



**ХЭНТИЙ АЙМГИЙН
МӨРӨН СУМЫН ЗАСАГ ДАРГЫН ТАМГЫН
ГАЗРЫН ДАРГЫН ТУШААЛ**

2025 оны 06 сарын 17 өдөр

Дугаар А/29

Мөрөн сум

**Байгууллагын мэдээллийн аюулгүй
байдлын журмыг батлах тухай**

Монгол улсын Засаг захиргаа, нутаг дэвсгэрийн нэгж, түүний удирдлагын тухай хуулийн 67 дугаар зүйлийн 67.5, 59 дүгээр зүйлийн 59.1.1 дэх заалтыг тус тус үндэслэн ТУШААХ нь:

1.Байгууллагын мэдээллийн аюулгүй байдлын бодлогыг хэрэгжүүлэх, мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмжтэй байдлыг хангах зорилгоор “Байгууллагын мэдээллийн аюулгүй байдлын журам”-ыг хавсралтаар баталсугай.

2.Байгууллагын мэдээллийн аюулгүй байдал хариуцсан ажилтан (систем админ)-аар Хууль эрх зүй, хүний нөөц хариуцсан мэргэжилтэн (Г.Хишигбаатар)-ыг томилсугай.

3.Энэхүү тушаалын хэрэгжилтэд хяналт тавьж ажиллахыг Нийгмийн бодлогын мэргэжилтэн (А.Алимаа)-д үүрэг болгосугай.

ДАРГА



Н.НАМЖИЛНОРОВ

ЗАСАГ ДАРГЫН ТАМГЫН ГАЗРЫН МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ХАНГАХ НИЙТЛЭГ ЖУРАМ (ТӨСӨЛ)

Нэг. Ерөнхий зүйл

1.1.1. Энэхүү журмын зорилго нь төрийн байгууллагуудын мэдээллийн технологи, систем, сүлжээ, өгөгдөл дотоод үйл ажиллагаатай холбоотой мэдээллийн аюулгүй байдлыг сахин хамгаалах, гаднын халдлага, дотоод эрсдэлийг бууруулах, халдлагаас урьдчилан сэргийлэх, итгэлтэй, тасралтгүй ажиллагааг хангахад оршино.

1.1.2. Байгууллага нь кибер аюулгүй байдлын хууль тогтоомж, энэ журам, олон улсын стандартад нийцүүлэн, өөрийн үйл ажиллагааны онцлог, цар хүрээг харгалзан кибер аюулгүй байдлыг хангах үйл ажиллагааны дотоод журмыг баталж, мөрдөнө.

1.1.3. Мэдээллийн аюулгүй байдал нь зөвхөн техник, программ хангамж бус харин байгууллагын соёл, сахилга бат, ёс зүйн асуудал мөн болно.

Хоёр. Зохион байгуулалт ба хариуцлага

2.1. Байгууллага нь мэдээллийн аюулгүй байдлыг хангах зорилгоор дор дурдсан бүтэц, оролцоог бий болгоно.

2.1.1. Мэдээллийн аюулгүй байдал хариуцсан ажилтан (систем админ) томилж, эрх үүргийг тодорхойлно.

2.1.2. Ажилтнуудыг мэдээллийн аюулгүй байдлын сургалт, дадлагад тогтмол хамруулна.

2.1.3. Эрх бүхий тусгай зөвшөөрөлтэй байгууллагаар 2 жилд 1 удаа кибер аюулгүй байдлын эрсдэлийн үнэлгээ хийлгэж, шаардлагатай төлөвлөгөөг боловсруулна.

Гурав. Мэдээллийн технологийн хэрэгцээ

3.1. Байгууллагын компьютеруудыг зөвхөн албан хэрэгцээнд ашиглана. Гадны этгээд ашиглах, хувийн хэрэглээ болон интернэтийн зүй зохисгүй албан бус зориулалтаар ашиглахыг хориглоно.

3.2. Нууцын зэрэглэлтэй мэдээлэл агуулсан төхөөрөмжийг зөвшөөрсөн бүсээс зөвшөөрөлгүйгээр гадагш гаргахгүй байх,

3.3. Байгууллага зөвшөөрснөөс бусад төрлийн программ хангамжийг ашиглахгүй байх,

3.2.1. Компьютер, зөөврийн төхөөрөмжид доорх тохиргоог хийнэ.

3.2.2. Нууц үгийн бодлого мөрдүүлэх (8+ тэмдэгт, том/ жижиг үсэг, тоо, тэмдэгт оролцуулсан).

3.2.3. Автомат түгжээ, дэлгэцийн хамгаалалт идэвхжүүлэх,

3.2.4. Хортой кодын эсрэг лицензтэй программ (endpoint security) суурилуулах.

Дөрөв. Сүлжээний аюулгүй байдал ба интернэт ашиглалт

4.1. Албан хаагчид интернэт ашиглахдаа мэдээллийн аюулгүй байдал, ёс зүй, дотоод журмыг баримтлан, дараах төрлийн вэб хуудасруу хандахыг хориглох,

- 4.1.1 Садар самуун, ялгаварлан гадуурхах, хүчирхийллийн агуулгатай сайтууд,
- 4.1.2 Torrent болон crack сайтууд * онлайн тоглоомын платформ
- 4.1.3 Программ хангамжийг хууль бусаар татах сайтууд
- 4.1.4 Нууц, хязгаарлалттай мэдээллийг гуравдагч этгээдэд ил тод дамжуулах боломжтой вэб, аппликейшн
- 4.2. Сүлжээний тохиргоог зөвхөн системийн админ хийж, бусад ажилтан дур мэдэн өөрчлөхийг хориглох,

Тав. Цахим шуудан болон мессенжэрийн зохицуулалт

- 5.1. Албан хэрэгцээнд зөвхөн байгууллагын домайн нэр бүхий цахим шуудан (nep@khentii.gov.mn) ашиглана.
- 5.2. Viber, Telegram, Messenger зэрэг олон нийтийн мессенжэр апплейшнийг нууц, албан мэдээлэл дамжуулах зорилгоор ашиглахыг хориглоно.
- Зөвхөн албан зөвшөөрөгдсөн цахим шуудан болон төрийн мэдээллийн eгг-emongolia.mn системийг ашиглана.

Зургаа. Нөөцлөлт ба мэдээллийн сан

- 6.1. Дотоод сүлжээний серверт хадгалагдах мэдээллийг долоо хоног тутам нөөцлөн архивлана.
- 6.2. Мэдээллийг хувийн зорилгоор ашиглах, гадагш тараах, нууцын зэрэглэлтэй файл хадгалахыг хориглоно.

Долоо. Хандалтын удирдлага

- 7.1. Байгууллагын мэдээллийн систем, мэдээллийн сүлжээний тоног төхөөрөмж байрлаж байгаа зориулалтын өрөөнд зөвшөөрөлгүй нэвтрэхийг хориглох бөгөөд өрөө нь дараах шаардлагыг хангасан байна.
 - 7.7.1 өрөөний хаалга цоожтой байх,
 - 7.7.2 дохиоллын системтэй байх,
 - 7.7.3 цонхны хамгаалалтай
 - 7.7.4 орох хаалганы дэргэд дүрст хяналтын системтэй байх,
 - 7.7.5 температур, чийгшил зэрэг орчны нөхцөлийг хянах, бүрдүүлэх хэрэгсэлтэй байх,
 - 7.7.6 хаалганы түлхүүр, эрхийг зөвхөн эрх бүхий ажилтан хадгалах,
- 7.2. Байгууллага мэдээллийн систем, мэдээллийн сүлжээний тоног төхөөрөмж байршуулах зориулалтын өрөөгүй бол энэ журмын 7.1-т заасан шаардлагад дүйцэх, тоног төхөөрөмжид зөвшөөрөлгүй этгээд хандахаас сэргийлсэн цоож, шүүгээ бүхий өрөөнд байршуулж болно.

Найм. Кибер халдлага ба хариу арга хэмжээ

- 8.1. Кибер зөрчил илэрсэн тохиолдолд Мэдээллийн аюулгүй байдал хариуцсан ажилтан даруй тэмдэглэл хөтөлж, шийдвэрлэнэ.
- 8.2. Халдлагын хариу арга хэмжээний төлөвлөгөөг жилд 1 удаа туршиж, шинэчилнэ.
- 8.3. Зөрчлийг бүртгэх, холбогдох байгууллагад мэдээлэх журам боловсруулж хэрэгжүүлнэ.

Ес. Хяналт ба сахилга бат

9.1. Байгууллагын удирдах албан тушаалтан кибер аюулгүй байдлыг хангах чиглэлээр дараах үүрэгтэй.

9.1.1. Байгууллагын кибер аюулгүй байдлыг хангах үйл ажиллагааг нэгдсэн удирдлагаар хангах, уялдуулан зохион байгуулах, байгууллагыг төлөөлөх,

9.1.2. Кибер аюулгүй байдлыг хангах бодлого, дүрэм журам батлах,

9.1.3. Кибер аюулгүй байдлыг хангах төлөвлөгөө гаргах, хэрэгжүүлэхэд шаардагдах нөөцийг байгууллагын жил бүрийн төсөв, төлөвлөгөөнд тусгах,

9.2. Байгууллагын кибер аюулгүй байдлыг хангах өдөр тутмын үйл ажиллагааг хариуцан гүйцэтгэх,

9.2.1. Байгууллагын кибер аюулгүй байдлыг хангах өдөр тутмын үйл ажиллагааг хариуцан гүйцэтгэх,

9.2.2. Холбогдох дүрэм журмыг боловсруулах, шинэчлэх санал боловсруулах,

9.2.3. Кибер аюулгүй байдлыг хангахад шаардлагатай үйл ажиллагаа, нөөцийг төлөвлөх,

9.3. Байгууллагын нийт ажилтан кибер аюулгүй байдлыг хангах чиглэлээр дараах үүрэгтэй.

9.3.1. энэ журам болон мэдээллийн аюулгүй байдлыг хангахтай холбоотой бусад дүрэм, журмыг дагаж мөрдөх,

9.3.2. илэрсэн хандлага, зөрчил, сэжигтэй тохиолдол бүрийг аюулгүй байдал хариуцсан ажилтанд мэдэгдэх,

9.3.3. Байгууллагын мэдээлэл, мэдээллийн систем, мэдээллийн сүлжээг зөвхөн албан хэрэгцээнд, заасан журам, зааврын дагуу хэрэглэх,

9.3.4. Байгууллагаас зохион байгуулж буй кибер аюулгүй байдлын мэдлэг олгох сургалтад хамрагдах,

9.4. Энэхүү журмыг зөрчсөн албан тушаалтан, байгууллагад холбогдох хууль тогтоомжид заасан хариуцлага хүлээлгэнэ.