



МОНГОЛ УЛСЫН
ХҮНИЙ ЭРХИЙН ҮНДЭСНИЙ КОМИССЫН
ДАРГЫН ТУШААЛ

2025 оны 11 сарын 20 өдөр

Дугаар А/53

Улаанбаатар хот

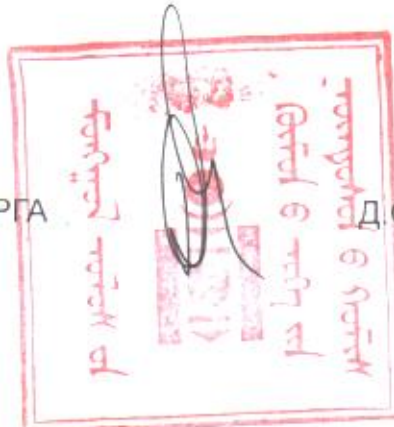
“Мэдээллийн аюулгүй байдлын бодлого”,
“Мэдээлэл технологийн үйл ажиллагааны журам”
батлах тухай

Монгол Улсын Хүний эрхийн Үндэсний Комиссын тухай хуулийн 19 дүгээр зүйлийн 19.1.6 дахь заалтыг үндэслэн ТУШААХ нь:

1. Хүний эрхийн Үндэсний Комиссын “Мэдээллийн аюулгүй байдлын бодлого”-ыг нэгдүгээр, “Мэдээлэл технологийн үйл ажиллагааны журам”-ыг хоёрдугаар хавсралтаар тус тус баталсугай.

2. “Мэдээллийн аюулгүй байдлын бодлого”, “Мэдээлэл технологийн үйл ажиллагааны журам”-ыг үйл ажиллагаандаа мөрдөж ажиллахыг Тамгын газрын нийт албан хаагчдад, хэрэгжилтийг хангуулах чиглэлээр зохион байгуулалтын арга хэмжээ авч, хяналт тавьж, тайлагнаж ажиллахыг Тамгын газар (Ц.Адъяахишиг)-т тус тус үүрэг болгосугай.

ДАРГА



Д.СҮНЖИД

1500100203

Монгол Улсын Хүний эрхийн Үндэсний
Комиссын даргын 2025 оны 11 дүгээр
сарын 20 ны өдрийн 4/53 дугаар тушаалын
нэгдүгээр хавсралт



МОНГОЛ УЛСЫН ХҮНИЙ ЭРХИЙН ҮНДЭСНИЙ КОМИССЫН МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН БОДЛОГО

Нэг. Нийтлэг үндэслэл

1.1. Комиссын мэдээллийн аюулгүй байдлын бодлогыг хэрэгжүүлэх, мэдээлэл солилцох тогтолцоог бүрдүүлэх, мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмжийг хангах, албан хэрэгцээний мэдээлэл, систем, тоног төхөөрөмжийн аюулгүй ашиглалтыг зохион байгуулах, мэдээлэл алдагдах, устгах эрсдэлээс урьдчилан сэргийлэх, эрсдэлийг бууруулахад энэхүү бодлогын зорилго оршино.

1.2. Монгол Улсын Хүний эрхийн Үндэсний Комисс (цаашид "Комисс" гэх)-ын мэдээллийн аюулгүй байдлыг хангахтай холбоотой бүхий л үйл ажиллагаанд Кибер аюулгүй байдлын тухай хууль, Хүний хувийн мэдээлэл хамгаалах тухай хууль, Нийтийн мэдээллийн ил тод байдлын тухай хууль, болон холбогдох бусад хууль тогтоомж, эрх зүйн актуудыг удирдлага болгоно.

1.3. Энэхүү бодлогын хэрэгжилтийг Комиссын Тамгын газрын албан хаагчид дагаж мөрдөх бөгөөд захиргааны асуудал хариуцсан нэгж хэрэгжилтийг хангуулах арга хэмжээг зохион байгуулж, өдөр тутмын хяналтыг нэгжийн дарга, ерөнхий хяналтыг Тамгын газрын дарга тавина.

1.4. Энэ бодлогод хэрэглэсэн нэр томъёог дор дурдсан утгаар ойлгоно.

1.4.1. "мэдээллийн хөрөнгө" гэж Комиссын үйл ажиллагаанд ашиглагдаж буй, хамгаалах шаардлагатай бүх төрлийн мэдээлэл, мэдээлэл хадгалах, боловсруулах төхөөрөмж, систем, программ хангамж, сүлжээ болон цаасан болон цахим мэдээллийн нөөцийг;

1.4.2. "мэдээллийн хөрөнгийн эзэмшигч" гэж мэдээлэл болон мэдээллийн хөрөнгийн хамгаалалт, хяналт, хандалтын зохицуулалтад хариуцлага хүлээх эрх бүхий этгээдийг тодорхойлсон байдлыг;

1.4.3. "нууцлалтай байдал" гэж Комиссын цуглуулсан мэдээлэл нь зөвхөн эрх бүхий албан хаагч хандах, ашиглах боломжтой байхаар зохион байгуулагдсан байдлыг;

1.4.4. "бүрэн бүтэн байдал" гэж мэдээллийг зөвхөн зөвшөөрөгдсөн этгээд өөрчлөх, засах, шинэчлэх боломжтой байх бөгөөд мэдээллийг санаатай болон санамсаргүйгээр устгах, өөрчлөхөөс хамгаалагдсан байдлыг;

1.4.5. "хүртээмжтэй байдал" гэж мэдээлэл, мэдээллийн систем, нөөц нь шаардлагатай үед хэн, хэрхэн хандах нь урьдчилан тодорхойлогдсон бөгөөд саадгүй, цаг алдалгүй ашиглах боломжтой байх байдлыг.

Хоёр. Мэдээллийн аюулгүй байдлыг хангах зорилт

2.1. Комиссын мэдээллийн аюулгүй байдлын бүх үйл ажиллагаа нь Монгол Улсын Кибер аюулгүй байдлын тухай хууль, Хүний хувийн мэдээлэл хамгаалах тухай болон холбогдох бусад хууль тогтоомж, эрх зүйн баримт бичигт бүрэн нийцсэн байна.

2.2. Комиссын Тамгын газрын албан хаагчид мэдээллийн аюулгүй байдалтай холбоотой аливаа шийдвэр, арга хэмжээг эрсдэлээс урьдчилан сэргийлэх бодлогод суурилан төлөвлөж, хэрэгжүүлнэ.

2.3. Байгууллагын бүтэц, мэдээллийн системийн цар хүрээ, нөөц бололцоонд нийцсэн мэдээллийн аюулгүй байдлын тогтолцоог бүрдүүлж, тогтмол хянаж, тасралтгүй сайжруулна.

2.4. Мэдээллийн аюулгүй байдлыг хангахад шаардлагатай мэдлэг, ур чадварыг хөгжүүлэх, соёл, хандлагыг төлөвшүүлэх зорилгоор ажилтан бүрийг хамарсан тогтмол сургалт, мэдээлэл түгээх үйл ажиллагааг хэрэгжүүлнэ.

2.5. Мэдээллийн аюулгүй байдлын хяналт, хэрэгжилт нь хэмжигдэхүйц шалгуур үзүүлэлттэй байх бөгөөд бодит мэдээлэл, нотолгоонд үндэслэсэн байна.

2.6. Мэдээлэл солилцох, дамжуулах, боловсруулах, хандах үйл явцыг бүртгэн, хяналттай, мөшгөгдөх боломжтой байдлаар зохион байгуулж, баримтжуулна.

2.7. Гуравдагч этгээдтэй хамтран ажиллах, мэдээлэл солилцох үед мэдээллийн аюулгүй байдлын шаардлагыг гэрээний нөхцөлд тусгаж, түүний хэрэгжилтэд зохих хяналт тавих үйл ажиллагааг хэрэгжүүлж ажиллана.

2.8. Мэдээлэлтэй харьцаж буй Комиссын Тамгын газрын албан хаагч, оролцогч талуудын мэдээллийн аюулгүй байдлын талаарх ёс зүй, хариуцлагын ойлголтыг нэмэгдүүлж, байгууллагын соёл, үнэт зүйлсэд нийцсэн хандлагыг төлөвшүүлэх бодлогыг дэмжин хэрэгжүүлнэ.

Гурав. Мэдээллийн хөрөнгийн зөвшөөрөгдөх хэрэглээ

3.1. Комиссын үйл ажиллагаанд ашиглагдаж буй мэдээллийн бүх төрлийн хөрөнгийг дараах нөхцөлийн хүрээнд ашиглахыг зөвшөөрнө:

3.1.1.мэдээллийн хөрөнгө, төхөөрөмж, систем, программ хангамжийг зөвхөн албан үүргээ хэрэгжүүлэх зорилгоор ашиглана.

3.1.2.мэдээллийн хөрөнгийн эзэмшигч нь тухайн хөрөнгийн нууцлал, бүрэн бүтэн байдал, хүртээмжийг хангаж, хамгаалалтын зохих хяналтыг хэрэгжүүлэх үүрэг хүлээнэ.

3.1.3.мэдээллийн хөрөнгө болон мэдээлэл агуулсан төхөөрөмжийг байгууллагаас гадагш авч гарах, дамжуулах шаардлагатай бол шууд удирдлагын зөвшөөрөл авна.

3.1.4.мэдээллийн хөрөнгийг зохисгүй ашиглах, вирус, хортой код, программын халдлага болон бусад цахим эрсдэлд өртөхөөс урьдчилан сэргийлэх арга хэмжээг хэрэгжүүлнэ.

3.1.5.албан хаагч хандах эрхийг хувийн зорилгоор ашиглаж, уг эрхээр хийгдсэн аливаа үйлдэлд бүрэн хариуцлага хүлээнэ.

3.1.6.мэдээллийн аюулгүй байдлын бодлогын дагуу зарим цахим хуудас, платформ, дотоод, гадаад сувгууд руу хандах эрхийг хязгаарлаж болно.

3.1.7.гарал үүсэл нь тодорхойгүй, итгэлгүй эх сурвалжаас мэдээлэл авсан тохиолдолд уг мэдээллийг албан үүргийн хэрэгцээнд ашиглахаас өмнө эх сурвалжийг шалгаж, баталгаажуулна.

3.1.8.интернэт болон дотоод сүлжээг албан бус, хувийн зорилгоор ашигласнаас үүдэлтэй аливаа сөрөг үр дагаврыг тухайн ажилтан бүрэн хариуцна.

3.1.9.спам, сэжигтэй холбоос, ёс зүйгүй агуулгатай цахим шуудан, мэдээлэл хүлээн авсан тохиолдолд мэдээллийн технологи хариуцсан албан хаагчид нэн даруй мэдэгдэнэ.

3.2. Дараах үйл ажиллагааг үл зөвшөөрөгдөх хэрэглээнд тооцож хориглоно.

3.2.1.мэдээллийн хөрөнгө, мэдээлэл агуулсан төхөөрөмжийг албан хэрэгцээнээс бусад зориулалтаар ашиглах;

3.2.2.албан хаагч өөрийн хандах эрхийг шууд болон шууд бусаар бусдад дамжуулах, ашиглуулах, бусдын эрхийг ашиглах;

3.2.3.зохиогчийн эрх, оюуны өмчийн эрхээр хамгаалагдаагүй, зөвшөөрөгдөөгүй программ хангамжийг ашиглах;

3.2.4.ажлын бус зорилгоор интернэтээс мэдээлэл татах, зөвшөөрөгдөөгүй программ хангамж суулгах, ашиглах;

3.2.5.гадны этгээдийг байгууллагын дотоод сүлжээнд нэвтрүүлэх, холбох.

Дөрөв. Мэдээллийн ангилал

4.1. Комиссын үйл ажиллагаанд ашиглагдаж буй бүх мэдээллийн хөрөнгийг тэдгээрийн эмзэг байдал, үнэ цэнэ, хууль, гэрээний шаардлага, байгууллагын нэр хүнд,

аюулгүй байдлын эрсдэлд үзүүлэх нөлөөллийг харгалзан дараах түвшинд ангилж, дараах хамгаалалтын хяналтуудыг хэрэгжүүлнэ:

- 4.1.1.мэдээллийн хөрөнгийг бүртгэх явцад тухайн хөрөнгийн ангиллын түвшнийг тодорхойлон бүртгэлд тусгана;
- 4.1.2.мэдээллийн ангиллыг мэдээллийн хөрөнгийн эзэмшигч хариуцан тодорхойлно;
- 4.2. Мэдээллийн ангиллыг өөрчлөх тохиолдолд зөвхөн ангиллын түвшнийг бууруулах зарчмыг баримтална;
- 4.2.1.Комиссын бүх төрлийн мэдээллийн хөрөнгийг дараах гурван түвшинд ангилна;
- 4.2.1.1.хаалттай: эмзэг, өндөр хамгаалалт шаардсан мэдээлэл;
- 4.2.1.2.дотоод: байгууллагын дотоод хэрэгцээнд зориулагдсан, дунд зэргийн хамгаалалт шаардсан мэдээлэл;
- 4.2.1.3.нээлттэй: олон нийтэд ил тод байж болох, хамгаалалт бага шаардсан мэдээлэл.
- 4.3. Мэдээллийн хөрөнгийн эзэмшигч нь мэдээллийн ангиллын түвшин бүрд тохирсон хяналтуудыг хэрэгжүүлэх бөгөөд жилд нэг удаа, шаардлагатай бол тухай бүр хөрөнгийн ангиллыг нягтлан шалгаж учирч болох эрсдэл, хууль эрх зүйн гэрээгээр хүлээсэн үүрэг, үнэ цэнэ, ач холбогдлын дагуу ангиллыг өөрчилж болно.
- 4.4. Мэдээллийн ангиллын түвшин бүрд хамаарах шалгуурыг дараах байдлаар тогтооно.
- 4.4.1.тухайн мэдээллийн үнэ цэнэ: мэдээллийн хөрөнгийн эрсдэлийн үнэлгээгээр тогтоосон албаны үйл ажиллагаанд нөлөөлөх нөлөөлөл;
- 4.4.2.мэдээллийн эмзэг чухал байдал: мэдээллийн хөрөнгийн эрсдэлийн үнэлгээгээр эрсдэлийн түвшин тогтоогдсон байдал;
- 4.4.3.хууль болон гэрээний шаардлага: сонирхогч талуудын шаардлага.
- 4.5. Мэдээллийн ангиллын түвшин бүрийн эрсдэлийг дараах байдлаар авч үзнэ:
- 4.5.1.хаалттай: Өндөр эрсдэлтэй буюу мэдээллийн аюулгүй байдал алдагдсанаар байгууллага, албан хаагч болон харилцагч байгууллагын нэр хүнд, үйл ажиллагаанд шууд болон шууд бусаар ноцтой хор хохирол учруулах, хууль зүйн хортой үр дагавар үүсэх боломжтой;
- 4.5.2.дотоод: Дунд эрсдэлтэй буюу мэдээллийн аюулгүй байдал алдагдсанаар байгууллага, албан хаагчийн нэр хүнд, үйл ажиллагаанд шууд болон шууд бусаар мэдэгдэхүйц хор хохирол учруулах, хууль зүйн сөрөг үр дагавар үүсгэх боломжтой;
- 4.5.3.нээлттэй: Бага эрсдэлтэй буюу байгууллага, албан хаагч болон харилцагч байгууллагад ямар нэг ноцтой эрсдэл үүсгэхгүй;
- 4.5.4.мэдээллийн хөрөнгүүд хандах эрхгүй эсвэл зөвшөөрөгдөөгүй этгээдэд нээлттэй болсон аливаа асуудлыг шууд удирдлагад мэдээлнэ.

Тав. Нууц үгийн хэрэглээ

- 5.1.Комиссын Тамгын газрын албан хаагчид мэдээлэл агуулсан төхөөрөмж, системд нэвтрэхдээ дараах нууц үгийн шаардлага хангасан байна:
- 5.1.1. таахад хялбар нууц үгийг ашиглахгүй байх; /жишээ нь нэвтрэх нэр, өөрийн овог нэр, утас, хувийн мэдээлэл агуулсан гэх мэт/
- 5.1.2. наймаас доошгүй тэмдэгтэй тоо, том, жижиг, үсэг, тусгай тэмдэгт заавал орсон байх;
- хуанлийн 180 хоног тутамд нууц үгийг шинэчилдэг байх;
- 5.1.3. нууц үг задарсан, бусдад дамжуулагдсан, нууцлал алдагдсан сэжиг илэрсэн эсвэл зайлшгүй шаардлагаар бусдад хуваалцсан бол нэн даруй зөрчлөөр бүртгүүлж холбогдох албан хаагчид мэдэгдэх;
- 5.1.4. албан хаагч өөрийн хандах эрхийн хүрээнд нууц үгээ сонгох, шинээр зохиох боломжтой байх;
- 5.1.5. албан хаагчид нууц үгээ ямар ч хэлбэрээр бичиж тэмдэглэн хадгалахгүй, бусдад хуваалцахгүй байж бүрэн аюулгүй байдлыг бүрэн хариуцах;
- 5.1.6. эмзэг системд нэвтрэх, админ эрх бүхий хэрэглэгчид хоёр болон түүнээс дээш хүчин баталгаажуулалт (нууц үг + нэг удаагийн код, биометрийн баталгаажуулалт, төхөөрөмж баталгаажуулалт гэх мэт)-ыг ашиглах.

Зургаа. Мэдээлэл дамжуулах

6.1. Комисс нь дотоод болон гадаад орчны оролцогч талуудтай мэдээлэл солилцох, дамжуулах үйл ажиллагааг мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмжийг хангах зарчмын хүрээнд мэдээлэл солилцох үйл ажиллагаанд дараах сувгуудыг ашиглана:

- 6.1.1. Комиссын дотоод цахим шуудангийн систем;
- 6.1.2. албан ёсны лицензтэй программ хангамж (Оффис 365 гэх мэт);
- 6.1.3. дотоод файлын сан, хуваалцах сүлжээ;
- 6.1.4. албаны утас;
- 6.1.5. харилцагч байгууллага хооронд ашиглаж байгаа харилцааны систем
- 6.1.6. Комиссын зөвшөөрсөн зөөврийн төхөөрөмж (флэш диск, хатуу диск, CD/DVD гэх мэт).

6.2. Байгууллагын нэгжийн удирдлагууд эрсдэлийн үнэлгээний үр дүн, үүссэн нөхцөл байдалд дүгнэлт хийж мэдээлэл солилцох суваг бүрд нэмэлт хяналт тогтоож болно.

6.3. Албан хаагч хаалттай мэдээллийг бусдад дамжуулах бол харьяалах нэгжийн удирдах албан тушаалтны зөвшөөрлөөр гүйцэтгэнэ.

6.4. Зөвшөөрөгдсөн сувгаар дамжуулах боломжгүй бусад суваг ашиглах шаардлагатай бол нэгжийн даргын зөвшөөрлөөр дамжуулна. Зөвшөөрлийг зөвшөөрөгдсөн сувгаар илгээж баталгаажуулсан байх шаардлагатай.

6.5. Гуравдагч талуудтай мэдээлэл солилцохдоо дараах дүрмийг баримтална:

6.5.1. харилцагч байгууллагатай мэдээлэл солилцохдоо холбогдох гэрээ, албан бичигт дурдсан хүрээнд мэдээлэл дамжуулна;

6.5.2. гэрээт байгууллагатай мэдээлэл солилцох тохиолдолд тухайн байгууллагатай байгуулсан гэрээнд үндэслэнэ.

Долоо. Бусад

7.1. Энэхүү бодлогыг зөрчсөн албан хаагчийн үйлдэл нь зөрчил, гэмт хэргийн шинжгүй бол Хөдөлмөрийн дотоод журмын дагуу хариуцлага хүлээлгэнэ.

7.2. Комиссын мэдээллийн технологийн аюулгүй байдлын хяналтыг Комиссын мэдээллийн технологийн үйл ажиллагааны журмаар зохицуулна.