Төсөл

ОНЦГОЙ БАЙДЛЫН БАЙГУУЛЛАГЫН
КИБЕР АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ЖУРАМ

Нэг. Нийтлэг үндэслэл

1.1. Энэхүү журмын зорилго нь Онцгой байдлын ерөнхий газар, харьяа анги, салбар, нэгж /цаашид байгууллага гэх/-ийн мэдээллийн систем, мэдээллийн сүлжээ, кибер аюулгүй байдлыг хангах болон түүнтэй холбоотой бусад үйл ажиллагаанд дагаж мөрдөх харилцааг зохицуулахад оршино.

1.2. Байгууллагын кибер аюулгүй байдлыг хангах үйл ажиллагааг хууль тогтоомж, стандартыг мөрдүүлэх, программ болон техник хангамжийн арга хэмжээ авах, хяналт шалгалт зохион байгуулах, сургалт, харилцан туршлага солилцох болон бусад хэлбэрээр хэрэгжүүлнэ.

1.3. Байгууллагын кибер аюулгүй байдлыг хангах үйл ажиллагаанд Кибер аюулгүй байдлын тухай хууль, Төрийн болон албаны нууцын тухай хууль, Нийтийн мэдээллийн ил тод байдлын тухай хууль, Монгол Улсын Засгийн газар, Кибер аюулгүй байдлын үндэсний зөвлөл, Цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллагаас гаргасан холбогдох эрх зүйн баримт бичиг, Монгол Улсын олон улсын стандарт, энэхүү журмыг мөрдлөг болгоно.

1.4. Байгууллагын кибер аюулгүй байдлыг хангах үйл ажиллагаанд Монгол Улсын үндэсний аюулгүй байдлыг хангах, төр, хуулийн этгээд, хүний хувийн нууцыг хамгаалах, шинжлэх ухаан, техник, технологийн дэвшилтэд шийдлийг сонгох зарчмыг баримтална.

1.5. Энэхүү журмыг кибер орон зай, кибер орчныг байгуулах, ашиглах, аюулгүй байдлыг хангах үйл ажиллагаанд байгууллагын нийт албан тушаалтан мөрдөнө.

Хоёр. Кибер аюулгүй байдлыг хангах удирдлага, зохион байгуулалт

2.1.Онцгой байдлын ерөнхий газарт байгууллагын кибер аюулгүй байдлыг хангах үйл ажиллагааг нэгдсэн удирдлагаар хангах кибер аюулгүй байдлын орон тооны бус зөвлөл (цаашид Зөвлөл гэх) байгуулж, зөвлөлийн ажиллах журмыг батална.

2.2.Зөвлөл нь Кибер аюулуй байдлын үндэсний стратеги төлөвлөгөөтэй уялдуулан байгууллагын кибер аулгуй байдлын бодлого, стратеги төлөвлөгөө, дүрэм, журам хэлэлцэж, батлуулна.

2.3.Кибер аюулгүй байдлыг хангахад шаардагдах зардлыг байгууллагын жил бүрийн төсөв, төлөвлөгөөнд тусган хэрэгжүүлнэ.

2.4.Байгууллагын кибер аюулгүй байдлыг хангах өдөр тутмын удирдлага, зохион байгуулалтын арга хэмжээг Холбоо, мэдээллийн технологийн газрын Кибер аюулгүй байдлын нэгж хариуцна.

2.5. Байгууллагын мэдээллийн систем, мэдээллийн сүлжээний үйл ажиллагаанд хэрэгжүүлэх 24/7 хяналтыг Кибер аюулгүй байдлын ажиллагааны төв хариуцна.

Гурав. Кибер аюулгүй байдлыг хангах чиглэлээр албан тушаалтнуудын хүлээх үүрэг:

3.1. Кибер аюулгүй байдлыг хангах чиглэлээр Онцгой байдлын анги, байгууллагын захирагч дараах эрх, үүргийг хэрэгжүүлнэ:

3.1.1.Онцгой байдлын анги, салбарын хэмжээнд кибер аюулгүй байдлын тухай хууль, тогтоомжийн хэрэгжилтийг зохион байгуулж удирдах, хяналт тавих;

3.1.2. Кибер аюулгүй байдлын чиг үүргийг гүйцэтгэх мэргэжлийн албан тушаалтан эсхүл хавсран гүйцэтгэх ажилтныг томилох, сургах, бэлтгэх;

3.1.3. Кибер аюулгүй байдлыг хангах үйл ажиллагааг боловсронгуй болгоход шаардлагатай хөрөнгийг төсөвтөө тусгах, санхүүжүүлэх саналаа эрх бүхий албан тушаалтанд танилцуулж, шийдвэрлүүлэх**.**

3.2. Кибер аюулгүй байдлыг хангах чиглэлээр байгууллагын албан тушаалтан, алба хаагч, ажилтан дараах үүргийг хэрэгжүүлнэ**:**

3.2.1. Кибер аюулгүй байдлын тухай хууль, тогтоомжийг дагаж мөрдөх;

3.2.2. Илэрсэн халдлага, зөрчил, сэжигтэй тохиолдол бүрийг кибер аюулгүй байдал хариуцсан нэгж, албан тушаалтанд мэдэгдэх;

3.2.3. Байгууллагын мэдээлэл, мэдээллийн систем, мэдээллийн сүлжээг зөвхөн албан хэрэгцээнд хэрэглэх**;**

3.2.4. Байгууллагаас зохион байгуулж буй кибер аюулгүй байдлын мэдлэг
олгох сургалтад хамрагдах;

3.2.5. Кибер аюулгүй байдлыг хангах талаар өгсөн зөвлөмж, шаардлагыг биелүүлэх;

3.3. Онцгой байдлын байгууллагын кибер аюулгүй байдлыг хангах нэгж, албан тушаалтан дараах үүргийг хэрэгжүүлнэ:

3.3.1. Кибер аюулгүй байдлын хууль тогтоомжийн хэрэгжилтийг зохион байгуулах;

3.3.2. Кибер аюулгүй байдлын хяналт шалгалт зохион байгуулан, үр дүнг тооцож, удирдлагад танилцуулах;

3.3.3. Кибер аюулгүй байдлыг хангах өдөр тутмын үйл ажиллагааг хариуцан гүйцэтгэх;

3.3.4.Кибер аюулгүй байдлын хэлтэс, Кибер аюулгүй байдлын ажиллагааны арга хэмжээг хэрэгжүүлж, үр дүнг тооцон танилцуулах,

3.3.5. Кибер аюулгүй байдлыг хангахад шаардлагатай үйл ажиллагаа, нөөцийг төлөвлөх;

3.3.6. Кибер аюулгүй байдлыг хангах мэргэшүүлэх сургалтад хамрагдах;

3.3.7 Кибер аюулгүй байдлыг хангах талаар анги, салбарын захирагч, алба хаагчдад мэргэжил арга зүй зөвлөгөө, туслалцаа үзүүлэх, сурталчлан таниулах.

3.4. Кибер аюулгүй байдлын хэлтсийн хэрэгжүүлэх арга хэмжээ:

3.4.1.Засгийн газрын 2022 оны 493 дугаар тогтоолоор баталсан Кибер аюулгүй байдлыг Үндэсний стратеги төлөвлөгөөтэй уялдуулан байгууллагын кибер аюулгүй байдлын стратеги төлөвлөгөөг боловсруулах.

3.4.2. Байгууллагын хэмжээнд мөрдөгдөх дараах журам, заавар, төлөвлөгөөг боловсруулж, хэрэгжилтэд хяналт тавина.

- "Кибер аюулгүй байдлын ажиллагааны төв"-ийн ажиллах журам, заавар,

- Мэдээллийн нууцын зэрэглэлээс хамаарч, танилцах, ашиглах, дамжуулах, хадгалах, хяналт тавихтай холбоотой уйл ажиллагааг зохицуулсан тусгайлсан журам,

- Хөдөлгөөнт төхөөрөмжийн ашиглалт, аюулгүй байдлыг хангах журам,

- Кибер халдлага, зөрчлийн үед дагаж мөрдөх ажиллагааны төлөвлөгөө,

- Кибер халдлага, зөрчилд хариу арга хэмжээ авах төлөвлөгөө,

- Кибер халдлага, зөрчилд өртсөн мэдээллийн систем, мэдээллийн сүлжээг нөхөн сэргээх төлөвлөгөө.

3.4.3.Албанд ашиглаж байгаа мэдээллийн технологийн программ, техник хангамжийг шалган баталгаажуулах;

3.4.4. Мэдээллийн аюулгүй байдлын аудит, кибер аюулгүй байдлын эрсдэлийн үнэлгээг хуульд заасан хугацаанд эрх бүхий байгууллагаар хийлгэж, тайланг кибер халдлага, зөрчилтэй тэмцэх төвд хүргүүлэх;

3.4.5.Мэдээллийн систем, сүлжээнд өөрчлөлт орсон, шинээр нэвтрүүлсэн, эрсдэлтэй нөхцөл байдал үүссэн үед эмзэг байдлын болон эрсдэлийн үнэлгээ хийнэ.

3.4.6. Эрсдэлийн үнэлгээний үр дүнг үндэслэн эрсдэлийг бууруулахад чиглэсэн арга хэмжээг төлөвлөж хэрэгжүүлэх;

3.4.7 Кибер аюулгүй байдлыг хангахтай холбоотой өөрийн үйл ажиллагааны онцлог, цар хүрээг харгалзан журам, заавар болон холбогдох баримт бичгийг боловсруулах, программ, техник технологийн шийдлийг судалж, зөвлөлд тухай бур танилцуулах.

3.4.8. Кибер аюулгүй байдал хариуцсан нэгж (алба хаагч) нь кибер аюулгүй байдлыг хангах мэдлэг олгох дараах сургалтыг зохион байгуулна.

3.4.8.1. Нийт бие бүрэлдэхүүнд жил бүрийн 1 дүгээр улиралд;

3.4.8.2. Шинээр болон шилжин томилогдсон ажилтныг томилогдсоноос
хойш 14 хоногт багтаан;

3.4.8.3.Гэрээгээр хамтран ажиллаж байгаа гуравдагч талын ажилтныг тухай бур хамруулна.

3.4.9. Кибер орчинд хандаж, мэдээлэлтэй ажиллах ажилтан, албан хаагч,
бусад этгээдтэй мэдээллийн нууц хадгалах болон кибер аюулгүй байдлыг хангах талаар үүрэг, хариуцлагыг тусгасан гэрээ байгуулж, нууцын баталгаа гаргуулна.

Дөрөв. Мэдээлэл, түүнийг агуулж байгаа мэдээллийн систем, мэдээллийн сүлжээг тодорхойлох

4.1.Мэдээллийн системийн хувьд:

4.1.1.Зарлан мэдээллийн систем

4.1.2 Гамшгийн удирдлагын нэгдсэн систем;

4.1.3.Орон зайн мэдээллийн систем;

4.1.4.Дохиолол-хяналтын мэдээллийн систем;

4.1.5. Гадаад (интернэт) холболттой мэдээллийн систем.

4.2. Мэдээллийн сүлжээний хувьд:

4.2.1 Онцгой байдлын мэдээллийн сүлжээ;

4.2.2. Зарлан мэдээллийн мэдээллийн сүлжээ;

4.2.3.дохиолол-хяналтын мэдээллийн сүлжээ;

4.2.4. гадаад (интернэт) мэдээллийн сүлжээ.

4.3. Журмын 4.1, 4.2-т заасан мэдээллийн систем, мэдээллийн сүлжээний нууцын зэрэглэл, мэдээлэл хариуцагчийг байгууллагын нууц хариуцсан нэгжтэй хамтран тодорхойлж, жагсаалтыг батлуулна.

4.4. Нууцын зэрэглэлтэй мэдээллийн систем, сүлжээ хариуцагчдад Засгийн газраас тогтоосон журмын дагуу нууцын нэмэгдэл олгоно.

Тав. Кибер халдлага, зөрчлөөс хамгаалах арга хэмжээ

5.1.Мэдээллийн систем, мэдээллийн сүлжээнд зөвшөөрөлгүй хандах, дамжуулах, өөрчлөх, устгахаас хамгаалж хандалтын удирдлагыг тодорхойлно.

5.2. Мэдээллийн систем, мэдээллийн сүлжээнд давуу эрхтэй (admin, root) хандах этгээдийг тухай бүр нь тогтоож, хандах эрхийн ашиглалтад кибер аюулгүй байдлыг хангах нэгжээс хяналт хэрэгжүүлж ажиллах бөгөөд шаардлагатай өөрчлөлтийг оруулна.

5.3.Мэдээллийн систем, мэдээллийн сүлжээний тоног төхөөрөмж байрлаж байгаа зориулалтын өрөөнд зөвшөөрөлгүй нэвтрэхийг хориглох бөгөөд өрөө нь Засгийн газрын 2023 оны 224 дүгээр тогтоолын 4.4 дэх хэсгийн шаардлагыг хангахаас гадна:

5.3.1. гал унтраах болон хөргөлтийн системтэй байх;

5.3.2. цахилгаан соронзон долгионы нөлөөллөөс хамгаалагдсан байх;

5.3.3.цахилгааны эх үүсвэр болон нөөц эх үүсвэр, бусад хамгаалах тоног хэрэгслээр тоноглогдсон байна.

5.4. Мэдээллийн систем, мэдээллийн сүлжээний тоног төхөөрөмж байршуулах зориулалтын өрөөгүй бол энэ журмын 5.4-т заасан шаардлагад дүйцэх зориулалтын зогсуур (Rack)-т байршуулж болно.

5.5. Ажилтан, албан хаагч бүр өөрийн эзэмшлийн мэдээлэл тээгч техник хэрэгсэл (суурин болон зөөврийн компьютер, таблет болон бусад)-ийн аюулгүй байдлыг хангана.

5.6. Үүлэн технологид суурилсан үйлчилгээг Засгийн газрын 2023 оны 224 дүгээр тогтоолоор батлагдсан нийтлэг журмын зохицуулалтад нийцүүлж ашиглана.

5.7.Байгууллага мэдээллийн систем, мэдээллийн сүлжээнээс мэдээлэл алдагдахаас урьдчилан сэргийлэх талаар дараах арга хэмжээг авч хэрэгжүүлнэ:

5.7.1.Алдагдах эрсдэлтэй мэдээллийг нууцын алба болон холбогдох газар, хэлтэстэй хамтран тодорхойлох;

5.7.2. Мэдээлэл алдагдаж болзошгүй мэдээллийн систем, мэдээллийн сүлжээ, төхөөрөмж, зөөврийн хэрэгслүүдийг тогтмол хянах;

5.7.3. Мэдээлэлд зөвшөөрөлгүй хандаж, ашиглах, устгах, өөрчлөх боломжийг эрхийн зохицуулалт болон техникийн хувьд хаах;

5.7.4. Мэдээлэл боловсруулж байгаа мэдээллийн систем, мэдээллийн сүлжээг халдлага, зөрчил, саатлын үед сэлгэн ажиллах боломжтой байхаар зохион байгуулах.

5.8. Байгууллага өөрийн мэдээллийн системийн хөгжүүлэлтийг бусдаар гүйцэтгүүлэх тохиолдолд оюуны өмчийн эрхийг хамгаалах талаар арга хэмжээг авч

хэрэгжүүлэх бөгөөд зохиогчийн эрхийн зөрчилгүй программ хангамж, хөгжүүлэлтийн санг, худалдан авч, ашиглана.

5.9. Мэдээллийн систем, мэдээллийн сүлжээний, өгөгдөл, тохиргоог нөөцлөх хуваарь гаргаж, хуваарийн дагуу тогтмол нөөцөлнө. Нөөцийн бүрэн бүтэн байдлыг шалган баталгаажуулна.

5.10.Мэдээллийн систем, мэдээллийн сүлжээнд хандсан, мэдээлэл оруулсан, өөрчилсөн зэрэг үйлдэл бүрийг бүртгэх үйлдлийн бүртгэл, мэдээллийг тодорхойлохдоо нийтлэг журмын зохицуулалтад нийцүүлэн хөтөлнө.

5.11.Мэдээллийн систем, мэдээллийн сүлжээний үйлдлийн бүртгэлийг Кибер аюулгүй байдлын тухай хуулийн 19.1-д заасны дагуу 1 жил буюу түүнээс дээш хугацаагаар хадгална.

Зургаа. Кибер халдлага, зөрчлийг илрүүлэх арга хэмжээ

6.1. Онцгой байдлын ерөнхий газрын Холбоо, мэдээллийн технологийн газар нь кибер халдлага, зөрчлийг илрүүлэх дараах арга хэмжээг авч хэрэгжүүлнэ:

6.1.1.Мэдээллийн систем, мэдээллийн сүлжээ, аюулгүй байдлын
тоног төхөөрөмжийн үйлдлийн бүртгэлийг нэгтгэн цуглуулж, дүн шинжилгээ хийж, тайлан гаргах;

6.1.2. Мэдээллийн систем, мэдээллийн сүлжээний хэвийн бус үйл ажиллагаа, үйлдлийг ноцтой байдлаар нь эрэмбэлж, эрэмбийн дарааллаар эрх бүхий ажилтан, албан хаагч, этгээдэд мэдээлэх нөхцөлийг бүрдүүлэх;

6.1.3. Байгууллагын ажилтан, албан хаагч, нийлүүлэгч, хэрэглэгч талаас кибер халдлага, зөрчил үйлдсэн, эсхүл өртсөн байж болзошгүй тохиолдлыг ирүүлэх;

6.1.4.Кибер аюулгүй байдлыг хангах техник хэрэгслийн хэвийн тасралтгүй, ажиллагааг хангах,

6.1.5.Байгууллагын мэдээллийн систем, сүлжээ, техникийн эмзэг байдлыг бууруулах, технологид суурилсан эрсдэлийн менежментийн чадавхыг бэхжүүлж, хяналт шалгалтыг тогтмол хугацаанд зохион байгуулах.

6.1.6.Мэдээллийн систем, мэдээллийн сүлжээнд тогтмол хугацаанд шинээр программ хангамж, систем нэвтрүүлсэн тохиолдолд эмзэг байдлыг тодорхойлох төлөвлөгөөт болон төлөвлөгөөт бус шалгалт явуулна.

6.1.7.Кибер халдлага, зөрчлийг илрүүлэх ажиллагааг туршин шалгаж, тогтмол сайжруулалт хийнэ.

6.1.8. Мэдээллийн систем, мэдээллийн сүлжээнд тохирсон аюулгүй байдлыг хангах систем (IDS/IPS, antimalware, WAF, Email filter, SIEM гох мэт)-ийг нэвтрүүлж хэрэглэнэ.

6.1.2. Төв, орон нутгийн Онцгой байдлын байгууллагын салбар, нэгж кибер халдлага, зөрчлийг илрүүлэх дараах арга хэмжээг авч хэрэгжүүлнэ:

6.1.2.1.Кибер аюулгүй байдлыг хангах техник хэрэгслийн хэвийн тасралтгүй, ажиллагааг хангах;

6.1.2.2.Биет орчныг хянах;

6.1.2.3.Мэдээллийн систем систем, мэдээллийн сүлжээнд үйлчилгээ авах
тохиолдолд тухайн үйлчилгээ үзүүлэгчийн уйл ажиллагаанд хяналт тавих;

6.2. Мэдээллийн систем, мэдээллийн сүлжээнд тогтмол хугацаанд, шинээ программ хангамж, систем нэвтрүүлсэн тохиолдолд эмзэг байдлыг тодорхойлох.

6.3.Мэдээллийн систем, мэдээллийн сүлжээнд кибер халдлага, зөрчил илэрсэн үед баталсан төлөвлөгөөний дагуу ажиллана.

Долоо. Кибер халдлага, зөрчилд хариу арга хэмжээ авах

7.1. Кибер халдлага, зөрчилд хариу арга хэмжээг баталсан төлөвлөгөөний дагуу хэрэгжүүлэх бөгөөд төлөвлөгөөнд дараах агуулгыг тусгасан байна:

7.1.1.Байгууллага дотор кибер халдлага, зөрчлийг мэдэгдэх албан тушаалтан;

7.1.2. Тохиолдлыг шинжилж, кибер халдлага, зөрчилд тооцох шалгуур үзүүлэлт;

7.1.3. Халдлага, зөрчлийн талаарх мэдээллийг илгээх, хүлээн авах суваг;

7.2.Байгууллага жилд нэгээс доошгүй удаа кибер халдлага, зөрчилд хариу арга хэмжээ авах төлөвлөгөөний дагуу дадлага, туршилт хийж, төлөвлөгөөг тогтмол шинэчилж сайжруулна.

Найм. Мэдээллийн систем, мэдээллийн сүлжээг нөхөн сэргээх арга хэмжээ

8.1.Кибер халдлага, зөрчилд өтсөн мэдээллийн систем, мэдээллийн сүлжээг нөхөн сэргээхдээ баталсан төлөвлөгөөний дагуу ажиллана.

8.2.Кибер халдлага, зөрчлийн хор уршгийг арилгах, хэвийн үйл ажиллагааг нөхөн сэргээхэд Засгийн газрын 2023 оны 224 дүгээр тогтоолоор батлагдсан нийтлэг журамд заасан арга арга хэмжээг хэрэгжүүлнэ.

8.3. Байгууллага жилд нэгээс доошгүй удаа нөхөн сэргээх дадлага, туршилт хийж, төлөвлөгөөг тогтмол шинэчилж сайжруулна.

8.4. Кибер халдлага, зөрчил, нөхөн сэргээх уйл ажиллагаа, түүний явц, үр дүнгийн талаарх мэдээллийг зөвлөлд, шаардлагатай тохиолдолд систем, сүлжээнд
холбогдсон талуудад тухай бур мэдэгдэнэ.

Ес.Хариуцлага

9.1. Энэ журмыг зөрчсөн албан тушаалтны үйлдэл нь гэмт хэрэг, зөрчлийн шинжгүй бол "Монгол Улсын цэргийн нийтлэг дүрэм"-д заасан сахилгын шийтгэл ногдуулна.