ЭМ, ЭМНЭЛГИЙН ХЭРЭГСЛИЙН ХЯНАЛТ,
ЗОХИЦУУЛАЛТЫН ГАЗРЫН ДАРГЫН
ТУШААЛ

2026 оны 08 сарын 28 өдөр Дугаар А/154 Улаанбаатар хот

Журам батлах тухай

Засгийн газрын агентлагийн эрх зүйн байдлын тухай хуулийн 8 дугаар зүйлийн 8.4 дэх хэсэг, Кибер аюулгүй байдлын тухай хуулийн 19 дүгээр зүйлийн 19.1.5 дахь заалт, 19.2 дахь хэсэг, Төрийн болон албаны нууцын тухай хуулийн 11 дүгээр зүйлийн 11.1.1 дэх заалт, Засгийн газрын 2022 оны 207 дугаар тогтоолын хавсралтаар батлагдсан "Онц чухал мэдээллийн дэд бүтэцтэй байгууллагын жагсаалт", Засгийн газрын 2023 оны 224 дүгээр тогтоолын хавсралтаар батлагдсан "Кибер аюулгүй байдлыг хангах нийтлэг журам"-ыг тус тус үндэслэн ТУШААХ НЬ:

1.Эм, эмнэлгийн хэрэгслийн хяналт, зохицуулалтын газрын "Кибер аюулгүй байдлыг хангах дотоод журам"-ыг нэгдүгээр хавсралтаар, "Сүлжээний болон хяналтын камерын өрөөнд нэвтрэх хүсэлтийн маягт"-ыг хоёрдугаар хавсралтаар, "Сүлжээний болон хяналтын камерын өрөөнд нэвтэрсэн бүртгэлийн журнал"-ыг гуравдугаар хавсралтаар, "Систем/программд хандах эрхийн хүсэлтийн маягт"-ыг дөрөвдүгээр хавсралтаар тус тус баталсугай.

2.Журмын хэрэгжилтийг хангаж ажиллахыг Эм, эмнэлгийн хэрэгслийн хяналт, зохицуулалтын газрын нийт албан хаагчдад үүрэг болгосугай.

3.Тушаалын хэрэгжилтэд хяналт тавьж ажиллахыг Захиргаа, удирдлагын газар (Т.Хонгорзул)-т даалгасугай.

4.Энэ тушаал батлагдсантай холбогдуулан газрын даргын 2024 оны 09 дүгээр сарын 06-ны өдрийн А/176 дугаар тушаалыг хүчингүй болсонд тооцсугай.

ДАРГЫН АЛБАН ҮҮРГИЙГ
ТҮР ОРЛОН ГҮЙЦЭТГЭГЧ П.АЛТАНЦЭЦЭГ

1526 010154

Эм, эмнэлгийн хэрэгслийн хяналт, зохицуулалтын
газрын 2026 оны 06 дугаар сарын 18-ны өдрийн
А/191 дугаар тушаалын нэгдүгээр хавсралт

ЭМ, ЭМНЭЛГИЙН ХЭРЭГСЛИЙН ХЯНАЛТ, ЗОХИЦУУЛАЛТЫН ГАЗРЫН КИБЕР АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ДОТООД ЖУРАМ

Нэг. Нийтлэг үндэслэл

1.1. Энэхүү журмын зорилго нь Эм, эмнэлгийн хэрэгслийн хяналт, зохицуулалтын газрын (цаашид "Агентлаг" гэх) мэдээллийн систем, мэдээллийн сүлжээ, мэдээллийн сан болон мэдээллийн дэд бүтцийн нууцлал, бүрэн бүтэн байдал, хүртээмж, хэвийн, найдвартай, тасралтгүй ажиллагааг хангах, кибер халдлага, кибер аюулгүй байдлын зөрчлөөс урьдчилан сэргийлэх, илрүүлэх, хариу арга хэмжээ авах, нөхөн сэргээхтэй холбоотой харилцааг зохицуулахад оршино.

1.2. Энэхүү журмыг Агентлагийн нийт албан хаагч, гэрээт болон түр ажилтан, мэдээллийн систем, мэдээллийн сүлжээ, мэдээлэлд нэвтрэх гуравдагч талын этгээд мөрдөнө.

1.3. Агентлаг үйл ажиллагаандаа Кибер аюулгүй байдлын тухай хууль, Төрийн болон албаны нууцын тухай хууль, Хүний хувийн мэдээлэл хамгаалах тухай хууль, Засгийн газрын 2023 оны 224 дүгээр тогтоолын хавсралтаар батлсан "Кибер аюулгүй байдлыг хангах нийтлэг журам", холбогдох стандарт, дүрэм, журам болон бусад хууль тогтоомжийг дагаж мөрдөнө.

1.4. Агентлаг нь кибер аюулгүй байдлыг хангах үйл ажиллагаанд MNS/ISO/IEC 27001:2022 болон эрсдэлийн үнэлгээнд холбогдох ISO/IEC 27005 стандартыг холбогдох хүрээнд баримтална.

1.5. Энэхүү журмыг жил бүр тогтмол хянан шинэчлэх бөгөөд хууль тогтоомж, байгууллагын бүтэц, мэдээллийн систем, мэдээллийн сүлжээ, технологийн орчинд өөрчлөлт орсон тухай бүр шаардлагатай шинэчлэл хийнэ.

1.6. Энэхүү журмын салшгүй хэсэг нь 2–4 дүгээр хавсралтаар батлсан маягт байна.

Хоёр. Нэр томьёо

2.1. "Мэдээлэл" гэж эзэмшиж, хадгалж байгаа төхөөрөмжөөс үл хамааран боломжит бүх хэлбэрээр оршин байгаа баримт бичиг, мэдээ, өгөгдөл, мэдээллийг;

2.2. "Мэдээллийн аюулгүй байдал" гэж мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмж болон тасралтгүй, найдвартай ажиллагааг хангах цогц арга хэмжээг;

2.3. “Хэрэглэгч” гэж Агентлагийн мэдээллийн систем, мэдээллийн сүлжээ, төхөөрөмжид эрхийн дагуу хандаж буй албан хаагч болон бусад этгээдийг;

2.4. “Кибер халдлага, зөрчил” гэж мэдээллийн систем, мэдээллийн сүлжээ, мэдээллийн дэд бүтцийн хэвийн ажиллагаа, мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмжид сөргөөр нөлөөлсөн буюу нөлөөлөх үйлдэл, нөхцөл байдлыг;

2.5. “Лог бүртгэл” гэж мэдээллийн систем, мэдээллийн сүлжээ, төхөөрөмжид хийгдсэн хандалт, үйлдэл болон аюулгүй байдлын үйл явдлын бүртгэлийг;

2.6. “Мэдээлэл технологийн асуудал хариуцсан инженер” гэж Агентлагийн мэдээллийн технологи, мэдээллийн систем, мэдээллийн сүлжээ, кибер аюулгүй байдлын өдөр тутмын хэрэгжилтийг хариуцан ажиллах албан тушаалтныг ойлгоно.

2.7 “Байгууллагын дотоод сүлжээний асуудал хариуцсан инженер” гэж Агентлагийн дотоод сүлжээ, компьютер, тоног төхөөрөмжийн өдөр тутмын хэвийн ажиллагааг хариуцан ажиллах албан тушаалтныг ойлгоно.

Гурав. Кибер аюулгүй байдлыг хангах зохион байгуулалт

3.1. Агентлаг нь кибер аюулгүй байдлыг хангах үйл ажиллагааг байгууллагын стратеги, жилийн төлөвлөгөө, төсөвтэй уялдуулан төлөвлөж хэрэгжүүлнэ.

3.2. Кибер аюулгүй байдлыг хангах үйл ажиллагаа хариуцсан албан тушаалтнаар Мэдээлэл технологийн асуудал хариуцсан инженерийг ажиллуулна.

3.3. Мэдээлэл технологийн асуудал хариуцсан инженер нь кибер аюулгүй байдлын шаардлагыг хэрэгжүүлэх, эрсдэлийг бууруулах арга хэмжээ төлөвлөх, хэрэгжилтийг хянах, зөрчил болон халдлагын үед анхан шатны хариу арга хэмжээ зохион байгуулах, бүртгэл хөтлөх, удирдлагад тайлагнах үүрэгтэй.

3.4. Агентлаг нь кибер аюулгүй байдлын мэдлэг олгох сургалтыг нийт албан хаагчдад жил бүр, шинээр томилогдсон ажилтанд томилогдсоноос хойш 1 сарын дотор, гуравдагч талын ажилтанд тухай бүр зохион байгуулна.

3.5. Кибер орчинд хандаж, мэдээлэлтэй ажиллах гуравдагч талтай гэрээ байгуулахдаа мэдээллийн нууцлал, кибер аюулгүй байдлын үүрэг, хариуцлагыг тусгана.

3.6. Мэдээлэл технологийн асуудал хариуцсан инженер нь хамгаалбал зохих мэдээлэл, мэдээллийн систем, мэдээллийн сүлжээ, мэдээлэл хариуцагчийн жагсаалтыг гаргаж, агентлагийн даргаар батлуулж, өөрчлөлт орсон тохиолдолд тухай бүр шинэчилнэ.

Дөрөв. Мэдээлэл, систем, сүлжээний хамгаалалт

4.1. Мэдээллийн нууцлалын зэрэглэлийг холбогдох хууль тогтоомжид нийцүүлэн тогтоож, мэдээлэлтэй танилцах, ашиглах, дамжуулах, хадгалах эрхийг ялгавартайгаар зохицуулна.

4.2. Сүлжээний болон хяналтын камерын өрөөнд байнгын болон түр нэвтрэх эрх бүхий албан хаагчдын нэрсийн жагсаалтыг Захиргаа, удирдлагын газрын дарга батална.

4.3. Батлагдсан жагсаалтад ороогүй албан хаагч болон гадны этгээд тус өрөөнд нэвтрэхдээ хүсэлтийн маягт бөглөж, бүртгэлийн журналд тэмдэглүүлэн Байгууллагын дотоод сүлжээний асуудал хариуцсан инженерийн хамт нэвтэрнэ.

4.4. Сүлжээний болон хяналтын камерын өрөө нь цоож, шаардлагатай тохиолдолд нэвтрэх хяналт, дүрст хяналтын систем, галын аюулгүй байдал, температур, чийгшлийн хяналтын хэрэгслээр хангагдсан байна.

4.5. Дотоод сүлжээг хэрэглэгчийн, серверийн, хяналтын камерын болон зочны утасгүй сүлжээ зэрэг зориулалтаар боломжит хэмжээнд тусгаарлаж, сүлжээний заагт галт хана болон зөвшөөрөлгүй урсгалыг шүүх хамгаалалт хэрэглэнэ.

4.6. Албан хаагч нь байгууллагаас олгосон компьютер, төхөөрөмжийг албан ажлын зориулалтаар ашиглаж, бусдад ашиглуулахгүй, зөвшөөрөлгүй төхөөрөмж холбохгүй, зөвшөөрөлгүй программ суулгахгүй.

4.7. Компьютер, системд нэвтрэх нэр, нууц үгийг бусдад дамжуулахгүй. Анхдагч нууц үгийг солих бөгөөд нууц үгийн бодлогыг байгууллагын системийн аюулгүй байдлын шаардлагад нийцүүлэн хэрэгжүүлнэ.

4.8. Программ хангамж, үйлдлийн системийн шинэчлэлтийг албан ёсны эх үүсвэрээс хийж, шинэчлэл суулгахаас өмнө шаардлагатай тохиолдолд туршилт, нийцлийн шалгалт хийнэ.

4.9. Мэдээллийн систем, мэдээллийн сүлжээнд өөрчлөлт оруулахдаа зөвшөөрөл, бүртгэл, шаардлагатай бол буцаах төлөвлөгөөтэй байна.

4.10. Агентлагийн үндсэн сервер, мэдээллийн систем нь Үндэсний дата төвд байрлаж, холбогдох гэрээ, үйлчилгээний нөхцөл болон аюулгүй байдлын шаардлагыг мөрдөнө. Мэдээлэл, өгөгдөл, тохиргоог 1 хоног тутамд нөөцөлж, нөөцийн бүрэн бүтэн байдлыг 2 сар тутамд шалган баталгаажуулна.

Тав. Хандалтын удирдлага, лог бүртгэл

5.1. Мэдээллийн систем, мэдээллийн санд хандах эрхийг энэ журмын хавсралтаар батлагдсан хүсэлтийн маягтыг үндэслэн ажил үүргийн шаардлагад нийцүүлэн олгоно.

5.2. Хандах эрхийг хамгийн бага эрхийн зарчимд үндэслэн олгож, давуу эрхтэй хэрэглэгчийг тухай бүр тогтоон хандалтын ашиглалтад хяналт тавина.

5.3. Албан хаагчийн шилжилт хөдөлгөөн, ажлаас чөлөөлөгдсөн, албан тушаал өөрчлөгдсөн мэдээллийг шийдвэр гарсан даруйд Хүний нөөцийн асуудал хариуцсан мэргэжилтнээс Мэдээлэл технологийн асуудал хариуцсан инженер болон

Байгууллагын дотоод сүлжээний асуудал хариуцсан инженерт мэдэгдэж, шаардлагатай эрхийг даруй өөрчилж, хүчингүй болгоно.

5.4. Нэвтрэх оролдлого, давуу эрхийн хандалт, нууц үгийн өөрчлөлт, хандалтын эрх олголт/өөрчлөлт/цуцлалт болон системийн аюулгүй байдлын холбогдох үйлдлийн логийг бүртгэнэ.

5.5. Лог бүртгэлд хэрэглэгчийн нэр буюу ID, огноо, цаг, хандалтын эх үүсвэр/төхөөрөмжийн мэдээлэл, үйлдэл, үр дүн зэрэг шаардлагатай мэдээллийг тусгана.

5.6. Онц чухал мэдээллийн дэд бүтэцтэй байгууллагын хувьд лог бүртгэлийг 1 жилээс доошгүй хугацаагаар хадгална. Халдлага, зөрчилтэй холбоотой логийг холбогдох шалгалт, мөрдөн шалгах ажиллагаа дуусах хүртэл устгахгүй.

5.7. Лог бүртгэлд зөвхөн эрх бүхий этгээд агетлагийн даргын зөвшөөрлийн дагуу хандана.

Зургаа. Эрсдэлийн үнэлгээ, аудит, хяналт

6.1. Кибер аюулгүй байдлын эрсдэлийн үнэлгээг жил тутам, эсхүл мэдээллийн систем, мэдээллийн сүлжээнд өөрчлөлт орох бүрд хэсэгчлэн, эрх бүхий байгууллагын шаардсанаар тухай бүр хийлгэнэ.

6.2. Эрсдэлийн үнэлгээг холбогдох хууль, журмын шаардлага болон ISO/IEC 27005 стандартыг баримтлан гүйцэтгүүлж, дүгнэлт, зөвлөмж, шаардлагын дагуу эрсдэлийг бууруулах арга хэмжээ авч хэрэгжүүлнэ.

6.3. Мэдээллийн аюулгүй байдлын аудитыг хоёр жил тутамд холбогдох хууль тогтоомж, стандартын шаардлагад нийцүүлэн хийлгэнэ.

6.4. Эрсдэлийн үнэлгээ, мэдээллийн аюулгүй байдлын аудитын тайланг хуульд заасан хугацаанд кибер халдлага, зөрчилтэй тэмцэх холбогдох төвд хүргүүлнэ.

6.5. Эрх бүхий байгууллагаас ирүүлсэн зөвлөмж, шаардлагыг тогтоосон хугацаанд, хугацаа заагаагүй бол ажлын 10 өдрийн дотор хэрэгжүүлж, хариу мэдэгдэнэ.

Долоо. Кибер халдлага, зөрчлийг илрүүлэх, мэдээлэх, хариу арга хэмжээ авах

7.1. Мэдээллийн систем, мэдээллийн сүлжээний хэвийн бус үйл ажиллагааг тогтмол хянаж, лог болон аюулгүй байдлын үйл явдлыг цуглуулан дүн шинжилгээ хийнэ.

7.2. Албан хаагч кибер халдлага, зөрчилд өртсөн байж болзошгүй тохиолдлыг нэн даруй Байгууллагын дотоод сүлжээний асуудал хариуцсан инженерт мэдэгдэнэ.

7.3. Байгууллагын дотоood сүлжээний асуудал хариуцсан инженер зөрчлийн шинж, цар хүрээнээс хамааран төхөөрөмж, хэрэглэгчийн эрх, сүлжээний холболтыг тусгаарлах, нотлох баримт, логийг хамгаалах, халдлагын тархалтыг хязгаарлах арга хэмжээ авна.

7.4. Кибер халдлага, зөрчлийн улмаас мэдээллийн систем, дэд бүтцийн хэвийн, тасралтгүй ажиллагаа алдагдсан бол холбогдох кибер халдлага, зөрчилтэй тэмцэх төвд даруй мэдэгдэнэ.

7.5. Төлөвлөгөөт үзлэг, өөрийн дэд бүтцээс гаднах сүлжээ, системийн гэмтэл, саатал, гэнэтийн болон давагдашгүй хүчний шинжтэй нөхцөл байдлын улмаас тасралтгүй ажиллагааг хангах боломжгүй болсон тохиолдолд холбогдох төв болон шаардлагатай хэрэглэгчдэд даруй мэдэгдэнэ.

7.6. Кибер халдлага, зөрчилтэй холбоотой нотлох баримтыг цуглуулж, эх хувийг хадгалан, хуулбарын бүрэн бүтэн байдлыг хангана.

Найм. Тасралтгүй ажиллагаа, сэргээн ажиллуулах

8.1. Гэмтэл, саатлын шалтгаан болон хамрах хүрээг тогтооно.

8.2. Үйлчилгээг тасралтгүй хангах түр арга хэмжээ авна.

8.3. Нөөц хуулбарын хуваарь, хадгалалтын хугацаа, сэргээх туршилтыг шаардлагатай давтамжаар хийж баримтжуулна.

Ес. Хориглох зүйлс

9.1. Зөвшөөрөлгүй этгээдэд компьютер, систем, сүлжээ, сервер, камерын өрөө болон мэдээлэлд хандах эрх олгох;

9.2. Нэвтрэх нэр, нууц үг, токен болон бусад нэвтрэх мэдээллийг бусдад дамжуулах, ашиглуулах;

9.3. Байгууллагын дотоод сүлжээнд зөвшөөрөлгүй төхөөрөмж, зөөврийн хадгалах хэрэгсэл холбох;

9.4. Зөвшөөрөлгүй программ хангамж, хортой код агуулсан файл, лицензгүй программ ашиглах;

9.5. Лог бүртгэл, мэдээллийн хамгаалалтын тохиргоог зөвшөөрөлгүй өөрчлөх, устгах;

9.6. Нууц болон хүний хувийн мэдээллийг зөвшөөрөлгүй хуулбарлах, дамжуулах, ил болгох.

Арав. Хариуцлага

10.1. Албан хаагч, гэрээт ажилтан болон гуравдагч тал нь энэхүү журмыг зөрчсөнөөс үүсэх үр дагаварт холбогдох хууль тогтоомж, гэрээ, албан тушаалын чиг үүрэгт заасан хариуцлага хүлээнэ.

10.2. Журмыг зөрчсөн тохиолдолд зөрчлийн шинж, үр дагаврыг харгалзан холбогдох хууль тогтоомж, хөдөлмөрийн дотоод журмын дагуу хариуцлага тооцно.

10.3. Гэмт хэргийн шинжтэй үйлдэл илэрвэл холбогдох байгууллагад шилжүүлж, шаардлагатай мэдээлэл, нотлох баримтыг хуульд нийцүүлэн хүргүүлнэ.

Эм, эмнэлгийн хэрэгслийн хяналт, зохицуулалтын
газрын 2026 оны .08. дугаар сарын .24.-ны өдрийн
А/134 дугаар тушаалын хоёрдугаар хавсралт

СҮЛЖЭЭНИЙ БОЛОН ХЯНАЛТЫН КАМЕРЫН ӨРӨӨНД НЭВТРЭХ ХҮСЭЛТИЙН МАЯГТ

1. Хүсэлт гаргагчийн мэдээлэл:

   Овог, нэр: _____
   Албан тушаал/байгууллага: _____
   Утас: _____

2. Нэвтрэх өрөө:

   [ ] Сүлжээний өрөө [ ] Хяналтын камерын өрөө

3. Зорилго:

   [ ] Засвар үйлчилгээ [ ] Үзлэг шалгалт [ ] Тоног төхөөрөмж суурилуулах/авах [ ]
   Бусад: _____

4. Нэвтрэх огноо, цаг: _____ Үргэлжлэх хугацаа: _____

5. Нэвтрэх хүмүүсийн нэр, байгууллага: (гуравдагч тал буюу гадны байгууллагын ажилтан бол овог нэр, регистрийн дугаар)

   1) _____ 2) _____ 3) _____

6. Хянасан инженер: _____ / _____/
   (гарын үсэг) (овог, нэр)
7. Зөвшөөрөл олгосон:

   Захиргаа, удирдлагын газрын дарга _____ / _____ /
   (гарын үсэг) (овог, нэр)

   Зөвшөөрсөн [ ] Зөвшөөрөөгүй [ ]

Эм, эмнэлгийн хэрэгслийн хяналт, зохицуулалтын
газрын 2026 оны 08 дугаар сарын 24-ны өдрийн
А/152 дугаар тушаалын гуравдугаар хавсралт

СҮЛЖЭЭНИЙ БОЛОН ХЯНАЛТЫН КАМЕРЫН ӨРӨӨНД НЭВТЭРСЭН БҮРТГЭЛИЙН ЖУРНАЛ

№	Огноо	Нэвтэрсэн цаг	Гарсан цаг	Нэр, албан тушаал/байгууллага	Зорилго, хийсэн ажил	Гарын үсэг

(Энэхүү бүртгэлийн журналыг тус өрөөний хаалганы дэргэд цаасан эсхүл цахим хэлбэрээр байршуулж, нэвтрэх тухай бүрд хөтөлнө)

Эм, эмнэлгийн хэрэгслийн хяналт, зохицуулалтын
газрын 2026 оны 09 дугаар сарын 28-ны өдрийн
А/157 дугаар тушаалын дөрөвдүгээр хавсралт

СИСТЕМ/ПРОГРАММД ХАНДАХ ЭРХИЙН ХҮСЭЛТИЙН МАЯГТ

1. Хүсэлт гаргагч: Овог, нэр _____ Газар/хэлтэс _____ Албан тушаал _____ Албаны имэйл, утас _____

2. Хүсэлтийн төрөл: [ ] Шинээр эрх авах [ ] Эрх өөрчлөх [ ] Эрх хасах/цуцлах

3. Систем/программын нэр: _____

4. Эрхийн түвшин: [ ] Админ [ ] Бичих [ ] Зөвхөн харах [ ] Бусад _____

5. Эрх шаардлагатай үндэслэл: _____

6. Эрхийн хугацаа: [ ] Хугацаагүй [ ] Түр, _____ оны __ сарын __ хүртэл

7. Хүсэлт гаргасан ажилтан: _____ /гарын үсэг/ Харьяалах нэгжийн дарга: _____ /гарын үсэг/

8. Инженерийн шийдвэр: [ ] Гүйцэтгэсэн [ ] Татгалзсан Тайлбар: _____

9. Хэрэглэгчийн нэр/ID: _____ Гүйцэтгэсэн огноо, цаг: _____ Инженер: _____ /гарын үсэг/