ХЭНТИЙ АЙМГИЙН
БОР-ӨНДӨР СУМЫН СОЁЛЫН ТӨВИЙН
ДАРГЫН ТУШААЛ

2026 оны 03 сарын 30 өдөр Дугаар А/05 Бор-Өндөр сум

Байгууллагын мэдээллийн аюулгүй байдлыг
хангах журам батлах тухай

Монгол Улсын Засаг захиргаа, нутаг дэвсгэрийн нэгж, түүний удирдлагын тухай хуулийн 67 дугаар зүйлийн 67.5, Монгол улсын Засгийн газрын 2023 оны 224 дүгээр тогтоолын хавсралт, Хэнтий аймгийн Засаг даргын 2025 оны 06 дугаар сарын 09-ны өдрийн А/336 дугаар Захирамж, Бор-Өндөр сумын Засаг даргын 2026 оны 03 дугаар сарын 25-ны өдрийн 217 тоот албан бичгийг тус тус үндэслэн ТУШААХ нь:

1. Байгууллагын мэдээллийн аюулгүй байдлын бодлогыг хэрэгжүүлэх, мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмжтэй байдлыг хангах зорилгоор Байгууллагын мэдээллийн аюулгүй байдлыг хангах журмыг баталсугай.

2. Дээрх журмыг өдөр тутмын үйл ажиллагаандаа мөрдлөг болгон ажиллахыг байгууллагын нийт ажилтнуудад үүрэг болгосугай.

3. Байгууллагын мэдээллийн аюулгүй байдлыг хангах журмыг ажилтнуудад танилцуулах, сургалт сурталчилгааны ажлыг зохион байгуулж ажиллахыг өвийн ажилтан (М.Мөнхзул)-д үүрэг болгосугай.

ДАРГА М.ЧУЛУУНЦЭЦЭГ

Соёлын төвийн даргын
2016 оны 03 дугаар сарын 30-ны
өдрийн А/03 дугаар тушаалын хавсралт

БОР-ӨНДӨР СУМЫН СОЁЛЫН ТӨВИЙН МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ЖУРАМ

Нэг. Ерөнхий зүйл

1.1. Энэхүү журмын зорилго нь байгууллагын мэдээллийн технологи, систем, сүлжээ, өгөгдөл дотоод үйл ажиллагаатай холбоотой мэдээллийн аюулгүй байдлыг сахин хамгаалах, гадны халдлага, дотоод эрсдэлийг бууруулах, халдлагаас урьдчилан сэргийлэх, тасралтгүй ажиллагааг хангахад оршино.

1.2. 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 нэг удаа кибер аюулгүй байдлын эрсдэлийн үнэлгээ хийлгүүлж, шаардлагатай төлөвлөгөөг боловсруулна.

Гурав. Мэдээллийн технологийн хэрэглээ

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 дээш тэмдэгт, том, жижиг үсэг, тоо, тэмдэгт оролцуулах).

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 интернет ашиглахдаа мэдээллийн аюулгүй байдал, ес зүй, дотоод журмыг баримтлан, дараах төрлийн веб хуудас руу 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 веб, 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 (нэр@gmail.com) ашиглана.

5.2. Viber, Telegram, Messenger зэрэг олон нийтийн мессенжэр аппликейшнийг нууц, албан мэдээлэл дамжуулах зорилгоор ашиглахыг хориглоно. Зөвхөн албан зөвшөөрөгдсөн цахим шуудан болон төрийн мэдээллийн егр.е- mongolia.mn системийг ашиглана.

Зургаа. Нөөцлөлт ба мэдээллийн сан

6.1. Дотоод сүлжээний серверт хадгалагдах мэдээллийг улиралд нэг удаа 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 хамгаалалттай байх;

7.7.4. орох хаалганы дэргэд дүрст хяналтын системтэй байх;

7.7.5.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 жил бүр гаргах

8.3. Зөрчлийг бүртгэх, холбогдох байгууллагад мэдээлэх

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 байдал хариуцсан ажилтан дараах үүрэгтэй:

9.2.1.байгууллагын кибер аюулгүй байдлыг хангах өдөр тутмын үйл ажиллагааг хариуцан гүйцэтгэх;

9.2.2.холбогдох дүрэм, журмыг боловсруулах, шинэчлэх санаачлах

9.2.3. кибер аюулгүй байдлыг хангахад шаардлагатай үйл ажиллагаа, нөөцийг төлөвлөх;

9.2.4. кибер аюулгүй байдлыг хангах мэргэшүүлэх сургалтад хамрагдах.

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 халдлага, 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.

2025 03 20