

Монгол Улсын Хүний эрхийн Үндэсний
Комиссын даргын 2025 оны 11 дүгээр
сарын 10-ны өдрийн 43 дугаар тушаалын
хоёрдугаар хавсралт



МОНГОЛ УЛСЫН ХҮНИЙ ЭРХИЙН ҮНДЭСНИЙ КОМИССЫН МЭДЭЭЛЭЛ ТЕХНОЛОГИЙН ҮЙЛ АЖИЛЛАГААНЫ ЖУРАМ

Нэг. Нийтлэг үндэслэл

1.1. Комиссын мэдээлэл технологийн үйл ажиллагааны журмыг хэрэгжүүлэх, мэдээлэл солилцох тогтолцоог бүрдүүлэх, мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмжийг хангах, албан хэрэгцээний мэдээлэл, систем, тоног төхөөрөмжийн аюулгүй ашиглалтыг зохион байгуулах, мэдээлэл алдагдах, устах эрсдэлээс урьдчилан сэргийлэх, эрсдэлийг бууруулахад энэхүү журмын зорилго оршино.

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

1.3. Энэхүү журмыг 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.

Хоёр. Нэвтрэх эрхийн удирдлага, зохион байгуулалт

2.1. Комиссын Тамгын газрын албан хаагчид цахим систем (intranet.gov.mn)-д шинээр нэвтрэх эрхийг олгохдоо дараах үйл ажиллагааг хэрэгжүүлнэ:

2.1.1. хүний нөөцийн асуудал хариуцсан албан хаагч intranet.gov.mn системд нэвтрэх эрхийг олгоно.

2.1.2. хүний нөөцийн асуудал хариуцсан албан хаагч оффис 365, төрийн цахим шууданд нэвтрэх эрхийг шинээр эрх нээлгэх хүсэлтийг мэдээллийн технологи хариуцсан албан хаагчид цахим шуудангаар илгээнэ.

2.1.3. мэдээллийн технологи хариуцсан албан хаагч тухайн хүсэлтэд үндэслэн шаардлагатай нэвтрэх эрхийг олгож, бүртгэлийн хуудсанд бүртгэнэ.

2.1.4. мэдээллийн технологи хариуцсан албан хаагч нь хүний нөөцийн асуудал хариуцсан албан хаагчид эрх олгосон талаар цахим шуудангаар мэдэгдэнэ.

2.2. Комиссын хэмжээнд аливаа арга хэмжээ зохион байгуулахдаа гадны хэрэглэгчид түр хугацааны эрх олгохдоо дараах үйл ажиллагааг хэрэгжүүлнэ. Үүнд:

2.2.1. арга хэмжээний зохион байгуулалтыг хариуцаж байгаа хэлтсийн дарга мэдээллийн технологи хариуцсан албан хаагчид гадны эрх олгох этгээдийн мэдээллийг эрх олгох хугацааны талаарх мэдээллийн хамт цахим шуудангаар илгээнэ.

2.2.2. мэдээллийн технологи хариуцсан албан хаагч нь хүсэлтэд үндэслэн түр хугацааны эрхийг нээж олгож бүртгэлийн хуудсанд бүртгэнэ.

2.2.3. түр хугацааны эрх нь тохируулсан хугацаа дуусмагц автоматаар идэвхгүй болох тохиргоотой байна.

2.2.4. эрх олгосон талаар хүсэлт гаргасан хэлтсийн даргад цахим шуудангаар мэдэгдэнэ.

2.3. Нэвтрэх эрхийг өөрчлөхдөө дараах үйл ажиллагааг хэрэгжүүлнэ:

2.3.1. Комиссын Тамгын газрын албан хаагчийн албан тушаал өөрчлөгдсөн тохиолдолд хүний нөөцийн асуудал хариуцсан албан хаагч нь нэвтрэх эрх өөрчлөх хүсэлтийг мэдээллийн технологи хариуцсан албан хаагч руу цахим шуудангаар илгээнэ.

2.3.2. мэдээлэл технологи хариуцсан албан хаагч хуучин эрхийг цуцалж, шинэ эрхийг олгож, бүртгэлийн хуудсанд бүртгэнэ.

2.3.3. хэрэглэгч болон хүний нөөцийн асуудал хариуцсан албан хаагч руу эрх олгосон талаар цахим шуудангаар мэдэгдэнэ.

2.4. Хэрэглэгчийн эрхийг цуцлахдаа дараах үйл ажиллагааг хэрэгжүүлнэ. Үүнд:

2.4.1. хүний нөөцийн асуудал хариуцсан албан хаагч ажлаас гарсан, шилжсэн зэрэг нэвтрэх эрхийг цуцлах хүсэлтийг мэдээллийн технологи хариуцсан албан хаагч руу цахим шуудангаар илгээнэ.

2.4.2. мэдээллийн технологи хариуцсан албан хаагч тухайн эрхийг цуцалж эрхийн бүртгэлийн хуудсанд бүртгэнэ.

2.4.3. хүний нөөцийн асуудал хариуцсан албан хаагч руу эрх цуцалсан талаар цахим шуудангаар мэдэгдэнэ.

2.4.4. шаардлагатай тохиолдолд хэрэглэгчийн эрхийг цуцлах хүсэлтийг хариуцсан хэлтсийн дарга гаргаж болно.

2.5. Нэвтрэх эрхийн хяналтыг дараах үйл ажиллагааны дагуу гүйцэтгэнэ:

2.5.1. Хяналт-шинжилгээ, үнэлгээ хариуцсан албан хаагч сар бүр хэрэглэгчийн эрхийн бүртгэлийн хуудсанд шаардлагагүй, давхардсан эрх олгосон эсэхэд шинжилгээ хийж тайланг захиргааны асуудал хариуцсан нэгжийн даргад танилцуулна.

Гурав. Сүлжээний аюулгүй байдлын удирдлага, зохион байгуулалт

3.1. Комиссын дотоод сүлжээг зориулалт, нэвтрэх эрхийн түвшнээр дараах гурван түвшинд тусгаарлана:

3.1.1. албаны дотоод сүлжээ: Албан хаагчдын компьютер, хэвлэгч, байгууллагын дотоод хэрэглээний төхөөрөмжүүд холбогдох бөгөөд зөвхөн шаардлагатай дотоод нөөц болон интернэтэд хандах эрхтэй байна;

3.1.2. төрийн нэгдсэн мэдээллийн сүлжээ: Байгууллагын сервер, өгөгдлийн сан, мэдээллийн системүүд байрлах бөгөөд зөвхөн зөвшөөрөгдсөн админ болон шаардлагатай үйлчилгээний порт, протоколоор дамжуулан хандалт зөвшөөрнө;

3.1.3. зочдын сүлжээ: Байгууллагын зочин, гадны хэрэглэгчдэд зориулсан тусдаа сүлжээ бөгөөд зөвхөн интернэтэд хандах эрхтэй, дотоод болон серверийн сүлжээ рүү хандалт хийх боломжгүй байна;

3.2. Сүлжээнүүдийг VLAN болон дэд сүлжээгээр тусгаарлаж, галт ханын дүрмээр харилцан хандалтыг хязгаарлана.

3.3. Зочдын сүлжээний нууц үгийг комиссын Мэдээллийн технологи хариуцсан албан хаагч удирдаж гурван сар тутамд шинэчилж байна.

3.4. Байгууллагын дотоод болон гадаад сүлжээний бүтэц, төхөөрөмжүүдийн уялдаа холбоог сүлжээний топологи зургийг физик болон логик хэлбэрээр боловсруулж, албаны нууцын түвшинд хадгална.

3.5. Сүлжээний топологи зурагт дараах мэдээллийг багтаана:

3.5.1. сүлжээний үндсэн архитектур (LAN, WAN, Wi-Fi, VPN гэх мэт);

3.5.2. төв болон дэд сүлжээний сегментүүд (VLAN, subnet);

3.5.3. сүлжээний гол төхөөрөмжүүд (router, switch, firewall, access point, сервер гэх мэт);

3.5.4. сүлжээ хоорондын холболт ба харилцан хязгаарлалтын зарчим;

3.6. Комиссын Тамгын газрын мэдээллийн аюулгүй байдлыг хангах зорилгоор веб контент шүүлтүүрийг байгууллагын сүлжээнд дараах байдлаар хэрэгжүүлнэ.

3.6.1. веб урсгалыг галт ханаар дамжуулж, хяналтын жагсаалтад хориглох веб хуудасны жагсаалтыг батлуулан шүүлтүүр хийнэ.

3.6.2. шүүлтүүрийн дүрэм, ангиллыг мэдээллийн технологи хариуцсан албан хаагч тогтмол шинэчилж, шинэ төрлийн аюул занал илрэхэд шуурхай хэрэгжүүлнэ.

3.7. Шаардлагатай тохиолдолд тодорхой сайтын хоригийг цуцлах хүсэлтийг харьяалах хэлтсийн даргад бичгээр болон цахимаар гаргаж, захиргааны асуудал хариуцсан нэгжийн дарга зөвшөөрсөн тохиолдолд нээж болно.

3.8. Веб контент шүүлтүүрийн тохиргоо, хориглох веб хуудасны жагсаалт нь Тамгын газрын албан хаагч нарт нээлттэй байна.

3.9. Мэдээллийн технологи хариуцсан албан хаагч байгууллагын мэдээллийн аюулгүй байдалд нөлөөлж болзошгүй мэдээллийг дотоод болон гадаад эх сурвалжаас цуглуулж, системтэйгээр шинжилж шаардлагатай арга хэмжээг тухай бүр зохион байгуулна.

Дөрөв. Тоног төхөөрөмжийн бэлэн байдал

4.1. Компьютер, тоног төхөөрөмжийг шинээр суурилуулахдаа дараах үйл ажиллагааг хэрэгжүүлнэ. Үүнд:

4.1.1. Хүний нөөцийн асуудал хариуцсан албан хаагч шинээр томилогдсон албан хаагчийн мэдээллийг мэдээллийн технологи хариуцсан албан хаагч руу цахим шуудангаар хүргүүлнэ.

4.1.2. Мэдээллийн технологи хариуцсан албан хаагч шинээр томилогдсон албан хаагчийн компьютер, тоног төхөөрөмжийг бэлтгэнэ:

4.1.2.1. үйлдлийн систем, хэрэгцээтэй программ хангамжийг суулгана;

4.1.2.2. сүлжээний тохиргоог хийнэ;

4.1.2.3. вирусийн эсрэг программ суулгаж, тохируулга хийнэ;

4.1.2.4. майкрософт оффис 365, төрийн цахим шууданд нэвтрэх эрхийг журмын 2.1. дэх заалтад заасны дагуу нээж олгоно;

4.1.3. Мэдээллийн технологи хариуцсан албан хаагч нь тоног төхөөрөмж, программ хангамжид өөрчлөлт оруулахдаа урьдчилан мэдэгдэнэ;

4.1.4. Мэдээллийн технологи хариуцсан албан хаагч нь шинээр томилогдсон албан хаагчид холбогдох тоног төхөөрөмжийг хүлээлгэн өгнө.

Тав. Зөрчлийн үед авах арга хэмжээ

5.1. Комиссын Тамгын газрын албан хаагч мэдээлэл цуглуулах, боловсруулах, ашиглахад илэрсэн аливаа мэдээллийг Тамгын газрын даргад нэн даруй мэдэгдэнэ.

5.2. Тамгын газрын дарга үүссэн нөхцөл байдалд үнэлгээ хийж мэдээллийн аюулгүй байдлын зөрчил мөн эсэхийг баталгаажуулна.

5.3. Хэрэв мэдээллийн аюулгүй байдлын зөрчил биш гэж үзвэл Хөдөлмөрийн дотоод журам заасны дагуу шийдвэрлэнэ.

5.4. Тамгын газрын дарга мэдээллийн аюулгүй байдлын зөрчлийг холбогдох нотлох баримтыг цуглуулж, шалтгааныг тогтоох ба дараах зарчмыг баримтална:

5.4.1. зөрчлийг бүртгэсэн үеэс эхлэн нотлох баримт цуглуулах, хадгалах, хамгаалах үйл ажиллагааг хэрэгжүүлнэ;

5.4.2. нотлох баримтын аюулгүй байдлыг хангах зорилгоор шинжилгээний үр дүн гарах хүртэл зөрчилтэй холбоотой хөрөнгийг тусгаарлах болон хандалтыг хянах арга хэмжээнүүдийг авч хэрэгжүүлнэ;

5.5. Тамгын газрын дарга зөвшөөрснөөс бусад тохиолдолд зөрчилтэй холбоотой аливаа мэдээллийг нууцална.

5.6. Зөрчилтэй холбоотой сахилгын хариуцлага тооцох зорилгоор нотлох баримтыг цуглуулж, гаргаж өгөхдөө Хөдөлмөрийн дотоод журамд заасан шаардлагад нийцүүлнэ.

5.7. Захиргааны асуудал хариуцсан нэгжийн Хяналт шинжилгээ, үнэлгээ хариуцсан албан хаагч нь мэдээллийн аюулгүй байдлын зөрчлийн бүртгэлийг бүртгэн хадгална.

5.8. Тамгын газрын дарга мэдээллийн аюулгүй байдлын зөрчлийг шийдвэрлэсэн байдал болон тухайн зөрчлийг дахин гарахгүй байхад чиглэсэн саналыг Комиссын даргад тухай бүр танилцуулна.

5.9. Мэдээллийн аюулгүй байдлын зөрчил гарах болсон шалтгааны талаар Захиргаа, удирдлагын хэлтсээс Тамгын газрын албан хаагчдад мэдээлэл өгч, бүртгэл хөтөлж баталгаажуулна.

Зургаа. Бусад

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