НИЙСЛЭЛИЙН ӨМЧИЙН ХАРИЛЦААНЫ ГАЗРЫН ДАРГЫН ТУШААЛ

2025 оны 03 сарын 10 өдөр Дугаар А/138 Улаанбаатар хот

Журам батлах тухай

Монгол Улсын Засаг захиргаа, нутаг дэвсгэрийн нэгж, түүний удирдлагын тухай хуулийн 67 дугаар зүйлийн 67.5 дахь хэсэг, Хүний хувийн мэдээлэл хамгаалах тухай хуулийн 20 дугаар зүйлийн 20.1.1 дэх хэсгийг тус тус үндэслэн ТУШААХ нь:

1.Нийслэлийн Өмчийн харилцааны газрын “Мэдээллийн аюулгүй байдлыг хангах дотоод журам”-ыг хавсралтаар батлалсугай.

2.Журмыг мөрдөн ажиллахыг газрын нийт албан хаагчдад үүрэг болгосугай.

3.Журмын хэрэгжилтэд хяналт тавьж ажиллахыг Захиргаа,удирдлагын хэлтэст (Т.Оюунтуул)-дтдаалгасугай.

ДАРГЫН АЛБАН ҮҮРГИЙГ ТҮР ОРЛОН ГҮЙЦЭТГЭГЧ В.ОЮУМАА

Нийслэлийн Өмчийн харилцааны газрын
даргын 2025 оны 10 сарын 10-ны өдрийн
А/18 тушаалын хавсралт

НИЙСЛЭЛИЙН ӨМЧИЙН ХАРИЛЦААНЫ ГАЗРЫН МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ДОТООД ЖУРАМ

НЭГ. Нийтлэг үндэслэл

1.1. Нийслэлийн өмчийн харилцааны газар /цаашид "Газар" гэх/-аас хуульд заасан чиг үүргээ хэрэгжүүлэх явцад олж авсан иргэн, аж ахуй нэгж, төрийн байгууллага, албан тушаалтны мэдээллийн аюулгүй байдлыг хангах, тэдгээрийг хамгаалахад энэ журмын зорилго оршино.

1.2. Хүний хувийн мэдээлэл хамгаалах тухай хуулийн 20 дугаар зүйлийн 20.1.1 дэх хэсэгт заасныг үндэслэн боловсруулав.

1.3. Журмын хэрэгжилтэд Захиргаа удирдлагын хэлтэс хяналт тавина.

ХОЁР. Газрын мэдээллийн аюулгүй байдлын тогтолцоонд хамаарах мэдээлэл, эд хөрөнгө

2.1. Журмын 1.1 дэх хэсэгт заасан мэдээллийг биет болон биет бус/цахим/ гэж ангилна.

2.2. Биет мэдээлэлд дараах мэдээлэл хамаарна:

2.2.1 Эрх зүйн баримт бичиг, үндсэн болон нэмэлт үйл ажиллагааны хүрээнд боловсруулсан болон цуглуулсан мэдээлэл, тайлан, төлөвлөгөө, төсөл хөтөлбөр, бүртгэлийн мэдээлэл, сургалтын материал, тараах хуудас, гарын авлага, хэвлэмэл зураг зэрэг бүх төрлийн цаасан суурьт мэдээллүүд;

2.2.2 Биет байдлаар оршин буй бусад төрлийн мэдээллүүд.

2.3 Биет бус мэдээлэл гэдэгт:

2.3.1 Биет мэдээллийн цахим хэлбэр, өгөгдлийн сан, файлын сан, цахим шуудан, дүрс бичлэг, дуу бичлэг, компьютер, гар утас, таблет дээрх мэдээлэл, мэдээллийн технологийн тусламжтай нээгдэх боломжтой мэдээлэл /флаш, диск, хард гэх мэт/;

2.3.2 Бусад төрлийн цахим мэдээллүүд тус тус хамаарна.

2.4 Байгууллагын мэдээллийн аюулгүй байдлын тогтолцоонд хамаарах эд хөрөнгө гэдэгт дараах эд хөрөнгийг хамааруулна:

2.4.1 Хэрэглээний болон тусгай зориулалтын программ хангамж, системүүд;

2.4.2 Өөрсдийн хөгжүүлсэн болон тусгай захиалгаар өөр этгээдээр хөгжүүлэлт хийлгэсэн программ хангамж, системүүд;

2.4.3 Серверийн болон Оффисын хэрэглээний компьютер, Тоног төхөөрөмжүүд /сервер, процессор, дэлгэц, хэвлэгч, хувилагч, сканер, зөөврийн компьютер, телефон, факсын аппарат, зөөврийн хард диск, флаш, CD/

2.4.4 Сүлжээний тоног төхөөрөмжүүд /файрвол, рутер, свич, салаалагч, сүлжээний утас/;

2.4.5 Серверийн үйл ажиллагааг дэмжих тоног төхөөрөмжүүд /хөргүүр, тог баригч, нөөц тэжээлийн үүсгүүр/;

2.4.6 Active Directory (AD) болон Domain Controller (DC) систем, тэдгээрийн сервер.

ГУРАВ. Мэдээллийн аюулгүй байдлыг хангах

3.1. Биет бус, цахим мэдээллийг илгээх буюу шилжүүлэх харилцаанд зөвхөн байгууллагын систем /ERP/, ажлын и-мэйл, факс, AD/DC систем зэргийг ашиглана.

3.2. Нийслэлийн нутгийн захиргааны байгууллагуудын дотоод систем буюу ERP болон нь албан хаагчдын өдөр тутмын үйл ажиллагаанд хэрэглэх үндсэн систем байна.

3.3. Журмын 2.2, 2.3 дахь хэсэгт хамаарах мэдээллийг албан хаагчид зөвхөн Газар болон нэгжийн даргын зөвшөөрснөөр иргэн, аж ахуй нэгж, төрийн байгууллагад гаргаж өгнө.

3.4. Төрийн байгууллага, албан тушаалтанд биет мэдээллийг шуудангаар илгээх, биеэр зөөвөрлөх байдлаар шилжүүлэхдээ түүний эх хувийг заавал хадгална.

3.5. Газарт шинээр ирсэн биет болон биет бус мэдээллийг бичиг хэргийн ажилтан заавал тэмдэглэж бүртгэлжүүлнэ.

3.6. Түр хугацаагаар гарах бол компьютерыг заавал түгжих буюу нууц үгээр хамгаалагдсан дэлгэцийн хамгаалалтыг ажиллуулна. Ажлын цаг дуусаж, албан хаагч явахдаа компьютер, тоног төхөөрөмжүүдийг унтрааж, цахилгааны хүчдэлээс салгана.

3.7. Нууц үгийг том, жижиг үсэг, тоо, тусгай тэмдэгт агуулсан байдлаар 8-12 оронтойгоор үүсгэнэ. Нууц үгээ ил бичиж тэмдэглэх, бусдад дамжуулахыг хориглоно.

3.8. Эхний нууц үгийг 6 сар тутамд шинэчилж байх, ингэхдээ хуучин нууц үгийг ахин хэрэглэхгүй, тэмдэгтүүдийг заавал солино.

3.9. AD нууц үгийн бодлогод тусгасан түүнтэй холбоотой Group Policy-г тохируулж өгсөн байж болно.

3.10. Дүрсний төхөөрөмж /камер/-ийн бичлэг нь мэдээллийн аюулгүй байдлыг хангах нэг үндэслэл болно.

3.11. Газрын холбогдох мэргэжилтэн /Программист, сүлжээний инженер/ биет бус, цахим мэдээллийн талаарх аливаа асуудалд албан хаагчдад туслалцаа үзүүлж ажиллана.

3.12. Гадаад сүлжээнээс хандах шаардлагатай тохиолдолд зөвхөн холбогдох мэргэжилтний зөвшөөрсөн буюу тохируулсан VPN ашиглан нэвтэрнэ.

3.13. Ямар нэг тодорхой шалтгаангүйгээр гэнэтийн э-мэйл ирсэн бол албан хаагч түүнийг нээх ёсгүй бөгөөд холбоосоор орохгүй байхыг баримтална.

3.14. Мэдээлэл хариуцагч камерын бичлэгт хамаарах мэдээллийн аюулгүй байдлыг хангах чиглэлээр доор дурдсан арга хэмжээ авна:

3.14.1. Мэдээллийг санаандгүйгээр гэмтээх, устгах, хандах эрх олгогдоогүй этгээд хандах, хууль бусаар мэдээллийг цуглуулах, боловсруулах, ашиглахаас хамгаалах арга хэмжээг авах;

3.14.2. Мэдээлэлд хандах эрхэд хязгаарлалт тогтоох, нууц үг, шифрлэлт хэрэглэх;

3.14.3. Нийтлэг хэрэглэж заншсан нууц үгийг хэрэглэхээс татгалзах, нууц үгийг бусдад түгээхгүй байх;

3.14.4. Мэдээллийн хандаж байгаа лог, бүртгэлд тогтмол хяналт тавих;

3.14.5. Мэдээллийн аюулгүй байдлыг хангах чиглэлээр авч хэрэгжүүлж байгаа арга хэмжээ, үр дүнгийн талаар тэмдэглэл хөтлөх.

ДӨРӨВ. Газар болон газрын ажилтны эрх, үүрэг

4.1. Газар нь журмын 1.1 дэх хэсэгт заасан мэдээллийн аюулгүй байдлыг хангах, тэдгээрийг хамгаалахад дараах эрхийг эдэлнэ:

4.1.1. Газрын албан хаагчид биет буюу цахим мэдээллийг зориулалтын дагуу ашиглаж байгаа эсэхэд хяналт тавих;

4.1.2. Аюулгүй байдлын шаардлагыг зөрчсөн албан хаагчид хариуцлага тооцох;

4.1.3. Шаардлагатай тохиолдолд албан хаагчдад байгаа бүх төрлийн мэдээллийг татаж шалгах.

4.2. Газар нь мэдээллийн аюулгүй байдлын талаар дараах үүргийг хүлээнэ:

4.2.1. Биет буюу цахим мэдээлэл гадагш алдагдахаас сэргийлэх;

4.2.2. Цахим мэдээллийн аюулгүй байдлыг хангахад холбогдох мэргэжилтэн /Программист, сүлжээний инженер/-ний тусламжтайгаар албан хаагчдыг мэргэжлийн удирдлагаар хангах;

4.2.3. Биет мэдээллийн эх хувь болон тэдгээрийн хуулбар; газрын тамга, тэмдэг, бланк бүхий баримт бичгүүд алдагдахаас сэргийлж хянамгай байх;

4.2.4. Байгууллагын албан хаагчдад мэдээллийн аюулгүй байдлыг хангахад чиглэсэн сургалт сурталчилгааг зохион байгуулах.

4.3. Ажилтны эдлэх эрх:

4.3.1. Биет бус, цахим мэдээлэлтэй холбоотой аливаа асуудлаар холбогдох мэргэжилтэн /Программист, сүлжээний инженер/-ээс зөвлөгөө мэдээлэл авах;

4.3.2. Журмын 4.1.3 дахь хэсэгт заасан тохиолдолд хувийн мэдээллээ өгөхгүй байх;

4.3.3. Мэдээллийг биет болон цахимаар ашиглах явцад мэдээллийн аюулгүй байдал алдагдах эрсдэлтэй гэж үзвэл мэргэжилтэн Газар, нэгжийн даргаас зөвлөмж хүсэх эрхтэй ба хариу өгтөл тухайн үүрэг даалгаврыг биелүүлэхгүй байх мөн эрхтэй.

4.4. Албан хаагч дараах үүргийг хүлээнэ:

4.4.1. Биет мэдээллийг зохих журмын дагуу ашиглах, архивд өгөх;

4.4.2. Биет бус, цахим мэдээллийг цуглуулах, ашиглах харилцаанд дур мэдэн аливаа үйлдэл хийхгүй байх;

4.4.3. Цахим халдлагад өртсөн үед төрийн албан хаагчдын нэгдсэн систем /ERP/ ашиглахгүй байх.

ТАВ. Хориглох зүйлс

5.1. Мэдээллийн аюулгүй байдлыг хангахад дараах зүйлсийг хориглоно:

5.1.1. Албан хаагчид ажлын компьютер, түүний бүрдэл хэсгийг бусдад дамжуулах буюу ашиглуулах;

5.1.2. Ажлын байранд хэрэглэдэг зөөврийн хадгалах төхөөрөмж /флаш, зөөврийн хард гэх мэт/-ийг бусдад дамжуулах, албан бусаар ашиглах;

5.1.3. Мэдээллийг тээх хэрэгслийг буруу хадгалах, гэмтээх, хаяж үрэгдүүлэх;

5.1.4. Суурин болон зөөврийн компьютерт зөвхөн албан ажлын хэрэгцээний мэдээллийг хадгалах бөгөөд хувийн мэдээллүүд (кино, зураг, дүрс бичлэг, дуу бусад файл гэх мэт)-ийг хадгалах;

5.1.5. Гадаад орчноос хандалт хийх шаардлага гарвал зөвхөн зөвшөөрөгдсөн буюу AD/DC дээр тохиргоо хийгдсэн нөхцөлд боломжтой ба өөр хэрэглэгч VPN болон бусад Remote программ ашиглан нэвтрэхийг хориглоно.

ЗУРГАА. Бусад

6.1. Хууль бусаар мэдээлэл задруулсан бол төрийн албаны тухай, хөдөлмөрийн тухай, зөрчлийн тухай хууль болон эрүүгийн хуулиар хариуцлага хүлээлгэх үндэслэл болно.

6.2. Журмын 6.1 дэх хэсэгт заасан зөрчил гаргасан албан тушаалтанд Газар хөдөлмөрийн дотоод журамд заасны дагуу арга хэмжээ авна.

6.3. Мэдээллийн аюулгүй байдлыг хангахтай холбоотой зайлшгүй зардлыг Газар хариуцна.

---oOo---