ТӨСӨЛ

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН АУДИТ, ХАРИЛЦАА ХОЛБОО, МЭДЭЭЛЛИЙН ТЕХНОЛОГИЙН АУДИТ ХИЙХ ЭТГЭЭДИЙГ БҮРТГЭХ, АУДИТ ХИЙХ ЖУРАМ

Нэг. Нийтлэг үндэслэл

1.1. Кибер аюулгүй байдлын тухай хуулийн 9 дүгээр зүйлд заасан мэдээллийн аюулгүй байдлын аудит хийх хуулийн этгээд, Харилцаа холбооны тухай хуулийн 30[1].1-д заасан харилцаа холбоо, мэдээллийн технологийн аудит хийх хуулийн этгээдэд тавигдах шаардлага, аудит хийх хуулийн этгээдийг бүртгэх, хугацааг сунгах, бүртгэлийг цуцлахтай холбогдсон харилцааг энэ журмаар зохицуулна.

1.2. Мэдээллийн аюулгүй байдлын аудит хийх хуулийн этгээд, харилцаа холбоо, мэдээллийн технологийн аудит хийх хуулийн этгээд цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллагад бүртгүүлснээр үйл ажиллагаа явуулна.

1.3. Цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллага холбогдох хууль, энэ журамд заасан нөхцөл, шаардлагыг хангасан хуулийн этгээдийг мэдээллийн аюулгүй байдлын аудит хийх хуулийн этгээд, харилцаа холбоо, мэдээллийн технологийн аудит хийх хуулийн этгээдээр тус тус бүртгэнэ.

1.4. Энэ журмын 3.1-т зааснаар бүртгүүлсэн хуулийн этгээд аудитын үйл ажиллагаа /цаашид “аудитын үйл ажиллагаа” гэх/-нд энэ журам, аргачлал болон холбогдох хууль тогтоомжийг мөрдлөг болгоно.

Хоёр. Аудитын үйл ажиллагаанд баримтлах зарчим

2.1.Аудитын үйл ажиллагаанд дараах зарчмыг баримтална.

2.1.1.Аудитын тухай хуулийн 7 дугаар зүйлд заасан хараат бус байдлыг баримтлах;

2.1.2.мэдээллийн нууцыг чандлан хадгалах, хууль болон ажил гүйцэтгэх гэрээнд заасан хүрээнд ашиглах;

2.1.3.аудитын үйл ажиллагаанд мэргэжлийн, үл итгэх байр сууринаас хандах;

2.1.4.нотолгоонд үндэслэсэн дүгнэлт гаргах, зөвлөмж өгөх, үнэн зөв тайлагнах;

2.1.5.энэ журмын 7-д заасан ёс зүйн дүрмийг баримтлах.

Гурав. Мэдээллийн аюулгүй байдлын аудит, харилцаа холбоо, мэдээллийн технологийн аудит хийх хуулийн этгээдэд тавигдах шаардлага

3.1. Мэдээллийн аюулгүй байдлын аудит, эсхүл харилцаа холбоо, мэдээллийн технологийн аудит хийх хуулийн этгээд дор дурдсан шаардлагыг хангасан байна.

3.1.1.Монгол улсад бүртгэлтэй хуулийн этгээд байх;

3.1.2.энэ журмын 3.1.3-т заасан мэргэжлээр 8-аас доошгүй жил ажилласан туршлага бүхий 3-аас доошгүй орон тооны ажилтантай байх;

3.1.3.мэдээллийн технологи, мэдээллийн систем, системийн аюулгүй байдал, мэдээллийн аюулгүй байдал, электроник, компьютерын ухаан, компьютерын сүлжээний аль нэг чиглэлээр магистр болон түүнээс дээш

боловсролын зэрэгтэй байх;

3.1.4.Мэдээлэл, холбооны технологийн салбарын Монгол Улсын мэргэшсэн, эсхүл зөвлөх инженерийн зэрэгтэй 1-ээс доошгүй орон тооны ажилтантай байх;

3.1.5.мэдээллийн системийн мэргэшсэн аудиторын хүчин төгөлдөр гэрчилгээтэй, эсхүл түүнтэй дүйцэхүйц агуулгаар 40 буюу түүнээс дээш цагийн сургалтад хамрагдаж, төгссөнийг нотолсон гэрчилгээ бүхий 1-ээс доошгүй орон тооны ажилтантай байх.

3.2. Мэдээллийн аюулгүй байдлын аудит хийх хуулийн этгээд энэ журмын 3.1-т заасан шаардлагаас гадна дараах шаардлагыг хангасан байна.

3.2.1.мэдээллийн аюулгүй байдлын удирдлагын тогтолцооны ахлах аудиторын хүчин төгөлдөр гэрчилгээ бүхий орон тооны ажилтантай байх;

3.2.2.орон тооны ажилчдын 50-аас доошгүй хувь нь мэдээллийн аюулгүй байдлын чиглэлээр 5-аас дээш жил ажилласан туршлагатай байх.

Дөрөв. Аудит хийх хуулийн этгээдийг бүртгэх, хугацааг сунгах, цуцлах

4.1.Мэдээллийн аюулгүй байдлын аудит, харилцаа холбоо, мэдээллийн технологийн аудит хийх хуулийн этгээдээр бүртгүүлэхдээ дараах баримт бичгийг бүрдүүлж, цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллагад хүргүүлнэ.

4.1.1.мэдээллийн аюулгүй байдлын аудит хийх, эсхүл харилцаа холбоо, мэдээллийн технологийн аудит хийх хуулийн этгээдээр бүртгүүлэх хүсэлт;

4.1.2.хуулийн этгээдийн улсын бүртгэлийн гэрчилгээний хуулбар;

4.1.3.энэ журмын 3 дугаар зүйлд заасан шаардлагыг хангаж буйг нотлох баримт бичиг;

4.1.4.ажилтнуудын анкет;

4.1.5.ажилтнуудын нийгмийн даатгалын шимтгэл төлөлтийн лавлагаа;

4.2. Цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллага хүсэлтийг ажлын 15 өдөрт багтаан шийдвэрлэнэ.

4.3. Цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллага энэ журмын 4.1-т дурдсан баримт бичгийн үнэн зөвийг магадлах үүднээс нэмэлт материал болон эх хувийг шаардаж болно.

4.4. Мэдээллийн аюулгүй байдлын аудит, харилцаа холбоо, мэдээллийн технологийн аудит хийх бүртгэл 3 жилийн хугацаатай байна.

4.5. Аудит хийх хуулийн этгээд энэ журмын 4.4-т заасан хугацаа дуусахаас нэг сарын өмнө хугацаа сунгуулах хүсэлт гаргана.

4.6. Аудит хийх бүртгэлтэй байх хугацаа сунгуулах хүсэлтэд дараах баримт бичгийг хавсаргана.

4.6.1. энэ журмын 3 дугаар зүйлд заасан мэдээлэл өөрчлөгдсөн бол холбогдох нотлох баримт;

4.6.2. ажилтнуудын нийгмийн даатгалын шимтгэл төлөлтийн лавлагаа;

4.6.3.ажилтнууд нь жил бүр мэргэжлээрээ 24 буюу түүнээс дээш цагийн сургалтад хамрагдаж, тасралтгүй суралцсаныг нотлох баримт

4.7. Цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллага энэ журмын 4.5-д заасан хүсэлтийг ажлын 15 өдөрт багтаан шийдвэрлэж, энэ журмын 4.4-т заасан хугацаагаар сунгана.

4.8.Мэдээллийн аюулгүй байдлын аудит, харилцаа холбоо, мэдээллийн технологийн аудит хийх бүртгэлийг дараах тохиолдолд цуцална:

4.8.1.хуулийн этгээдийн хүсэлтээр;

4.8.2.ажилтнуудын эрх, үүрэг, хариуцлагаа хэрэгжүүлэх нөхцөл боломжийг бүрдүүлээгүй;

4.8.3.аудит хийх хуулийн этгээдээр бүртгүүлэхдээ хуурамч баримт бичиг бүрдүүлсэн;

4.8.4. хуулийн этгээд татан буугдсан;

4.8.5. аудитын тайланг хуурамчаар үйлдсэн, баталгаажуулсан нь тогтоогдсон;

4.8.6. энэ журмын 4.5-т заасан хугацаанд хүсэлт ирүүлээгүй.

Тав. Аудит хийх хуулийн этгээдийн эрх, үүрэг

5.1.Аудит хийх хуулийн этгээд дараах эрхтэй.

5.1.1.аудит хийхэд шаардлагатай үнэн зөв баримт бичиг, мэдээллээр хангахыг үйлчлүүлэгч байгууллагаас гэрээний хүрээнд шаардах;

5.1.2.үйлчлүүлэгч байгууллага гэрээнд заасан үүргээ биелүүлээгүй бол үйлчилгээ үзүүлэхээс татгалзах;

5.1.3.аудит хийх ажлын цар хүрээнээс хамаарч тухайн чиглэлийн мэргэшсэн мэргэжилтнийг гэрээгээр ажиллуулах;

5.1.4.шаардлагатай гэж үзвэл хариуцлагын гэрээгээр хүлээсэн үүргээ даатгуулах;

5.1.5.үйлчлүүлэгч байгууллагын гомдлыг хянан шийдвэрлэхэд шаардлагатай нотлох баримтыг холбогдох байгууллагад гаргаж өгөх, өөрийн үйл ажиллагаа, тайлангийн үнэн зөвийг батлах;

5.1.6.хуульд заасан бусад эрх.

5.2.Аудит хийх хуулийн этгээд Кибер аюулгүй байдлын тухай хуулийн 9.4-т зааснаас гадна дараах үүрэгтэй.

5.2.1.аудитын багийн ахлагч аудиторын эрхтэй байх;

5.2.2.үйлчлүүлэгч байгууллагаас тавьсан хууль ёсны шаардлагыг биелүүлэх;

5.2.3.аудит хийх явцад үйлчлүүлэгч болон гуравдагч этгээдээс хүлээн авсан баримт бичгийн бүрэн бүтэн, нууцлалтай байдлыг хангах;

5.2.4.аудит хийх явцад олж авсан мэдээллийн нууцыг хадгалах;

5.2.5.гүйцэтгэсэн аудитын дүгнэлт, зөвлөмжийн үнэн зөв байдал, үр дагаврыг бүрэн хариуцах;

5.2.6.өөрийн буруутай үйл ажиллагааны улмаас учруулсан хохирлыг барагдуулах;

5.2.7.аудитын үйлчилгээний эрхийг хүчингүй болгосон тохиолдолд гэрээ дуусгавар болоогүй үйлчлүүлэгчид ажлын 3 хоногт багтаан мэдэгдэх.

5.2.8.Цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллагад дараах мэдээлэл бүхий тайланг жил бүрийн 1 дүгээр

сарын 20-ны дотор хүргүүлнэ. Үүнд:

5.2.8.1.тайлангийн хугацаанд хийж гүйцэтгэсэн ажлын жагсаалт, тайлан;

5.2.8.2.аудиторууд нь жил бүр мэргэжлээрээ 24 буюу түүнээс дээш цагийн сургалтад хамрагдсаныг нотлох баримт.

5.3.Аудит хийхээр бүртгүүлсэн хуулийн этгээд нь мэдээллийн технологи, мэдээллийн аюулгүй байдлын чиглэлээр үйлчилгээ үзүүлснээс хойш тухайн байгууллагад хоёр жилийн хугацаанд мэдээллийн аюулгүй байдлын аудит, харилцаа холбоо, мэдээллийн технологийн аудит хийхийг хориглоно.

Зургаа. Аудит хийх хуулийн этгээдийн орон тооны ажилтны эрх, үүрэг

6.1.Ажилтан дараах эрхтэй байна.

6.1.1.мэргэжлийн холбоонд элсэх;

6.1.2.мэргэжлийн ур чадвараа нэмэгдүүлэх зорилгоор ажил олгогчоос дэмжлэг авах;

6.1.3.аудит хийх боломжгүй нөхцөл байдал үүссэн тохиолдолд холбогдох талуудад шуурхай мэдэгдэж шийдвэрлүүлэх;

6.2. Ажилтан нь Кибер аюулгүй байдлын тухай хуулийн 9.2.2-т зааснаас гадна дараах үүрэгтэй:

6.2.1.холбогдох мэдээллийг цуглуулах, ашиглахдаа төрийн болон албаны нууц, байгууллагын нууц болон хувь хүний нууцын тухай хуульд заасан хэм хэмжээг баримтлах;

6.2.2.холбогдох стандарт, аргачлал, зааврын дагуу аудитын үйлчилгээ үзүүлэх;

6.2.3.үйлчлүүлэгчээс хамрах хүрээнээс давсан нэмэлт материал шаардахгүй байх;

6.2.4.мэргэжлийн сургалтад тогтмол хамрагдаж ур чадвараа тасралтгүй хөгжүүлэх;

6.2.5.олон төрлийн мэдээлэлд дүн шинжилгээ, дүгнэлт хийх, баримт бичгийн боловсруулалт хийх ур чадварт тасралтгүй суралцах;

6.2.6.гэрээний хүрээнд үйлчлүүлэгчийг үнэн зөв, бодит мэдээллээр хангах;

6.2.7.энэ журамд заасан ёс зүйн хэм хэмжээг эрхэмлэн ажиллах;

6.2.8.аудит хийх хуулийн этгээдийн хууль бус шаардлагаас татгалзах, эрх олгох байгууллагад нэн даруй мэдэгдэх.

Долоо. Аудит хийх хуулийн этгээдийн ажилтны ёс зүйн дүрэм

7.1.Аудитын үйл ажиллагаанд хууль дээдлэх, шударга байх, хараат бус байх, нууцыг чандлан сахих, мэргэжлийн байх, нотолгоонд суурилж үнэлэлт өгөх зарчмуудыг баримтлан дараах ёс зүйн дүрмийг мөрдөнө.

7.1.1.хууль ёсыг дээдэлж, шударга ёсыг эрхэмлэх;

7.1.2.эрх мэдлээ урвуулан ашиглахгүй байх;

7.1.3.мэргэжлийн ур чадвар, мэдлэгийг эрхэмлэх;

7.1.4.байгууллагын болон нийтийн ашиг сонирхлыг хохироох, гэмт хэргийн шинжтэй аливаа үйлдэл, эс үйлдлийг гаргахгүй байх;

7.1.5.үйлчлүүлэгчийн болон ажил олгогч, оролцогч талуудын ашиг сонирхлыг эрхэмлэх;

7.1.6.оюуны өмчийг дээдлэх, холбогдох хууль тогтоомжийг биелүүлэх;

7.1.7.үүсэж болзошгүй аливаа ашиг сонирхлын зөрчлөөс урьдчилан сэргийлэх;

7.1.8.үйлчлүүлэгч, ажил олгогчид үйлчилгээ үзүүлэхдээ ялгаварлан гадуурхахгүй, эрэмбэлэн харьцахгүй байх;

7.1.9.аливаа хууль бус үйлдэл, эс үйлдэхүйн талаар хууль сахиулах байгууллагуудтай хамтран ажиллах;

7.1.10.шударга өрсөлдөөний зарчим баримтлах, бусад аудиторын нэр хүндэд халдах аливаа үйлдэл хийхгүй байх;

7.1.11.үйлчлүүлэгч, ажил олгогч талуудын хувийн болон хууль ёсны нууцад хүндэтгэлтэй хандаж, мэдээлэлд нэвтрэхгүй, ашиглахгүй, задруулахгүй байх;

7.1.12.хувь хүний харилцааны доголдолгүй, шашин шүтлэг, соёлын үнэт зүйлсэд ёс зүйтэй ханддаг байх.

Найм. Үйлчлүүлэгч байгууллагын эрх, үүрэг

8.1.Үйлчлүүлэгч байгууллага дараах эрхтэй.

8.1.1.аудит хийх хуулийн этгээдийн ажилтантай холбоотой гомдлыг аудит хийх хуулийн этгээд, цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллагад гаргаж шийдвэрлүүлэх;

8.2.2.аудитын дүгнэлтэд тайлбар гаргах, байгууллагын болон хувь хүний нууцтай холбоотой мэдээллийг хамгаалуулах;

8.2.3.хуульд заасан бусад.

8.2.Үйлчлүүлэгч байгууллага дараах үүрэгтэй.

8.2.1.аудитын явцад ажиллах нөхцөл боломжоор хангах, нотлох баримтыг цаг тухайд нь гаргаж өгөх;

8.2.2.аудит хийх хуулийн этгээдийн ажилтны тухай гомдолд хамаарах нотлох баримтыг гаргаж өгөх;

8.2.3.аудит хийх хуулийн этгээдийн талаарх гомдолд хамаарах нотлох баримтыг цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллагад гаргаж өгөх;

8.2.4.аудитын үйлчилгээ үзүүлэх гэрээнд заасан ажил үүргийг гүйцэтгэхтэй холбогдсон баримт, нотолгоог гаргаж өгөх, ажиглалт, асуулга, ярилцлага, тулган баталгаажуулалт хийх нөхцөл боломжоор хангах.

Ес. Цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллагын үүрэг

9.1. Цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллага Кибер аюулгүй байдлын тухай хуулийн 12.1.6-т зааснаас гадна дараах үүрэгтэй байна.

Энэ журмын хэрэгжилтийг хангах арга хэмжээ авах, хяналт шалгалт зохион байгуулах;

9.2.Үйлчлүүлэгч байгууллагын ирсэн хүсэлт, санал гомдлыг шийдвэрлэх,

холбогдох талуудад шаардлага хүргүүлэх;

9.3.Мэдээллийн аюулгүй байдлын аудит хийх эрх олгох, сунгах, хүчингүй болгохтой холбоотой мэдээллийн сан бүрдүүлэх, олон нийтэд мэдээлэх ажлыг зохион байгуулах.

Арав. Гомдол, маргааныг шийдвэрлэх

10.1.Үйлчлүүлэгч байгууллага болон аудит хийх хуулийн этгээдийн ажилтан аудит хийх бүртгэлтэй хуулийн этгээдтэй холбоотой гомдлыг цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллагад гаргаж болно.

10.2.Цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллага нь гомдлыг 30 хоногт багтаан шалгаж, хариуг гомдол гаргагч талд мэдэгдэнэ.

---o0o---

ТӨСӨЛ

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН АУДИТ ХИЙХ, ХАРИЛЦАА ХОЛБОО, МЭДЭЭЛЛИЙН ТЕХНОЛОГИЙН АУДИТ ХИЙХ АРГАЧЛАЛ

Нэг. Нийтлэг үндэслэл

1.1. Мэдээллийн аюулгүй байдлын аудит, харилцаа холбоо, мэдээллийн технологийн аудит нь байгууллагын бүтэц, стратеги зорилго, удирдлага, дүрэм журам, үйл ажиллагааны процесс, тоног төхөөрөмж, мэдээллийн систем, сүлжээний бүрэн бүтэн, нууцлалтай, хүртээмжтэй, аюулгүй, найдвартай ажиллагааг хангах зорилгоор аудитын нотолгоог үндсэн шалгуур, холбогдох стандартын дагуу үнэлж үл нийцлийг илрүүлж, дүгнэлт өгөх, илэрсэн үл нийцлийг арилгах арга хэмжээг зөвлөхөд оршино.

1.2. Аудитор гэж аудитын үйл ажиллагаа эрхэлж байгаа аудитын багийн ахлагч, бусад гишүүнийг ойлгоно.

1.3. Мэдээллийн аюулгүй байдлын аудитын үйл ажиллагаанд энэ аргачлалын нэгдүгээр хавсралтад заасан агуулгыг хамааруулан ойлгоно.

1.4. Харилцаа холбоо, мэдээллийн технологийн аудитын үйл ажиллагаанд энэ аргачлалын хоёрдугаар хавсралтад заасан агуулгыг хамааруулан ойлгоно.

Хоёр. Хамрах хүрээ

2.1. Кибер аюулгүй байдлын тухай хуулийн 9.1-д заасан мэдээллийн аюулгүй байдлын аудит хийхээр бүртгүүлсэн хуулийн этгээд мэдээллийн аюулгүй байдлын аудитын үйл ажиллагаанд энэ журмын 1.3-т заасан агуулга, энэ аргачлалыг мөрдлөг болгоно.

2.2. Харилцаа холбооны тухай хуулийн 30^1.1-д заасан харилцаа холбоо, мэдээллийн технологийн аудит хийхээр бүртгүүлсэн хуулийн этгээд харилцаа холбоо, мэдээллийн технологийн аудитын үйл ажиллагаанд энэ журмын 1.4-т заасан агуулга, энэ аргачлалыг мөрдлөг болгоно.

Гурав. Аудитын зарчмууд

3.1. Хууль дээдлэх, шударга байх

3.1.1. Аудитор нь аудитын үйл ажиллагаанд холбогдох хууль, дүрэм, журам, стандарт болон аудиторын ёс зүйг чанд мөрдөж, шударга байх;

3.1.2. Аудитор нь аудитын үйлчилгээг бодитой, шударгаар үзүүлэхэд харшлах, ашиг сонирхлын зөрчил үүсгэж болзошгүй аливаа нөхцөлийг урьдчилан тооцоолж сэргийлэх, татгалзах;

3.1.3. Аудитор нь аудитын үйл ажиллагааны тайлан, дүгнэлт, зөвлөмжийг хуурамчаар үйлдэхгүй байх;

3.1.4. Аудитор нь тухайн асуудалд бодитой хандаж, үнэн зөв, бүрэн гүйцэд тайлан, дүгнэлт, зөвлөмж гаргах.

3.2. Хараат бус байх

3.2.1. Аудитор нь үйлчлүүлэгч, ажил олгогчоос хараат бус байх;

3.2.2. Аудитор нь аудитын үйл ажиллагаанд үл итгэх байр сууринаас хандах;

3.2.3. Аудитор нь ашиг сонирхлын зөрчлөөс ангид байж хамаарал бүхий этгээд, ашиг сонирхлын зөрчил бүхий хуулийн этгээдийн үйл ажиллагаанд аудит хийхгүй байх;

3.2.4. Аудитор нь хараат бусаар мэргэжлийн тайлан, дүгнэлт, зөвлөмжийг гаргах;

3.2.5. Аудиторын эрхээ хэрэгжүүлэхэд нөлөөлөх, хараат бус байдлыг алдагдуулах дарамт, шахалтаар бусдын эрхшээлд орж болзошгүй аливаа нөхцөл үүсэхээс сэргийлж эрх бүхий байгууллагад мэдэгдэх, үүссэн тохиолдолд үйлчилгээ үзүүлэхээс татгалзах;

3.2.6. Аудитор нь хууль бус шаардлагаас татгалзах, өөрийн ашиг сонирхлыг хамгаалуулахын тулд хууль бус үйлдлийг шаардаж байгаа ажил олгогч болон үйлчлүүлэгчээс татгалзах;

3.2.7. Аудитор нь хоорондоо зөрчилдөх 2 ба түүнээс дээш ашиг сонирхлыг нэг зэрэг төлөөлөхгүй байх;

3.2.8. Аудитор нь аудит хийх явцад үйлчлүүлэгчийн ашиг сонирхол өөр үйлчлүүлэгчийн ашиг сонирхолтой зөрчилдөх нөхцөл байдал үүсвэл аудитын багийн ахлагчид нэн даруй мэдэгдэх.

3.3. Нууцыг чандлан сахих

3.3.1. Аудитор нь аудитын үйл ажиллагааны үр дүнд олж авсан, үйлчлүүлэгчээс эсхүл хуулиар олон нийтэд нээлттэй байхаар тогтоосон мэдээллээс бусад мэдээллийг гуравдагч этгээдэд задруулах, нийтэд ил болгох, хувийн зорилгоор ашиглахгүй байх;

3.3.2. Аудитор нь үйлчлүүлэгчийн мэдээллийн нууцыг хадгалах үүрэгтэй танилцах, дагаж мөрдөх.

3.4. Мэргэжлийн байх

3.4.1. Аудитор нь мэргэжлийн мэдлэг, ур чадвараа тогтмол хөгжүүлэх;

3.4.2. Аудитор нь мэдлэг, ур чадвар, туршлагыг эзэмшсэн, мэргэжлийн үйлчилгээг үзүүлэх;

3.4.3. Аудитыг үйлчлүүлэгчтэй байгуулсан гэрээнд заасан хугацаанд хариуцлагатай хийж гүйцэтгэх;

3.4.4. Аудитын багийг мэдлэг, ур чадвар, туршлага бүхий гишүүдээр бүрдүүлэх;

3.4.5. Бусад аудиторын нэр хүндэд сөргөөр нөлөөлөх аливаа үйлдэл хийхгүй байх.

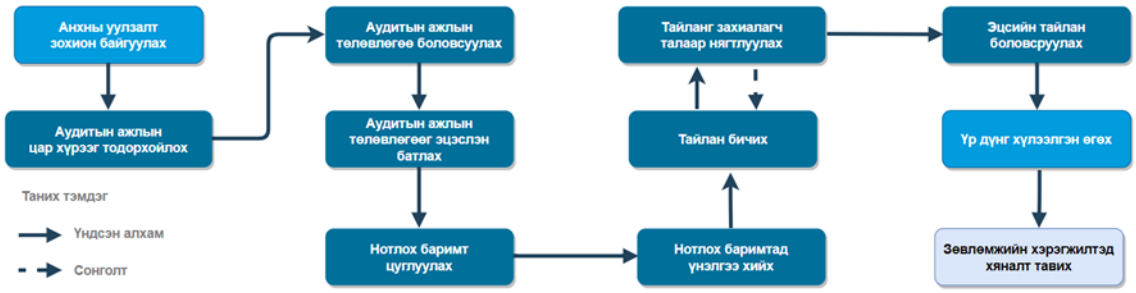
3.5. Нотолгоонд суурилж үнэлэлт өгөх

3.5.1. Аудитын тайлан, дүгнэлт, зөвлөмж нь хангалттай, баталгаажсан нотолгоонд суурилах;

3.5.2. Аудитын нотлох баримт нь бэлэн байгаа бодит мэдээлэлд үндэслэх.

Дөрөв. Аудитын үйл ажиллагаа

4.1. Аудитын үйл ажиллагаа нь аудитын төлөвлөлт, аудитын үйл ажиллагаа, аудитын үр дүн, дүгнэлт гэсэн үндсэн хэсгүүдээс бүрдэнэ. Аудитын үйл ажиллагааг зохих стандарт, дүрэм, журмын дагуу хангалттай, чанартай гүйцэтгэх шаардлагатай. Үйлчлүүлэгч байгууллага зөвлөмжийн хэрэгжилтийг хариуцан зохион байгуулна. Аудитын зорилго, хамрах хүрээ, шалгуур үзүүлэлтийг өөрчлөх бол зохицуулалтыг гэрээнд тусгаж, мөрдөнө. Аудитын үйл ажиллагааны ерөнхий бүдүүвчийг Зураг 1-д харуулав. Үйлчлүүлэгчийн хүсэлтээр аудитын зөвлөмжийн хэрэгжилтэд хяналт тавьж болох бөгөөд үүнийг гэрээнд тусгана.



Зураг 1. Ерөнхий бүдүүвч

Тав. Аудитыг төлөвлөх, гүйцэтгэх

5.1. Аудитыг дараах алхмын дагуу хийж гүйцэтгэнэ:
- 5.1.1. Аудитын эхний уулзалт хийх;
- 5.1.2. Аудитын багийн бүрэлдэхүүнийг батлах;
- 5.1.3. Хамрах хүрээг тодорхойлж, төлөвлөгөө боловсруулах;
- 5.1.4. Нотлох баримт цуглуулах, баталгаажуулах;
- 5.1.5. Нотлох баримтыг үнэлэх;
- 5.1.6. Дүгнэлт гаргах, үйлчлүүлэгчид танилцуулах;
- 5.1.7. Тайланг нягтлуулах;
- 5.1.8. Тайланд зөвлөмжийн хэрэгжилтийг шалгах зааврыг тусгах.

5.2. Аудит эхлэхээс өмнө аудитын үйл ажиллагаанд оролцох аудиторуудыг үйлчлүүлэгч, түүний эрх бүхий албан тушаалтнуудаас хараат бус, ашиг сонирхлын зөрчилгүй эсэхийг үнэлж, бичгээр баталгаажуулна.

5.3. Аудит хийх байршил, зохион байгуулалтын нэгж, аудит хийх үйл явц, хугацаа, зохион байгуулалт, тайлагналтыг харилцан тохиролцож, аудитын хамрах хүрээг тодорхойлно.

5.4. Аудитын төлөвлөгөө болон хуваарь боловсруулахад дараах нөхцөлийг харгалзана:
- 5.4.1. Аудитын төлөвлөгөөнд үйлчлүүлэгч байгууллагад холбогдох хууль, дүрэм журмаар хүлээлгэсэн үүрэг, стратеги бодлого, үйл ажиллагаа, орчин нөхцөл, бүтэц зохион байгуулалт, дэд бүтэцтэй танилцах ажлыг тусгана. Шаардлагатай тохиолдолд үйлчлүүлэгч байгууллагаас сургалт авах, нууцын гэрээ байгуулж болно.
- 5.4.2. Аудитын төлөвлөгөөг хангалттай, шаардлага хангахуйц, үнэн бодит мэдээлэлд тулгуурлан боловсруулах бөгөөд гуравдагч байгууллагаас үйлчилгээ авдаг бол тухайн байгууллагын оролцоог хангаж болно.
- 5.4.3. Аудитын төлөвлөгөөнд аудитын үйл ажиллагаанд оролцогч талуудын үүрэг, хариуцлага, оролцоог нарийвчлан тусгана.
- 5.4.4. Аудитын баг болон үйлчлүүлэгч байгууллагын цаг хугацаа, нөөц боломжид тулгуурлан гадаад, дотоод хүчин зүйлийг тооцож, төлөвлөгөөг боловсруулна.
- 5.4.5. Аудит хийх хуваарьт аудит хийх мэдээллийн систем, дэд бүтэц, байгууламж, тэдгээрт хийгдэх үйл ажиллагаа, үргэлжлэх хугацаа болон үйлчлүүлэгч байгууллагын удирдлагатай хийх уулзалт, аудитын багийн уулзалт, аюулгүй ажиллагааны зааварчилгаа, аудитын үйл ажиллагааны хугацаа, хаалтын хурлын хуваарь, үргэлжлэх хугацаа зэргийг тусгана. Аудитын хамрах хүрээнээс

хамаарч аудитын багт тухайн чиглэлд мэргэшсэн боловсон хүчнийг гэрээгээр ажиллуулж болно.

5.5. Аудитын төлөвлөгөөнд дараах агуулгыг тусгана:
- 5.5.1. Зорилго, ач холбогдол;
- 5.5.2. Гадаад, дотоод хүчин зүйл;
- 5.5.3. Аудитын ажлын хамрах хүрээ;
- 5.5.4. Аудитын шалгуур үзүүлэлт;
- 5.5.5. Аудитын эхлэх, дуусах хугацаа, байршил;
- 5.5.6. Аудитын багийн гишүүд, тэдгээрийн хүлээх үүрэг, ажиллах цагийн хуваарь;
- 5.5.7. Аудит хийх аргачлал, стандарт;
- 5.5.8. Аудитын хугацаанд зохион байгуулах албан ёсны хурал;
- 5.5.9. Аудитын үед мэдээлэлд хандах эрхийн түвшин, хугацаа;
- 5.5.10. Мэдээллийн нууцлалын асуудал.

5.6. Аудитын төлөвлөгөө, хуваарийг талууд харилцан тохиролцож, гарын үсэг зурж баталгаажуулснаар аудитын ажлыг эхэлсэнд тооцно.

5.7. Аудитын төлөвлөгөөнд өөрчлөлт оруулах шаардлагатай болсон тохиолдолд талууд зөвшилцөж, шийдвэрлэнэ.

5.8. Аудитор нь дараах баримт бичгүүдийг бэлтгэх шаардлагатай:
- 5.8.1. Нууцлалын баталгааны хуудас;
- 5.8.2. Аудитын хянан магадалгааны хуудас;
- 5.8.3. Аудитын нотлох баримтын бүртгэлийн хуудас;
- 5.8.4. Нотлох баримтын шалгуурын үнэлгээний хуудас.

5.9. Аудитын нотлох баримт цуглуулахад дараах нөхцөлийг харгалзана:
- 5.9.1. Аудитор нь аудитын нотлох баримтын үнэн зөв байдалд эргэлзээ төрвөл нөхцөл байдлын талаарх мэдээлэл, түүнийг хэрхэн үнэлсэн тэмдэглэлийг шалгуурын үнэлгээний хуудсанд тодорхой тусгана.
- 5.9.2. Аудитын үйл ажиллагааны явцад аливаа хязгаарлах хүчин зүйл, нөхцөл байдал үүссэн бол түүний талаар тодорхой бичиж тэмдэглэнэ.
- 5.9.3. Аудитор нь нотлох баримт бүрдүүлэх зорилгоор системд нэвтэрч мэдээлэл олж авах, системийн лог бүртгэлийг хуулбарлан авах, системээс гаргадаг тайлантай танилцах, автомат хэрэгслүүдийг ашиглах зэрэг үйлдлийг гүйцэтгэнэ.
- 5.9.4. Аудитын нотлох баримтыг дараах аргуудаар цуглуулж болно:
  - 5.9.4.a. Түүвэр судалгаа, ярилцлага;
  - 5.9.4.b. Аудитын хянан магадалгааны хуудас;
  - 5.9.4.c. Байгууллагын болон системийн үйл ажиллагааны үе шат, процесс, дүрэм журам, түүний хэрэгжилтэд хянан магадалгаа хийх;
  - 5.9.4.d. Системд нэвтэрч мэдээлэл олж авах;
  - 5.9.4.e. Олон нийтэд нээлттэй мэдээлэл, халдлагын мэдээллийн сан зэрэг бусад эх сурвалжаас судалгаа хийх;
  - 5.9.4.f. Мэдээллийн системийн хяналтын хэрэгслийг ашиглах.
- 5.9.5. Мэдээллийн аюулгүй байдлын аудитын шалгуурын хүрээнд энэ аргачлалын Нэгдүгээр хавсралтад заасан жишиг нотлох баримтыг ашиглаж болно.

5.10. Аудитын нотлох баримтын хүрээнд дараах агуулгыг тусад нь заавал судална:

5.10.1. Өмнөх аудит, эрсдэлийн үнэлгээний тайлан, дүгнэлт, зөвлөмж;
5.10.2. Өмнөх аудит, эрсдэлийн үнэлгээний хүрээнд хэрэгжүүлсэн арга хэмжээ;
5.10.3. Байгууллагын үйл ажиллагааны чиглэл, цар хүрээ;
5.10.4. Байгууллагын дотоод журам, дүрэм;
5.10.5. Салбарын стандарт, бодлого, журам, дүрэм;
5.10.6. Үйл ажиллагааны баримт бичиг, зөвшөөрөл;
5.10.7. Хууль эрх зүйн орчин;
5.10.8. Хөдөлмөрийн аюулгүй ажиллагаанд баримтлах дүрэм, журам;
5.10.9. Байгууллагын онцлогоос хамаарсан бусад баримт бичиг.

5.11. Аудиторын бодитоор хийж гүйцэтгэх үйл ажиллагаа
5.11.1. Нэвтрэлт, танилт, баталгаажуулалтыг үнэлэх;
5.11.2. Физик аюулгүй байдлыг үнэлэх;
5.11.3. Нөөцлөх, сэргээх үйл ажиллагааг үнэлэх;
5.11.4. Программ хангамж, системийн оролт ба гаралтын үзүүлэлтийг үнэлэх;
5.11.5. Өгөгдлийн сангийн үнэлгээ хийх;
5.11.6. Халдлага илрүүлэх автомат систем зэрэг автомат системүүдийн ажиллагааг турших.

5.12. Аудитор нь дараах мэдээллийн хөрөнгийг хамгаалагдсан эсэхийг үнэлнэ:
5.12.1. Өгөгдөл (гадаад эсхүл дотоод, бүтэцтэй ба бүтэцгүй, график, дуу, дүрс, системийн баримт бичиг гэх мэт);
5.12.2. Программ хангамж (гарын авлага, програмчлагдсан процедур);
5.12.3. Технологиуд (техник хангамж, үйлдлийн систем, өгөгдлийн сангийн удирдлагын систем, сүлжээ, мультимедиа гэх мэт);
5.12.4. Мэдээллийн систем, хэрэгслийг эзэмших, дэмжихэд шаардлагатай нөөцүүд;
5.12.5. Мэдээллийн систем, мэдээллийн технологийн үйлчилгээг төлөвлөх, зохион байгуулах, эзэмших, хүргэх, дэмжих, хянах ажилтнуудын мэдлэг, ур чадвар, бүтээмж.

5.13. Аудитор нь дараах агуулгын хүрээнд аудит хийхтэй холбоотой эрсдэлийг хянах шаардлагатай. Үүнд:
5.13.1. Аудит хийхтэй холбоотой эрсдэл буюу алдааны магадлалыг урьдчилан тооцож, аудитын явцад тогтмол хянах;
5.13.2. Аудитын нотлох баримтаар ашиглах мэдээллийн үнэн зөв, хангалттай эсэхийг үнэлсэн байх. Түүнчлэн үйлчлүүлэгч шийдвэр гаргахад сөргөөр нөлөөлж болзошгүй алдаатай нотлох баримт байгаа эсэхийг үнэлж, нөлөөллийн хэмжээг тодорхойлох;
5.13.3. Нотлох баримтын үнэн зөв байдал, нарийвчлалтай холбоотой эрсдэлтэй нөхцөл үүсвэл энэ талаарх мэдээллийг болон хэрхэн үнэлгээ өгсөн тухай тайланд тусгах.

5.14. Эрсдэлийн удирдлагыг дараах алхмын дагуу хэрэгжүүлнэ:
5.14.1. Эрсдэлийг илрүүлэх;
5.14.2. Эрсдэлийг үнэлэх;
5.14.3. Эрсдэлийн хариу үйлдлийг тодорхойлох;
5.14.4. Дүгнэлт гаргах;
5.14.5. Зөвлөмж боловсруулах.

5.15. Эрсдэлийн үнэлгээг кибер аюулгүй байдлын эрсдэлийн үнэлгээ хийх аргачлалын дагуу хийнэ.

Зургаа. Аудитын тайлан боловсруулах

6.1. Аудит хийх зорилгын дагуу цуглуулсан мэдээллийг судалж, нотолгоонд суурилсан, эрсдэлийг тооцсон, товч, тодорхой, хараат бус үнэлгээ, дүгнэлт, зөвлөмж гаргах бөгөөд талууд харилцан тохиролцож, гарын үсэг зурснаар аудитын эцсийн тайлан бий болно.

6.2. Аудитын үйл явц, нотолгоо цуглуулахтай холбоотой тодорхой бус эрсдэлийг үнэлж дүгнэхдээ одоогийн болон ирээдүйд үүсэж болзошгүй эрсдэлийг хамтад нь тооцно.

6.3. Байгууллагын онцлогоос шалтгаалан аудитын үйл явц, нотолгоо цуглуулахад эрсдэл, хязгаарлалт үүсэж болзошгүй нөхцөл үүссэн бол түүнийг тайлан, дүгнэлт, зөвлөмжид тусгана.

6.4. Аудитын нотлох баримт, үл нийцэл бүрээр үнэлгээ, дүгнэлт гаргана.

6.5. Аудитын зөвлөмжид учирч болзошгүй аливаа эрсдэлээс урьдчилан сэргийлэх, байгууллагын үйл ажиллагааны хүрээнд мөрдөж буй хууль, тогтоомж, стандартын хэм хэмжээ, мэдээллийн аюулгүй байдлыг сайжруулах арга хэмжээ болон тухайн зөвлөмжийн хэрэгжилтийг шалгах зааврыг тусгана.

6.6. Аудитын явцад олж илрүүлсэн байгууллагын ололт амжилт, давуу тал, онцлог шийдлийг тайланд тусгах нь тайлангийн үнэлэмжийг нэмэгдүүлнэ.

Долоо. Үр дүнг хүлээлгэн өгөх

7.1. Аудитын тайланг гэрээнд заасан хугацаанд үйлчлүүлэгчид хүлээлгэн өгөх ба тайлан нь үйлчлүүлэгч байгууллагын өмч байна.

7.2. Аудитын тайлангийн нууцыг хадгалах хугацаа тайланг бүрэн хүлээлгэж өгснөөс хойш 5 жилээс багагүй байна.

7.3. Нууцын баталгаат хугацаа дуусаагүй бол тайланг бүхэлд нь эсхүл хэсэгчлэн ил болгох, аудитын явцад олж авсан нотолгоо зэргийг хуульд зааснаас бусад тохиолдолд бусдад задруулж, дамжуулахыг хориглоно.

7.4. Аудитор нь аудитын аливаа мэдээллийг олон нийтэд нээлттэй болгох бол үйлчлүүлэгчид урьдчилан мэдэгдэж зөвшөөрөл авна.

7.5. Аудитын тайланд дараах зүйлсийг зайлшгүй тусгана:

- 7.5.1. Аудитын ерөнхий танилцуулга, зорилго;
- 7.5.2. Аудитын хамрах хүрээ, цаг хугацаа, аргачлал;
- 7.5.3. Үйлчлүүлэгчийн ерөнхий мэдээлэл;
- 7.5.4. Аудиторын мэдээлэл;
- 7.5.5. Аудитын шалгуур үзүүлэлт, стандарт, баримтлах зарчим;
- 7.5.6. Аудитын үнэлгээ, эрсдэлийн үнэлгээ, эрсдэлийн үнэлгээний матриц;
- 7.5.7. Аудитаар илэрсэн үл нийцэл;
- 7.5.8. Аудитын дүгнэлт;
- 7.5.9. Аудитын дүгнэлт, нотлох баримтын хувьд аудитор, үйлчлүүлэгч хоорондын санал зөрөлдөөнтэй шийдэгдээгүй асуудлууд;

7.5.10. Үл нийцлийг залруулах зөвлөмж, хэрэгжүүлэх хугацаа, зөвлөмжийн хэрэгжилтийг шалгах заавар;
7.5.11. Тайлангийн нууцлал;
7.5.12. Үйлчлүүлэгч байгууллагын аудиторт өгөх санал, дүгнэлт.

7.6. Аудитын тайланг хүлээлгэн өгөхөөс өмнө тайланг дүгнэх, магадлах уулзалт хийж, үйлчлүүлэгчид аудитын үр дүн, авч хэрэгжүүлэх арга хэмжээг танилцуулна.
7.7. Үйлчлүүлэгч байгууллагаар тайланг бүрэн хянуулж, аудитор нотлох баримтыг бодит үнэнээс зөрүүтэй ойлгож, дүгнэсэн бол шаардлагатай засварыг оруулна.
7.8. Аудитын үр дүнд тодорхойлогдсон үл нийцлийг залруулах дүгнэлт, зөвлөмжийг албан ёсны хурлаар танилцуулж, санал болгосон зөвлөмжийг хэрэгжүүлэх талаар зөвлөгөө өгнө.
7.9. Аудитор нь үл нийцлийг залруулах ерөнхий төлөвлөгөөг үйлчлүүлэгч байгууллагад гаргаж өгнө.
7.10. Аудиторын зөвлөмжийг үр дүнтэй хэрэгжүүлэхэд үйлчлүүлэгч тал аудитораас тусламж, зөвлөгөө авч болно.

---o0o---

ТӨСӨЛ
Мэдээллийн аюулгүй байдлын аудит,
харилцаа холбоо, мэдээллийн технологийн
аудит хийх аргачлалын Нэгдүгээр хавсралт

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН АУДИТЫН ЖИШИГ НОТЛОХ БАРИМТ

1. Байгууллагын бүтэц, зохион байгуулалт
   1.1. Байгууллагын мэдээллийн аюулгүй байдлын удирдлагын тогтолцоо бүрдсэн байдал, үйл ажиллагааны төлөвлөгөөтэй эсэх;
   1.2. Мэдээллийн болон бусад хөрөнгө, мэдээллийн аюулгүй байдлыг хангах процесс тодорхой эсэх, бичиг баримтад тусгагдсан эсэх;
   1.3. Байгууллагын мэдээлэл болон мэдээллийн технологийн хөрөнгийн хандах, ашиглахтай холбоотой хандалтын хяналтын матриц эсвэл түүнтэй дүйцэх бичиг баримт байгаа эсэх, түүний хэрэгжилтэд хяналт тавьдаг эсэх;
   1.4. Хууль эрх зүйн хүрээнд мэдээллийн аюулгүй байдлыг хангах нууцлалын гэрээг ажилчид, харилцагч болон бусад талуудтай байгуулдаг эсэх, гэрээний загвартай эсэх;
   1.5. Мэдээллийн аюулгүй байдлыг хангах зорилгоор жил бүр тодорхой төсөв баталдаг эсэх, түүний тодорхой хувийг лицензтэй программ хангамжийн эрх худалдан авах эсхүл сунгахад зарцуулдаг эсэх;
   1.6. Мэдээллийн аюулгүй байдлыг ханган ажиллахад шаардлагатай мэдлэг мэдээллээр ажилтнууд, удирдлага, харилцагч талуудыг хангадаг эсэх;
   1.7. Хуулийн хүрээнд мэдээллийн аюулгүй байдлын аудит, эрсдэлийн үнэлгээг тухай бүр хийлгэдэг эсэх;
   1.8. Байгууллагын ашиглаж буй техник технологи, мэдээллийн системийн дэд бүтэц, программ хангамжид чиглэсэн эмзэг байдал, хортой код болон шинэ технологийн талаарх мэдээлэл, зөвлөгөөг цаг алдалгүй авах мэдээллийн эх сурвалжтай эсэх;
   1.9. Шинэ ажилтан болон тоног төхөөрөмж, программ хангамж худалдан авахтай холбоотой харилцааг зохицуулах тогтолцоо бүрдсэн байдал:
      1.9.1. Шинээр ажилтан авахад программ хангамж, тоног төхөөрөмжийн эрх, үүргийн харилцааг зохицуулах боломжтой эсэх;
      1.9.2. Шинэ ажилтны ажлын байранд шаардагдах бичиг баримтын бүрдэл бэлэн эсэх, кибер аюулгүй байдлын талаар тусгасан эсэх;
      1.9.3. Шинээр ажлын байр бий болох болон тоног төхөөрөмж, программ хангамж худалдан авах, хандив, тусламжаар авах үед хөрөнгийн ангилал, эзэн оноох, ашиглах эрхийн талаар тогтоосон бичиг баримттай эсэх.
2. Мэдээллийн технологийн төсөл хэрэгжүүлэх, мэдээллийн систем худалдан авах, нэвтрүүлэх үеийн зааврыг тусгадаг тогтолцоотой, эрсдэлийн үнэлгээ хийлгэдэг эсэх.
3. Мэдээллийн аюулгүй байдлын бодлого, журам

3.1. Хууль, стандарт, бизнесийн хэрэгцээ, шаардлагыг хангахуйц мэдээллийн аюулгүй байдалд дэмжлэг үзүүлэх бодлогын баримт бичигтэй эсэх;

3.2. Тухайн баримт бичгийг байгууллагын нийт ажилтнууд шаардлагатай бол хамтрагч байгууллагуудад танилцуулж, дагаж мөрдөх, хэрэгжилтэд хяналт тавьдаг эсэх;

3.3. Мэдээллийн аюулгүй байдлын холбогдох баримт бичгүүд нь Монгол Улсын үндэсний аюулгүй байдлын үзэл баримтлалын 3.6 дахь хэсэг, кибер аюулгүй байдлын үндэсний стратеги болон кибер аюулгүй байдлыг хангах нийтлэг журамд нийцэж буй эсэх;

3.4. Мэдээллийн аюулгүй байдлын бодлого, журамд дараах зүйлсийг тусгасан эсэх:

3.4.1. Хандалтын хяналтын матриц, аргачлалтай эсэх;

3.4.2. Мэдээллийн ангилал болон тухайн мэдээллийн эзэн, мэдээлэл хариуцагчийг тодорхойлсон эсэх;

3.4.3. Физик болон орчны аюулгүй байдлын асуудлуудыг тусгасан эсэх;

3.4.4. Төгсгөлийн хэрэглэгчийн асуудлуудыг тусгасан эсэх:

3.4.4.a. Суурин хэрэглэгчийн асуудал;

3.4.4.b. Хөдөлгөөнт хэрэглэгч асуудал;

3.4.4.c. Гуравдагч байгууллагатай харилцах, тэдгээрийн цахим харилцааны зохицуулалтын асуудал;

3.4.4.d. Мэдээлэл ашиглах, боловсруулах, дамжуулах, хадгалах, хамгаалах, устгах асуудлууд;

3.4.4.e. Программ хангамж суулгах, устгах болон эдгээртэй холбоотой бүртгэлийн асуудлууд;

3.4.4.f. Тоног төхөөрөмжийг зүй зохистой хэрэглэх асуудлууд.

3.4.4.g. Зөөврийн төхөөрөмжүүдийг байгууллагын төхөөрөмжид холбохтой холбоотой асуудлууд.

3.4.5. Нөөцлөлт болон нөөцөөс сэргээхтэй холбоотой асуудлууд;

3.4.6. Мэдээлэл дамжуулах асуудлууд;

3.4.7. Хортой программаас хамгаалах арга, аргачлал;

3.4.8. Криптографын асуудлууд;

3.4.9. Сүлжээний дэд бүтцийн аюулгүй байдлын асуудлууд;

3.4.10. Ажиллагсдын хувийн мэдээллийн нууцлал, хамгаалалттай холбоотой асуудлууд;

3.4.11. Хамтрагч байгууллагуудтай холбоотой мэдээллийн технологийн хэрэглээ, хандалтын хэм хэмжээг тусгасан эсэх.

4. Мэдээллийн аюулгүй байдлын бодлого, журмын аудит хийх асуудлууд

4.1. Бодлого, журамд заасан асуудал бүрд хариуцагчийг оноосон, хариуцсан асуудлын хүрээнд шийдвэр гаргах эрх бүрдсэн эсэх;

4.2. Бодлого, журмыг байгууллагын ажилтан бүр мэддэг эсэх, түүнчлэн дагаж мөрддөг эсэх;

4.3. Бодлого, журам нь холбогдох хууль болон стандартууд дахь шаардлагыг хангасан эсэх.

5. Зохистой хэрэглээний бодлого

5.1. Нууц үгийн зохистой хэрэглээ
  5.1.1. Байгууллагын системүүдэд нууц үгийн бодлого, шаардлага хэрэгжүүлдэг эсэх;
  5.1.2. Нууц үгийн түвшинтэй эсэх:
    5.1.2.a. Хэрэглэгчийн түвшний нууц үг;
    5.1.2.b. Админ хэрэглэгчийн түвшний нууц үг гэх мэт.
  5.1.3. Систем, дэд бүтэц, программ хангамжийн өгөгдмөл нууц үгийг ашигладаг эсэх;
  5.1.4. Нууц үгийг криптографын алгоритмаар хамгаалдаг эсэх;
  5.1.5. Нууц үгийг дахин ашиглах, солихгүй удаан байх зэргээс хамгаалдаг эсэх.
5.2. Интернэтийн зохистой хэрэглээ
  5.2.1. Байгууллагын интернэт сүлжээг ажлын бус, хууль бус зориулалтаар ашиглахаас сэргийлсэн эсэх;
  5.2.2. Интернэт хандалтыг зохицуулах бодлого, журамтай эсэх;
  5.2.3. Аюулгүй байдал хангагдаагүй системд хандахыг хязгаарладаг эсэх.
5.3. Цахим шуудан болон бусад холбогдох хэрэгслийн зохистой хэрэглээ
  5.3.1. Байгууллагын цахим шууданг зөвхөн бизнесийн зорилгоор ашиглах, түүнд хяналт тавьдаг эсэх;
  5.3.2. Үл танигдах эх сурвалжаас ирсэн цахим шуудан, хавсралт файл, холбоосны аюулгүй байдлыг шалгадаг эсэх;
  5.3.3. Нууцлалтай, маш нууц ангиллын мэдээллийг нууцлалгүй дэд бүтцээр дамжуулахгүй байх зохицуулалт хийгдсэн эсэх.
5.4. Компьютерын зохистой хэрэглээ
  5.4.1. Аливаа компьютерын дэлгэцийг ашиглаагүй үед түгжих талаарх зохицуулалт;
  5.4.2. Хувийн төхөөрөмжийг байгууллагын сүлжээнд ашиглахад ажилтнуудын мөрдөх мэдээллийн аюулгүй байдлын журам;
  5.4.3. Шинэ төхөөрөмж сүлжээнд ажиллуулахад зохицуулсан бодлого журам;
  5.4.4. Албан ёсны эрхтэй программ хангамж, үйлдлийн систем ашигладаг байдал;
  5.4.5. Нууцад хамаарах цахим мэдээллийг нээлттэй байлгахаас сэргийлж дэлгэцийн өнцгийг тохируулдаг эсэх.
5.5. Ухаалаг утас, зөөврийн төхөөрөмжийн зохистой хэрэглээ
  5.5.1. Ухаалаг утас ашиглан байгууллагын сүлжээ, дэд бүтэц, системийн орчинд ажиллах бол түүний аюулгүй байдлыг хангах бодлого, зохицуулалттай эсэх:
    5.5.1.a. Аюулгүй байдлыг шалгах бодлого, зохицуулалттай, түүнийг хэрэгжүүлдэг эсэх;
    5.5.1.b. Нууц үгийн бодлогыг хэрэгжүүлдэг эсэх;
    5.5.1.c. Автоматаар түгжигдэх зэрэг бодлого хэрэгжүүлдэг эсэх;
  5.5.2. Танилт, баталгаажуулалт хийгдсэний дараа байгууллагын системд нэвтрэх, ажиллах боломжтой талаарх зохицуулалт хийгдсэн эсэх;

5.5.3. Зөөврийн төхөөрөмжид суурин төхөөрөмжийн шаардлагаас нэмэлт аюулгүй байдлын шаардлага тавигддаг эсэх;

5.5.4. Зөөврийн төхөөрөмжид хадгалагдаж буй мэдээллийн нууцлалыг хамгаалах бодлого, шийдлийг хэрэгжүүлдэг эсэх.

5.6. Биет мэдээллийн зохистой хэрэглээ

5.6.1. Биет мэдээллийг ашиглаагүй үедээ цоож бүхий хамгаалалттай эд хогшилд түгжиж, байршуулдаг эсэх;

5.6.2. Тухайн эд хогшил байршиж буй байрлал, биет мэдээллийн ангиллаас хамааруулан физик аюулгүй байдлыг ханган ажилладаг эсэх;

5.6.3. Мэдээллийн ангиллаас хамааруулан хэвлэх, хувилах үеийн аюулгүй байдлыг ханган ажилладаг эсэх.

5.7. Хүний нөөцийн аюулгүй байдлын бодлого

5.7.1. Ажлын анкет бөглөсөн ажил горилогч бүрийн товч намтарт бичигдсэн мэдээллийг нягтлах тогтолцоо, аргачлалтай эсэх;

5.7.2. Мэргэжлийн болон бусад ур чадварын баталгаажуулалтыг нягтлах аргачлалтай эсэх;

5.7.3. Ажилтны хандах мэдээллийн ангиллаас хамаарч хүний нөөцтэй холбоотой шалгалтыг ялгаатай гүйцэтгэдэг эсэх;

5.7.4. Байгууллагын нууц буюу түүнээс дээш ангиллын мэдээлэлд хандаж буй бүх ажилтантай нууцын гэрээ байгуулдаг эсэх, хуулийн заалтыг тодорхой тусгадаг эсэх;

5.7.5. Байгууллагын мэдээллийн аюулгүй байдлын бодлого журам, хүрэх үр дүн, зорилгыг тодорхой заасан эсэх, ажилчид түүнийг нээлттэй мэдэх боломжтой, хэрэгжүүлэх тогтолцоотой эсэх;

5.7.6. Ажилтнуудын мэдээллийн аюулгүй байдлын мэдлэг, ур чадварыг нэмэгдүүлэх сургалтын тогтолцоотой эсэх, сургалтын агуулгыг ажилтны ажлын байрны тодорхойлолттой уялдуулдаг эсэх;

5.7.7. Сургалт нь оролцогчдын оролцоог хангадаг эсэх:

5.7.7.a. Танхимаар эсхүл бие даан суралцах боломжийг бүрдүүлсэн эсэх;

5.7.7.b. Вебд суурилсан эсхүл сургалтын тусгай программ хангамжид суурилан сургалт зохион байгуулах системтэй эсэх;

5.7.7.c. Сургалтын агуулгад дараах зүйлс орсон эсэх:

5.7.7.d. Байгууллагын мэдээллийн аюулгүй байдлын бодлого, дүрэм журам;

5.7.7.e. Аюулгүй байдлын халдлага, зөрчлийг мэдээлэх тухай;

5.7.7.f. Мэдээллийн аюулгүй байдлын суурь ойлголт.

5.7.8. Сургалтын агуулгыг сайжруулах талаар санал авах аргачлалтай эсэх;

5.7.9. Ажилтан ажлын байраа солиход тухайн ажлын байранд шаардлагатай сургалтаар хангах боломжтой эсэх.

6. Мэдээллийн хөрөнгийн удирдлага

6.1. Мэдээллийн хөрөнгийг тодорхойлж, тохиромжтой аюулгүй байдлын ажиллагааг тодорхойлох

6.1.1. Байгууллагын мэдээллийн хөрөнгийг тодорхойлох, аюулгүй байдлын уялдаа холбоог хангах талаар ажилладаг эсэх;

6.1.2. Мэдээллийн хөрөнгийн ашиглагдаж эхэлсэн он, сар, өдөр болон үйлдвэрлэгчийг тодорхойлдог эсэх;

6.1.3. Хөрөнгийн хувилбарын дугаарыг тодорхой бүртгэдэг эсэх;

6.1.4. Мэдээллийн хөрөнгө, мэдээллийн хөрөнгийн эзэн хоорондын ажиллагааны уялдаа холбоог хангах, ашиглалтын хэм хэмжээнд зохицуулалт хийдэг эсэх;

6.1.5. Мэдээллийн хөрөнгө үүсэхээс устгах хүртэл бүх шатны харилцааг зохицуулсан бичиг баримттай эсэх, мэдээллийн ангиллын хугацааг тодорхой заасан эсэх;

6.1.6. Мэдээллийн хөрөнгийг хуулбарлах, олшруулах, түгээх хэм хэмжээг тогтоосон эсэх;

6.1.7. Мэдээллийн хөрөнгийг буруу ашигласан нь тогтоогдсон тохиолдолд авах арга хэмжээг тодорхой заагдсан эсэх (мэдээллийн хөрөнгийн хуулбарыг буруугаар ашиглах нь эх хувийн адил хариуцлага хүлээх болохыг заах гэх мэт).

6.2. Мэдээллийн ангилал

6.2.1. Мэдээллийн хөрөнгийн үнэлгээг мэдээллийн үнэ цэнэ, ач холбогдлын зэрэг, эмзэг байдал зэргээр нь ангилдаг эсэх;

6.2.2. Мэдээллийн хөрөнгө бүрийн үнэлгээг ангилалд тулгуурлан тооцох тогтолцоотой эсэх.

6.3. Зөөврийн хадгалах төхөөрөмжийн асуудлууд

6.3.1. Мэдээллийн хөрөнгийг хадгалж буй зөөврийн төхөөрөмжийн аюулгүй байдлын асуудлыг шийдвэрлэх боломжтой эсэх:

6.3.1.a. Мэдээллийг устгахдаа дахин сэргэх боломжгүй байдлаар устгадаг эсэх;

6.3.1.b. Зөөврийн төхөөрөмжийн нууцлалыг хангасан эсэх, криптографын арга ашигладаг эсэх;

6.3.1.c. Зөөврийн төхөөрөмжийг үйлдвэрлэгчээс заасан горимд хадгалдаг эсэх;

6.3.2. Мэдээллийг устгахдаа дахин сэргэх боломжгүй байдлаар устгадаг эсэх;

6.3.3. Өгөгдөл алдагдахаас сэргийлэх зорилгоор нөөцлөлт зэрэгт ашигласан зөөврийн төхөөрөмжийн аюулгүй байдлыг хангасан эсэх;

6.3.4. Төхөөрөмжийг зөөвөрлөх үеийн аюулгүй ажиллагааны тухай заасан эсэх:

6.3.4.a. Найдвартай тээврийн хэрэгсэл эсхүл шуудангийн үйлчилгээний байгууллагаар үйлчлүүлдэг эсэх;

6.3.4.b. Шуудангийн үйлчилгээний байгууллагатай гэрээтэй ажилладаг эсэх.

7. Хандалтын хяналт (Хандалт удирдлагын бодлого)

7.1. Мэдээллийн хөрөнгийн ангилал, тоног төхөөрөмжийн ангилал зэрэг боломжит хувилбарт тулгуурласан хандалт хяналтын матрицтай эсэх;

7.2. Компьютер, тоног төхөөрөмж болон бусад нөөцөд нэвтрэлт хийж ханддаг эсэх;

7.3. Мэдээллийн систем болон бусад маш чухал, чухал ангиллын нөөцүүдэд хоёр алхамт баталгаажуулалт хийж, нэвтэрдэг эсэх;

7.4. Эрхийн хязгаарлалтыг боломжит хамгийн бага түвшинд байлгадаг эсэх;

7.5. Эрх олгох үйл ажиллагаа нь тодорхой эсэх:

7.5.1. Эрхийн хүсэлт гаргадаг байх;

7.5.2. Хүсэлтийг хянадаг байх;

7.5.3. Эрхийн зохицуулалтыг хийдэг байх;

7.5.4. Эрхийн хэрэгжилт, ашиглалтад тодорхой хугацааны давтамжтай хяналт, шалгалт хийдэг байх.

7.6. Зөөврийн төхөөрөмжид нэвтрэлтийн арга ашиглах, хандалтын эрхийг тодорхой заасан эсэх;

7.7. Систем, техник хангамж, дэд бүтцэд хандах эрхийн өөрчлөлтийг автоматаар хийх боломжтой эсэх;

7.8. Хэрэглэгчид зөвхөн өөрийн эрхийн хүрээнд төхөөрөмж, мэдээллийн систем, мэдээллийн хөрөнгө, дэд бүтцэд ханддаг эсэх;

7.9. Хэрэглэгчид төхөөрөмж, мэдээллийн систем, мэдээллийн хөрөнгө, дэд бүтцийг ашиглахдаа зөвхөн шаардлагатай хэсгүүдэд ханддаг эсэх;

7.10. Сүлжээний орчинд аюулгүй ажиллах эрхийн асуудал тусгагдсан эсэх:

7.10.1. Сүлжээний орчинд ажиллах ажилтнуудын хэрэглэх үйлчилгээг тодорхой заасан зохицуулалттай эсэх;

7.10.2. Зайнаас хандах хэрэглэгчид нууцлалтай хандалт (VPN зэрэг) ашигладаг эсэх;

7.10.3. Сүлжээнд холбогдохын өмнө баталгаажуулалт хийдэг эсэх;

7.10.4. Сүлжээний мониторингийн шийдэлтэй эсэх;

7.10.5. Хэрэглэгчийн эрх үүсгэх, хязгаарлах, устгах механизм тодорхой эсэх:

7.10.5.a. Эрхийн хүчинтэй хугацааг тодорхой заасан эсэх;

7.10.5.b. Эрх үүсгэхэд админ болон бусад удирдах түвшний эсхүл мэдээллийн технологийн ажилтан нууц үгийг таах боломжгүй хэлбэрээр үүсгэх, хэрэглэгчид эхний хандалтын дараа нууц үгээ сольдог эсэх.

7.11. Системийн түвшинд хэрэглэгчийн эрхийн түвшнийг зааж өгсөн эсэх:

7.11.1. Системийн хэрэглэгч болон функц ашиглалтын эрхийн түвшнийг заасан матрицтай эсэх, түүний дагуу эрхийн хязгаарлалтыг хийдэг эсэх;

7.11.2. Функцуудын хэрэглээг унших, бичих, устгах зэргээр ялгаатай зааж өгсөн эсэх;

7.11.3. Хэрэглэгчийн хэрэглээний лог бүртгэлийг хийдэг эсэх;

7.11.4. Бусад аппликейшн, программ хангамжуудын эрхийн түвшнийг матрицад зааж өгсөн эсэх.

7.12. Системд бүрэн нэвтрэх хүртэл системийн мэдээллийг харуулдаггүй эсэх;
7.13. Системд нэвтэрсэн хэрэглэгчийн эрхэд заасан мэдээллийг харуулдаг эсэх, хэрэглэгчийн хандсан мэдээлэл бүрийг бүртгэдэг эсэх;
7.14. Зөвшөөрөлгүй хандалт хийх үед нэвтрэх тусламжийн мэдээллийг харуулахгүйгээр зохицуулсан эсэх;
7.15. Нэвтрэлт, нууц үгэнд чиглэсэн халдлагаас хамгаалдаг эсэх;
7.16. Нууц үгийг сүлжээний орчинд шифрлэн дамжуулдаг эсэх;
7.17. Нууц үгийг гараас оруулах үед дэлгэцэд харагдах байдлыг нууцалдаг эсэх;
7.18. Идэвхтэй үйлдэл хийхгүй тодорхой хугацаа өнгөрсний дараа тухайн холболтыг автоматаар салгадаг эсэх;
7.19. Нэвтрэлтийн лог бүртгэлийн мэдээллийг тодорхой хугацаанд хадгалдаг эсэх.

8. Криптограф
8.1. Мэдээллийн нууцлалтай, бүрэн бүтэн байдлыг хангах зорилгоор криптографын аргачлал ашигладаг эсэх;
8.2. Криптографын мэдээлэлд дараах зүйлсийг тусгасан байгаа эсэх:
8.2.1. Түлхүүрийн нууцлалыг хангасан эсэх;
8.2.2. Ялгаатай системүүдэд ялгаатай түлхүүр ашигладаг эсэх;
8.2.3. Түлхүүрийг хадгалах, хэрэглэх эрхийн хязгаарлалтыг тодорхой заасан эсэх.

9. Физик аюулгүй байдал болон орчны аюулгүй байдлын асуудлууд
9.1. Физик аюулгүй байдлыг хангах хамрах хүрээг тодорхойлсон эсэх;
9.2. Гэмт хэрэг, зөрчлөөс урьдчилан сэргийлэх чиглэлийн үйл ажиллагааг тусгасан эсэх;
9.3. Галын аюулгүй байдлыг хангадаг эсэх;
9.4. Серверийн өрөө болон бусад дэд бүтэц эсхүл нууц буюу түүнээс дээш түвшний мэдээлэл хадгалж буй орчинд нэвтрэх үеийн физик аюулгүй байдлын тогтолцоотой эсэх;
9.5. Тэжээлийн эх үүсвэр, тэжээлээс үүдэлтэй эрсдэлийг бууруулах зохицуулалтыг хийсэн эсэх;

10. Үйл ажиллагааны аюулгүй байдлын асуудлууд
10.1. Тоног төхөөрөмж, дэд бүтцэд үйлдлийн систем суулгах журмууд;
10.2. Тоног төхөөрөмж, дэд бүтцийн үйлдлийн системийг шинэчлэхэд зориулсан нөөцлөлтийн бодлого, бүртгэлийн систем, тогтолцоо;
10.3. Тоног төхөөрөмж, дэд бүтцэд үйлчилгээ хийх, суурилуулах зэрэгт аюулгүй байдлыг хангах зохицуулалт;
10.4. Тоног төхөөрөмж, дэд бүтцэд, системийг сайжруулах болон хөгжүүлэлтийн тогтолцоо;
10.5. Ажлын цагийн хүрээнд үйлдлийн систем ажиллах эсвэл илүү цагаар ажиллах үеийн зохицуулалт;
10.6. Аливаа ажил гүйцэтгэх явцад үүссэн мэдээллийн аюулгүй байдалтай холбоотой асуудлыг шийдвэрлүүлэх аргачлал, ажлын дараалал;
10.7. Хяналтын программ;

10.7.1. Систем, программ хангамжийн бүх түвшний үйлдлийн түүхчилсэн бүртгэл /Event log/;

10.7.2. Цагийн синхрончлол.

10.8. Хортой программаас хамгаалах систем эсхүл программ хангамжтай эсэх;

10.9. Зөвшөөрөлтэй болон хориглосон программын жагсаалттай эсэх;

10.10. Цахим шуудангаар ирсэн холбоос, хавсралт материал, бусад шинэ материал хуулах, дамжуулах, хадгалах бүрд хортой кодыг шалгадаг эсэх.

11. Холбоо, сүлжээ, дэд бүтцийн аюулгүй байдлын асуудлууд

11.1. Утасгүй сүлжээний аюулгүй байдлыг хангадаг эсэх;

11.2. Сүлжээгээр дамжиж буй өгөгдлийн аюулгүй байдлыг хангадаг эсэх;

11.3. Байгууллагын сүлжээнд ажиллаж буй аливаа мэдээллийн систем, серверт бусад орчноос хандах үеийн аюулгүй байдлыг хангадаг эсэх;

11.4. Сүлжээг шаардлагатай дэд хэсгүүдэд хувааж, аюулгүй байдлын тохиргоо хийсэн эсэх.

12. Мэдээллийн систем нэвтрүүлэх үе шатууд, шалгалтууд (Мэдээллийн систем суурилуулах, хөгжүүлэх, үйлчилгээ хийх):

12.1. Өөрийн ашиглаж буй мэдээлэл, тоног төхөөрөмж, мэдээллийн системийн найдвартай, аюулгүй ажиллагааг хариуцах тогтолцоотой эсэх;

12.2. Программ хангамжийн шинэчлэлтийн бодлого, гарын авлагатай эсэх;

12.3. Программ хангамж нэвтрүүлэлтийн аргачлалтай эсэх;

12.4. Программ хангамжийн хэрэглээний сургалтын бодлого, журамтай эсэх;

12.5. Турших өгөгдлийн аюулгүй байдлыг хангах бодлоготой эсэх.

13. Гуравдагч этгээдийн хамтын ажиллагаа

13.1. Мэдээллийн ангилал, хандах этгээдийг тодорхойлсон удирдамж, бодлоготой эсэх;

13.2. Аюулгүй байдлыг хангах хэм хэмжээг заадаг эсэх;

13.3. Гуравдагч байгууллагуудтай харилцах хамтын ажиллагааны бичиг баримттай эсэх;

13.4. Байгууллагын мэдээллийн системд хандсан талаар бүртгэл хөтөлдөг эсэх.

14. Кибер халдлага, зөрчлийн удирдлага, зохицуулалт

14.1. Кибер халдлага, зөрчлийн удирдлагын журамтай эсэх, уг журамд дараах зүйлсийг тусгасан эсэх:

14.1.1. Кибер халдлага, зөрчлийн үед авах хариу арга хэмжээг төлөвлөх, бэлтгэдэг эсэх;

14.1.2. Мэдээллийн аюулгүй байдлын зөрчил, тохиолдлыг хянах, илрүүлэх, шинжилгээ хийх, тайлагнадаг эсэх;

14.1.3. Кибер халдлага, зөрчлийн үйлдлүүдийг бүртгэдэг эсэх;

14.1.4. Мэдээллийн аюулгүй байдлын тохиолдлыг үнэлэх, эмзэг сул байдлыг үнэлдэг эсэх;

14.1.5. Кибер халдлага, зөрчлийн дараа мэдээллийн системийг нөхөн сэргээх, холбогдох байгууллага эсхүл хэрэглэгчид даруй мэдэгдэх хариу арга хэмжээ авах ажиллагааг заасан эсэх;

14.1.6. Кибер халдлага, зөрчилд хариу өгөх асуудлыг тусгасан эсэх;

14.2. Кибер халдлага, зөрчилд өртсөн, өртсөн байж болзошгүй тохиолдолд кибер халдлага, зөрчилтэй тэмцэх холбогдох төвд даруй мэдэгддэг эсэх;

14.3. Мэдээллийн аюулгүй байдлын аудитын тайланг хүлээн авснаас хойш нэг сарын дотор кибер халдлага, зөрчилтэй тэмцэх холбогдох төвд хүргүүлдэг эсэх;

14.4. Кибер халдлага, зөрчлийн улмаас мэдээллийн систем, дэд бүтцийн хэвийн үйл ажиллагаа алдагдсан, тасралтгүй үйл ажиллагааг хангах боломжгүй болсон даруйд энэ талаар кибер халдлага, зөрчилтэй тэмцэх холбогдох төвд мэдэгддэг эсэх;

15. Бизнесийн тасралтгүй үйл ажиллагааны удирдлага

15.1. Мэдээллийн аюулгүй байдлын тасралтгүй үйл ажиллагааг төлөвлөх, шалгах, дүгнэх тогтолцоотой эсэх;

15.1.1. Байгууллагын нэгж, хэлтэс болон харилцагч талуудын оролцоо, хэм хэмжээг тодорхой тусгасан баримт бичигтэй эсэх;

15.1.2. Байгууллагын үйл ажиллагаанд учирч болох онцгой нөхцөл байдал үүсэхэд авч хэрэгжүүлэх арга хэмжээний төлөвлөгөөтэй эсэх;

15.1.3. Байгууллагын мэдээллийн системийн хүртээмжтэй байдлын шаардлагыг хангахуйц хангалттай нэмэлт нөөцтэй эсэх.

ТӨСӨЛ
Мэдээллийн аюулгүй байдлын аудит,
харилцаа холбоо, мэдээллийн технологийн
аудит хийх аргачлалын Хоёрдугаар хавсралт

ХАРИЛЦАА ХОЛБОО, МЭДЭЭЛЛИЙН ТЕХНОЛОГИЙН АУДИТ ХИЙХ АЖИЛЛАГААНД ШААРДАХ НОТЛОХ БАРИМТ

Нэгдүгээр бүлэг: Мэдээллийн технологийн удирдлагын тогтолцооны хяналт

А хэсэг: Мэдээллийн технологийн бодлого, зохицуулалт

1.1. Мэдээллийн технологийн стратегийн бодлого, удирдлага
  1.1.1. Мэдээллийн технологийн стратегийн бодлоготой эсэх;
  1.1.2. Мэдээллийн технологийн стратегийн бодлогыг хэрэгжүүлэх стандарт, фрэймворк ашигладаг эсэх.
1.2. Удирдлага, зохион байгуулалтын бүтэц
  1.2.1. Мэдээллийн технологийн бодлогыг хэрэгжүүлэх нэгжтэй эсэх;
  1.2.2. Захирлуудын зөвлөл, дээд удирдлагын үүрэг хариуцлагыг тодорхойлсон эсэх:
    1.2.2.1. Захирлуудын зөвлөл;
    1.2.2.2. Удирдлага;
    1.2.2.3. Мэдээллийн технологийн нэгж.
  1.2.3. Мэдээллийн технологи хариуцсан нэгжийн үүрэг хариуцлагын матриц, сэлгэн ажиллах төлөвлөгөөтэй эсэх;
  1.2.4. Мэдээллийн технологийн удирдлага, зохион байгуулалтын бүтэц ба гүйцэтгэлд аудит хийх баримт бичгүүдтэй эсэх.
1.3. Мэдээллийн технологийн холбогдох дүрэм, журмууд
  1.3.1. Мэдээллийн технологийн үйл ажиллагаанд холбогдох стандарт, баримт бичгүүдийг мөрддөг эсэх;
  1.3.2. Мэдээллийн технологи ашиглан үйл ажиллагааныхаа бүтээмжийг нэмэгдүүлэх бодлогыг хэрэгжүүлж, хэрэгжилтэд хяналт тавьдаг эсэх;
  1.3.3. Байгууллагын ажилтнууд болон бусад оролцогч талуудад зориулан боловсруулсан заавар, журамтай эсэх.
1.4. Мэдээллийн технологийн эрсдэлийн удирдлага
  1.4.1. Эрсдэлийн удирдлагын аргачлал, үе шатны дагуу мэдээллийн технологийн эрсдэлийн удирдлагыг хэрэгжүүлдэг эсэх;
    1.4.1.1. Мэдээллийн технологийн хөрөнгийн бүртгэлийг хөтөлдөг эсэх;
    1.4.1.2. Мэдээллийн технологийн хөрөнгөд учирч болзошгүй аюул болон эмзэг байдлын үнэлгээг хийдэг эсэх;
    1.4.1.3. Мэдээллийн технологийн болон бусад нөлөөллийн үнэлгээг хийдэг эсэх;
    1.4.1.4. Мэдээллийн технологийн эрсдэлийг урьдчилан илрүүлэх, тодорхойлох, тооцоолох, үнэлэх ажлыг хийдэг эсэх;
    1.4.1.5. Мэдээллийн технологийн эрсдэлийн хариу үйлдлийг боловсруулсан эсэх;

1.4.1.6. Мэдээллийн технологийн эрсдэлийг бууруулах болон урьдчилан сэргийлэх арга хэмжээ авах, эрсдэлийн хяналтыг найдвартай хэрэгжүүлдэг эсэх.

1.4.2. Эрсдэлийн үнэлгээний аргуудыг (чанарын үнэлгээний арга, тоон үнэлгээний арга) ашигладаг эсэх.

Б хэсэг: Мэдээллийн технологийн удирдлагын тогтолцоо

1.5. Мэдээллийн технологийн нөөцийн удирдлага

1.5.1. Мэдээллийн технологийн хөрөнгө оруулалтын бодлого, төслийн удирдлагын хэрэгжилтийн хяналтын тогтолцоотой эсэх (үнэлгээний хуудас ашигладаг эсэх);

1.5.2. Хүний нөөцийн удирдлага болон мэдээллийн технологийн хэрэглээний уялдаа холбоо хангагдсан эсэх;

1.5.3. Мэдээллийн аюулгүй байдлын удирдлагыг хэрэгжүүлдэг эсэх.

1.6. Мэдээллийн технологийн худалдан авалтын удирдлага

1.6.1. Аутсорсинг хийх бодлого, туршлага, чадавх, нөөцтэй эсэх;

1.6.2. Гуравдагч этгээдээс үйлчилгээ авах удирдлагын тогтолцоотой эсэх;

1.6.3. Гуравдагч этгээдээс авсан үйлчилгээнд хийгдэх/хийгдсэн өөрчлөлтийг удирдах тогтолцоотой эсэх;

1.6.4. Аутсорсинг ба гуравдагч этгээдийн аудитын тайлан.

1.7. Мэдээллийн технологийн гүйцэтгэлийн хяналт ба тайлан

1.7.1. Гүйцэтгэлийг оновчлох арга хэрэгслүүдийг ашигладаг эсэх.

1.8. Мэдээллийн технологийн чанарын удирдлага, чанарын баталгаа.

Хоёрдугаар бүлэг: Мэдээллийн технологийн дэд бүтцийн хяналт

А хэсэг: Мэдээллийн технологийн үйл ажиллагааны хяналт

2.1. Мэдээллийн технологийн нөөц нь байгууллагын одоогийн болон ирээдүйн шаардлагыг хангах боломжтой эсэх (мэдээллийн технологийн дэд бүтэц нь өөрчлөгдөж буй эрэлт хэрэгцээг хангахуйц уян хатан байж чадах эсэх);

2.2. Мэдээллийн системийн өдөр тутмын гүйцэтгэлийг хянадаг эсэх;

2.3. Мэдээллийн технологийн үйл ажиллагааны баримтжуулалт

2.3.1. Мэдээллийн технологийн системийн хэвийн бөгөөд аюулгүй ажиллагааг хангах дүрэм журамтай эсэх:

2.3.1.1. Цахим хэрэгслээр боловсруулсан өгөгдлийг удирдах дүрэм журамтай эсэх;

2.3.1.2. Гэнэтийн осол, техникийн саатал гарах үед авч хэрэгжүүлэх үйл ажиллагааны дүрэм журамтай эсэх;

2.3.1.3. Системийг дахин ачаалах, сэргээх процедурын дүрэм журамтай эсэх;

2.3.1.4. Бусад: өгөгдлийг нөөцлөх, серверийн өрөөний удирдлага, аюулгүй байдал зэрэг өдөр тутмын болон засвар үйлчилгээний үйл ажиллагааг баримтжуулсан эсэх.

2.4. Мэдээллийн зөөврийн хэрэгслүүд, тэдгээрийг хянадаг эсэх;

2.5. Хуваарийн дагуу багц боловсруулалтыг тогтоосон дарааллын дагуу гүйцэтгэж, мэдээллийн технологийн процессыг автоматжуулсан эсэх;

2.6. Халдлага, зөрчлийн удирдлагыг хэрэгжүүлдэг эсэх;

2.6.1. Зөвшөөрөлгүй үйл ажиллагааг хянадаг эсэх.

2.7. Хэвийн бус нөхцөл байдлыг илрүүлэх, түүний үндэслэл болон шалтгааныг илрүүлж, шийдвэрлэдэг асуудлын удирдлагыг хэрэгжүүлдэг эсэх;

2.8. Техник болон программ хангамжийн засвар үйлчилгээг тогтмол хийдэг эсэх;

2.8.1. Үйлчилгээний түвшний хэлцэл (SLA, Service level agreement), түүний хэрэгжилтийг хянадаг эсэх.

2.9. Сүлжээний удирдлага ба хяналт

2.9.1. Сүлжээ хэвийн, оновчтой ажиллаж байгаа эсэх;

2.9.2. Сүлжээн дэх өгөгдлийг хамгаалах, сүлжээг зөвшөөрөлгүй хандалтаас зохих ёсоор хамгаалсан эсэх;

2.9.3. Алсын зайн төхөөрөмжийг удирдах боломжтой эсэх;

2.9.4. Сүлжээний хүртээмж, гүйцэтгэлийг хянадаг эсэх;

2.9.5. Сүлжээний орчны аюулгүй байдлыг хангах хяналтыг бий болгосон эсэх.

Б хэсэг: Орчны хяналт

2.10. Мэдээллийн технологийн үйлчилгээнд зөвшөөрөлгүй нэвтрэхээс урьдчилан сэргийлэх хяналтыг хэрэгжүүлдэг эсэх:

2.10.1. Системд учирч буй аюул занал, системийн бүрэлдэхүүн хэсгүүдийн эмзэг байдал, тохиолдсон ослын нөлөөллийг тодорхойлох эрсдэлийн үнэлгээг тогтмол хийдэг эсэх;

2.10.2. CCTV, халдлагын дохиолол, товчлуурын хослол, хамгаалалтын харуул, цоожтой өрөө, биометрийн төхөөрөмж ашиглах зэрэг нийтлэг биет хандалтын хяналтыг хэрэгжүүлдэг эсэх;

2.10.3. Биет төхөөрөмжүүд нь гал түймэр, ус чийг, газар хөдлөлт зэрэг байгалийн давагдашгүй хүчин зүйлээс гадна цахилгаан тасрах, биет гэмтэл, хулгай зэрэг аюулаас бүрэн хамгаалагдсан эсэх.

В хэсэг: Хандалтын эрхийн хяналт

2.11. Хандалтын эрхийн хязгаарлалтыг боломжит хамгийн бага түвшинд байлгадаг эсэх:

2.11.1. Хэрэглэгчид зөвхөн тодорхойлсон эрхийн хүрээнд мэдээллийн технологийн дэд бүтэц, мэдээллийн систем, мэдээллийн хөрөнгө, төхөөрөмжид ханддаг эсэх;

2.11.2. Аюулгүй байдлын систем, байгууллагын эмзэг нөөцөд хандах хандалт нь эрх бүхий цөөн тооны ажилтнуудаар хязгаарлагддаг эсэх;

2.11.3. Ажилтнуудын ажил үүрэг, хариуцлагад үл нийцэх бусад чиг үүргийг гүйцэтгэхийг хязгаарласан эсэх;

2.11.4. Мэдээллийн нөөцийг эмзэг, чухал байдлаар ангилсан эсэх;

2.11.5. Эрх бүхий хэрэглэгчдийн жагсаалт, тэдгээрийн нэвтрэх эрхийг тодорхойлж, хяналт тавьдаг эсэх;

2.11.6. Хандалтыг хянах, аюулгүй байдлын илэрхий зөрчлийг шалгаж, зохих арга хэмжээг авдаг эсэх.

2.12. Ажилтнуудад зориулсан нууц үгийн аюулгүй байдлыг хангах дүрэм журамтай эсэх:

2.12.1. Хандалтын төвлөрсөн тогтолцоо эсхүл нэг нэвтрэх эрхээр олон системд нэвтрэх механизмыг хэрэгжүүлдэг эсэх.

2.13. Зайлшгүй шаардлагатай нөөц, файл, хэрэгслийг хамгаалдаг эсэх:

2.13.1. Өгөгдлийн файл – боловсруулалтын мэдээлэл хадгалсан файл эсхүл өгөгдлийн санг нөөцөлж авдаг эсэх;

2.13.2. Аппликэйшн – зөвшөөрөлгүй хандалтыг ихэсгэх, мэдээлэл алдах, залиланд өртөх эрсдэлийг нэмэгдүүлдэг хязгааргүй хандалттай программ байгаа эсэх;

2.13.3. Нууц үгийн файл - нууц үг хадгалагдсан файл, хэрэглэгчдийн системийн хандалтын эрхийн мэдээллийг найдвартай хамгаалдаг эсэх, хэрэглэгчдийн нэр ба нууц үгийг олж авсан этгээдэд хариуцлага тооцдог эсэх;

2.13.4. Системийн программ хангамж, хэрэгсэл – засварлагч, хөрвүүлэгч, программыг алхам алхмаар алдааг шалгагч зэрэг системийн өгөгдөл хадгалсан файлууд болон программ хангамжид нэмэлт, өөрчлөлт оруулахад ашиглаж болох хэрэгслүүдэд хандах хандалтыг хязгаарлах эсэх;

2.13.5. Үйлдлийн бүртгэлийн лог файл – системд хийгдсэн үйлдлийн бүртгэлийн лог файлыг хадгалдаг, хянадаг, зүй бус үйлдэлд хариуцлага тооцдог эсэх.

Г хэсэг: Өөрчлөлтийн удирдлага, хяналт

2.14. Өөрчлөлт хийх, тохируулах, хувилбар гаргах, алдаа засах зэрэгт өөрчлөлтийн удирдлагыг хэрэгжүүлдэг эсэх;

2.15. Өөрчлөлтийн удирдлага, хяналтын түвшин.

2.15.1. Техник хангамж буюу компьютер, дагалдах төхөөрөмж, сүлжээний тоног төхөөрөмж;

2.15.2. Программ хангамж, байгууллагын бизнесийн үйл ажиллагаанд ашигладаг бие даасан хэрэглээний систем болох үйлдлийн систем, бусад программ хангамжууд.

2.16. Системийн өөрчлөлтийн хяналтыг хэрэгжүүлдэг эсэх:

2.16.1. Үйл ажиллагааг сайжруулахын тулд мэдээллийн системд өөрчлөлт хийдэг эсэх;

2.16.2. Өгөгдлийн сан, сүлжээний шаардлагаас хамаарч системд өөрчлөлт оруулдаг эсэх;

2.16.3. Системийн хүчин чадлыг төлөвлөх, өргөтгөх зорилгоор өөрчлөлт байнга хийдэг эсэх;

2.16.4. Системд гарсан алдаа, доголдлыг тухай бүр засварладаг эсэх;

2.16.5. Системийн аюулгүй байдлыг сайжруулах шаардлагатай өөрчлөлтийг холбогдох өөрчлөлтийн хүсэлтийн дагуу системд хийдэг эсэх;

2.16.6. Тодорхой давтамжтайгаар тогтмол шинэчлэлтийг хийдэг эсэх;

2.16.7. Холбогдох хууль тогтоомж, бизнесийн үйл ажиллагаатай нийцүүлэн шаардлагын өөрчлөлтийг хийдэг эсэх;

2.16.8. Өөрчлөлтийн хүсэлтийг хэрэгжүүлэх, удирдлагын зөвшөөрөл олгох журамтай эсэх;

2.16.9. Өөрчлөлт оруулсан программ хангамжийг ашиглахаас өмнө бодит хугацааны горимд туршдаг эсэх;

2.16.10. Системд хийсэн дурын өөрчлөлтийн үр ашигтай байдлын тооцоог хийдэг эсэх;
2.16.11. Системд хийсэн өөрчлөлт, сайжруулалтын бүртгэлийг хөтөлдөг эсэх;
2.16.12. Системд алдаа гарсан тохиолдолд түүний үйл ажиллагааг сэргээх төлөвлөгөөтэй эсэх;
2.16.13. Системд яаралтай өөрчлөлт хийх журамтай эсэх;
2.16.14. Өөрчлөлтийг эрэмбэлж, хэрэгжүүлдэг эсэх.

Гуравдугаар бүлэг: Байгууллагын системийн хэрэглээний хяналт

3.1. Байгууллагад ашиглагдаж байгаа программ хангамжийн бие даасан боловсруулалтыг хянах системийн хэрэглээний хяналтыг хэрэгжүүлдэг эсэх;
3.2. Системийн хэрэглээний хяналтад шаардлагатай системийн үндсэн үйл ажиллагааны процессын зураглал, өгөгдлийн урсгалын диаграмм, үндсэн гаралтын тодорхойлолт, системд хадгалагдсан мэдээллийн файлуудын бүтцийн тодорхойлолт зэрэг мэдээлэл байдаг эсэх;
3.3. Оролт-боловсруулалт-гаралтын системийн хэрэглээний хяналтыг хэрэгжүүлдэг эсэх:
  3.3.1. Оролтын хяналтын хэрэгжүүлэлт
    3.3.1.1. Боловсруулахаар хүлээн авсан өгөгдөл нь бодитой, бүрэн бүтэн, өмнө нь боловсруулагдаагүй, үнэн зөв, зохих зөвшөөрөлтэй эсэх;
    3.3.1.2. Өгөгдлийг үнэн зөв, давхардалгүй оруулсан эсэх.
  3.3.2. Оролт болон үүссэн өгөгдлийн бүрэн бүтэн байдал, үнэн зөв боловсруулсан эсэхийг хянадаг боловсруулалтын хяналтыг хэрэгжүүлдэг эсэх:
    3.3.2.1. Нэг удаагийн боловсруулалтын өгөгдөл нь үнэн зөв эсэх;
    3.3.2.2. Нэг удаагийн боловсруулалтын өгөгдөл нь гүйцэд боловсруулагдсан эсэх;
    3.3.2.3. Нэг удаагийн боловсруулалтын өгөгдөл нь давтагдашгүй эсэх;
    3.3.2.4. Бүх боловсруулалтын өгөгдөл нь хүчинтэй эсэх;
    3.3.2.5. Компьютерын процесс нь аудит хийх боломжтой эсэх.
  3.3.3. Системийн гаралтыг бүрэн дууссан, үнэн зөв, алдаагүй хуваарилагдсан эсэхийг баталгаажуулдаг гаралтын хяналтыг хэрэгжүүлдэг эсэх:
    3.3.3.1. Гаралтыг цаг тухайд нь гаргаж, эрх бүхий хэрэглэгчдэд түгээдэг эсэх;
    3.3.3.2. Баримт бичгийн нууцлалаас хамаарч хяналт хийдэг эсэх;
    3.3.3.3. Алдаа болон төлөвлөгдөөгүй тохиолдлыг судалж, арга хэмжээ авдаг эсэх.

Дөрөвдүгээр бүлэг: Байгууллагын сүлжээ, мэдээллийн аюулгүй байдал, арга хэмжээний хяналт

А хэсэг: Байгууллагын сүлжээний байдлын хяналт

4.1. Сүлжээний хяналтыг хэрэгжүүлэлт
  4.1.1. Сүлжээний аюулгүй байдлын бодлоготой эсэх;

4.1.2. Сүлжээний логик болон физик зохион байгуулалтыг тодорхойлсон баримт бичигтэй эсэх;
4.1.3. Системд нэвтрэх нэр, нууц үг, хандалтын эрхийн матриц, эрх олгох, зөвшөөрөх асуудлыг баримтжуулж, хандалтын эрхийн хяналтыг хэрэгжүүлдэг эсэх;
4.1.4. Сүлжээ хариуцсан ажилтнуудын үйл ажиллагаанд хяналт тавьдаг эсэх;
4.1.5. Сүлжээний үйл ажиллагааг автоматаар бүртгэж, зөвшөөрөлгүй үйл ажиллагааг шалгадаг эсэх;
4.1.6. Сүлжээний ашиглалт, хүчин чадлыг хянахад сүлжээний удирдлага, хяналтын багц, төхөөрөмжийг ашигладаг эсэх;
4.1.7. Гадны зөвлөх, ханган нийлүүлэгчдэд сүлжээнд алсын зайнаас нэвтрэх боломжийг олгосон тохиолдолд тэдгээрийн хандалтад хяналт тавьдаг эсэх;
4.1.8. Тодорхой нөхцөлд сүлжээн дэх өгөгдлийг шифрлэдэг эсэх;
4.1.9. Сүлжээнд хувийн эсхүл тусгай зориулалтын шугамыг ашигладаг эсэх.

4.2. Сүлжээ ба төгсгөлийн төхөөрөмжийн аюулгүй байдлыг хянадаг эсэх.
4.3. Вебд суурилсан харилцаа холбооны технологиудын аюулгүй байдлыг хянадаг эсэх.

Б хэсэг: Мэдээллийн аюулгүй байдлын арга хэмжээний хяналт

4.4. Байгууллагын мэдээллийн хөрөнгийг нууцлах арга, аргачлалтай эсэх:
4.4.1. Нууцлалын суурь системтэй эсэх;
4.4.2. Хувийн болон нийтийн түлхүүрийн алгоритмыг хэрэгжүүлдэг эсэх;
4.4.3. Нийтийн түлхүүрийн дэд бүтцийг ашигладаг эсэх;
4.5. Мэдээллийн системийн аюулгүй байдлын хяналтыг хийдэг эсэх;
4.6. Мэдээллийн аюулгүй байдлын мэдлэг олгох сургалтын хөтөлбөртэй эсэх;
4.7. Мэдээллийн систем, дэд бүтцийн халдлагын төрөл ба техникийг тодорхойлсон эсэх:
4.7.1. Эрсдэл учруулах хүчин зүйлийг тодорхойлдог эсэх;
4.7.2. Кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, илрүүлэх, хариу арга хэмжээний аргачлалтай эсэх.
4.8. Аюулгүй байдлыг шалгах арга, хэрэгслийг ашигладаг эсэх:
4.8.1. Аюулгүй байдлын туршилт хийх хэрэгсэл, аргыг ашигладаг эсэх;
4.8.2. Сүлжээний нэвтрэлтийн туршилтыг хийдэг эсэх;
4.8.3. Халдлагын талаарх мэдээллийг ашигладаг эсэх.
4.9. Аюулгүй байдлын хяналтын техник, хэрэгсэл ашигладаг эсэх:
4.9.1. Халдлага илрүүлэх, эсэргүүцэх систем (IDS/IPS)-тэй эсэх.
4.10. Кибер халдлага, зөрчлийн хариу арга хэмжээний удирдлагын тогтолцоотой эсэх;
4.11. Нотлох баримттай ажиллах тогтолцоотой эсэх:
4.11.1. Дижитал тоног төхөөрөмжийн орчинд нотлох баримт цуглуулж, түүнийг хамгаалдаг эсэх.

Тав. Бизнесийн үйл ажиллагааны тасралтгүй байдал, гамшгаас сэргийлэх, сэргээх хяналт

5.1. Бизнесийн нөлөөллийн үнэлгээг хийдэг эсэх:
   5.1.1. Үйл ажиллагааны ангилал, хяналт шинжилгээг хийдэг эсэх.
5.2. Системийн уян хатан байдлыг тодорхойлдог эсэх.
   5.2.1. Программ хангамжийн уян хатан байдал, гамшгийн дараах нөхөн сэргээх арга, аргачлалтай эсэх;
   5.2.2. Харилцаа холбооны дэд бүтцийн уян хатан чанар, гамшгийн дараах нөхөн сэргээх арга, аргачлалтай эсэх.
5.3. Нөөцлөх, хадгалах ба дахин сэргээх бодлого, зохицуулалт, арга, аргачлалтай эсэх;
5.4. Бизнесийн хэвийн үйл ажиллагааны төлөвлөгөөтэй эсэх;
   5.4.1. Бизнесийн тасралтгүй ажиллагааны төлөвлөгөөнд мэдээллийн технологи, мэдээллийн системийн тасралтгүй ажиллагааны төлөвлөгөө, тестлэх төлөвлөгөө тусгагдсан эсэх;
   5.4.2. Гамшгийн үеийн нөхөн сэргээлтийн арга хэмжээг тодорхойлж, хэрэгжүүлдэг эсэх;
   5.4.3. Бизнесийн тасралтгүй ажиллагааны төлөвлөгөөний процесс, бодлого, төлөвлөгөөн дэх халдлага, зөрчлийн удирдлага, дүгнэлтийг гаргадаг эсэх.
5.5. Гамшгийн дараах нөхөн сэргээх төлөвлөгөөтэй эсэх:
   5.5.1. Халдлага, зөрчил тохиолдсон эсэхийг тодорхойлох, түүнийг нөхөн сэргээх төлөвлөгөө, стратегитай эсэх;
   5.5.2. Гамшгийн дараах нөхөн сэргээх төлөвлөгөө боловсруулах, шалгах аргатай эсэх.

ТӨСӨЛ
Маягт №1

Нууцын баталгааны хуудас (загвар)

Байгууллага: .....

Газар, хэлтэс, нэгж: .....

Аудиторын овог нэр: .....

Регистрийн дугаар: .....

Албан тушаал: .....

..... -д Мэдээллийн аюулгүй байдлын/Харилцаа холбоо, мэдээллийн технологийн аудитын үйлчилгээ үзүүлэх багийн ахлагч/гишүүн би Төрийн болон албаны нууцын тухай, Байгууллагын нууцын тухай, Хувь хүний нууцын тухай хууль болон бусад холбогдох хууль тогтоомжид үндэслэн дараах нөхцөлийг хүлээн зөвшөөрч энэхүү баталгааг гаргаж байна.

1. Би аудитын үйл ажиллагааны хүрээнд олж мэдсэн, танилцсан, хадгалж байсан, аудитын үйл ажиллагаандаа ашиглаж байсан, боловсруулсан төрийн болон албаны нууцад хамаарах Хүснэгт 1-д заасан зүйлсийг хэсэгчлэн болон бүхлээр нь цаашид задруулахгүй, нууцыг чанд хадгалж, хамгаалахаа баталж байна.

2. Би аудитын үйл ажиллагааны хүрээнд олж мэдсэн, танилцсан, хадгалж байсан, аудитын үйл ажиллагаандаа ашиглаж байсан, боловсруулсан байгууллагын нууцад хамаарах Хүснэгт 2-т заасан зүйлсийг хэсэгчлэн болон бүхлээр нь цаашид задруулахгүй, нууцыг чанд хадгалж, хамгаалахаа баталж байна.

3. Би аудитын үйл ажиллагааны хүрээнд олж мэдсэн, танилцсан, хадгалж байсан, аудитын үйл ажиллагаанд ашиглаж байсан, боловсруулсан хувь хүний нууцад хамаарах Хүснэгт 3-т заасан зүйлсийг хэсэгчлэн болон бүхлээр нь цаашид задруулахгүй, нууцыг чанд хадгалж, хамгаалахаа баталж байна.

4. Байгууллагын болон хувь хүний нууцыг задруулсан тохиолдолд Монгол Улсын холбогдох хууль болон Байгууллагын мэдээллийн аюулгүй байдлын журам, Байгууллагын дотоод журмын дагуу хариуцлага хүлээнэ гэдгээ бүрэн ухамсарлаж байна.

Байгууллагын нууцад хамаарах зүйлсийн жагсаалт болон нууц хадгалах хугацаа:

№	Файлын нэр	Аудиторын хүлээн авсан хэлбэр	Мэдээллийн төрөл	Нууц хадгалах хугацаа
1				
2				

Хүснэгт 1. Төрийн болон албаны нууцад хамаарах зүйлсийн жагсаалт

ТӨСӨЛ

№	Файлын нэр	Аудиторын хүлээн авсан хэлбэр	Мэдээллийн төрөл	Нууц хадгалах хугацаа
1				
2				

Хүснэгт 2. Байгууллагын нууцад хамаарах зүйлсийн жагсаалт

Хувь хүний нууцад хамаарах зүйлсийн жагсаалт болон нууц хадгалах хугацаа

№	Файлын нэр	Аудиторын хүлээн авсан хэлбэр	Мэдээллийн төрөл	Нууц хадгалах хугацаа
1				
2				

Хүснэгт 3. Хувь хүний нууцад хамаарах зүйлсийн жагсаалт

БАТАЛГАА ГАРГАСАН:

…… ……..

(Ажилтны нэр) (Гарын үсэг)

ТӨСӨЛ
Маягт №2

Аудиторын мэдээлэл (загвар)

Байгууллага: .....

Аудитын төрөл: Мэдээллийн аюулгүй байдлын аудит/Харилцаа холбоо, мэдээллийн технологийн аудит

Танай байгууллагад дээрх төрлийн аудитын үйлчилгээ үзүүлэх баг нь эрх бүхий дараах гишүүдээс бүрдэнэ.

№	Аудиторын овог, нэр	Эрхийн төрөл	Сертификатын мэдээлэл	Бусад
1				
2				

Хүснэгт 4. Аудиторын мэдээлэл

Мэдээллийн үнэн зөвд баталгаа гаргасан: .....

(Нэр, албан тушаал)