ТӨСӨЛ

КИБЕР АЮУЛГҮЙ БАЙДЛЫН ЭРСДЭЛИЙН ҮНЭЛГЭЭ ХИЙХ ЖУРАМ

Нэг. Нийтлэг үндэслэл

1.1.Кибер аюулгүй байдлын тухай хуулийн 8 дугаар зүйлд заасан кибер аюулгүй байдлын эрсдэлийн үнэлгээ хийх үйл ажиллагаа, түүний аргачлал, эрсдэлийн үнэлгээ хийх эрх бүхий этгээд /цаашид “хуулийн этгээд” гэх/-ийг бүртгэх, болон түүнтэй холбоотой бусад харилцааг энэхүү журмаар зохицуулна.

1.2.Кибер аюулгүй байдлын эрсдэлийн үнэлгээ гэж Кибер аюулгүй байдлын тухай хуулийн 4 дүгээр зүйлийн 4.1.9-д заасан үйл ажиллагааг ойлгоно.

1.3.Энэ журмын 1.2-т заасан хуулийн этгээд нь кибер аюулгүй байдлын эрсдэлийн үнэлгээ хийх үйл ажиллагаанд холбогдох хууль тогтоомж болон энэхүү журам, аргачлалыг мөрдлөг болгоно.

Хоёр. Эрсдэлийн үнэлгээ хийх үйл ажиллагаанд баримтлах зарчим

2.1. Эрсдэлийн үнэлгээ хийх үйл ажиллагаанд дараах зарчмыг баримтална.

2.1.1.хараат бус байх;

2.1.2.мэдээллийн нууцлалыг чанд сахих;

2.1.3.ашиг сонирхлын зөрчилгүй байх;

2.1.4.мэргэжлийн байр сууринаас хандах;

2.1.5.нотолгоонд үндэслэсэн байх;

2.1.6.үнэн зөв байх;

2.1.7.хуульд нийцсэн байх.

Гурав. Кибер аюулгүй байдлын эрсдэлийн үнэлгээ хийх хуулийн этгээдийг бүртгэх

3.1.Цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллага /цаашид “бүртгэх эрх бүхий байгууллага” гэх/ холбогдох хууль, энэ журамд заасан нөхцөл, шаардлагыг хангасан хуулийн этгээдийг Тагнуулын ерөнхий газрын саналыг харгалзан кибер аюулгүй байдлын эрсдэлийн үнэлгээ хийх хуулийн этгээдээр бүртгэнэ.

3.2.Эрсдэлийн үнэлгээ хийх хуулийн этгээд доор дурдсан шаардлагыг хангасан байна:

3.2.1.Монгол Улсад бүртгэлтэй хуулийн этгээд байх;

3.2.2.гурваас доошгүй орон тооны ажилтантай байх;

3.2.3.энэ зүйлийн 3.3-т заасан хүчин төгөлдөр гэрчилгээ бүхий орон тооны ажилтантай байх;

3.2.4.эрсдэлийн үнэлгээ хийх багийн гишүүдийн 50-иас доошгүй хувь нь мэдээллийн аюулгүй байдлын чиглэлээр 3-аас дээш жил ажилласан байх.

3.3. Олон улсын мэргэжлийн холбоо, стандартын байгууллага, эсхүл түүнтэй дүйцэхүйц байгууллагаас олгосон мэдээллийн аюулгүй байдлын гэрчилгээ нь удирдлагын түвшний болон ур чадварын гэрчилгээнээс бүрдэнэ:

3.3.1.удирдлагын түвшний гэрчилгээ гэж байгууллагын засаглал, бүтэц, үйл ажиллагааны эрсдэлийг удирдлагын түвшинд үнэлж, тооцоолох чадварыг нотолсон байхыг ойлгоно;

3.3.2.ур чадварын гэрчилгээ гэж удирдлагын түвшинд тооцоолж, тодорхойлсон эрсдэлийг техникийн түвшинд баталгаажуулж, шаардлагатай шалгалтуудыг хийх чадварыг нотолсон байхыг ойлгоно.

3.4.эрсдэлийн үнэлгээ хийх багийг тухайн чиглэлээр 5-аас доошгүй жил ажилласан, олон улсын мэргэжлийн холбоо, стандартын байгууллагаас олгосон мэдээллийн аюулгүй байдлын хүчин төгөлдөр гэрчилгээтэй орон тооны ажилтан ахална.

3.5.Кибер аюулгүй байдлын эрсдэлийн үнэлгээ хийх хуулийн этгээд нь бүртгэх эрх бүхий байгууллагад бүртгүүлэхдээ дараах баримт бичгийг бүрдүүлнэ:

3.5.1.үйлчилгээ эрхлэх хүсэлт (өргөдөл);

3.5.2.хуулийн этгээдийн улсын бүртгэлийн гэрчилгээний хуулбар;

3.5.3.энэ журмын 3.2-т заасан шаардлагыг хангаж буйг нотлох баримт бичиг, гэрчилгээний хуулбар;

3.5.4.ажилтны танилцуулга;

3.5.5.ажилтны нийгмийн даатгалын шимтгэл төлөлтийн лавлагаа.

3.6.Бүртгэх эрх бүхий байгууллага нь өргөдлийг хүлээн авснаас хойш ажлын 10 өдөрт багтаан шийдвэрлэнэ.

3.7.Бүртгэх эрх бүхий байгууллага энэ журмын 3.5-д дурдсан баримт бичгийн үнэн зөвийг магадлах үүднээс нэмэлт материал болон эх хувийг шаардаж болно.

3.8. Бүртгэх эрх бүхий байгууллага нь кибер аюулгүй байдлын тухай хуулийн 8.1-д заасан эрсдэлийн үнэлгээ хийх хуулийн этгээдийн жагсаалтыг энэ журмын 3.2-д заасан шаардлагад үндэслэн жилд 1 удаа тодотгоно.

3.9.Олон улсын мэргэжлийн холбоо, стандартын байгууллага, эсхүл түүнтэй дүйцэхүйц байгууллагаас олгосон мэдээллийн аюулгүй байдлын гэрчилгээний жагсаалтыг Цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллага болон боловсролын асуудал эрхэлсэн төрийн захиргааны төв байгууллага хамтарч батална.

3.10.Эрсдэлийн үнэлгээ хийх хуулийн этгээдийг бүртгэлээс доор дурдсан үндэслэлээр хасна:

3.10.1.хуулийн этгээд өөрөө хүсэлт гаргасан;

3.10.2.эрсдэлийн үнэлгээ хийх үйлчилгээ эрхлэхээр бүртгүүлэхдээ хуурамч баримт бичиг бүрдүүлсэн нь тогтоогдсон;

3.10.3.хуулийн этгээд татан буугдсан;

3.10.4.хууль тогтоомжоор хориглосон үйл ажиллагаа явуулсан;

3.10.5.эрсдэлийн үнэлгээний тайланг хуурамчаар үйлдсэн нь тогтоогдсон;

3.10.6.эрсдэлийн үнэлгээ хийх үйл ажиллагаанд баримтлах зарчмыг зөрчсөн нь нотлогдсон;

3.10.7.ажилтны энэхүү журмын 3.3-д заасан гэрчилгээний хүчинтэй байх хугацаа дууссан эсхүл ажилтны хөдөлмөрийн гэрээ дуусгавар болсон.

3.11.Хуулийн этгээд төрийн мэдээллийн нэгдсэн сүлжээнд холбогдсон болон онц чухал мэдээллийн дэд бүтэцтэй төрийн өмчит хуулийн этгээдэд эрсдэлийн үнэлгээ хийх зөвшөөрөл хүсэхдээ энэ журмын 3.5-д заасан баримт бичгийг бүрдүүлж Тагнуулын ерөнхий газарт хүргүүлнэ.

Дөрөв. Эрсдэлийн үнэлгээ хийх хуулийн этгээдийн эрх, үүрэг

4.1. Эрсдэлийн үнэлгээ хийх хуулийн этгээд дараах эрхтэй байна:

4.1.1.эрсдэлийн үнэлгээ хийх ажлын цар хүрээнээс хамаарч тухайн чиглэлийн мэргэшсэн мэргэжилтнийг гэрээгээр ажиллуулах;

4.1.2.захиалагч эрсдэлийн үнэлгээ хийхэд шаардагдах баримт бичиг, мэдээллээр хангаагүй, гэрээгээр хүлээсэн үүргээ биелүүлээгүй тохиолдолд үйлчилгээ үзүүлэхээс татгалзах.

4.2. Эрсдэлийн үнэлгээ хийх хуулийн этгээд дараах үүрэгтэй байна:

4.2.1.захиалагч байгууллагын гомдлыг хянан шийдвэрлэхэд шаардлагатай нотлох баримт болон үйл ажиллагааны тайланг хамгаалах;

4.2.2. захиалагч болон гуравдагч этгээдээс авсан баримт бичгийн нууцлал, бүрэн бүтэн байдлыг хангах;

4.2.3.гүйцэтгэсэн ажлын дүгнэлт, зөвлөмжийн үнэн зөв байдлыг бүрэн хариуцах;

4.2.4.эрсдэлийн үнэлгээ хийхдээ тухайн системийн тогтвортой, найдвартай ажиллагааг хангаж ажиллах;

4.2.5.энэ журмын 3.2.3-т заасан гэрчилгээ бүхий ажилтан ажлаас гарсан тохиолдолд бүртгэх эрх бүхий байгууллагад мэдэгдэх;

4.2.6.эрсдэлийн үнэлгээний явцад захиалагч байгууллага нь кибер аюулгүй байдлын эсрэг гэмт хэрэг, зөрчил гаргасан, гарах нөхцөл байдал үүсгэсэн бол зохих байгууллагад даруй мэдэгдэх;

4.2.7.онц чухал мэдээллийн дэд бүтэцтэй байгууллагын үйлдвэрлэлийн удирдлагын системийн үйл ажиллагааг тасалдуулах, доголдол үүсгэх үйлдэл хийхгүй байх;

4.2.8.жил бүрийн I дүгээр улиралд багтаан өмнөх жилд хийж гүйцэтгэсэн ажлын жагсаалт, түүнтэй холбогдох мэдээллийг бүртгэх эрх бүхий байгууллагад хүргүүлэх.

Тав.Гомдол, маргааныг шийдвэрлэх

ТӨСӨЛ

5.1.Захиалагч байгууллага эрсдэлийн үнэлгээ хийх хуулийн этгээдтэй холбоотой гомдлыг нотлох баримтын хамт бүртгэх эрх бүхий байгууллагад гаргаж болно.

5.2.Бүртгэх эрх бүхий байгууллага нь гомдлыг 30 хоногт багтаан шалгах ба гомдлыг хариуг бичгээр эсхүл амаар мэдэгдэж, тэмдэглэл хөтөлнө.

ТӨСӨЛ

КИБЕР АЮУЛГҮЙ БАЙДЛЫН ЭРСДЭЛИЙН ҮНЭЛГЭЭ ХИЙХ АРГАЧЛАЛ

Нэг.Нэр томьёоны тайлбар

1.1.Энэ аргачлалд ашигласан дараах нэр томьёог доор дурдсан утгаар ойлгоно.

1.1.1.“Эрсдэл” гэж аюул занал тохиолдох магадлал, түүнээс үүдэн гарах сөрөг нөлөөллийг;

1.1.2.“Хөрөнгө” гэж тоон болон чанарын үнэлгээгээр тодорхойлогдох байгууллагын үнэт зүйлийг;

1.1.3.“Аюул занал” гэж мэдээлэлд зөвшөөрөлгүй нэвтрэх, устгах, задруулах, өөрчлөх замаар байгууллагын үйл ажиллагаа, эд хөрөнгө, ажилтан, бусад байгууллагад сөргөөр нөлөөлөх үйл явдлыг;

1.1.4.“Эмзэг байдал” гэж байгууллагын хөрөнгөд үүсэж болох сул тал, цоорхойг;

1.1.5.“Магадлал” гэж байгууллагын эмзэг байдлыг ашиглан аюул заналын хохирол учруулж болох боломж болон тухайн аюул заналын тохиолдлын давтамжийг;

1.1.6.“Нөлөөлөл” гэж мэдээллийг зөвшөөрөлгүй задруулах, өөрчлөх, устгах, мэдээллийн системийн хүртээмжтэй байдлыг алдагдуулах зэрэг аюул заналаас үүсэж болох хохирлын хэмжээг;

1.1.7.“Кибер аюулгүй байдлын хяналт” гэж хөрөнгийг хамгаалах, аюул занал тохиолдохоос сэргийлэх, түүнийг илрүүлэх, хариу арга хэмжээ авах, хохирлын хэмжээг бууруулах, нөхөн сэргээх үйлдлийг гүйцэтгэх бүх төрлийн хяналтуудыг;

1.1.8.“Эрсдэлийг тэсвэрлэх чадвар” гэж байгууллагын дааж чадах эрсдэлийн хэмжээ.

Хоёр.Эрсдэлийн үнэлгээнд бэлтгэх, төлөвлөх

2.1.Эрсдэлийн үнэлгээнд бэлтгэхэд дараах зүйлсийг тодорхойлно:

2.1.1.эрсдэлийн үнэлгээний зорилго
2.1.2.эрсдэлийн үнэлгээний хамрах хүрээ
2.1.3.эрсдэлийг тэсвэрлэх чадвар
2.1.4.эрсдэлийн үнэлгээ хийх баг, тэдгээрийн үүрэг хариуцлага, оролцоо
2.1.5.ажлын эхлэх, дуусах хугацаа
2.1.6.эрсдэлийн үнэлгээ хийхэд ашиглах аргачлал,
2.1.7.эрсдэлийн үнэлгээний явцад мэдээллийн системд хандах эрхийн түвшин
2.1.8.нууцлалын баталгаа

2.2.Эрсдэлийг тэсвэрлэх чадварыг нөөц, эрсдэлийн түвшин болон учруулж болох хохирлын хэмжээ, хуулийн хүрээнд авч үзэж буй шаардлага зэргийг харгалзан үзэж тодорхойлно.

2.3.Эрсдэлийн үнэлгээнд дараах оролцогч талуудын үүрэг, хариуцлагыг тодорхойлно:

2.3.1.байгууллагын удирдлага
2.3.2.эрсдэлийн удирдлагын нэгж
2.3.3.технологи ба үйл ажиллагааны нэгж
2.3.4.кибер аюулгүй байдлын нэгж
2.3.5.байгууллагын дотоод нэгжүүд
2.3.6.харилцагч байгууллага болон гуравдагч этгээд

2.4.Энэхүү аргачлалд нийцсэн олон улсад дагаж мөрддөг эрсдэлийн үнэлгээний аргачлал (ISO/IEC 27005, NIST SP800-30, OCTAVE, CORAS, FAIR гэх мэт)-аас сонгож ашиглана.

Гурав.Эрсдэлийг тодорхойлох

3.1.Эрсдэлийн үнэлгээний хамрах хүрээнд хамаарах цахим мэдээлэлтэй холбоотой биет болон биет бус хөрөнгийн жагсаалтыг дараах байдлаар гаргана:

3.1.1.хөрөнгийн нэр
3.1.2.хөрөнгийн нууцлалын зэрэг
3.1.3.хөрөнгийн хариуцагч
3.1.4.хөрөнгийн байрлал
3.1.5.хөрөнгийн төрөл

3.2.Хөрөнгийн эмзэг байдлыг технологи, зохион байгуулалт, хүний нөөцийн түвшинд автомат болон механикаар тодорхойлно.

3.3.Аюул заналыг олон улсад хүлээн зөвшөөрөгдсөн аюул заналын загварчлалын арга (Threat modelling)-аас ашиглан тодорхойлж болно.

3.4.Байгууллагад хэрэгжиж буй кибер аюулгүй байдлын хяналтыг удирдлага, зохион байгуулалт, техник-технологи, биет байдлын бүлэгт ангилж үнэлнэ.

3.5.Байгууллагын хөрөнгийн нууцлагдсан, бүрэн бүтэн, хүртээмжтэй байдалд аюул занал учирснаар үүсэх бодит болон бодит бус хохирлын хэмжээгээр нөлөөллийг тодорхойлно.

3.6.Байгууллагын хөрөнгөд хамааралтай эмзэг байдлыг ашиглан учирч болох аюул заналын магадлалыг дараах зүйлсийг хамааруулан тодорхойлно:

3.6.1.байгууллагад хэрэгжиж буй кибер аюулгүй байдлын хяналт

3.6.2.техник хэрэгсэл дээр суурилсан баталгаажуулалт

3.6.3.эрсдэлийн үнэлгээ хийж буй этгээдийн үнэлэлт

3.6.4.өнгөрсөн хугацаанд байгууллага дээр тохиолдсон халдлагын давтамж

3.6.5.олон улсад хүлээн зөвшөөрөгдсөн мэргэжлийн байгууллагын аюул заналын тайлан

3.6.6.халдагч этгээдийн зорилго, ур чадвар, ашиглаж буй хэрэгсэл

3.7.Энэхүү аргачлалын 3.6-д тодорхойлж буй магадлалыг эрсдэлийн үнэлгээ хийж буй гишүүн бүр харилцан адилгүй тодорхойлж болно.

Дөрөв.Эрсдэлийг үнэлэх, шинжилгээ хийх

4.1.Энэхүү аргачлалын 2, 3 дугаар бүлэгт заасан үйл ажиллагаанаас гарсан үр дүнд үндэслэн эрсдэлийг нөлөөлөл болон магадлалын хэмжээгээр үнэлнэ.

4.2.Эрсдэлийг аюул занал эсвэл хөрөнгөд суурилсан байдлаар үнэлж болно.

4.3.Эрсдэлийн үнэлгээг тоон, чанарын болон хосолсон үнэлгээг ашиглан хийнэ:

4.3.1.хөрөнгөд учрах нөлөөлөл болон магадлалыг тоон байдлаар илэрхийлэх боломжтой тохиолдолд тоон үнэлгээг хийнэ.

4.3.2.хөрөнгөд учрах нөлөөлөл болон магадлалыг бодитоор илэрхийлэх боломжгүй тохиолдолд магадлал болон нөлөөллийн хүснэгтийн аргыг ашиглан чанарын үнэлгээг хийнэ.

Тав.Эрсдэлийг эрэмбэлэх, хариуцагчийг тодорхойлох

5.1.Энэхүү аргачлалын 4 дүгээр бүлэгт зааснаар тодорхойлсон үр дүнд үндэслэн эрсдэлийг түвшингээр эрэмбэлнэ.

5.2.Эрсдэлд хариу арга хэмжээ авах хариуцагчийг тодорхойлно.

5.3.Эрсдэлийг бууруулах зөвлөмжийг боловсруулна.

Зургаа.Тайлан боловсруулах болон үр дүнг танилцуулах

6.1.Эрсдэлийн үнэлгээний тайланг удирдлагын түвшинд зориулсан хураангуй болон техник багт зориулсан дэлгэрэнгүй тайлан гэсэн 2 төрлөөр гаргана.

6.2.Эрсдэлийн үнэлгээний тайланд дараах үндсэн шаардлага тавигдана:

6.2.1.ойлгомжтой, цэгцтэй байх;
6.2.2.товч бөгөөд шаардлагатай гол мэдээллүүдийг агуулсан байх;
6.2.3. эрсдэлийн үнэлгээний үр дүнг бүрэн тусгасан байх;
6.2.4. эрсдэлийг бууруулах зөвлөмжийг тусгасан байх;

6.2.5. тайланг боловсруулсан болон шинэчилсэн огноо, хүний нэр тусгагдсан байх;

6.2.6.тайланд оруулах шаардлагатай нэмэлт мэдээллүүдийг хавсралтаар оруулах;

6.2.7.тайлан эрсдэлийн үнэлгээ хийсэн хуулийн этгээд болон үйлчлүүлэгч талаар бүрэн хянагдан, зөвшөөрөгдсөн байх.

6.3.Хураангуй тайланд дараах зүйлсийг тусгана:

6.3.1.эрсдэлийн үнэлгээний хугацаа, хийгдсэн өөрчлөлтүүд;

6.3.2.эрсдэлийн үнэлгээний зорилго;

6.3.3.эрсдэлийн үнэлгээний хамрах цар хүрээ;

6.3.4.эрсдэлийн үнэлгээний ерөнхий үр дүнг график, хүснэгт, тоон мэдээллийн үзүүлэлтийг тусгасан байх;

6.3.5.эрсдэлийн үнэлгээний үр дүнд гарсан эрсдэл тус бүрийн жагсаалт;

6.3.6. өмнө хийгдсэн эрсдэлийн үнэлгээний зөвлөмжийг хэрэгжүүлсэн эсэх.

6.4.Дэлгэрэнгүй тайланд дараах зүйлсийг тусгана:

6.4.1.эрсдэлийн үнэлгээ хийх явц, үр дүнд нөлөөлөхүйц хүчин зүйл, нөхцөл байдал үүссэн эсэх;

6.4.2.эрсдэлийг тэсвэрлэх чадвар;

6.4.3.эрсдэлийн үнэлгээ хийх явцад авсан шаардлагатай шийдвэрүүдийг дурдах.