МОНГОЛБАНКНЫ
ЕРӨНХИЙЛӨГЧИЙН ТУШААЛ

2018 оны 3 сарын 6 өдөр Дугаар А-57 Улаанбаатар хот

Тушаалд өөрчлөлт оруулах тухай

Төв банк (Монголбанк)-ны тухай хуулийн 28 дугаар зүйлийн 1 дэх хэсгийг үндэслэн ТУШААХ нь:

1.Монголбанкны Ерөнхийлөгчийн 2017 оны 6 дугаар сарын 29-ний өдрийн А-189 дүгээр тушаалын 2 дахь заалтыг дор дурдсанаар өөрчилсүгэй:

1/ Тушаалын 2 дахь заалт:

"2. Банкны мэдээллийн технологийн шалгуур үзүүлэлтийн журмын 2.6 дахь заалтыг 2019 оны 01 дүгээр сарын 01-ний өдрөөс, 3.2, 6.1.2 дахь заалтыг 2021 оны 01 дүгээр сарын 01-ний өдрөөс эхлэн хэрэгжүүлэхээр тогтоосугай."

2.Энэ тушаалыг холбогдох банкуудад хүргүүлж ажиллахыг Хяналт шалгалтын газар (Н.Батсайхан)-т үүрэг болгосугай.

МОНГОЛБАНКНЫ
ЕРӨНХИЙЛӨГЧ Н.БАЯРТСАЙХАН

14 0351

Tushaal 2018.doc

МОНГОЛБАНКНЫ ЕРӨНХИЙЛӨГЧИЙН ТУШААЛ

2017 оны 6 сарын 29 өдөр Дугаар А-189 Улаанбаатар хот

Журам батлах тухай

Төв банк (Монголбанк)-ны тухай хуулийн 28 дугаар зүйлийн 1 дэх хэсгийн 2 дахь заалтыг үндэслэн ТУШААХ нь:

1.“Банкны мэдээллийн технологийн шалгуур үзүүлэлтийн журам”-ыг хавсралт ёсоор батлсугай.

2.Дээрх журмын 3.2, 7.3 дахь заалтыг 2018 оны 01 дүгээр сарын 01-ний өдрөөс, 2.6, 6.1.2 дахь заалтыг 2019 оны 01 дүгээр сарын 01-ний өдрөөс эхлэн хэрэгжүүлэхээр тогтоосугай.

3.Энэхүү тушаалын биелэлтэд хяналт тавьж ажиллахыг Хяналт шалгалтын газар (Н.Батсайхан)-т үүрэг болгосугай.

МОНГОЛБАНКНЫ ЕРӨНХИЙЛӨГЧ Н.БАЯРТСАЙХАН

14-1228

Tushaal 2017.doc

Монголбанкны Ерөнхийлөгчийн 2017 оны 06 дугаар сарын
29–ны өдрийн А/139 дугаар тушаалын хавсралт

БАНКНЫ МЭДЭЭЛЛИЙН ТЕХНОЛОГИЙН ШАЛГУУР ҮЗҮҮЛЭЛТИЙН ЖУРАМ

НЭГ. НИЙТЛЭГ ҮНДЭСЛЭЛ

1.1. Энэхүү журмын зорилго нь Төв банк (Монголбанк)-ны тухай хууль, Банкны тухай хууль болон Үндэсний төлбөрийн системийн тухай хууль тогтоомжийг үндэслэн олон улсын COBIT тогтолцоо болон төлбөрийн картын мэдээллийн аюулгүй байдлын PCI DSS стандартад үндэслэн банкны мэдээллийн технологи, түүний үйл ажиллагаа, мэдээллийн системд гарч болох эрсдэлийг удирдах, аюулгүй байдлыг хангах, ерөнхий шалгуур үзүүлэлтийг тогтоож тэдгээрийн биелэлтэд хяналт тавихад оршино.

1.2. Энэхүү журам нь Төв банк (Монголбанк)-аас Монгол Улсад банкны үйл ажиллагаа эрхлэх зөвшөөрөл авсан банкинд ашиглагдаж байгаа мэдээллийн технологи, мэдээллийн систем, түүний үйл ажиллагаанд үйлчилнэ.

1.3. Банк нь энэ журамд нийцүүлэн өөрийн үйл ажиллагааны онцлог, цар хүрээ болон боловсронгуй байдалтай уялдуулан Мэдээллийн технологитой холбоотой дотооддоо баримтлах бодлого, дүрэм, журам, заавар холбогдох бусад баримт бичгийг боловсруулан мөрдөж ажиллана.

1.4. Дараах нэр томьёог дор дурдсан утгаар ойлгоно:

1.4.1. “Банкны оролцогч тал /bank stakeholders/” гэж тухайн банкны үйл ажиллагаанд нөлөөлж буй эсвэл нэгдмэл ашиг сонирхол бүхий бүлгийг;

1.4.2. “Үндсэн төв /primary processing center/” гэж үндсэн бүртгэлийн систем, дэд систем тэдгээрийн сервер, тоног төхөөрөмж байршиж буй төвийг;

1.4.3. “Нөөц төв /alternative processing center/” гэж үндсэн төвд онцгой нөхцөл үүссэн үед хэвийн үйл ажиллагааг ханган ажиллах зорилго бүхий үндсэн бүртгэлийн нөөц систем, түүний сервер, тоног төхөөрөмж байршиж буй төвийг;

1.4.4. “Үндсэн бүртгэлийн систем” гэж банкны санхүүгийн үндсэн бүртгэлийг хөтлөн явуулж буй систем, програм хангамжийг;

1.4.5. “Дэд систем” гэж үндсэн бүртгэлийн системээс бусад банкны систем програм хангамжийг;

1.4.6. “Мэдээллийн систем” гэж үндсэн бүртгэлийн болон дэд системүүдийг;

1.4.7. “Гуравдагч тал /third party vendors/” гэж авч үзэж буй асуудлуудад оролцож буй талуудаас тусгаар, хамааралгүй хувь хүн, байгууллагыг;

1.4.8. “Үйлчилгээ үзүүлэгч /vendor/” гэж гэрээгээр үйлчилгээ, бүтээгдэхүүн нийлүүлэгч бие даасан хараат бус хувь хүн, байгууллагыг;

1.4.9. “Гүйлгээний лог бүртгэл /log/” гэж үндсэн бүртгэлийн системийн санхүүгийн гүйлгээ хийсэн, хийхийг завдсан дэлгэрэнгүй түүхийг;

1.4.10. “Үйлдлийн лог бүртгэл /log/” гэж үндсэн бүртгэлийн системд нэвтэрсэн, өөрчлөлт хийсэн, хийхийг завдсан болон өөрчлөлт хийсэн үйлдлийн түүхийг;

1.4.11. “Лог бүртгэл” гэж гүйлгээний болон үйлдлийн лог бүртгэлийг;

1.4.12. “Мэдээллийг эзэмшигч /data owner/” гэж тухайн мэдээллийг хариуцагч, хэрэглэгч, банкны нэгжийг;

1.4.13. “Бүрэн бүтэн байдал /integrity/” гэж мэдээллийн үнэн зөв, бүрэн бүтэн байдлыг хангасан байдлыг;

1.4.14. “Мэдээллийн технологийн ерөнхий хяналт, удирдлага /General control/” гэж мэдээллийн технологийн бүхий л үйл ажиллагааг хамарсан хяналтыг;

1.4.15. “Тусгайлсан хяналт, удирдлага /application control/” гэж мэдээллийн технологийн тодорхой нэгэн үйл ажиллагаа, мэдээллийн технологийн нэгжид хэрэгжүүлэх хэсэгчилсэн хяналтыг;

1.4.16. “Хоёр шаттай баталгаажуулалт /two-phase authentication/” гэж хоёр үе шаттайгаар хэрэглэгчийг танин баталгаажуулах аргачлалыг;

1.4.17. “Харилцагч” гэж банктай гэрээ байгуулж, банкны үйлчилгээг ашиглаж буй хувь хүн, хуулийн этгээдийг;

1.4.18. “Хэрэглэгч” гэж мэдээллийн системийг ашиглаж буй банкны ажилтныг;

1.4.19. “Хэрэглэгчийн эрх” гэж хэрэглэгчийн мэдээллийн системд хандаж хийх үйлдлийг тодорхойлсон хэм хэмжээг;

1.4.20. “Эрхийн матриц” гэж хэрэглэгчийн мэдээллийн системд хандаж хийх үйлдлийг ажлын байрны чиг үүрэгт тохируулан зааж өгсөн хүснэгтийг;

1.4.21. “Хэрэглэгчийн эрхийн бүлэг” гэж хэрэглэгчийн ажлын байрны тодорхойлолтод тулгуурлан хийх үйлдлийг нэгтгэж тодорхойлсон бүлгийг;

1.4.22. “Мастер дата /master data/” гэж мэдээллийн системүүд зэрэг ашиглаж буй мэдээллийн эх үүсвэрийг;

1.4.23. “Мета дата /meta data/” гэж өгөгдлийн тухай өгөгдөл буюу ямар нэг мэдээллийг тодорхойлж тайлбарласан мэдээллийг;

1.4.24. “Татгалзах эрхгүй байдал /non-repudiation/” гэж ямар нэг үйлдэл хийгдсэн, учрал тохиолдол болсон байхад түүнийг дараа нь үгүйсгэх боломжгүй байх шинж чанар, чадварыг;

1.4.25. “Биет хандалт /physical access/” гэж компьютер, сервер бусад тоног төхөөрөмжийг биечлэн ашиглахыг;

1.4.26. “Логик хандалт /logical access/” гэж биет хандалтыг ашиглан мэдээллийн систем, өгөгдлийн сан болон бусад мэдээлэлд хандахыг;

1.4.27. “CISA гэрчилгээ /CISA certificate/” гэж Мэдээллийн системийн аудит болон хяналтын холбоо /ISACA/-оос олгодог мэдээллийн системийн аудиторын гэрчилгээг;

1.4.28. “COBIT тогтолцоо /COBIT framework/” гэж Мэдээллийн технологийн засаглалын институт /ITGI/ болон Мэдээллийн системийн аудит болон хяналтын холбоо /ISACA/-оос гаргасан Мэдээллийн технологийн ерөнхий хяналт, удирдлагын тогтолцоог;

1.4.29. “Нууцлалын алгоритм /encryption algorithm/” гэж криптографи ашиглан мэдээлэл унших боломжгүй хэлбэрт хувиргах нууцлалын алгоритмыг;

1.4.30. “Нууцлал /encryption/” гэж нууцлалын алгоритмыг ашиглан мэдээлэл нууцлахыг;

1.4.31. “Түлхүүрийн дэд бүтэц /key infrastructure/” гэж түлхүүрийн гэрчилгээг олгох, хадгалах ба устгах үүрэгтэй бүтцийг;

1.4.32. “Түлхүүрийн удирдлага /key management/” гэж криптографи түлхүүрүүдийг үүсгэх, хадгалах, тараах, сэргээх, устгах, архивлах, баталгаажуулах, хэрэглэх удирдлагыг;

1.4.33. “Хэш функц /hash function/” гэж дурын хэмжээтэй мэдээллийг тодорхой тогтмол хэмжээтэй мэдээлэл буюу хайлт хийх боломжтой хүснэгт хэлбэрт шилжүүлэх функцийг;

1.4.34. “Сэргээн ажиллуулах зорилтот хугацаа /recovery time objective/“ гэж мэдээллийн системийн үйл ажиллагаа тасалдсан тохиолдолд үйл ажиллагааг сэргээн ажиллуулахад шаардлагатай хугацааг;

1.4.35. “Үйлчилгээний хүргэлтийн зорилго /service delivery objective/“ гэж сэргээгдсэн мэдээлэл болон үйл ажиллагааны хүлээн зөвшөөрөгдөх түвшин ба цар хүрээг;

1.4.36. “Сэргээгдсэн цэгийн зорилго /recovery point objective/” гэж сэргээгдсэн мэдээлэл болон үйл ажиллагааны хүлээн зөвшөөрөгдөх алдагдлын түвшинг;

1.4.37. “Эмзэг байдал /vulnerability/” гэж аливаа аюулыг хэрэгжүүлэх, халдлага үйлдэхэд ашиглаж болох суваг, сул цоорхой байдлыг;

1.4.38. “Онцгой нөхцөл” гэж мэдээллийн систем болон сервер тоног төхөөрөмжийн алдаа, хүний санаатай болон санамсаргүй үйлдэл, гал түймэр, газар хөдлөлт, хүчтэй салхи, үер, аянга зэрэг гэнэтийн осол, байгалийн гамшиг болон бусад шалтгаанаар мэдээллийн систем хэвийн үйл ажиллагаагаа алдахыг;

1.4.39. “Нэвтрэлтийн туршилт /penetration test/” гэж мэдээллийн систем болон нууц мэдээлэлд зөвшөөрөлгүй хандах боломж олгох аюулгүй байдлын сул тал, эмзэг байдлыг илрүүлэх зорилготой туршилтыг;

1.4.40. “Үйлчилгээ бусниулах халдлага /denial of service/” гэж санаатайгаар мэдээллийн системийг хандах боломжгүй болгох, үйл ажиллагаа чиг үүргийг саатуулж улмаар системд нэвтрэх халдлагыг;

1.4.41. “Тархсан үйлчилгээ бусниулах халдлага /distributed denial of service/” гэж олон систем, сервер, компьютерыг хамарсан нэг зорилготой үйлчилгээ бусниулах халдлагыг;

1.4.42. “Сошиал инженеринг /social engineering/” гэж аюулгүй байдалд халдаж, системийн алдаа гаргах зорилгоор хувь хүнээс хувийн болон нууц мэдээлэл авах, сэтгэлзүйн дайралт, халдлага хийх үйлдлийг.

ХОЁР. МЭДЭЭЛЛИЙН ТЕХНОЛОГИЙН СТРАТЕГИ

2.1. Банк өөрийн компанийн засаглалтай уялдсан мэдээллийн технологийн засаглалтай байна.

2.2. Мэдээллийн технологийн стратеги төлөвлөгөөг банкны бизнесийн стратеги төлөвлөгөөтэй уялдуулж боловсруулна.

2.3. Мэдээллийн технологийн стратеги төлөвлөгөөг ханган ажиллахын тулд банк нь удирдлагын зохистой бүтэц, шаардлагатай төсөв, хүний нөөцтэй байна.

2.4. Банк мэдээллийн технологийн стратеги төлөвлөгөөг дэмжих бодлого, дүрэм, журам, заавар болон бусад баримт бичгийг боловсруулах бөгөөд банкны оролцогч талд тухай бүр танилцуулж байна.

2.5. Мэдээллийн технологи болон мэдээллийн системүүдийн өөрчлөлттэй уялдуулан

бодлого, дүрэм, журам, заавар болон бусад баримт бичгийг тогтмол шинэчлэн сайжруулна.

2.6. Мэдээллийн технологийн ерөнхий хяналт, удирдлагын тогтолцоо болгож банк нь хамгийн багадаа COBIT 4.1 тогтолцоог баримтална.

ГУРАВ. МЭДЭЭЛЛИЙН СИСТЕМИЙН БИЕТ БАЙРШИЛ

3.1. Үндсэн болон нөөц төвүүд нь Монгол Улсын нутаг дэвсгэрт байрлана.

3.2. Нөөц төв нь үндсэн төв байрлаж байгаа байршлаас хамгийн багадаа 200 км зайтай үндсэн төвд нөлөөлөх боломжтой онцгой нөхцөлд өртөхөөргүй газар зүйн алслагдмал байршилд байна.

3.3. Үндсэн төвийн тасралтгүй, найдвартай ажиллагаанд дараах шаардлагыг тавина. Үүнд:

3.3.1. Үндсэн төвийн тоног төхөөрөмж, мэдээллийн систем, програм хангамжийн засвар, үйлчилгээ, шинэчлэлийг тогтмол хийх;

3.3.2. Үндсэн төвийн тоног төхөөрөмж, мэдээллийн систем, програм хангамжийн тохиргоо, түүнд орсон өөрчлөлт бүрийг баримтжуулж, хадгалах;

3.3.3. Үндсэн төвд зөвхөн эрх бүхий ажилтан нэвтрэх бөгөөд нэвтрэх бүрд бүртгэл хөтлөх;

3.3.4. Үндсэн төв нь цахилгааны нэмэлт эх үүсвэр болох тог баригч (UPS), эрчим хүчний нэмэлт шугам, генератортай байх;

3.3.5. Үндсэн төвийн сервер, сүлжээний тоног төхөөрөмж, хөргөлтийн систем, агаарын чийгшил тохируулагч систем, гал унтраах систем, серверийн өрөөний мэдрэгчийг цахилгааны нэмэлт эх үүсвэрт холбосон байх;

3.3.6. Үндсэн төвийг, нөөц төвтэй үндсэн ба нөөц шугамаар шууд холбосон байх.

3.4. Нөөц төвийн тасралтгүй, найдвартай ажиллагаанд дараах шаардлагыг тавина. Үүнд:

3.4.1. Нөөц төвд зөвхөн эрх бүхий ажилтан нэвтрэх бөгөөд нэвтрэх бүрд бүртгэл хөтлөх;

3.4.2. Нөөц төвийн тоног төхөөрөмж, мэдээллийн систем, програм хангамжийн засвар, үйлчилгээ, шинэчлэлийг тогтмол хийх;

3.4.3. Нөөц төвийн тоног төхөөрөмж, мэдээллийн систем, програм хангамжийн тохиргоо, түүнд орсон өөрчлөлт бүрийг баримтжуулж, хадгалах;

3.4.4. Нөөц төв нь цахилгааны нэмэлт эх үүсвэр болох тог баригч (UPS), эрчим хүчний нэмэлт шугам, генератортай байх;

3.4.5. Нөөц төвийн сервер, сүлжээний тоног төхөөрөмж, хөргөлтийн систем, агаарын чийгшил тохируулагч систем, гал унтраах систем, серверийн өрөөний мэдрэгчийг цахилгааны нэмэлт эх үүсвэрт холбосон байх;

3.4.6. Нөөц төвийг үндсэн төвтэй сүлжээний үндсэн ба нөөц шугамаар холбосон байх;

ДӨРӨВ. ЭРСДЭЛИЙН УДИРДЛАГА

4.1. Харилцагчид мэдээллийн технологид суурилсан банк, санхүү болон холбогдох бусад үйлчилгээг үзүүлэхдээ банкны стратеги зорилт, бизнес төлөвлөгөө болон банкны мэдээллийн технологийн хүчин чадал, эрсдэл даах түвшинд тохируулан эрсдэлийг тодорхойлж, үнэлж, хянаж, тайлагнаж, удирдах зорилгоор эрсдэлийн удирдлагын бодлого, дүрэм, журам болон бусад баримт бичгийг боловсруулан үйл ажиллагаандаа тогтмол хэрэгжүүлнэ.

4.2. Банкны мэдээллийн технологийн эрсдэлийн удирдлага нь дараах асуудлуудад анхаарал хандуулна. Үүнд:

4.2.1. Технологийн өөрчлөлтийн банкны мэдээллийн систем болон үйл ажиллагаанд үзүүлэх сөрөг нөлөөлөл;

4.2.2. Мэдээллийн технологитой холбоотой гадна болон дотоодын эх үүсвэртэй луйвар, залилан, хууран мэхлэх оролдлого, нууцлал алдагдах, тэдгээртэй холбоотой аюулгүй байдлын алдаа дутагдлын эрсдэл;

4.2.3. Банкны нэн чухал үйл ажиллагаанд үйлчилгээ үзүүлэгчээс үйлчилгээ авсан тохиолдолд үйлчилгээ үзүүлэгчийн ажлын гүйцэтгэлд тогтмол хяналт тавихаас гадна эрсдэл тулгарсан тохиолдолд үйлчилгээг шилжүүлэх, дараагийн үйлчилгээ үзүүлэгчийг хүлээн авах төлөвлөгөө боловсруулна;

4.2.4. Банкны үндсэн үйл ажиллагаанд сөргөөр нөлөөлөхүйц онцгой нөхцөл гарсан үед үйл ажиллагааг тасралтгүй үргэлжлүүлэх боломжийг хангах төлөвлөгөө боловсруулна. Ялангуяа, гадны хүчин зүйлд өртөмтгий үйл ажиллагаа болон дэд бүтцэд нөлөөлж болзошгүй аюулыг үнэлж, эдгээр эрсдэлтэй тулгарсан тохиолдолд нэн чухал бизнесийн үйл ажиллагааг тасалдалгүй үргэлжлүүлэх төлөвлөгөөтэй байна;

4.2.5. Харилцагч гүйлгээг хүлээн зөвшөөрөхгүй байх эрсдэлийг бууруулах үүднээс

банк гүйлгээний лог бүртгэлийг 10 жил, үйлдлийн лог бүртгэлийг 3 жил хадгална;

4.2.6. Лог бүртгэлийн бүрэн бүтэн байдалд халдаж болзошгүй аюулыг тогтмол хянах бөгөөд лог бүртгэлийг лог бүртгэлийн сервер дээр хуулж давхар хадгална.

ТАВ. ТУСГАЙЛСАН ХЯНАЛТ, УДИРДЛАГА

5.1. Аюулгүй байдал:

5.1.1. Банкны удирдлага нь аюулгүй байдлын хяналтын үйл ажиллагааг хэрэгжүүлэн тогтмол хянаж ажиллах бөгөөд зөвхөн хэрэглэгчийн эрх, эрхийн матриц, хэрэглэгчийн эрхийн бүлэгт тулгуурласан хандалтыг зөвшөөрдөг байхын зэрэгцээ мэдээллийг эзэмшигч баталгаажуулснаар ажилтанд тухайн мэдээлэлд хандах эрхийг олгоно.

5.1.2. Хэрэглэгч бүр өөрийн гэсэн дахин давтагдашгүй хэрэглэгчийн нэр, нууц үгтэй байх бөгөөд зөвхөн өөрийн хэрэглэгчийн нэр, нууц үгийг ашиглан зөвшөөрөгдсөн мэдээллийн систем болон мэдээлэлд хандана.

5.1.3. Нийтийн сүлжээгээр дамжуулан мэдээллийн системд хандах тохиолдолд хэрэглэгчийг таних хоёроос доошгүй шаттай баталгаажуулалтыг ашиглах бөгөөд мэдээллийг дамжуулахад нууцлалтай холболт ашиглана.

5.1.4. Хэрэглэгчийн эрхийг зөвхөн тухайн ажилтны ажил үүргийн хуваарийн дагуу хандах шаардлагатай мэдээллийн систем, мэдээлэлд хандах хязгаарлалттай олгоно. Мөн нэг хэрэглэгчид бүх эрхийг олгохыг хориглох ба шат дараалсан хяналттай байна.

5.1.5. Хэрэглэгчийн эрхийн бүлгийг тухайн хэрэглэгчийн эрхийн бүлэгт хамаатай мэдээллийн систем болон мэдээлэлд хандах байдлаар тодорхойлно. Энэхүү хэрэглэгчийн эрхийн бүлгийг ажил үүргийн зөв зохистой хуваарилалт, тусгаарлалтыг дэмжсэн байдлаар тодорхойлж ялгана.

5.1.6. Хэрэглэгчийн эрх болон хэрэглэгчийн эрхийн бүлгүүдийг тогтмол хянан шалгаж, банкны бүтэц зохион байгуулалт, мэдээллийн технологи болон

мэдээллийн системийн өөрчлөлтөд нийцүүлэн тухай бүр шинэчилнэ.

5.2. Гүйлгээний бүрэн бүтэн байдал:

5.2.1. Банк мета дата, мастер дата болон гүйлгээ бүрийн бүрэн бүтэн байдлыг хангах зорилгоор тогтмол лог бүртгэл хийх бөгөөд тухайн лог бүртгэлд өөрчлөлт орсон бол тухайн өөрчлөлтийг буцаан сэргээх хэмжээний дэлгэрэнгүй мэдээллийг багтаана.

5.2.2. Гүйлгээний лог бүртгэл нь сүүлийн 10 жил, үйлдлийн лог бүртгэл нь сүүлийн 3 жилийн мэдээллийг агуулах бөгөөд дараах шаардлагыг хангана. Үүнд:

5.2.2.1. Мэдээлэлд хандаж өөрчлөлт хийсэн, өөрчлөх оролдлого хийсэн хүн, хэрэглэгч, мэдээллийн системийг бүртгэнэ.

5.2.2.2. Өөрчлөлт хийсэн, өөрчлөх оролдлого хийсэн он, сар, өдөр, цаг, минут, секундийн мэдээллийг бүртгэнэ.

5.2.2.3. Өөрчлөлт хийсэн, өөрчлөх оролдлого хийсэн мэдээллийн систем болон мэдээллийг бүртгэх бөгөөд өөрчлөлтийн өмнөх утга болон шинэчлэгдсэн утгыг бүртгэнэ.

5.2.2.4. Зөвхөн зөвшөөрөгдсөн хэрэглэгч лог бүртгэлийн системд хандаж лог бүртгэлийг харах эрхтэй байна.

5.2.2.5. Лог бүртгэлийн мэдээллийг зөвхөн хадгалах хугацаа хэтэрсэн тохиолдолд устгаж болно.

5.2.2.6. Лог бүртгэлийн систем нь зөвшөөрөлгүй хандах оролдлого бүрийг бүртгэнэ.

5.2.2.7. Лог бүртгэлд тогтмол хяналт тавих бөгөөд бүрэн бүтэн байдал алдагдсан тохиолдлыг тухай бүр илрүүлж, засан залруулах арга хэмжээ авна.

5.2.2.8. Банкны харилцагчтай холбоотой гүйлгээ хийх гэрээ бүхий үйлчилгээ үзүүлэгч нь энэхүү журмын дагуу лог бүртгэлийг хийх бөгөөд лог бүртгэлд хандах эрхийг банкинд нээлттэй байлгана.

5.3. Татгалзах эрхгүй байх байдал:

Харилцагч гүйлгээг хүлээн зөвшөөрөөгүй тохиолдолд банк тухайн харилцагч гүйлгээг хийсэн гэдгийг батлах зорилгоор дараах мэдээлэл бүхий лог бүртгэлийг харилцагчтай хуваалцана. Үүнд:

5.3.1. Харилцагчийг нотлох хувь хүний мэдээлэл;

5.3.2. Хандалтын мэдээлэл буюу IP хаяг;

5.3.3. Гүйлгээний он, сар, өдөр, цаг, минут, секунд.

5.4. Өгөгдөл оруулах хяналт, удирдлага:

5.4.1. Өгөгдөл оруулах хяналт, удирдлага нь холбогдох журам болон хяналтууд дараах үүргийг биелүүлж байгаа эсэхийг баталгаажуулна. Үүнд:

5.4.1.1. Хүлээж авсан өгөгдлийн бүрэн бүтэн байдал;

5.4.1.2. Хүлээж авсан өгөгдлийн өмнө нь боловсрогдоогүй байдал;

5.4.1.3. Хүлээж авсан өгөгдлийн алдаагүй байдал;

5.4.1.4. Шаардлагатай зөвшөөрөл авсан байдал;

5.4.1.5. Мэдээллийн системд давхардаж ороогүй байдал.

5.4.2. Хэрэглэгч болон гадны эх үүсвэрээс өгөгдөл шууд авах тохиолдолд өгөгдлийг шалгаж баталгаажуулдаг хяналттай байна.

5.4.3. Өгөгдөл шинээр үүсгэх, оруулахад дараах хяналтууд байна. Үүнд:

5.4.3.1. Өгөгдөл оруулах зөвшөөрөл;

Өгөгдөл хүлээн авах мэдээллийн систем бүрийн өгөгдөл оруулах зөвшөөрлийг тодорхой болгож, мөрддөг байна.

5.4.3.2. Багцын хяналт;

Тоо ширхгийн нийт дүн, гүйлгээний нийт дүн, баримт бичгийн нийт дүн болон хэш функцийн нийт дүнг тулган баталгаажуулах зэрэг багцын хяналтыг хийхээс гадна зарим өгөгдлийг гараар оруулсан тохиолдолд, эх өгөгдөл болон гараар тооцоолсон өгөгдлийн нийт дүн нь компьютерын нийт дүнтэй нийцэж байгаа эсэхийг шалгана.

5.4.3.3. Алдааны тайлан;

Банк өгөгдөл оруулахтай холбоотой үүсэж болох алдааг зохицуулах, тайлагнах баримт бичгийг боловсруулсан байна. Уг баримт бичиг нь багц өгөгдөл орох үед алдаа илэрсэн бол энэхүү багцыг бүхэлд нь буцаах, алдааг засагдтал хүлээх, хүлээн авч боловсруулсны дараа алдааг гараар засаж залруулга хийх шаардлагатай гэж тэмдэглэх зэрэг шийдлүүдээс сонгох боломжуудыг дурдсан байна.

5.5. Өгөгдөл боловсруулах болон түүний алдааг зохицуулах хяналт, удирдлага:

Өгөгдөл боловсруулах болон түүний алдааг зохицуулах хяналт, удирдлага нь хүлээж авах өгөгдөл үнэн зөв боловсруулагдан гарч байгаа эсэхэд хяналт тавих бөгөөд дараах хяналтын арга хэмжээг авсан байна. Үүнд:

5.5.1. Гүйлгээний боловсруулалтын бүрэн бүтэн байдлыг хангах;

5.5.2. Гүйлгээ бүр дахин давтагдашгүй байх;

5.5.3. Бүх гүйлгээ хүчин төгөлдөр байх;

5.5.4. Компьютерын үйл ажиллагаанд аудит хийж шалгах боломжтой байх;

5.5.5. Мэдээллийн систем хүлээж авах болон мэдээллийн системээс гарах өгөгдлийг шалган баталгаажуулах;

5.5.6. Зөв мэдээлэл, файлуудыг боловсруулах;

5.5.7. Боловсруулалтын үе шатуудаар дамжих өгөгдлийг зөв зохистой дамжуулах;

5.5.8. Боловсруулалтын өмнө, боловсруулалтын үеэр болон боловсруулалтын дараах өгөгдлүүдийг тулган шалгаж байх;

5.5.9. Боловсруулалтын явцад алдаа илрүүлсэн тохиолдолд алдаа гаргасан этгээдэд буцааж, алдааг арилгаж, залруулга хийсний дараагаар дахин боловсруулалт хийх;

5.5.10. Өгөгдлийн шинэчлэлийг хянах;

5.5.11. Өгөгдөл боловсруулалтад өөрчлөлт хийх хүсэлт, баталгаажуулалт болон зөвшөөрлийг хянах;

5.5.12. Өгөгдлийн боловсруулалт дахь алдааны боловсруулалт;

Гүйлгээ саатахаас урьдчилан сэргийлэх зорилгоор өгөгдлийн боловсруулалтаас өмнө алдааг илрүүлэх, тогтоох аргачлалтай байна.

5.6. Өгөгдөл хадгалах хяналт, удирдлага:

Өгөгдөл хадгалах хяналт, удирдлага нь мета дата, мастер дата болон урт хугацааны суурь өгөгдлийн бүрэн бүтэн байдлыг хадгалах зорилготой. Мета дата, мастер дата болон урт хугацааны суурь өгөгдөлд хадгалагдаж буй мэдээлэл нь санхүүгийн болон үйл ажиллагааны тайлан, тэдгээрийн боловсруулалтад чухал үүрэг гүйцэтгэдэг тул өндөр түвшинд хамгаалах бөгөөд дараах хяналтын арга хэмжээг авна. Үүнд:

5.6.1. Өгөгдөл нэмэх, засах үйлдлийг зөвхөн зөвшөөрөгдсөн болон хянагдсан үед хийнэ.

5.6.2. Өгөгдөлд хандах логик болон биет хандалтыг хязгаарлаж, хяналт тавих бөгөөд зөвхөн банкны мэдээллийн ангилал, хэрэглэгчийн эрхийн матрицын дагуу хандах эрхийг олгоно.

5.6.3. Өгөгдлийн шинэчлэлтэй холбоотой журам, зааврыг батлуулж гаргасан байна.

5.6.4. Өгөгдлийг хадгалах үйл явцыг хараат бус этгээдээр тогтмол хянуулж, өгөгдлийн шинэчлэлтэй холбоотой журам, зааврын хэрэгжилтийг шалгана.

5.7. Гарах өгөгдлийн хяналт, удирдлага:

Гарах өгөгдлийн хяналт, удирдлага нь гарах өгөгдөл бүрэн бүтэн байхын зэрэгцээ зөв хуваарилагдаж очиж байгаа эсэхийг хянах зорилготой. Өгөгдөл гарах сүүлийн үе шатуудад хийгдэх хяналт, удирдлага нь өмнөх үе шатууд үнэн зөв хийгдсэн байдлыг баталгаажуулж, залруулах бөгөөд дараах хяналтуудаас бүрдэнэ. Үүнд:

5.7.1. Өгөгдөл нь цаг тухайд нь үнэн зөв боловсруулагдан хуваарилагдаж байна.

5.7.2. Тогтмол логик болон биет хяналтын дор байх бөгөөд гарах өгөгдлийн нууцлал болон хэрэглэгчдийн хандалтын түвшинд дараах шаардлага тавигдана. Үүнд:

5.7.2.1. Гарах өгөгдөлд зөвхөн зөвшөөрөгдсөн, эрх бүхий хэрэглэгчид хандана.

5.7.2.2. Сүлжээгээр дамжин хэрэглэгчид хүрэх гарах өгөгдлийг нууцлалтай холболт ашиглан дамжуулна.

5.7.2.3. Гарах биет өгөгдөлд зөвхөн зөвшөөрөгдсөн, хязгаарлагдмал орчинд хандах боломжийг олгоно.

5.7.3. Гарах өгөгдөл нь тухайн өгөгдөл оруулах үеийн хяналтын тохиргоо, параметр үзүүлэлттэй бүрэн тохирч байна.

5.7.4. Өгөгдлийн бүрэн бүтэн, алдаагүй байдлыг шалгаж баталгаажуулна:

Дэлгэрэнгүй лог бүртгэл нь энэхүү баталгаажуулалтыг хялбарчлах бөгөөд үйл ажиллагааны тайланг үнэн зөв гарсан эсэхийг шалгахад дэмжлэг болохоос гадна алдаатай өгөгдлийг тодорхойлоход тусална.

5.7.5. Гарах өгөгдөл нь алдаагүй байна:

Алдаа гарсан тохиолдолд эрх бүхий хэрэглэгч алдаатай гарах өгөгдлийг засан залруулж болох бөгөөд энэ арга хэмжээг журам, заавар бусад баримт бичгээр зохицуулсан байна.

ЗУРГАА. ДОТООД АУДИТ

6.1. Банкны дотоод аудитын нэгж нь дараах шаардлагыг хангасан мэдээллийн мэдээллийн аудитортой байна. Үүнд:

6.1.1. Мэдээллийн технологийн аудитор нь мэдээллийн технологийн чиглэлээр бакалавр болон түүнээс дээш зэрэгтэй, мэдээллийн технологийн чиглэлээр гурваас доошгүй жилийн ажлын туршлагатай байна.

6.1.2. Мэдээллийн технологийн аудитор нь CISA гэрчилгээтэй байна. CISA гэрчилгээ бүхий мэдээллийн технологийн аудитор байхгүй тохиолдолд CISA гэрчилгээ бүхий мэдээллийн технологийн аудитортой гуравдагч талаар мэдээллийн технологийн аудитыг хийлгэнэ.

6.2. Мэдээллийн технологийн үйл ажиллагаа болон мэдээллийн системд хийх тусгайлсан хяналт, удирдлагын аудитыг хамгийн багадаа улиралд нэг удаа хийнэ. Аудитын тайланг дараа улирлын эхний сарын 10-ны өдрийн дотор Монголбанкны Хяналт шалгалтын газарт хүргүүлнэ.

6.3. Тайланг ирүүлэхдээ аудитаар илэрсэн асуудлуудыг эрсдэл болон шийдвэрлэх боломжит хугацаагаар эрэмбэлэн жагсаасан байна.

ДОЛОО. ХӨНДЛӨНГИЙН АУДИТ

7.1. Санхүүгийн тайланд хөндлөнгийн аудит хийх баг нь CISA гэрчилгээ бүхий аудитортой байна. CISA гэрчилгээ бүхий аудитор байхгүй тохиолдолд шаардлага хангасан гуравдагч талаас мэдээллийн технологийн аудитын үйлчилгээ авч болно.

7.2. Санхүүгийн хөндлөнгийн аудит хийх баг нь санхүүтэй холбоотой мэдээллийн системд мэдээллийн технологийн тусгайлсан хяналт, удирдлагын аудитыг хийх бөгөөд COBIT тогтолцоонд суурилсан мэдээллийн технологийн тусгайлсан хяналт, удирдлагын үр дүнгийн талаар дүгнэлт бүхий тайлан гаргах бөгөөд тус тайланг санхүүгийн тайлантай хамтад нь Монголбанкны Хяналт шалгалтын газарт ирүүлнэ.

7.3. COBIT тогтолцоонд суурилсан Мэдээллийн технологийн ерөнхий хяналт, удирдлагын аудитыг хамгийн багадаа хоёр жилд нэг удаа хийх бөгөөд тус аудитын тайланг, тайлан бэлэн болсноос хойш 14 хоногийн дотор Монголбанкны Хяналт шалгалтын газарт хүргүүлнэ.

НАЙМ. ЛОГ БҮРТГЭЛ

8.1. Банк нь гүйлгээний лог бүртгэлийн сүүлийн 10, үйлдлийн лог бүртгэлийн сүүлийн 3 жилийн түүхийг лог бүртгэлд хадгална.

8.2. Лог бүртгэлийн систем нь бизнесийн тасралтгүй ажиллагааны төлөвлөгөөг мөн адил ханган ажиллана.

8.3. Лог бүртгэлийг үйлдлийн системд бүртгэхийн зэрэгцээ лог бүртгэлийн серверт бодит цагт давхар бүртгэнэ.

8.4. Лог бүртгэлийн серверт хандах эрх хязгаарлалттай байх бөгөөд нэг хэрэглэгч үйлдлийн систем болон лог бүртгэлийн системд хоёуланд нь хандах эрхтэй байж болохгүй.

8.5. Лог бүртгэлийн серверээс мэдээлэл устгах боломжийг бүрэн хязгаарлана.

ЕС. МЭДЭЭЛЛИЙН ТЕХНОЛОГИЙН ҮЙЛЧИЛГЭЭ АВАХ

9.1. Мэдээллийн технологийн үйлчилгээг үйлчилгээ үзүүлэгчээс авах тохиолдолд банк эрсдэлийн удирдлагад болон үйлчилгээ үзүүлэгчид хяналт тавих бөгөөд дараах хяналтын арга хэмжээнүүд хэрэгжүүлнэ. Үүнд:

9.1.1. Үйлчилгээ үзүүлэгчээс үйлчилгээ авах тохиолдолд үүдэн гарах дэд бүтцийн эрсдэлийг хянана.

9.1.2. Мэдээллийн технологийн үйлчилгээ авах гэрээ байгуулахаас өмнө үйлчилгээ үзүүлэгчийг магадлан шалгана.

9.1.3. Мэдээллийн технологийн үйлчилгээ авах гэрээ болон үүсэх харилцаа нь банкны эрсдэлийн удирдлага, мэдээллийн аюулгүй байдал, харилцагчийн мэдээллийн нууцлалын бодлого, журам болон холбогдох бусад баримт

бичгүүдтэй нийцтэй байна.

9.1.4. Мэдээллийн технологийн үйлчилгээ авах гэрээний дагуу банк өөрийн мэдээллийг үйлчилгээ үзүүлэгчтэй хуваалцах тохиолдолд үйлчилгээ үзүүлэгчийн эрсдэлийн удирдлага, мэдээллийн аюулгүй байдал, харилцагчийн мэдээллийн нууцлалын бодлого, журам болон холбогдох бусад баримт бичгүүд нь банкны энэхүү баримт бичгүүдтэй нийцтэй байна.

9.1.5. Үйлчилгээ үзүүлэгч нь банкны дагаж мөрддөг хууль эрх зүйн баримт бичгийн холбогдох заалтыг мөн адил дагаж мөрдөнө.

9.2. Банк үйлчилгээ үзүүлэгчээс үйлчилгээ авсан тохиолдолд үйлчилгээ үзүүлэгч банкны өмнө хариуцлага хүлээх бөгөөд доорх заалтуудыг гэрээнд тусгана. Үүнд:

9.2.1. Гүйцэтгэлийн хэмжигдэхүүн, зорилтууд болон гүйцэтгэл хангалтгүй тохиолдолд гэрээг цуцлах, ногдуулах торгууль, хохирол барагдуулах заалтууд;

9.2.2. Гэрээний хугацаа дууссан эсвэл гэрээ хүчингүй болсон тохиолдолд үйлчилгээ үзүүлэгч үйлчилгээг өөр үйлчилгээ үзүүлэгч эсвэл банкинд шилжүүлэн өгөх заалтууд;

9.2.3. Гэрээний хэрэгжилтийн хугацаанд бий болох, худалдан авах, мөн хуваалцах өмч хөрөнгийн эзэмших эрхийг тодорхой заасан заалтууд;

9.2.4. Үйлчилгээ үзүүлэгч нь банкны үйл ажиллагааны бодлого, журам болон холбогдох бусад баримт бичгийг дагаж мөрдөх талаарх заалтууд;

9.2.5. Үйлчилгээ үзүүлэгч нь үйлчилгээг туслан гүйцэтгэгчээс авах зөвшөөрөл болон туслан гүйцэтгэгчээс авах үйлчилгээний хязгаарыг заасан заалтууд;

9.2.6. Туслан гүйцэтгэгчийн зөвшөөрөл авсан тохиолдолд үндсэн гэрээт үйлчилгээ үзүүлэгчид тавигдах шаардлагууд туслан гүйцэтгэгчид мөн адил үйлчлэхийг туслан гүйцэтгэгчтэй хийх гэрээнд заасан байна.

АРАВ. МЭДЭЭЛЛИЙН ТЕХНОЛОГИЙН АУДИТЫН ҮЙЛЧИЛГЭЭГ ГЭРЭЭТ ГҮЙЦЭТГЭГЧЭЭС АВАХ

Банк нь мэдээллийн технологийн аудитын үйлчилгээг гуравдагч талд даатгах боломжтой бөгөөд гуравдагч тал нь дараах шаардлагыг хангасан байна. Үүнд:

10.1. Гуравдагч тал буюу мэдээллийн технологийн аудитын үйлчилгээ үзүүлэгч байгууллага нь CISA гэрчилгээтэй, мэдээллийн технологийн чиглэлээр бакалавр болон түүнээс дээш зэрэгтэй, мэдээллийн технологийн чиглэлээр таваас доошгүй жилийн ажлын туршлагатай үүнээс мэдээллийн технологийн аудитын чиглэлээр хоёроос доошгүй жилийн ажлын туршлагатай мэдээллийн технологийн аудитортай байна.

10.2. Тухайн банкинд сүүлийн гурван жил бүтээгдэхүүн, үйлчилгээ нийлүүлээгүй байна. Үүнд хөндлөнгийн аудитын үйлчилгээ хамаарахгүй.

10.3. Мэдээллийн технологийн аудит хийх гуравдагч талын хувьцаа эзэмшигч болон гүйцэтгэх удирдлага нь Банкны тухай хуулийн 3.1.2-т заасны дагуу банкны холбогдох этгээд байж болохгүй.

10.4. Мэдээллийн технологийн аудит хийх гуравдагч тал болон банк хоорондын эрх, үүрэг, хариуцлагатай холбоотой харилцааг зохицуулах зорилгоор гэрээ байгуулах бөгөөд тус гэрээ нь энэхүү журмын заалтуудтай бүрэн нийцсэн байна.

АРВАН НЭГ. НУУЦЛАЛ

Банк нь мэдээллийг эрсдэлийн үнэлгээ болон мэдээллийн нууцлалын зэрэгт

үндэслэн задруулахаас урьдчилан сэргийлж аюулгүй байдал болон нууцлалыг хангасан байдлаар хадгалах бөгөөд нууцлал, аюулгүй байдал нь дараах шаардлагыг хангана. Үүнд:

11.1. Мэдээллийг өндөр зэрэглэлийн нууцлалын алгоритм ашиглан нууцална.

11.2. Мэдээллийг хадгалах болон нийтийн сүлжээ ашиглан дамжуулах тохиолдолд өндөр зэрэглэлийн нууцлал болон нууцлалтай холболт ашиглана.

11.3. Нууцлалын алгоритм нь олон нийтэд аюулгүй байдлыг хангасан буюу найдвартай гэж хүлээн зөвшөөрөгдсөн алгоритм байх бөгөөд өндөр зэрэглэлийн түлхүүр ашиглана.

11.4. Банк өөрийн нууцлалын алгоритмуудад хяналт тавих бөгөөд шаардлага хангаж байгаа эсэхийг тогтмол шалгаж шинэчлэн сайжруулна.

11.5. Аюулгүй байдлыг хангасан түлхүүрийн дэд бүтцийг дэмжих түлхүүр болон нууцлалын удирдлагын шаардлагыг банкны ажилтан, үйлчилгээ үзүүлэгч, болон банкны оролцогч талуудад ханган ажиллана.

АРВАН ХОЁР. ХАРИЛЦАГЧИЙН МЭДЛЭГ

Харилцагчийн банкны үйлчилгээтэй холбоотой мэдлэг нь аюулгүй байдлын чухал хэсэг бөгөөд банк дараах мэдээллүүдийг банкны ажилтан болон харилцагчид тогтмол хүргэж байна. Үүнд:

12.1. Дараах үйлчилгээг ашиглах үед гарч болох эрсдэл, онцгой тохиолдол. Үүнд:

12.1.1. Мобайл банк;

12.1.2. Интернет банк;

12.1.3. Гар утас;

12.1.4. АТМ;

12.1.5. Банкны үйлчилгээний бусад сувгууд.

12.2. Харилцагч тогтмол мөрдсөнөөр эрсдэлийг бууруулахад чиглэсэн аюулгүй байдлын болон урьдчилан сэргийлэх арга хэмжээ;

12.3. Банкны үйлчилгээний сувгуудтай холбоотой түгээмэл болон шинээр гарч буй эрсдэл, аюул занал, алдаа, дутагдал, эмзэг байдал;

12.4. Харилцагч тулгарсан асуудлыг хэрхэн шийдэх, санал гомдол гаргах, банкны эрсдэлтэй тулгарсан тохиолдолд алдааг хэрхэн засах, хохирлыг хэрхэн барагдуулах талаарх мэдээлэл;

12.5. Татгалзах эрхгүй байдлын эрсдэлийн удирдлагын хяналт болон холбогдох лог бүртгэл;

12.6. Санаатай бус дахин давтагдсан харилцагчийн хувийн мэдээллийн задрал.

АРВАН ГУРАВ. БИЗНЕСИЙН ТАСРАЛТГҮЙ АЖИЛЛАГААНЫ ТӨЛӨВЛӨГӨӨ

Банк дараах шаардлага бүхий бизнесийн тасралтгүй ажиллагааны төлөвлөгөө /цаашид БТАТ гэх/-г боловсруулж хэрэгжүүлнэ. Үүнд:

13.1. Оролцогч тус бүрийн үүрэг, хариуцлагыг төлөвлөгөөнд тодорхой тусгана.

13.2. Бизнесийн үйл ажиллагаанд учирч болох онцгой нөхцөлийн эрсдэлийн үнэлгээ.

13.3. Дараах бүрэлдэхүүн хэсэг бүхий бизнесийн нөлөөллийн үнэлгээ. Үүнд:

13.3.1. Банкны нэн чухал бизнесийн үйл ажиллагаа;

13.3.2. Банкны нэн чухал бизнесийн үйл ажиллагааг дэмжиж буй дэд бүтэц, түүний

эрсдэлийн түвшин;

13.3.3. Сэргээн ажиллуулах зорилтот хугацаа;

13.3.4. Үйлчилгээний хүргэлтийн зорилго;

13.3.5. Сэргээгдсэн цэгийн зорилго.

13.4. БТАТ нь нөөц төвийг зохицуулсан заалтуудтай байна.

13.5. БТАТ нь дараах үндсэн бүрэлдэхүүн хэсгүүдтэй байна. Үүнд:

13.5.1. Гэмтлийн өмнөх бэлэн байдал ба төлөвлөлт;

13.5.2. Нөөц төвийн бэлэн байдал;

13.5.3. БТАТ-ний үүрэг хариуцлага ба багийн гишүүд;

13.5.4. БТАТ-г хэрэгжүүлэх аргачлал ба нөөц төвд үйл ажиллагааг шилжүүлэх;

13.5.5. БТАТ-г дуусгах;

13.5.6. Үйл ажиллагааг нөөц төвөөс буцаан үндсэн төвд шилжүүлэх.

13.6. БТАТ-ний сургалтын төлөвлөгөө;

13.7. БТАТ-ний туршилтын төлөвлөгөө ба туршилтын үр дүнгийн тайлан;

13.8. БТАТ-ний засвар үйлчилгээ ба шинэчлэл.

АРВАН ДӨРӨВ. ТӨЛБӨРИЙН КАРТЫН МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН СТАНДАРТ

Банк нь PCI DSS буюу төлбөрийн картын мэдээллийн аюулгүй байдлын стандартын дараах ерөнхий шаардлагуудыг хэрэгжүүлнэ. Үүнд:

14.1. Аюулгүй байдлыг хангасан найдвартай сүлжээ болон систем байгуулах;

14.1.1. Карт эзэмшигчийн мэдээллийг хамгаалах галт ханын тохиргоо суулган ажиллуулах;

14.1.2. Үйлчилгээ үзүүлэгч болон үйлдвэрээс ирсэн өгөгдмөл /default/ хэрэглэгчийн нэр, нууц үг болон бусад өгөгдмөл аюулгүй байдлын тохиргоо, параметрүүдийг ашиглахгүй байх.

14.2. Карт эзэмшигчийн мэдээллийг хамгаалах;

14.2.1. Хадгалагдсан (өгөгдлийн сан болон бусад) карт эзэмшигчийн мэдээллийг хамгаалах;

14.2.2. Карт эзэмшигчийн мэдээллийг нийтийн сүлжээгээр дамжуулах тохиолдолд өндөр түвшний нууцлал болон нууцлалтай холболт ашиглана.

14.3. Эмзэг байдлын удирдлагын тогтолцоо хэрэгжүүлэх;

14.3.1. Мэдээллийн системийг вирус болон бусад төрлийн хорлон сүйтгэх програм хангамжуудаас хамгаалах бөгөөд вирусийн эсрэг програм хангамжийг тогтмол шинэчлэн сайжруулах;

14.3.2. Аюулгүй байдлыг хангасан найдвартай мэдээллийн систем хөгжүүлэх.

14.4. Хэрэглэгчийн эрхийн хяналтын арга хэмжээ хэрэгжүүлэх;

14.4.1. Карт эзэмшигчийн мэдээлэлд хандах хэрэглэгчийн эрхийг зөвхөн шаардлагатай хэрэглэгчид олгох;

14.4.2. Мэдээллийн системийн бүрэлдэхүүн хэсгүүдэд хандах хэрэглэгчийн эрхийг тодорхойлж, хандалтыг баталгаажуулж хяналт тавих;

14.4.3. Карт эзэмшигчийн мэдээлэл бүхий сервер, компьютерт биет хандалт хийхийг хязгаарлах, шаардлагатай бол хаах.

14.5. Сүлжээнд тогтмол хяналт тавих, нэвтрэлтийн туршилт хийх;

14.5.1. Сүлжээ болон карт эзэмшигчийн мэдээллийн хандалтын лог бүртгэлд хяналт тавих;

14.5.2. Аюулгүй байдлын систем, түүний үйл ажиллагаанд нэвтрэлтийн туршилт тогтмол хийх.

14.6. Банкны нийт ажилтнуудыг хамруулсан мэдээллийн аюулгүй байдлын бодлого хэрэгжүүлэх.

АРВАН ТАВ. НЭВТРЭЛТИЙН ТУРШИЛТ

15.1. Нэвтрэлтийн туршилтыг банк нь хамгийн багадаа жилд нэг удаа, гуравдагч талаар хамгийн багадаа хоёр жилд нэг удаа хийлгэх бөгөөд туршилтын явцад илэрсэн эмзэг байдлыг цаг алдалгүй шийдвэрлэнэ.

15.2. Нэвтрэлтийн туршилтын явцад санамсаргүйгээр мэдээллийн систем унах, зогсох магадлалтай тул туршилтыг мэдээллийн системийн ачаалал бага үед дараах түвшинд хийнэ. Үүнд:

15.2.1. Нөлөө бүхий мэдээллийн систем;

15.2.2. Харилцаа холбооны дэд бүтцийн болон сүлжээний төхөөрөмж;

15.2.3. DNS үйлчилгээ;

15.2.4. Эцсийн хэрэглэгчийн компьютер, зөөврийн компьютер болон бусад мобайл төхөөрөмж;

15.2.5. Цахим шуудангийн үйлчилгээ;

15.2.6. Өгөгдлийн сангийн систем;

15.2.7. Веб хуудас болон веб мэдээллийн систем;

15.2.8. Мобайл мэдээллийн систем;

15.2.9. Утасгүй сүлжээний систем (Wi-Fi, GSM гэх мэт);

15.2.10. ATM-ийн систем;

15.2.11. Үйлчилгээ бусниулах халдлага;

15.2.12. Тархсан үйлчилгээ бусниулах халдлага;

15.2.13. Сошиал инженеринг туршилт.

15.3. Нэвтрэлтийн туршилтыг дараах хандалтын буюу нэвтрэх цэгүүдэд хийнэ. Үүнд:

15.3.1. Интернет;

Интернетээр шууд хандах боломжтой банкны бүх үйлчилгээ болон мэдээллийн системд дараах хэрэглэгчийн төрлийг ашиглан туршилтыг хийнэ. Үүнд:

15.3.1.1. Бүртгэлгүй гадны хэрэглэгч буюу мэдээллийн системд хандах эрхгүй дурын интернет хэрэглэгч;

15.3.1.2. Банкны харилцагч буюу мэдээллийн системд интернетээр хандах эрхтэй банкны харилцагч.

15.3.2. Банкны дотоод сүлжээ;

Банкны дотоод хэрэглэгч болгон хандах боломжтой мэдээллийн системд

дараах хэрэглэгчийн төрлийг ашиглан туршилтыг хийнэ. Үүнд:

15.3.2.1. Банкны ажилтан;

a. Хамгийн түгээмэл ашиглагддаг банкны хэрэглэгчийн эрх;

b. Банкны дотоод администратор хэрэглэгчийн эрх.

15.3.2.2. Банкны зочин.

a. Тодорхой мэдээллийн системд тогтмол хандах эрх бүхий урт хугацааны үйлчилгээ үзүүлэгч болон харилцагч байгууллага;

b. Дотоод сүлжээгээр дамжуулан интернетэд хандах боломжтой, дотоодын мэдээллийн системд хязгаарлалтай хандах эрх бүхий богино хугацааны банкны зочин.

15.3.3. Салбар сүлжээ.

Салбар сүлжээний хэрэглэгч хандах боломжтой мэдээллийн системд дээрх жагсаалтын банкны ажилтан болон зочны бүх төрлийг ашиглан туршилтыг хийнэ.

15.4. Нэвтрэлтийн туршилтын явцад илэрсэн үр дүнг эрсдэлийн түвшингийн дагуу дараах зэрэглэлээр ангилна. Үүнд:

15.4.1. Онцгой эрсдэл;

Бага түвшний чадвартай этгээд халдлага хийж банкны мэдээллийн системийн хяналт болон удирдлагыг гартаа авах боломжтой.

15.4.2. Шийдвэрлэх шаардлагатай эрсдэл;

Өндөр түвшний чадвартай этгээд халдлага хийж банкны мэдээллийн системийн хяналт болон удирдлагыг гартаа авах боломжтой.

15.4.3. Өндөр зэрэглэлийн эрсдэл;

Интернетээр дамжуулан мэдээллийн системд хязгаарлалтай хандах боломжтой эсвэл үйлчилгээг бусниулах буюу татгалзуулах боломжтой.

15.4.4. Дунд зэрэглэлийн эрсдэл;

Банкны дотоод сүлжээ болон салбар сүлжээгээр дамжуулан үйлчилгээг бусниулах буюу татгалзуулах боломжтой.

15.4.5. Доод зэрэглэлийн эрсдэл.

Мэдээллийн системийн сул тал, дутагдлыг арилгаж аюулгүй байдлыг хангах арга хэмжээ дутмаг хийгдсэнтэй холбоотой, мэдээллийн системд хохирол учруулах эрсдэл багатай халдлага.

15.5. Нэвтрэлтийн туршилтын явцад илэрсэн үр дүнг дараах дэлгэрэнгүй тайлбарын хамт тайланд тусгана.

15.5.1. Дахин давтагдашгүй бүртгэлийн дугаар;

15.5.2. Илэрсэн үр дүнг илэрхийлэх нэр(SQL injection, Man-in-the-middle гэх мэт);

15.5.3. Эрсдэлийн зэрэглэл буюу 15.4-т тодорхойлсон зэрэглэл;

15.5.4. Илэрсэн үр дүнгийн үзүүлэх нөлөө;

15.5.5. Хандалтын цэг буюу IP хаяг;

15.5.6. Хэрэглэгчийн төрөл буюу 15.3-т тодорхойлогдсон хэрэглэгчийн төрөл;

15.5.7. Халдлагад өртсөн мэдээллийн систем буюу URL хаяг, IP хаяг, домэйн нэр

болон халдлагад өртсөн мэдээллийн систем, үзүүлсэн нөлөөллийн талаар тодорхой тайлбар;

15.5.8. Үр дүнгийн талаар дэлгэрэнгүй тайлбар;

15.5.9. Илэрсэн эмзэг байдлыг арилгах заавар болон зөвлөмж.

АРВАН ЗУРГАА. ХАРИУЦЛАГА

Монголбанк энэ журмын биелэлтэд хяналт тавьж, журмын заалтыг зөрчсөн этгээдэд Банкны тухай хууль болон бусад холбогдох хууль тогтоомжийн дагуу хариуцлага хүлээлгэнэ.

_____oOo_____