivost: informacije bi trebale biti dostupne samo ovlašćenim korisnicima;

   1.2. Integritet: očuvanje tačnosti i potpunosti informacionog sistema;

   1.3. Dostupnost: pristup sistemu IT ovlašćenim korisnicima u bilo kom trenutku.
2. Banka mora stalno da upravlja bezbednosnim procesom informacionog sistema. Banka mora da identifikuje i prati potrebe bezbednosti informacionog sistema, barem na osnovu rezultata procene rizika tog sistema i obaveza proizašlih iz unutrašnjih akata ili ugovornih odnosa.
3. Banka treba da odredi kriterijume, metode i postupke za klasifikaciju informacija prema stepenu osetljivosti i kritičnosti - u pogledu mogućih posledica povrede poverljivosti, njihovog integriteta i dostupnosti.
4. Bezbednost informacija i sve aktivnosti u vezi sa tim treba da budu u skladu sa svim važećim zakonima koji se odnose na informacije i rad institucije.

## Član 10
## Fizička bezbednost informacionih sistema

1. Banka mora da preduzme neophodne mere zaštite kako bi sprečila svaki neovlašćeni fizički pristup, intervenciju ili oštećenje informacija, opreme za obradu informacija i bankarske operacije na osnovu standarda ISO 27002.
2. Banka treba da stvori procedure za pristup i rad u zonama bezbednosti za sve zaposlene i spoljne strane. Zone bezbednosti moraju biti zaštičene kontrolom pristupa kako bi se obezbedilo da samo ovlašćeni zasposleni imaju pristup.
3. Oprema se mora održavati radi zaštite od kvarova, kako bi se obezbedila stalna dostupnost integriteta i bila podržana u slučaju prekida usled kvara pomoćne opreme, prirodnih nepogoda, zlonamernih ili slučajnih napada itd.

4. Bezbednosne mere se takođe moraju odrediti i za korišćenu opremu koja se nalazi izvan prostorija banke u zavisnosti od lokacije i moraju se uzeti u obzir rizici pri određivanju neophodnih kontrola.
5. Sva oprema koja sadrži informacije mora biti verifikovana da bi se obezbedilo da svi licencirani podaci i softver budu uklonjeni pre odlaganja, uništavanja ili ponovne upotrebe, kako bi se sprečio povratak originalnih informacija.
6. Svim korisnicima se mora podići svest o bezbednosnim zahtevima i postupcima za zaštitu opreme bez nadzora.
7. Banka mora da odredi kriterijume, metode i postupke za čist sto, u cilju zaštite informacija.
8. Ugovorne obaveze za zaposlene i spoljne pružaoce usluga IT trebale bi odražavati politike banke o bezbednosti informacije. Svi zaposleni i spoljni pružaoci usluga IT moraju razumeti odgovornost razmatranih uloga.
9. Kada je prikladno za sprovođenje, banka će odrediti da zaposleni i spoljni pružaoci usluga sačuvaju informacije dobijene tokom vršenja njihovih aktivnosti čak i u određenom vremenu nakon prekida ugovornog sporazuma sa zaposlenim ili spoljnim pružaocima usluga IT-a.
10. Banka treba da odredi akcije i mere koje treba preduzeti u slučaju kršenja bezbednosnih zahteva od strane zaposlenih ili spoljnih pružalaca usluga IT-a.

**Član 11**
**Upravljanje sredstvima IT-a**

1. Banka treba da identifikuje sva sredstva IT-a.
2. Banka mora da vodi inventar celokupnih sredstava sa svim potrebnim informacijama, uključujući vrstu sredstava, format, lokaciju, informacije o backup-u (gde se može sprovesti), informacije o licenci i vrednost za biznis.
3. Banka treba da utvrdi i dokumentuje vlasništvo i klasifikaciju celokupnih sredstava koja se odnose na obradu informacija.
4. Vlasnik imovine biće odgovoran da:
   4.1. Obezbedi da se informacije i sredstva koja se odnose na obradu informacija klasifikuju prema osetljivosti;
   4.2. Redovno odredi i pregleda ograničenja pristupu i klasifikaciji.
5. Banka će odrediti pravila o prihvatljivom korišćenju informacija i sredstava koja se odnose na obradu informacija.

## Član 12
## Upravljanje računarskom mrežom

1. Računarskom mrežom banke mora se upravljati i kontrolisati radi zaštite informacija sistema i aplikacija. Banka treba da sprovede kontrolu kako bi obezbedila zaštitu poverljivosti i integriteta informacija u mreži i zaštitu usluga od neovlašćenog pristupa na osnovu standarda ISO 27002.
2. Za upravljanje računarskim mrežama banka mora da odredi:
   2.1. Procedure za upotrebu i upravljanje uslugama i opremom mreže radi ograničavanja pristupa uslugama mreže i aplikacijama;
   2.2. Postavljanje posebnih kontrola radi zaštite poverljivosti i integriteta podataka koji prolaze kroz javne ili bežične mreže (eng. wireless);
   2.3. Tehnologije koja se sprovodi za bezbednost usluga mreža kao što su autentifikacija, enkriptovanje i kontrola mrežnih veza;
   2.4. Grupa informacionih usluga, korisnika i informacionih sistema treba da budu izolovana od javnih mreža;
   2.5. Posebnu kontrolu treba posvetiti pristupima spoljnih pružaoca usluga u slučajevima potrebe za interkonekciju (veza sa trećim stranama).

## Član 13
## Upravljanje pristupom korisnika

1. Banka će upravljati pristupom informacionim sistemima kroz odgovarajuće unutrašnje procedure za upravljanje pravima za pristup korisnika. Unutrašnje procedure treba da sadrže kriterijume za pristup, autorizaciju, identifikaciju i potvrdu korisnika u skladu sa standardima ISO27001.
2. Svaki korisnik mora biti jedinstven i sistem treba da odredi kriterijume za postavljanje lozinke u skladu sa standardima ISO 27000. Pre davanja pristupa informacionim sistemima, unutrašnji radnici banke i spoljni pružaoci usluga moraju potpisati sporazum o čuvanju poverljivosti i neotkrivanju informacija.
3. Banka će obezbediti da autorizacija za pristup korisnicima informacionim sistemima bude odobrena od strane lica koja su odgovorna za te sisteme i da se zasniva na principu najnižeg mogućeg pristupa sistemu, omogućavajući im obavljanje radnih zadataka. Banka bi trebalo da najmanje na svakih šest meseci pregleda prava za pristup korisnika sistemima od velike važnosti na osnovu procene rizika i najmanje na godišnjem nivou za pristup svim svim ostalim sistemima.
4. U upravljanju pravima za pristup korisnika, banka mora posebno autorizovati privilegovani pristup i /ili pristup iz udaljenosti informacionom sistemu. Svi pristupi i aktivnosti privilegovanih korisnika i pristup iz udaljenosti mora biti praćen.

5. Pristup sa daljine informacionim sistemima treba omogućiti dvofaktornim metodama autentifikacije (eng. Two factor authentication). Komunikacija između uređaja koji će pristupiti informacionom sistemu sa daljine mora imati mere enkriptovanja *end-to-end* za svaku sesiju komunikacije.
6. Banka treba da prati i čuva događaje (eng. events) bezbednosti informacija u svojoj infrastrukturi na osnovu standarda ISO 27001.

**Član 14**
**Unutrašnja revizija informacionog sistema**

1. Zahtevi koji su određeni Uredbom o unutrašnjoj kontroli i unutrašnjoj reviziji sprovode se na reviziju informacionog sistema.
2. Delatnost oblasti IT-a treba da bude podvrgnuta najmanje periodičnom godišnjem pregledu koji se fokusira na metodologiji koja je zasnovana na riziku.
3. Reviziju IT-a treba da obavljati nadležna lica u okviru funkcije unutrašnje revizije ili spoljna lica koja su ugovorena za tu svrhu.

**Član 15**
**Čuvanje informacija**

1. Čuvanje infromacije (backup) se treba izvršiti u skladu sa unutrašnjim procedurama banke.
2. Unutrašnji akti iz stava 1. ovog člana treba da sadrže najmanje sledeće elemente:
   2.1. Određivanje potrebnog nivoa backup-a informacije;
   2.2. Držanje tačnih i potpunih podataka o backup-u informacija, kao i dokumentovane postupke za povraćaj backup-ova;
   2.3. Vrstu (eng. Full, incremental, differential) i frekvenciju backup-ova prema složenosti biznisa.
3. Raspored izrade backup-ova treba da bude određen tako da obezbedi da se sve informacije i softver mogu oporaviti u slučaju nesreće ili kvara opreme.
3. Backup-ovi treba da se čuvaju na drugoj lokaciji, na dovoljnoj udaljenosti da ne budu ugroženi od istih pretnji kao u centralnoj lokaciji.
4. Backup-ovima treba pružiti odgovarajući nivo fizičke zaštite i zaštite životne sredine u skladu sa standardom koji se sprovodi u centralnoj lokaciji.
5. Backup-ove treba redovno testirati, obezbeđujući da su pouzdani i upotrebljivi po potrebi.
6. Backup-ove treba zaštititi od neovlašćenog pristupa putem enkriptovanja.
7. Trajanje čuvanja nformacija treba da bude u skladu sa važećim zakonodavstvom.

## Član 16
## Soba sa serverima

1. Zahtevi koji su određeni u Uredbi o minimalnim bezbednosnim zahtevima sprovode se na sobu sa serverima.
2. Pored zahteva iz stava 1. ove uredbe, banka mora da odredi uslove pristupa osoblja i trećih lica ovlašćenih za pristup sobi sa serverima u slučaju hitnih slučajeva.
3. Soba sa serverima treba da bude ograničena na pristup samo ovlašćenom osoblju i da bude praćena evidentiranjem ulaska / izlaska osoblja i spoljnih lica u ovim prostorijana.

## Član 17
## Nastavak rada nakon prestanka kao rezultat
## vanrednih događaja

1. Radsi neprekidnog rada svih sistema IT-a, banka treba da izradi postupak za stalni rad.
2. Banka mora da usvoji plan za analizu uticaja na biznis (BIA) koji će analizirati prestanak aktivnosti, i koji će sadržati:
   2.1. Procese koji su prioritetniji kao i potrebne resurse za te procese;
   2.2. Završne aktivnosti koje treba postići (eng. Service Delivery Objective);
   2.3. Krajnje vreme oporavka (eng. Recovery Time Objective);
   2.4. Krajnja tačka oporavka (eng. Recovery Point Objective).
3. Odbor direktora banke mora da usvoji plan kontinuiteta biznisa na godišnjoj osnovi, kao i plan oporavka od nepogoda, koji reguliše stvaranje uslova za oporavak i dostupnost resursa informacionog sistema potrebnih za završetak kritičnih procesa biznisa.
4. Plan kontinuiteta biznisa i oporavka od nepogoda treba da sadrži najmanje sledeće zahteve:
   4.1. procedure koje treba preduzeti u slučaju prekida rada sistema;
   4.2. ažuriranu lista svih potrebnih ljudskih i tehničkih resursa za obnavljanje kontinuiteta biznisa;
   4.3. informacije o odgovornim licima i njihovim zamenicima koji će biti odgovorni za oporavak rada u slučaju nepredviđenih događaja, uključujući njihove određene zadatke i odgovornosti, kao i plan unutrašnjih i spoljnih linija komunikacije;
   4.4. alternativnu lokaciju u slučaju prekida biznisa i oporavka u funkciji procesa biznisa na primarnoj lokaciji. Ova lokacija treba da ima odgovarajuću udaljenost od primarnog centra, kako bi se izbegao uticaj istih opasnosti na obe lokacije.
5. Za sprovođenje planova prema stavu 4 ovog člana, Banka će obezbediti da svi zaposleni budu upoznati sa njihovim ulogama i odgovornostima u hitnim slučajevima.

6. Banka će uskladiti planove sa promenama biznisa, uključujući promene u proizvodima, aktivnostima, procesima i sistemima sa promenama u životnoj sredini, kao i sa politikom biznisa i strategijom biznisa.
7. Banka će izvršiti testiranje planova, najmanje jednom godišnje i nakon nastanka značajnih promena, izvršiće dokumentovanje istih kao i tih testova.
8. U upravljanju kontinuitetom biznisa, Banka uzima u obzir aktivnosti koje su poverene trećim stranama i zavisnosti od usluga ovih strana.
9. U slučaju okolnosti koje zahtevaju sprovođenje plana kontinuiteta poslovanja i plana za aktivnosti oporavka u slučaju nepogode, Banka će o tome obavestiti Centralnu banku Republike Kosovo, najkasnije dan nakon nastanka takvih okolnosti. Centralna banka Republike Kosovo može zatražiti dodatnu dokumentaciju o relevantnim činjenicama u vezi sa ovim okolnostima i odrediti rok za podnošenje ovog dokumenta.

## Član 18
## Dokumentovanje aktivnosti IT-a

Banka održava kompletnu i ažuriranu dokumentaciju o organizaciji, opremi, sistemima, pristupima i drugim važnim faktorima vezanim za aktivnost IT-a. Takva dokumentacija će dokazati da je usklađenost sa zahtevima ove uredbe stalna.

## Član 19
## Mere poboljšanja

Svako kršenje odredbi ove uredbe biće podložno merama poboljšanja i kaznenim merama kao što je određeno u Zakonu o Centralnoj banci Republike Kosovo i Zakonu o bankama, mikrofinansijskim institucijama i nebankarskim finansijskim institucijama.

## Član 20
## Stupanje na snagu

Ova uredba stupa na snagu šest (6) meseci nakon datuma njenog usvajanja.

Flamur Mrasori

Predsednik Odbora Centralne banke Republike Kosovo