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

Në bazë të nenit 35, paragrafi 1, nënparagrafi 1.1, të Ligjit nr. 03/L-209 për Bankën Qendrore të Republikës së Kosovës (Gazeta Zyrtare e Republikës së Kosovës, nr. 77/16 gusht 2010), të ndryshuar dhe plotësuar me Ligjin nr. 05/L -150 për Bankën Qendrore të Republikës së Kosovës (Gazeta Zyrtare e Republikës së Kosovës, nr.10/03 prill 2017), si dhe nenin 7, paragrafi 7.4, nënparagrafi (c), nenin 15, paragrafi 15.7, nënparagrafi (e), dhe nenin 22, paragrafi 22.7, nënparagrafi (e), të Ligjit nr. 04/L-101 për Fondet Pensionale të Kosovës (Gazeta Zyrtare e Republikës së Kosovës, nr. 10/8 maj 2012), i ndryshuar dhe plotësuar me Ligjin Nr. 05/L -116, për ndryshimin dhe plotësimin e Ligjit Nr. 04/L-101 për Fondet Pensionale të Kosovës, i ndryshuar dhe plotësuar me Ligjin Nr. 04/L-115 dhe Ligjin Nr. 04/L-168 (Gazeta Zyrtare e Republikës së Kosovës nr. 3/17 janar 2017), Bordi i Bankës Qendrore, në mbledhjen e mbajtur më 28 shkurt 2024, miratoi këtë:

RREGULLORE PËR SISTEMET DHE SIGURINË E INFORMACIONIT PËR FONDET PENSIONALE

Neni 1
Qëllimi dhe fushëveprimi

1. Qëllimi i kësaj rregulloreje është të përcaktojë kriteret dhe kushtet minimale që duhet të plotësojnë fondet pensionale për organizimin dhe për funksionimin e sistemeve të tyre të teknologjisë së informacionit (në tekstin e mëposhtëm të TI-së), të cilat mundësojnë uljen e rrezikut operacional që mund të shkaktohet nga keqpërdorimi i sistemeve të TI-së, si dhe të ruajë besueshmërinë e këtyre sistemeve në mbështetjen e aktiviteteve të fondeve pensionale. Kriteret dhe kushtet minimale të përcaktuara në këtë rregullore kanë të bëjnë me menaxhimin, sigurinë dhe punën e sistemeve të informacionit të fondeve pensionale, si dhe sigurimin e vazhdimësisë së punës në rast të ndonjë ngjarjeje të fatkeqësisë.
2. Kjo rregullore zbatohet për fondet pensionale që operojnë në Republikën e Kosovës të referuar në vijim me fondi/et ose fondi/et pensionale.

Neni 2
Përkufizimet

1. Të gjitha shprehjet e përdorura në këtë rregullore kanë të njëjtin kuptim siç janë të përcaktuara në nenin 1 të Ligjit nr. 04/L-101 për Fondet Pensionale të Kosovës dhe nenin 1 të Ligjit nr. 04/L-168 për ndryshimin dhe plotësimin e Ligjit nr. 04/L-101 për Fondet Pensionale të Kosovës dhe/ose me përkufizimet për qëllimin e kësaj rregulloreje si në vijim:
   1.1. **Sistemi i informacionit** – nënkupton grupin e tërësishëm teknologjik që përbëhet nga infrastruktura (komponentët softuerikë dhe harduerikë), fondet (institucioni), njerëzit dhe procedurat për mbledhjen, përpunimin, shfaqjen dhe përdorimin e të dhënave dhe informacionit, transmetimin dhe ruajtjen;

1.2. **Përdoruesit e sistemit të informacionit** – nënkupton të gjithë personat që janë të autorizuar për të përdorur sistemet e informacionit (punonjësit në institucion, punonjësit e kompanive tjera që kanë qasje në informatat e sistemit të fondeve pensionale);

1.3. **Fond pensional** – nënkupton Fondin e Kursimeve Pensionale, si dhe fondet tjera pensionale të licencuara nga BQK.

1.4. **Komponentët e softuerit** – nënkupton të gjitha llojet e sistemit operativ, softueri aplikativ, veglat e zhvillimit të softuerit dhe sisteme tjera softuerike;

1.5. **Komponentët harduerikë** – nënkupton pajisjet kompjuterike, pajisjet e rrjetave, mediumet për ruajtjen e të dhënave dhe pjesa tjetër pajisje teknike, që shërbejnë si mbështetje për funksionimin e sistemeve të informacionit;

1.6. **Asete** – nënkupton asetet e prekshme dhe asetet e paprekshme që kanë vlerë për fondin pensional.

1.7. **Tavolinë e pastër** – nënkupton largimin e të gjitha dokumenteve dhe aseteve të tjera konfindenciale nga tavolina e punës gjatë periudhës së pambikëqyrur dhe në përfundim të orarit të punës.

1.8. **Ofruesi i jashtëm i shërbimit** – nënkupton personin fizik apo juridik i cili në bazë të një marrëveshjeje të shkruar i ofron shërbim fondit për funksionet e deleguara nga fondi;

1.9. **Incident** – nënkupton një ngjarje të paplanifikuar që nuk është pjesë normale e operacioneve dhe që ndërpret një proces apo një shërbim ose redukton kualitetin e shërbimit;

1.10. **Zona e serverëve** – nënkupton zonën ku ruhen dhe qëndrojnë kryesisht serverët dhe pajisje të tjera ndihmëse, që nevojiten për shërbimet e komunikimit, sinjalizimit dhe pajisje të tjera elektronike ku ruhen shënimet e bankës.

1.11. **Standarde të pranuara ndërkombëtarisht -** nënkupton ISO/IEC 27000 seria; NIST 800; COBIT; ITIL e të ngjashme.

1.12. **Shërbimet cloud** – nënkuptojnë resurse të infrastrukturës, hapësirës dhe aplikacioneve që ekzistojnë në internet (ang. Infrastructure as a Service (IaaS), Platform as a Service (PaaS) dhe Software as a Service (SaaS)). Ofruesit e këtyre shërbimeve/resurseve kontraktojnë me pranuesit e shërbimeve, për t'ju lejuar përdorimin e resurseve kompjuterike pa pasur nevojë të blejnë ose mirëmbajnë pajisje fizike apo softuerike.

Neni 3
Menaxhimi i sistemeve të informacionit

1. Fondi pensional duhet të krijojë një sistem të informacionit të përshtatshëm i cili duhet të përfshijë kërkesat si në vijim:

1.1. Të ketë funksionalitetin, kapacitetin dhe performancën që ofrojnë mbështetje që kërkohet nga proceset e aktiviteteve të fondit;

1.2. Ofron informacion në kohë, të saktë dhe të plotë për marrjen e vendimeve të institucionit dhe menaxhimin e rrezikut, për të mundësuar siguri dhe funksionim të qëndrueshëm të fondit pensional;

1.3. Ofron kontrollë të përshtatshme të verifikimit/validimit të të dhënave, gjatë procesit të përpunimit dhe gjatë nxjerrjes së të dhënave, për të parandaluar pasaktësi dhe mospërputhje në të dhëna dhe informacione;

2. Fondi pensional, bën monitorimin, rregullimin dhe përmirësimin e vazhdueshëm të procesit të menaxhimit të TI-së për të zvogëluar ekspozimin ndaj rrezikut dhe duke ruajtur sigurinë dhe funksionalitetin e tij.

Neni 4
Struktura organizative për menaxhimin e TI-së

1. Fondi pensional në strukturën e tij organizative duhet të themelojë njësi të TI-së me staf të mjaftueshëm në numër dhe të përshtatshëm për të siguruar, që fusha e TI-së menaxhohet në mënyrë efikase të bazuar në standarde të pranuara ndërkombëtarisht. Ndarja e detyrave duhet të bëhet sipas standardeve të pranuara ndërkombëtarisht me përgjegjësi dhe kompetenca të përcaktuara qartë për procesin e menaxhimit të TI-së dhe sigurisë së informacionit. Kjo njësi duhet të dokumentojë raporte të rregullta informuese së paku në baza tremujore për menaxhmentin e lartë të fondit pensional.
2. Fondi pensional duhet të përcaktojë personin përgjegjës për sigurinë e informacionit i cili duhet të menaxhojë sigurinë e sistemit të informacionit dhe të harmonizojë politikat dhe proceset për sigurinë e informacionit lidhur me funksionet dhe platformat teknologjike. Personi përgjegjës i raporton drejtorit menaxhues dhe duhet të jetë i pavarur nga njësitë tjera organizative. Personi përgjegjës duhet të raportojë përmes drejtorit menaxhues së paku një herë në vit dhe sipas nevojës te Bordi i drejtorëve i cili duhet të informohet për operacionet dhe funksionet lidhur me sigurinë e informacionit.
3. Në rastin e delegimit të funksioneve të TI-së tek ofruesi i jashtëm i shërbimit (ang. outsource) fondi pensional duhet të caktojë së paku një punonjës të brendshëm të specializuar në fushën e teknologjisë së informacionit, si përgjegjës për koordinimin dhe mbarëvajtjen e funksioneve të TI-së.

Neni 5
Strategjia, Politikat dhe Procedurat për menaxhimin e TI-së dhe sigurinë e informacionit

1. Fondi pensional përcakton strategjinë dhe kërkesa të sigurisë për veprimtarinë e sistemeve të TI-së, politikat për teknologji dhe siguri të informacionit, si dhe procedura për proceset e fushës.
2. Fondi pensional në përputhje me strategjinë e institucionit miraton strategji për zhvillimin e sistemeve të TI-së.
3. Bordi drejtues është përgjegjës për miratimin e politikave të teknologjisë dhe sigurisë së informacionit dhe së paku në baza vjetore duhet të vlerësojë përshtatshmërinë e politikave dhe të kryejë rishikimin e tyre.
4. Strategjia dhe politikat të TI-së miratohen nga Bordi i drejtorëve ndërsa procedura e TI-së miratohen nga Menaxhmenti i lartë.
5. Në rastet kur fondi pensional siguron të gjithë ose një pjesë të veprimtarisë (ose të sistemeve) së tij të TI-së nga ofrues të jashtëm të shërbimit, atëherë fondi pensional miraton procedurë të

brendshme për delegimin e funksioneve për sigurimin e përputhshmërinë me kërkesat e kësaj rregullore për siguri dhe për mirëfunksionim të këtyre sistemeve.

6. Procedura e brendshme për delegimin e funksioneve sipas paragrafit 5 të këtij neni duhet të përfshijnë së paku, elementet si në vijim:
   6.1. Identifikimin e funksioneve që delegohen dhe vlerësimin e ndikimit që ka delegimi i atyre funksioneve;
   6.2. Procedurat për delegimin e funksioneve, përfshirë kriteret për përzgjedhjen e pranuesit të funksioneve të deleguara;
   6.3. Afatet dhe metodat e raportimit të pranuesit të funksioneve të deleguara, te fondi;
   6.4. Mënyrat e monitorimit të pranuesit të funksioneve të deleguara, nga ana e fondit pensional;
7. Politikat dhe procedurat për menaxhimin e TI-së duhet të përcaktojnë së paku elementet në vijim:
   7.1. Administrimi dhe operimi i sistemeve të TI-së;
   7.2. Struktura organizative për menaxhimin e TI-së;
   7.3. Infrastruktura harduerike e fushës së TI-së (diagramet e konfigurimeve);
   7.4. Klasifikimi i dokumentacionit dhe mbrojtja e sistemeve dhe të dhënave;
   7.5. Backup-i të dhënave të sistemeve;
   7.6. Menaxhimi i ndryshimeve të sistemeve (ang. change management);
   7.7. Menaxhimi i incidenteve;
   7.8. Menaxhimi i rrezikut të sistemeve të TI-së;
   7.9. Përcaktimi i mekanizmave të sigurisë së sistemeve të TI-së;
   7.10. Menaxhimi i palëve të treta.
8. Fondi pensional duhet të sigurojë zbatimin e të gjitha politikave dhe procedurave të brendshme të miratuara në lidhje me TI, si dhe të sigurojë që të gjithë përdoruesit e TI të jenë të informuar për përmbajtjen e këtyre politikave dhe procedurave në përputhje me autorizimet dhe përgjegjësitë e tyre.

Neni 6
Zhvillimi dhe prokurimi i sistemeve të TI-së

1. Fondi pensional për të minimizuar rrezikun, duhet të ndjekë trendin e zhvillimeve të sistemeve duke u përkujdesur që të shfrytëzojë vetëm versionet e azhurnuara dhe të mbështetura nga ofruesit e tyre.
2. Fondi pensional duhet të siguroj hartimin dhe miratimin procedurave të brendshme për mënyrën se si realizon zhvillimet, ndryshimet, testimet, vlefshmërinë dhe sigurimin e cilësisë për të zbutur dobësitë e mundshme ose ndërprerjet operacionale në sistemet e saj të TI-së. Sistemet e TI-së vendosen në operim *live*, vetëm pasi punonjësi i specializuar që realizon verifikimin e zbatueshmërisë së procedurave dhe të mirëfunksionimit të sistemeve të japë miratimin e tij të dokumentuar.

3. Përpara vendosjes së sistemit, duhet të kryhet një vlerësim i rrezikut dhe analizës së përputhshmërisë për të siguruar që sistemi plotëson kërkesat e sigurisë, performancës dhe funksionalitet.
4. Në rastet e blerjes së sistemeve fondi duhet të ndjekë një proces prokurimi të standardizuar. Ky proces duhet të përfshijë një vlerësim të plotë të reputacionit të furnizuesit, stabilitetit financiar dhe historikut në ofrimin e zgjidhjeve softuerike të sigurta dhe të besueshme. Marrëveshjet duhet të përshkruajnë qartë pritshmëritë e fondit në lidhje me masat e sigurisë, marrëveshjet e nivelit të shërbimit dhe kërkesat për mbrojtjen e të dhënave.
5. Nëse fondi zgjedh zhvillimin e softuerit të brendshëm, ajo duhet të krijojë një proces të zhvillimit të ciklit jetësor të softuerit (SDLC). Ky proces duhet të përfshijë identifikimin dhe zbatimin e praktikave të sigurta të kodimit, rishikimet e rregullta të kodit, vlerësimet e cenueshmërisë dhe testimin në çdo fazë të zhvillimit. Fondi duhet gjithashtu të krijojë mekanizma për mirëmbajtjen e vazhdueshme, përditësimet dhe monitorimin e performancës dhe sigurisë së softuerit.
6. Ofruesi i jashtëm i shërbimit gjatë implementimit dhe punës në sisteme nuk duhet në asnjë mënyrë të ketë qasje në versionet e sistemit që janë në produksion (live). Kontraktorët dhe palët e tjera të jashtme duhet që të gjitha ndryshimet t'i testojnë në një ambient testues.

Neni 7
Delegimi i funksioneve të TI-së tek ofrues të jashtëm të shërbimit

1. Fondi pensional është përgjegjës për të siguruar që aktiviteti i TI-së kryhet në përputhje me të gjitha kërkesat e përcaktuara në këtë rregullore edhe në rastet ku i gjithë ose një pjesë e aktivitetit të TI-së, sigurohet nga ofrues i jashtëm i shërbimit të TI-së.
2. Para përzgjedhjes së ofruesit të jashtëm të shërbimit të TI-së, fondi duhet të ndërmarrë aktivitetet si në vijim:
   2.1. Përcaktimin e standardeve minimale që ofruesi i jashtëm i shërbimit të TI-së duhet të përmbushë dhe të cilat duhet të harmonizohen me planin e vazhdimësisë së biznesit;
   2.2. Kryerjen e vlerësimit të rrezikut të operacioneve të fondit pensional që mund të lindin nga përdorimi i shërbimit të jashtëm të ofruar gjatë procesimit të aktiviteteve të fondit pensional;
   2.3. Përcaktimin e mënyrës së monitorimit të shërbimit dhe kualitetit të operimit të kompanisë, situatës financiare dhe profilin e rrezikut përmes testimit periodik të pajtueshmërisë me politikën e sigurisë së sistemit të informacionit;
   2.4. Të bëjë përcaktimin e duhur të veprimtarisë së ofruesit të jashtëm të shërbimit të TI-së nga aspekti ligjor dhe financiar, si dhe nga aspekti i mënyrës se si menaxhon sigurinë e sistemit të informacionit të përcaktuar në këtë rregullore;
   2.5. Përcaktimin e menaxhimit të koordinuar të incidenteve të sigurisë.
   2.6. Përcaktimin e masave të nevojshme për shmangien e konfliktit të interesit;
3. Marrëveshja në mes fondit pensional dhe ofruesit të jashtëm të shërbimit të TI-së duhet të përcaktohet përmes kontratës së shkruar e cila ndër të tjera duhet të përfshijë:
   3.1. Të dhënat e palëve të ndërlidhura (fondi pensional dhe ofruesi i jashtëm i shërbimit të TI-së);
   3.2. Përshkrimin e funksioneve të deleguara;

3.3. Të drejtat dhe detyrimet e palëve të ndërlidhura;

3.4. Trajtimin dhe ruajtjen e konfidencialitetit të të dhënave;

3.5. Afatet kohore të ofrimit të shërbimit dhe periudhën e njoftimit për përfundimin e kontratës e cila është e mjaftueshme për gjetjen e zgjidhjeve alternative; ;

3.6. Nivelin e ofrimit të shërbimit (ang. Service level agreement);

3.7. Dispozitë që përcakton se ofruesi i jashtëm i shërbimit të TI-së, do t'i nënshtrohet mbikëqyrjes nga ana e BQK-së lidhur me aktivitetet e deleguara të TI-së;

3.8. Dispozitë që përcakton që ofruesit të shërbimit të TI-së të kryejnë veprimtarinë e tij në përputhje me legjislacionin në fuqi, kërkesat, rregullatorët, si dhe politikat e miratuara nga fondi pensional dhe për të bashkëpunuar me BQK-në për sa i përket funksioneve të deleguara;

3.9. Të drejtën e fondit pensional për t'u informuar në lidhje me mbarëvajtjen e funksioneve të deleguara nga ofruesi i jashtëm i shërbimeve të TI-së, si dhe të drejtën e fondit për të dhënë udhëzime të përgjithshme apo të veçanta në lidhje me kryerjen e funksioneve të deleguara;

3.10. Të drejtën e fondit pensional të inspektojë dhe kontrollojë veprimtarinë e ofruesit të jashtëm të shërbimit të TI-së lidhur me aktivitetet e deleguara të TI-së.

3.11. Detyrimin e ofruesit të jashtëm të shërbimit të TI-së për të informuar menjëherë fondin pensional për çdo fakt që mund të ketë një ndikim të rëndësishëm në aftësinë e tij për të kryer në mënyrë efikase dhe efektive veprimtarinë e tij sipas kërkesave ligjore në fuqi;

4. Ofruesi i jashtëm i shërbimit nuk mund t'i nënkontraktojë shërbimet përveç nëse është përcaktuar në marrëveshjen bazë të lidhur në mes fondit pensional dhe këtij ofruesi të shërbimit.

5. Fondi pensional është i obliguar të menaxhojë rreziqet që rrjedhin nga marrëdhëniet kontraktuale me ofruesit e jashtëm të shërbimit, aktivitetet e të cilëve kanë të bëjnë me sistemin e informacionit që është në përdorim nga fondi pensional.

6. Fondi pensional është i obliguar të monitorojë vazhdimisht metodën dhe cilësinë e aktiviteteve të kontraktuara nga ofruesi i jashtëm.

Neni 8
Siguria e sistemeve të informacionit

1. Siguria e sistemeve të informacionit bazohet në përcaktimin e përmbushjes së kritereve të mëposhtme:

1.1. Konfidencialiteti: informacioni duhet të jetë i qasshëm vetëm për përdoruesit e autorizuar;

1.2. Integriteti: ruajtje e saktësisë dhe plotësisë së sistemit të informacioni;

1.3. Disponueshmëria: qasje në çdo kohë në sistemin e informacionit për përdoruesit e autorizuar.

2. Fondi pensional duhet të menaxhojë në vazhdimësi procesin e sigurisë së sistemit të informacionit. Fondi pensional duhet të identifikojë dhe monitorojë nevojat për sigurinë e sistemit të informacionit, të paktën duke u bazuar në rezultatet e vlerësimit të rrezikut të atij sistemi dhe detyrimet që lindin nga aktet e brendshme apo marrëdhëniet kontraktuale.

3. Fondi pensional duhet të përcaktojë procedurat, metodat dhe kriteret për klasifikimin e informacionit sipas shkallës së ndjeshmërisë dhe relevancës - në lidhje me pasojat e mundshme të shkeljes së konfidencialitetit, integritetit të tyre dhe disponueshmërinë.
4. Fondi pensional duhet të sigurojë, që siguria e informacionit dhe të gjitha aktivitetet që ndërlidhen me të, duhet të jenë në pajtueshmëri me të gjitha ligjet në fuqi që kanë të bëjnë me informatat dhe operacionet e institucionit.

Neni 9
Siguria në shërbimet e hapësirave *cloud*

1. Pranuesi i shërbimeve *cloud* duhet të përgatitë dhe përcaktojë politikë dhe procedurë për menaxhimin e shërbimeve *cloud*.
2. Ofruesit e shërbimeve *cloud* duhet të kenë eksperiencë dhe reputacion afirmativ në ofrimin e shërbimeve *cloud*.
3. Ofruesit e shërbimeve *cloud* duhet t'i përmbahen standardeve të pranuara ndërkombëtarisht për të garantuar sigurinë, integritetin dhe konfidencialitetin e të dhënave të përpunuara, të ruajtura ose të transferuara përmes platformave të tyre, gjithnjë duke respektuar praktikat, procedurat dhe politikën për siguri të informacionit të pranuesit të shërbimeve, si dhe duke respektuar të gjitha ligjet dhe rregulloret në fuqi. Ofruesit e këtyre shërbimeve duhet të vendosin masa gjithëpërfshirëse sigurie që përfshijnë klasifikimin dhe mbrojtjen e të dhënave, kontrollet e qasjes, metodat e enkriptimit, planin dhe procedurat e reagimit ndaj incidenteve dhe planin e rimëkëmbjes nga fatkeqësitë dhe vazhdimësisë së punës.
4. Pranuesit e shërbimeve në hapësirat *cloud* duhet të vlerësojnë masat e sigurisë të zbatuara nga ofruesit e shërbimeve *cloud* dhe të monitorojnë rregullisht pajtueshmërinë e tyre për të zbutur rreziqet e mundshme që cenojnë sigurinë e të dhënave ose qasjen e paautorizuar.
5. Kontrollet e sigurisë së pranuesit të shërbimeve (procedurat operative, procedurale apo teknike, për të mbrojtur integritetin, konfidencialitetin dhe saktësinë e të dhënave dhe sistemeve të informacionit të pranuesit të shërbimeve) duhet të zbatohen nga ofruesi i shërbimeve *cloud* në mënyrë korrekte dhe efektive.
6. Ofruesit e shërbimeve *cloud* duhet të ofrojnë hapësirën *cloud* e cila është fizikisht e ndarë nga hapësirat e klientëve të tjerë, si dhe duhet të posedojnë procedura dhe politika të mbledhjes dhe ruajtjes së gjurmëve të auditimit për t'u siguruar se çdo aktivitet monitorohet në mënyrë efektive.
7. Qasjet nga larg në sistemet e informacionit të hostuara në hapësirat *cloud* duhet të mundësohen me metodat për autentikim me dy apo më shumë faktorë (ang. Multi -factor authentication). Komunikimi mes pajisjes që qaset në shërbimet/resurset e hostuara në *cloud* nga larg duhet të ketë të vendosura masat e enkriptimit *end-to-end* për çdo seancë të komunikimit.
8. Konfigurimet e infrastrukturës, lista e shërbimeve/resurseve që ofrohen në hapësirat *cloud,* si dhe lista e aplikacioneve që funksionojnë në hapësirat *cloud* duhet të jetë transparente dhe e dokumentuar në mënyrë të detajuar.
9. Ofruesi i shërbimeve *cloud* duhet të ofrojë procedurë dhe politikë të krijimit, testimit dhe mbrojtjes së kopjeve rezervë e cila është në përputhje me politikat dhe procedurat e pranuesit të shërbimeve.

10. Në rast të ndodhjes së një qasje të paautorizuar ose ndonjë incidenti sigurie, ofruesve të shërbimeve *cloud* u kërkohet të raportojnë menjëherë incidente të tilla tek autoritetet rregullative dhe tek pranuesi i shërbimit.
11. Ofruesit e shërbimeve *cloud* duhet të ofrojnë dokumentacion transparent në lidhje me praktikat e tyre të sigurisë dhe ta bëjnë këtë dokumentacion të disponueshëm për shqyrtim gjatë procesit të ekzaminimit apo auditimit.
12. Duhet të bëhet *penetration* test dhe vlerësim i dobësive dhe rreziqeve të mundshme të sigurisë që lidhen me mbajtjen e të dhënave dhe sistemeve të informacionit në hapësirat *cloud* së paku një herë në vit.
13. Ofruesi i shërbimeve duhet të posedoj politikë apo procedurë për fshirjen e sigurtë të të dhënave (ang. Secure data deletion) dhe shkatërrimin e infrastrukturës me rastin e shkëputjes së kontratës apo largimin e shërbimeve resurseve nga përdorimi.
14. BQK posedon të drejtën për të kryer ekzaminime dhe vlerësime të rregullta të ofruesve të shërbimeve *cloud* në industrinë e pensioneve për të verifikuar përputhjen e standardeve dhe praktikave më të mira për siguri të informacionit.

Të gjitha kërkesat e kësaj rregulloreje për sistemet e informacionit aplikohen përshtatshmërisht edhe për ofruesit e shërbimeve *cloud* që lidhen me shërbimet në hapësirat *cloud*.

Neni 10
Menaxhimi i rrezikut për sistemet e informacionit

1. Fondi pensional vendos kritere për rrezikun e lejueshëm në lidhje me përdorimin e sistemeve të saj të informacionit sipas standardeve të pranuara ndërkombëtarisht.
2. Të paktën një herë në vit ose në çdo rast ndryshimesh të rëndësishme të kërkesave të sigurisë së informacionit, fondi pensional kryen analiza të rrezikut të sistemeve të informacionit për të siguruar që ky rrezik mbahet brenda kufijve të pranueshëm lidhur me veprimtarinë e fondit. Rezultatet e analizës së rrezikut dokumentohen.
3. Procesi i vlerësimit të rrezikut përfshin, por pa u kufizuar në, hapat e mëposhtëm:
   3.1. Identifikimi i kërkesave dhe objektivave të sistemit.
   3.2. Vlerësimi i dobësive dhe rreziqeve të mundshme të sigurisë që lidhen me sistemin.
   3.3. Vlerësimi i ndikimit të mundshëm në operacionet e fondit, privatësinë e të dhënave dhe konfidencialitetin e subjektit të të dhënave.
   3.4. Vlerësimi i përputhshmërisë së sistemit me sistemet tjera dhe infrastrukturën ekzistuese.
   3.5. Vlerësimi i zgjerueshmërisë, besueshmërisë dhe mirëmbajtjes së sistemit.
   3.6. Analiza e çështjeve të mundshme të pajtueshmërisë ligjore dhe rregullative.
   3.7. Vlerësimi i implikimeve financiare dhe burimore të zbatimit, blerjes ose zhvillimit të brendshëm.
4. Bazuar në rezultatet e vlerësimit të rrezikut, fondi duhet të zhvillojnë një plan për zbutjen e rrezikut që përshkruan masat e nevojshme për të minimizuar rreziqet e identifikuara. Plani i zbutjes së rrezikut duhet të përfshijë, por pa u kufizuar në:

4.1. Zbatimi i masave të duhura të sigurisë për mbrojtjen e të dhënave.

4.2. Krijimi i procedurave të kopjimit dhe rikuperimit te të dhënave.

4.3. Integrimi i sistemit me sistemet tjera dhe infrastrukturën ekzistuese.

4.4. Sigurimi i trajnimit dhe mbështetjes së nevojshme për punonjësit e përfshirë në zbatimin, blerjen ose zhvillimin e softuerit.

4.5. Pajtueshmërinë me kërkesat ligjore dhe rregullative përkatëse.

4.6. Shpërndarja e burimeve adekuate financiare dhe njerëzore për të siguruar zbatimin, blerjen ose zhvillimin e suksesshëm të brendshëm.

5. Fondet duhet të rishikojnë dhe përditësojnë rregullisht vlerësimin e rrezikut dhe planin e zbutjes së rrezikut gjatë gjithë ciklit jetësor të softuerit për të adresuar çdo rrezik të shfaqur ose ndryshim në kërkesat e fondit dhe mjedisin operativ.
6. Fondi pensional duhet të njoftojë BQK-në me shkrim në rast të identifikimit të incidenteve, në sistemet e informacionit dhe ndryshimeve në funksionet kyçe të proceseve të rëndësishme të sistemeve të informacionit të cilat mund të pengojnë ose rrezikojnë institucionin, jo më vonë se një ditë pune pas ndodhjes së incidentit.
7. Menaxhimi i rrezikut të sistemit të informacionit duhet të përfshijë të gjithë sistemin e informacionit të fondit të integruar në të gjitha fazat e zhvillimit të tij.
8. Menaxhimi i rrezikut të sistemit të informacionit duhet të përfshijë planin vjetor të vetëdijesimit të punonjësve të fondit për përdorimin adekuat të shërbimeve të ofruara përmes sistemit të informacionit të fondit.

Neni 11
Siguria fizike e sistemeve të informacionit

1. Fondi pensional duhet të ndërmarrë masa të nevojshme të sigurisë për të ndaluar çdo qasje fizike të paautorizuar, ndërhyrje apo dëmtim i informatave, pajisjeve përpunuese të informatave dhe operacioneve të fondit bazuar në standardet e pranuara ndërkombëtarisht.
2. Fondi pensional duhet të krijojë procedura të qasjes dhe punës për zonat e sigurisë për të gjithë punonjësit dhe palët e jashtme. Zonat e sigurisë duhet të jenë të mbrojtura përmes kontrolleve të qasjes për të siguruar që vetëm punonjësit e autorizuar të kenë qasje.
3. Masat e sigurisë duhet të caktohen edhe për pajisjet e përdorura dhe vendosura jashtë objekteve të fondit pensional varësisht prej lokacionit dhe duhet të merren në konsideratë rreziqet gjatë përcaktimit të kontrolleve të nevojshme.
4. Pajisjet duhet të mirëmbahen për t'u mbrojtur nga dështimet, për të siguruar disponueshmëri të vazhdueshme e integritet dhe të mbështeten nga ndërprerjet si rezultat i dështimeve të pajisjeve ndihmëse, katastrofave natyrore, sulmeve keqdashëse, apo aksidentale etj.
5. Të gjitha pajisjet që përmbajnë informacion duhet të verifikohen për të siguruar se të gjitha të dhënat dhe softuerët e licencuar janë larguar para hedhjes, shkatërrimit ose ripërdorimit, për të pamundësuar rikthimin e informacionit origjinal.
6. Të gjithë shfrytëzuesit duhet të vetëdijesohen për kërkesat e sigurisë dhe procedurat për mbrojtjen e pajisjeve të pambikëqyrura.

7. Fondi duhet të përcaktojë kritere, metoda dhe procedura për tavolinë të pastër me qëllim të mbrojtjes së informacionit.
8. Obligimet kontraktuale për punonjësit dhe ofruesit e jashtëm të shërbimit të TI-së duhet të reflektojnë politikat e fondit pensional për sigurinë e informacionit. Të gjithë punonjësit dhe ofruesit e jashtëm të shërbimit të TI-së duhet të kuptojnë përgjegjësitë për rolet që konsiderohen.
9. Ku është e përshtatshme për aplikim, fondi përcakton se punonjësit dhe ofruesit e jashtëm të shërbimeve ruajnë informacionin e marrë gjatë ushtrimit të veprimtarisë së tyre edhe për një periudhë të caktuar pas ndërprerjes së marrëveshjes kontraktuale me punonjësin apo ofruesit e jashtëm të shërbimit të TI-ve.
10. Fondi duhet të përcaktojë veprimet dhe masat që duhet të ndërmarrë në rast të shkeljes së kërkesave të sigurisë nga punonjësit ose ofruesit e jashtëm të shërbimit të TI-së.

Neni 12
Menaxhimi i rrjetave kompjuterike

1. Rrjeti kompjuterik i fondi duhet të menaxhohet dhe kontrollohet me qëllim të mbrojtjes së informacionit të sistemeve dhe aplikacioneve. Fondi duhet të implementojë kontrollë për të siguruar mbrojtjen e konfidencialitetit dhe integritetit të informacionit në rrjet dhe mbrojtjen e shërbimeve nga qasjet e paautorizuara bazuar në standardet e pranuara ndërkombëtarisht.
2. Për menaxhimin e rrjetave kompjuterike fondi duhet të përcaktojë:
   2.1. Procedura për përdorimin dhe menaxhimin e shërbimeve dhe pajisjeve të rrjetit me qëllim të kufizimit të qasjeve në shërbimet e rrjetit dhe aplikacionet;
   2.2. Vendosjen e kontrollave të veçanta për mbrojtjen e konfidencialitetit dhe integritetit të të dhënave që kalojnë përmes rrjeteve publike ose pa tela (ang. wireless);
   2.3. Teknologjinë e aplikuar për sigurinë e shërbimeve të rrjetit si autentikimi, enkriptimi dhe kontrollet e lidhjeve në rrjet;
   2.4. Grupet e shërbimeve të informacionit, shfrytëzuesit dhe sistemet e informacionit duhet të izolohen nga rrjetat publike;
   2.5. Kontrolla të veçanta duhet kushtuar qasjeve të ofruesve të jashtëm të shërbimit në rastet e nevojës për interkoneksion (lidhjet me palët e treta).

Neni 13
Menaxhimi i aseteve të sistemeve të informacionit

1. Fondi duhet të identifikojë të gjitha asetet në sistemet e informacionit.
2. Fondi duhet të mbajë inventarin e të gjitha aseteve me të gjitha informacionet e nevojshme, duke përfshirë këtu tipin e asetit, formatin, lokacionin, informacionet mbi backup-in (aty ku është i aplikueshëm), informacionet mbi licencën dhe vlerën për biznesin.
3. Fondi duhet të përcaktojë dhe dokumentojë pronësinë dhe klasifikimin e të gjitha aseteve të lidhura me procesimin e informacioneve.
4. Pronari i asetit është përgjegjës për:

4.1. Të siguruar se informacionet dhe asetet e lidhura me procesimin e informacioneve janë të klasifikuar sipas ndjeshmërisë;

4.2. Të përcaktojë dhe rishikojë rregullisht kufizimet në qasje dhe klasifikim.

5. Fondi duhet të përcaktojë rregullat mbi përdorimin e pranueshëm të informacioneve dhe aseteve të lidhura me procesimin e informacioneve.

Neni 14
Menaxhimi i qasjes së përdoruesve

1. Fondi menaxhon qasjet në sistemet e informacionit përmes procedurave të brendshme përkatëse për menaxhimin të drejtave për qasje të përdoruesve. Procedurat e brendshme duhet të përmbajnë kritere për qasje, autorizim, identifikim dhe vërtetim të përdoruesve sipas standardeve të pranuara ndërkombëtarisht.
2. Çdo shfrytëzues duhet të jetë unik dhe sistemi duhet të përcaktojë kriteret e vendosjes së fjalëkalimit sipas standardeve të pranuara ndërkombëtarisht. Para dhënies së qasjes në sistemet e informacionit, si punëtorët e brendshëm të fondit edhe ofruesit e jashtëm të shërbimit, duhet të nënshkruajnë në marrëveshje për ruajtjen e konfidencialitetit dhe mos zbulimit të informacionit.
3. Fondi duhet të sigurohet që autorizimi i qasjes së përdoruesve në sistemet e informacionit të bëhet nga personat përgjegjës të atyre sistemeve dhe të bazohet në parimin e qasjes më të ulët të mundshme në sistem, duke mundësuar kryerjen e detyrave të punës. Fondi duhet që së paku në baza 6 mujore të rishikojë të drejtat e qasjes së përdoruesve në sistemet e rëndësisë së lart bazuar në vlerësimin e rrezikut dhe së paku në baza vjetore të gjitha sistemet tjera.
4. Në menaxhimin e të drejtave të qasjes së përdoruesve, fondi duhet që në mënyrë të veçantë të autorizojë qasje të privilegjuar dhe/ose qasjet nga larg në sistemin e informacionit. Të gjitha qasjet dhe aktiviteti i përdoruesve të privilegjuar dhe qasjet nga larg duhet të monitorohen.
5. Qasjet nga larg në sistemet e informacionit duhet të mundësohen me metodat për autentikim me dy apo me shume faktorë (ang. Multi - factor authentication). Komunikimi mes pajisjes që qaset në sistemin e informacionit nga larg duhet të ketë të vendosura masat e enkriptimit *end-to-end* për çdo seancë të komunikimit.
6. Fondi pensional duhet të monitorojë dhe ruaj ngjarjet (ang. events) e sigurisë së informacionit në infrastrukturën e tyre duke u bazuar në standardet të pranuara ndërkombëtarisht.

Neni 15
Ruajtja e informacionit

1. Ruajtja e informacionit (backup) duhet të bëhet sipas procedurave të brendshme të fondit pensional.
2. Aktet e brendshme sipas paragrafit 1 të këtij neni duhet të përmbajnë së paku elementet si në vijim:

2.1. Caktimin e nivelit të nevojshëm të backup-it të informacionit;

2.2. Mbajtjen e të dhënave të sakta dhe të kompletuara mbi backup-in e informacioneve, si dhe procedurat e dokumentuara të rikthimit të backup-ëve;

2.3. Llojin (ang. Full, incremental, differential) dhe frekuencën e backup-ëve sipas kompleksitetit të biznesit.

3. Orari i krijimit të backup-ëve duhet të caktohet duke u siguruar që të gjitha informacionet dhe softueri mund të rimëkëmben në rast të fatkeqësive ose dështimit të pajisjeve.
4. Backup-ët duhet të ruhen në një lokacion të dytë, në një distancë të mjaftueshme për të mos qenë të rrezikuar nga kërcënime të njëjta me lokacionin qendror.
5. Backup-ëve duhet t'iu jepet niveli i duhur i mbrojtjes fizike dhe mjedisore konsistent me standardin e aplikuar në lokacionin qendror.
6. Backup-ët duhet të testohen rregullisht, duke siguruar që ata janë të besueshëm dhe të shfrytëzueshëm kur nevojiten.
7. Backup-ët duhet të mbrohen nga qasjet e paautorizuara përmes enkriptimit.
8. Kohëzgjatja e ruajtjes së informacionit duhet të bëhet sipas legjislacionit në fuqi.

Neni 16
Auditimi i brendshëm i sistemit të informacionit

1. Kërkesat e përcaktuara nga rregullorja për kontrollet e brendshme dhe auditimin e brendshëm zbatohen për auditmin e sistemit të informacionit.
2. Veprimtaria e fushës së TI-së duhet t'i nënshtrohet së paku rishikimit periodik vjetor që fokusohet në metodologjinë e bazuar në rrezik.
3. Auditimet e TI-së duhet të kryhen nga personat kompetent në kuadër të funksionit të auditimit të brendshëm ose nga persona të jashtëm të kontraktuar për këtë qëllim.
4. Të gjitha kërkesat e kësaj rregulloreje dhe rregullores së përcaktuar në paragrafin 1 të këtij neni mbesin të zbatueshme në rastet kur aktivitetet e auditimit të brendshëm kontraktohen.

Neni 17
Dhoma e serverëve

1. Dhoma e serverëve duhet të jetë e veçantë nga zyrat e tjera të fondit pensional dhe duhet të vendoset në brendësi të objekteve të fondit.
2. Për të mundësuar ruajtjen e shënimeve dhe vazhdimësinë e biznesit (si back-up) në rast të fatkeqësive apo katastrofave natyrore, fondi duhet të caktojnë edhe një lokacion tjetër rezervë, ku vendosen serverët e nevojshëm. Ky lokacion rezervë duhet të vendoset në largësi nga qendra kryesore e fondit, sipas standardeve të pranuara ndërkombëtarisht për këtë lëmi.
3. Fondi pensional në dhomën e serverit të tyre qendror dhe në lokacionin rezervë për ruajtjen e shënimeve, duhet të plotësojnë kërkesat e mëposhtme të sigurisë për dhomën e serverëve:

   3.1. të ketë pajisjet e nevojshme për mbajtjen e temperaturës në nivelin e duhur;

   3.2. të kenë pajisjet e nevojshme për mbajtjen e lagështisë në nivelin e duhur;

   3.3. të ketë mbrojtje elektronike me:

      3.3.1. sensorë sizmikë;

3.3.2. sensorë lëvizjeje;

3.3.3. sensorë tymi.

3.4. të ketë sistem monitorimi me kamera për:

3.4.1. hyrjen në këtë dhomë; dhe

3.4.2. ambientin e brendshëm të kësaj dhome.

3.5. të ketë mbrojtje nga zjarri.

3.6. të jetë i pajisur me një burim të dytë dhe të vazhdueshëm të energjisë elektrike.

4. Dhoma e serverëve duhet të jetë e kufizuara për qasje vetëm për personelin e autorizuar me metodat për autentikim me dy apo më shumë faktorë dhe të monitorohet përmes evidentimit të hyrje / daljeve të stafit dhe personave të jashtëm në këto hapësira.

5. Fondi pensional duhet të përcaktojë kushtet e qasjes së personelit dhe palëve të treta të autorizuara për qasje në dhomën e serverëve në rast të urgjencave.

6. Me kërkesë të fondit, Banka Qendrore e Republikës së Kosovës mund të bëjë përjashtime nga disa kërkesa të parapara në paragrafin 3 të këtij neni, por në të njëjtën kohë BQK-ja në vazhdimësi mund të kërkojë përmbushjen e kërkesave minimale të sigurisë për zyrat e caktuara.

Neni 18

Vazhdimësia e operimit pas ndërprerjes si rezultat i ngjarjeve të jashtëzakonshme

1. Fondi pensional duhet të vendosë proces të menaxhimit në vazhdimësinë e punës me qëllim që të sigurojë funksionim të papenguar dhe të vazhdueshëm të të gjitha sistemeve dhe proceseve kritike, si dhe t'i kufizojë humbjet në kushte të veprimit jo të rregullt duke u bazuar në standardet e pranuara ndërkombëtarisht.

2. Fondi pensional duhet të menaxhojë me vazhdimësinë e punës në bazë të analizës të ndikimeve të veprimtarisë dhe vlerësimit të rreziqeve, e cila duhet të përfshijë:

2.1. Përcaktimin e proceseve kritike të punës të domosdoshme për funksionim të papenguar dhe të vazhdueshëm të fondit pensional;

2.2. Përcaktimin e resurseve dhe sistemeve të nevojshme për kryerjen e proceseve individuale të punës, si dhe lidhjet dhe varësitë ndërmjet tyre;

2.3. Vlerësim të rrezikut për secilin nga proceset individuale të punës, si dhe gjasat për ndodhjen e rasteve të padëshiruara dhe ndikimin e tyre në vazhdimësinë e punës, humbjet financiare dhe reputacioni i fondit pensional;

2.4. Përcaktimin e nivelit të rreziqeve të pranueshme dhe teknikat për zbutjen e rreziqeve të identifikuara;

2.5. Përcaktimin e kohëzgjatjes së ndërprerjes së pranueshme të punës për secilin nga proceset.

3. Fondi pensional duhet të aprovojë një plan për analizën e ndikimit në biznes (BIA) që analizon ndërprerjen e aktiviteteve, që së paku përmban:

3.1. Proceset që janë më me prioritet, si dhe resurset e nevojshme për këto procese;

3.2. Aktivitetet finale që duhet të arrihen (ang. Service Delivery Objective);

3.3. Kohën e fundme të rimëkëmbjes (ang. Recovery Time Objective);

3.4. Pika e fundme e kthimit (ang. Recovery Point Objective).

4. Bordi drejtues i fondit pensional duhet, të miratojë në baza vjetore Planin e Vazhdimësisë së Biznesit, si dhe Planin e Rimëkëmbjes nga Fatkeqësitë, i cili rregullon krijimin e kushteve për rimëkëmbjen dhe disponueshmërinë e resurseve të sistemit informativ të nevojshme për të kryer proceset kritike të biznesit.

5. Plani i Vazhdimit të Biznesit dhe ai i Rimëkëmbjes nga Fatkeqësitë duhet të përfshijë së paku kërkesat në vijim:

5.1. procedurat që duhet ndërmarrë në rast të ndërprerjes së funksionimit të sistemeve;

5.2. një listë të përditësuar të të gjitha resurseve të nevojshme njerëzore dhe teknike për të rivendosur vazhdimësinë e biznesit;

5.3. informacion në lidhje me personat përgjegjës dhe zëvendësit e tyre të cilët janë përgjegjës për rimëkëmbjen e operacioneve në rast të ngjarjeve të paparashikuara, duke përfshirë detyrat e tyre të përcaktuara dhe përgjegjësitë, si dhe planin e linjave të brendshme dhe të jashtme të komunikimit;

5.4. një lokacion alternativ në rast të ndërprerjes së biznesit dhe rimëkëmbjes në funksion proceseve të biznesit në lokacionin primar. Ky lokacion duhet të ketë distancën e duhur nga qendra primare, me qëllim të shmangies së ndikimit të rreziqeve të njëjta në të dy lokacionet.

6. Për zbatimin e planeve sipas paragrafit 5 të këtij neni fondi pensional siguron që të gjithë punonjësit të njihen me rolet dhe përgjegjësitë e tyre në raste urgjente.

7. Fondi pensional harmonizon planet me ndryshimet e biznesit, duke përfshirë ndryshimet në produktet, aktivitetet, proceset dhe sistemet, me ndryshimet në mjedis, si dhe me politikën e biznesit dhe strategjinë e biznesit.

8. Fondi pensional teston planet, së paku një herë në vit dhe pas shfaqjes së ndryshimeve të rëndësishme, si dhe dokumenton rezultatet e këtyre dhe testeve.

9. Në menaxhimin e vazhdimësisë së biznesit, fondi pensional merr parasysh aktivitetet që u janë besuar palëve të treta dhe varësinë nga shërbimet e këtyre palëve.

10. Në rast të rrethanave që kërkojnë zbatimin e planit të vazhdimësisë së biznesit dhe planit për aktivitetet e rimëkëmbjes në rast të një fatkeqësie, fondi pensional njofton Bankën Qendrore të Republikës së Kosovës, jo më vonë se ditën pas shfaqjes së rrethanave të tilla. Banka Qendrore e Republikës së Kosovës mund të kërkojë dokumentacion shtesë lidhur me faktet relevante në lidhje me këto rrethana dhe të përcaktojë afat për dorëzimin e këtij dokumenti.

Neni 19
Dokumentimi i veprimtarisë së TI-së

Fondi pensional mban dokumentacion të plotë dhe të përditësuar të organizimit, të pajisjeve, të sistemeve, të qasjeve dhe të faktorëve të tjerë të rëndësishëm që lidhen me veprimtarinë e TI-së. Një dokumentacion i tillë provon se përputhshmëria me kërkesat e kësaj rregulloreje është e vazhdueshme.

Neni 20
Masat përmirësuese

Çdo shkelje e dispozitave të kësaj rregulloreje është jetë subjekt i masave përmirësuese dhe ndëshkuese siç përcaktohet në Ligjin për Bankën Qendrore të Republikës së Kosovës dhe Ligjit për Fondet Pensionale të Kosovës.

Neni 21
Hyrja në fuqi

1. Kjo rregullore hyn në fuqi në ditën e miratimit të saj.
2. Fondet pensionale duhet të sigurojnë pajtueshmërinë me të gjitha dispozitat e aplikueshme deri më 30 qershor 2024.

Bashkim Nurboja
Kryetar i Bordit të Bankës Qendrore të Republikës së Kosovës