ОРХОН АЙМГИЙН
ИРГЭДИЙН ТӨЛӨӨЛӨГЧДИЙН ХУРЛЫН
ДАРГЫН ЗАХИРАМЖ

2023 оны 12 дугаар сарын 11 Дугаар А/183 Баян-Өндөр сум

Мэдээллийн аюулгүй байдлыг хангах
журам шинэчлэн батлах тухай

Монгол Улсын Засаг захиргаа, нутаг дэвсгэрийн нэгж, түүний удирдлагын тухай хуулийн 48 дугаар зүйлийн 48.3 дахь хэсэг, Кибер аюулгүй байдлын тухай хуулийн 7 дугаар зүйлийн 7.2 дахь хэсэг, Монгол Улсын Засгийн газрын 2023 оны 06 дугаар сарын 07-ны өдрийн 224 дүгээр тогтоолоор батлагдсан “Кибер аюулгүй байдлыг хангах нийтлэг журам”-ын 1 дүгээр зүйлийн 1.2 дахь хэсэг, Мэдээллийн аюулгүй байдлын менежментийн тогтолцооны ISO 27001:2013 олон улсын стандартыг тус тус үндэслэн ЗАХИРАМЖЛАХ нь:

1.Аймгийн иргэдийн Төлөөлөгчдийн Хурлын байгууллагын “Мэдээллийн аюулгүй байдлыг хангах журам”-ыг хавсралтаар шинэчлэн баталсугай.

2.Журмын хэрэгжилтийг ханган, хяналт тавьж ажиллахыг аймгийн иргэдийн Төлөөлөгчдийн Хурлын Нарийн бичгийн дарга бөгөөд ажлын албаны дарга (Б.Ганзориг)-д даалгасугай.

ДАРГА Д.МӨНХБАТ

Аймгийн иргэдийн Төлөөлөгчдийн Хурлын даргын
2023 оны 12 дугаар сарын 11-ний өдрийн
А/183 дугаар захирамжийн хавсралт

АЙМГИЙН ИРГЭДИЙН ТӨЛӨӨЛӨГЧДИЙН ХУРЛЫН БАЙГУУЛЛАГЫН “МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ЖУРАМ”

Баримт бичгийн код: БҮЖ-08
Журмын агуулга

Нэг.Зорилго

1.1.Аймгийн иргэдийн Төлөөлөгчдийн Хурал (цаашид “байгууллага” гэх)-ын байгууллагын мэдээллийн систем, мэдээллийн сүлжээний кибер аюулгүй байдлыг хангах, кибер халдлага, кибер аюулгүй байдлын зөрчлийг илрүүлэх, хариу арга хэмжээ авах, урьдчилан сэргийлэх, нөхөн сэргээх болон оролцогч талуудын эрх, үүргийн харилцааг зохицуулахад оршино.

1.2.Аймгийн иргэдийн Төлөөлөгчдийн Хурал нь энэхүү журам, Кибер аюулгүй байдлыг хангах нийтлэг журам мөрдөнө.

1.3.Энэхүү журамд өөрчлөлт оруулах бол Кибер аюулгүй байдлыг хангах нийтлэг журмын 1.4-т заасныг удирдлага болгоно.

Хоёр.Хамрах хүрээ

Аймгийн иргэдийн Төлөөлөгчдийн Хурлын байгууллагын хэмжээнд мөрдөж ажиллана.

Гурав.Баримт бичгийн хариуцагч

3.1. Баримт бичгийг хариуцагч нь Бодлогын хэрэгжилт, иргэний оролцооны хэлтэс байна.

3.2. Журмыг 2 хувь үйлдэх бөгөөд нэг хувийг байгууллагын Дотоод ажил, архив, бичиг хэрэг хариуцсан мэргэжилтэнд, нөгөө хувь нь нарийн бичгийн дарга, хуулбарласан хувиуд нь хэлтсийн дарга нарт байна.

Дөрөв.Гүйцэтгэлийн хэмжүүр

4.1. Журмын хэрэгжилтийн тайлан

4.2. Бодлого, журамд өгөх өөрчлөлтийн саналын тоо, тэдгээрийн өөрчлөлтийн тоо

4.3. Бодлого, журмыг танилцуулсан бүртгэлийн жагсаалт

Тав.Нэр томьёоны тодорхойлолт, товчилсон үгс

1.Нэр томьёоны тодорхойлолт

1.1."**Антивирусын программ**" гэж компьютерыг вирусээс хамгаалах зориулалт бүхий программыг;

1.2."**Хамгаалалтын төхөөрөмж**" гэж сүлжээний хандалтыг зохицуулах төхөөрөмж /Firewall, router гэх мэт/;

1.3."**Virtual Private Network**(цаашид VPN гэх)" гэж нууцлалын тусгай алгоритм болон түлхүүрээр үүсгэсэн, мэдээллийг нууцлан дамжуулах сүлжээг:

1.4."**Зөөврийн төхөөрөмж**" гэж зөөврийн компьютер, зөөврийн диск, USB флаш диск, мемори карт, CD, DVD зэргийг;

1.5."**Серверийн сүлжээ**" гэж чухал сервер компьютеруудыг холбох зориулалттай, илүү хүчин чадалтай, бусад сүлжээнээс тусгаарлагдсан, энэхүү сүлжээ рүү хандах хандалтыг IP хаяг болон портоор хязгаарласан сүлжээг;

1.10."**Мэдээллийн хөрөнгө**" гэж мэдээлэл ба түүнийг хадгалах, дамжуулах, боловсруулах, зөөвөрлөх зориулалт бүхий бүхий л төрлийн мэдээллийн хэрэгсэл, тоног төхөөрөмж, зөөврийн төхөөрөмж, бусад системүүдийг ойлгоно;

2.Товчилсон үгийн тайлбар

МАБ-мэдээллийн аюулгүй байдал
БТХЭЗХ-Бодлого төлөвлөлт, хууль эрх зүйн хэлтэс
БХИОХ-Бодлогын хэрэгжилт, иргэний оролцооны хэлтэс
МАБХА-мэдээллийн аюулгүй байдал хариуцсан ажилтан
МАБ-мэдээллийн аюулгүй байдал
МТХХХА-мэдээлэл технологи хөгжүүлэлт, хэрэгжүүлэлт хариуцсан ажилтан

Зургаа.Мэдээллийн удирдлага

6.1.Нууцын зэрэглэл: Төрийн болон албаны нууцын тухай хууль болон холбогдон батлагдсан журмаар зохицуулна. (Аймгийн иргэдийн Төлөөлөгчдийн Хурлын даргын 2023 оны 10 дугаар сарын 06-ны өдрийн А/136 дугаар захирамжаар батлагдсан "Аймгийн иргэдийн Төлөөлөгчдийн Хурлын Төрийн болон албаны нууцын журам")

6.2.Нууц хариуцсан ажилтан нууцын зэрэглэлийг илэрхийлсэн тэмдэглэгээг тогтмол хийж, хяналт тавина.

6.3.Мэдээллийн аюулгүй байдал хариуцсан ажилтан нь жил бүр эсхүл шинээр мэдээлэл бий болсон, мэдээлэл эзэмшигч өөрчлөгдсөн зэрэг тохиолдолд маягт-04 дагуу мэдээллийн жагсаалт болон дамжуулах матрицид өөрчлөлт оруулах, шинэчлэх ажлыг ажлын 7 хоногийн дотор авч хэрэгжүүлнэ.

6.4.Мэдээллийн системийн зэрэглэл: Байгууллагын хэмжээнд ашиглаж буй мэдээллийн системийг чухал шинж чанараар нь маягт-05 заасны дагуу дараах байдлаар зэрэглэн ангилна. Үүнд:

6.4.1.Маш чухал: Байгууллагын үндсэн үйл ажиллагаандаа тогтмол ашигладаг бөгөөд зогсолт, доголдол нь байгууллагын нэр хүнд, ашигт ажиллагаанд сөргөөр нөлөөлөх системүүд;

6.4.2.Чухал: Байгууллагын дотоод үйл ажиллагаанд тогтмол ашигладаг бөгөөд зогсолт саатал доголдол нь өдөр тутмын үйл ажиллагааг удаашруулах системүүд;

6.4.3.Ердийн: Байгууллагын үйл ажиллагаанд дэмжлэг үзүүлэх зорилготой саатал доголдол нь шууд хохирол учруулахгүй системүүд;

6.5.Мэдээлэл боловсруулалт

6.5.1.Мэдээллийн хөрөнгийг боловсруулах үйл ажиллагааг нууцын зэрэглэлээс хамаарч Аймгийн иргэдийн Төлөөлөгчдийн Хурлын "Төрийн болон албаны нууцын журам"-д заасан дагуу хэрэгжүүлнэ.

6.5.2.Нийт албан хаагчид албаны үйл ажиллагаандаа e-office.erdenet.mn программ хангамжийг ашиглана.

6.5.3.Албан хаагч ажлаас чөлөөлөгдсөн, халагдсан тохиолдолд e-office.erdenet.mn программ хангамжийг ашиглах эрхийг ажил хүлээлцсэн өдрөөс эхлэн дуусгавар болно.

6.6.Мэдээлэл хадгалах, дамжуулах

6.6.1.Байгууллагын мэдээлэл хадгалдаг, боловсруулдаг, дамжуулдаг компьютер, зөөврийн төхөөрөмжийг нууц үгээр хамгаалсан байна.

6.6.2.Албан хаагч бүр өөрийн ажил үүргийн хүрээнд хариуцаж байгаа эсхүл албан үүрэг мэргэжлийн үйл ажиллагааны дагуу танилцсан, олж мэдсэн нууцын зэрэглэлтэй мэдээллийг чанд хадгалах үүрэгтэй ба бусдад аливаа хэлбэрээр задруулах үйлдэл, эс үйлдэл хийхийг хориглоно.

6.6.3.Мэдээллийн хөрөнгийг хадгалах, хамгаалах, дамжуулах, устгах үйл ажиллагааг нууцын зэрэглэлээс хамаарч аймгийн иргэдийн Төлөөлөгчдийн Хурлын "Төрийн болон албаны нууцын журам"-д заасан дагуу хэрэгжүүлнэ.

6.6.4.Мэдээллийн жагсаалт болон дамжуулах матрицын дагуу байгууллагын хэмжээнд ашиглаж буй мэдээллийн хөрөнгийг дамжуулна.

6.6.5.Зөөврийн төхөөрөмж дахь байгууллагын мэдээллийг хянах, удирдах, устгах боломжтой нэгдсэн удирдлага бүхий байдлаар тохируулж болно.

6.6.6. Мэдээллийн технологи, хөгжүүлэлт хариуцсан ажилтан нь албан хаагч бүрийн ажлын шаардлагаар ашигладаг зөөврийн төхөөрөмж дэх байгууллагын мэдээллийн хамгаалалтын дараах арга хэмжээг тогтмол авч хэрэгжүүлэн, түлхүүрийг чандлан хадгална. Үүнд:

- Зөөврийн мэдээлэл тээгч: Нууц үгээр хамгаалсан байх
- Зөөврийн компьютер: 3DES, SHA-2, AES256 гэх мэт сайн туршлагаар хүлээн зөвшөөрөгдсөн алгоритм ашиглан үйлдлийн системтэй хатуу дискийг энкриптлэнэ.
- Энкриптийн түлхүүрийг нууц үгээр хамгаалж хадгална.

6.6.7.Албан хаагч нь зөөврийн мэдээлэл тээгчийг албаны хэрэгцээнд 6.6.6 мэдээллийн технологи, хөгжүүлэлт хариуцсан ажилтны хяналтын дор ашиглаж болно.

6.6.8.Байгууллагын хэмжээнд ашиглагдаж буй байгууллагын болон албан хаагчийн өмчлөлийн бүх зөөврийн төхөөрөмж болон тээгчийг дараах утгаар ойлгоно. Үүнд:

- Зөөврийн төхөөрөмж гэж авч явахад хялбар тооцоолох чадвартай процессор санах ой хадгалах бүрдэл хэсэг бүхий төхөөрөмжүүдийг
- Зөөврийн тээгч гэж тооцоолох төхөөрөмж ажиллаж байх үед түүнд залгаж салгаж авч болдог өгөгдөл хадгалах зориулалттай аливаа төрлийн жижиг төхөөрөмжүүдийг.

6.6.9.Зөөврийн тээгчийг ажлын компьютерт залгаж ашиглана. Мэдээлэл технологи хөгжүүлэлт, хэрэгжүүлэлт хариуцсан ажилтны зөвшөөрөлгүйгээр байгууллагын өмчид бүртгэлтэй зөөврийн тээгчийг байгууллагын өмчид бүртгэлгүй өөр бусад компьютерт холбох, түүн дээр ашиглахыг хориглоно.

6.6.10.Зөөврийн төхөөрөмж, тээгчийг дараах байдлаар хэрэглэхийг зөвшөөрнө:

6.6.10.1.Өөрийн үндсэн үйл ажиллагаа чиг үүргээ гүйцэтгэх;

6.6.10.2.Цаг агаарын болон бусад нийгмийн мэдээлэлд хандах;

6.6.10.3.Цахим захиа шалгах, бичих, харилцах;

6.6.10.4.Шуурхай харилцах хэрэгслүүд ашиглах;

6.6.10.5.Хөдөлмөрийн бүтээмж дээшлүүлэх төрөл бүрийн программ хэрэглээнүүдийг ашиглах;

6.6.11.Албан хаагч бүр компьютер, зөөврийн төхөөрөмж дээрх мэдээллийг үүлэн технологи болон серверт давхар хадгалж болно.

6.7.Хандах эрх

6.7.1. Мэдээлэл, түүнийг агуулж байгаа мэдээллийн систем, мэдээллийн сүлжээнд зөвшөөрөлгүй хандах, дамжуулах, өөрчлөх, устгахаас хамгаалж хандалтын удирдлагыг мэдээлэл технологи хөгжүүлэлт, хэрэгжүүлэлт хариуцсан ажилтан хариуцна.

6.7.2. МТХХХА мэдээлэл, түүнийг агуулж байгаа мэдээллийн систем, мэдээллийн сүлжээнд хандах эрхийг хүний нөөцийн асуудал хариуцсан нэгжээс маягт-1 дагуу зөвшөөрөл авсаны үндсэн дээр олгож, маягт-2 дагуу бүртгэл хөтөлж, хяналт тавьж ажиллана. Тухай бүр шаардлагатай өөрчлөлтийг оруулж болно.

6.7.3. Байгууллагын мэдээллийн систем, мэдээллийн сүлжээнд давуу эрхтэй хандах этгээд нь МАБХ ажилтан, мэдээлэл технологи хөгжүүлэлт, хэрэгжүүлэлт хариуцсан ажилтан нар байна.

6.8. Өөрчлөлтийн удирдлага

6.8.1.Байгууллагын кибер аюулгүй байдалд нөлөөлж болох бүхий л өөрчлөлтийг маягт-03 дагуу бүртгэх бөгөөд бүртгэлийг мэдээлэл технологи хөгжүүлэлт, хэрэгжүүлэлт хариуцсан ажилтан бүртгэнэ.

6.9.Харилцаа холбоо

6.9.1.Байгууллага нь харилцаа холбооны матрицыг маягт-06 дагуу тодорхойлж удирдлага болгон ажиллана.

6.9.2.Мэдээлэл эзэмшигчид нь жил бүр харилцаа холбооны матрицыг шинэчлэн МАБХ ажилтанд хүргүүлнэ.

6.9.3.МАБ хариуцсан ажилтан нь мэдээлэл эзэмшигчдээс ирүүлсэн матрицыг хянан, нэгтгэж Ажлын албаны даргаар хянуулж батлуулна.

6.9.4. МАБ хариуцсан ажилтан нь батлагдсан харилцаа холбооны матрицыг байгууллагын албан хаагчдад хүргүүлэх бөгөөд хэрэгжилтийн явцад хяналт тавьж ажиллана.

6.10.Хяналт хэмжилт

6.10.1.МАБХ ажилтан нь мэдээллийн аюулгүй байдлын гүйцэтгэл, мэдээллийн аюулгүй байдлын тогтолцооны үр дүнг жил бүр хяналт хэмжилтийн журмыг үндэслэн үнэлж Ажлын албаны даргад танилцуулна.

6.10.2.Энэхүү журмын 6.10.1-д заасны дагуу хяналт хэмжилтийг хийхэд нэгжүүд шаардлагатай мэдээллээр хангаж ажиллана.

6.10.3.Ажлын албаны дарга нь 6.10.1-д заасан үр дүнг тухай бүр Хурлын даргад танилцуулна.

6.4.Кибер аюулгүй байдлын эрсдэл авч хэрэгжүүлэх арга хэмжээ

6.4.1.МАБ-н эрсдэлийн үнэлгээг дотооддоо жилд 2 удаа үнэлнэ.

Долоо. Зохистой хэрэглээ

7.1.Нууц үг

7.1.1.Албан хаагч нь төхөөрөмжид нэвтрэхэд нууц үг ашиглах ба системээс үүсгэсэн анхны нууц үгийг заавал сольдог байна.

7.1.2.Албан хаагч нь нууц үгийн шаардлагыг дараах байдлаар хангана. Үүнд:

- Тэмдэгтийн урт 8-аас дээш байх
- Том үсэг, жижиг үсэг цифр тусгай тэмдэгт ашиглах
- Хагас жил бүр эсвэл түүнээс богино хугацаанд тогтмол сольдог байх
- Зөвхөн хэрэглэгч өөрөө мэддэг байх буюу бусадтай хуваалцахгүй байх
- Хэрэглэгчийн нэрээс өөр байх
- Өөрийн хүүхэд эцэг эх ах дүүгийн нэр төрсөн он сараар өгөхгүй байх
- Амархан тааж болох утасны дугаар болон дараалсан тоо өгөхгүй байх

7.2.Мэдээллийн технологи, хөгжүүлэлт хариуцсан ажилтан нууц үгийн, чанарын шаардлага хангасан эсэхэд хяналт тавьж, тохиргоо хийнэ.

7.3.Компьютер дотоод системийн нууц үгийг бусдад ашиглуулах, дамжуулахыг хатуу хориглоно.

7.4.Цэвэр ширээ, цэвэр дэлгэц

7.4.1.Ажлын компьютер, тоног төхөөрөмжийг ашиглахгүй байгаа үед албаны болон нууц мэдээлэл агуулсан цаасан суурьтай баримт бичиг, цахим мэдээлэл агуулсан санах төхөөрөмж, тээгч, аппарат хэрэгслүүд зохих түвшинд хамгаалагдсан байна

7.4.2.Албан хаагч нь нууц мэдээлэл бүхий бүх баримт бичиг, түүнийг агуулсан зөөврийн мэдээлэл тээгчийг түгжээтэй шургуулга, шүүгээнд хийж түгжинэ.

7.4.3.Шургуулга, шүүгээний цоожны түлхүүрийг ил задгай орхихыг хориглоно.

7.4.4.Төрийн болон албаны нууц мэдээлэл хэвлэсэн байж болох бүх цаасан хог хаягдлыг хогийн тусгай саванд хийж дараа нь сэргээх боломжгүйгээр устгаж байна. Ийм хог хаягдлыг ердийн хогийн саванд хийхийг хориглоно.

7.4.5.Албан хаагч нь ажлын байраа 5 минутаас дээш хугацаагаар орхин явах үедээ компьютер дэлгэцээ заавал түгждэг байна.

7.4.6.Шуудан хүлээн авах, илгээх цэгийг зохих ёсоор хамгаалж, принтер, факсын аппаратыг байнгын хараа хяналтад байлгана.

7.4.7.Олшруулагч төхөөрөмж, сканер, дижитал камер, гар утас, бусад олшруулагч төхөөрөмжийг зөвшөөрөлгүй ашиглахаас хамгаалж зохих код, нууц үгээр хамгаалсан байна.

7.4.8.Цахим баримт бичгийг десктоп – desktop дээр хадгалахыг хориглоно. Хатуу диск дээр болон хамгаалагдсан хавтаст хадгална. Албаны болон нууц мэдээллийг шифрлэлтийн журмын дагуу шифрлэн хадгална.

7.4.9.Ажлаасаа тарах үед ширээн дээр байгаа бүх баримт бичгийг хурааж цоожтой саванд хийж түгжинэ.

7.5.Компьютер

7.5.1.Албан хаагч нь суурин болон зөөврийн компьютерыг албан хэрэгцээний зориулалтаар ашиглана.

7.5.2.Албан хаагч нь зөөврийн компьютерыг гадуур ашиглах үедээ хулгайд алдах, гээх болон ашиглах явцад эвдэрч гэмтсэнээс шалтгаалан мэдээлэл алдагдах урьдчилан сэргийлж хадгалж хамгаална. Хараа хяналтгүй орхихгүй байна.

7.5.3.Байгууллагын компьютер, тоног төхөөрөмжид зөвшөөрөлгүй гадны төхөөрөмж холбох, мэдээлэл авах, солилцох болон албан хэрэгцээний бус мэдээллийг хадгалахгүй байна.

7.5.4.Мэдээллийн технологи, хөгжүүлэлт хариуцсан ажилтан олон нийтийн газар байрлаж буй дэлгэцэн компьютер, сүлжээний принтер зэрэг нийтийн хандалттай тоног төхөөрөмжийг байгууллагын камерын тусгалд харагдахаар байрлуулсан байна.

7.5.5.Албан хаагч нь суурин болон зөөврийн компьютерыг хувийн хэрэгцээнд ашиглахыг хориглоно.

7.5.6.Байгууллагын тоног төхөөрөмжийн засвар үйлчилгээг мэдээллийн технологи хариуцсан ажилтан оношилж засварлуулна.

7.6.Хэрэглээний программ хангамж

7.6.1.Мэдээлэл технологи хөгжүүлэлт, хэрэгжүүлэлт хариуцсан ажилтан нь байгууллагад ашиглах хэрэглээний программ хангамжийн жагсаалтыг маягт-07 дагуу гаргах бөгөөд байгууллага зөвшөөрснөөс бусад төрлийн программ хангамжийг ашиглахгүй.

7.6.2.Байгууллагын нэгжүүдэд мэдээлэл, мэдээллийн системийн техник болон программ хангамжийг санаатай болон санамсаргүй үйлдэл, зөвшөөрөгдөөгүй хандалт, өөрчлөлт, буруу үйлдэл, тохиргоо, алдагдлаас хамгаалах зорилгоор техник болон программ хангамжийн боловсруулалт, нийлүүлэлт, суурилуулалт, тохиргоо, үйлчилгээг ижил төвшинд гүйцэтгэнэ.

7.6.3.Техник болон программ хангамжид өөрчлөлт оруулах, вирусээс хамгаалах, тохиргоог өөрчлөх гэх мэт үйлдлийг хийхдээ мэдээлэл технологи хөгжүүлэлт, хэрэгжүүлэлт хариуцсан ажилтнаар гүйцэтгүүлж, холбогдох бүртгэлийг маягт-08 дагуу хөтөлнө.

7.6.4.Байгууллагын программ хангамжийн мэдээллийн аюулгүй байдал нь байгууллагын худалдаж авсан буюу дээд байгууллагаас нийлүүлсэн,

боловсруулсан систем, мэдээллийн сан, программ хангамж, тусгай хэрэгслийн тохиргооны цогц байна.

7.6.5.Программ хангамжийг дараах байдлаар хамгаална. Үүнд:

- Тухайн программ хангамжийн боломжит бүх хамгаалалтыг ашиглах;
- Шаардлагагүй программ хангамжийг суурилуулахгүй байх;
- Программ хангамжийн үйлдвэрлэгчийн түлхүүр үгийг хадгалах;
- Хэрэглээний болон үйл ажиллагааны программ хангамжийг сайтар эзэмших;
- Программ хангамжийн тусгай файл руу хандах эрхийг хязгаарлах;
- Системийн программ хангамж руу хандах эрхийг хязгаарлах;

7.7.Цахим шуудан

7.7.1.Нийт албан хаагчид албаны үйл ажиллагаанд хувийн цахим шуудан, олон нийтийн сувгийг ашиглах, түүгээр дамжуулан мэдээлэл зөөвөрлөх, хадгалахыг хориглоно.

7.7.2.Албаны хэрэгцээнд зөвхөн дотоод e-office.erdenet.mn цахим шуудан болон албаны mail.gov.mn хаягийг ашиглана.

7.7.3.Албан хаагч ажлаас чөлөөлөгдсөн тохиолдолд e-office.erdenet.mn цахим шуудан болон албаны mail.gov.mn хаягийг ашиглах эрхийг ажил хүлээлцсэн өдрөөс эхлэн дуусгавар болно

7.8.Сүлжээ

7.8.1.Албан хаагчид нь дотоод хэрэгцээнд тохируулсан хэрэглэгчийн сүлжээг албан хэрэгцээндээ ашиглана.

7.8.2.Албан хаагчид нь дотоод сүлжээнд холбогдсон Компьютер, ухаалаг гар утас гэх мэт төхөөрөмжөөс утасгүй сүлжээ /hotspot/ цацахыг хориглоно.

7.8.3.Сүлжээний аюулгүй байдал, үйлчилгээг мэдээлэл технологи хөгжүүлэлт, хэрэгжүүлэлт хариуцсан ажилтан хариуцна.

7.9.Хөрөнгийн устгал

7.9.1.Компьютер, зөөврийн төхөөрөмжийг бусдад шилжүүлж байгаа болон ашиглалтаас гаргасан тохиолдолд өөр дээр нь хадгалагдах бүхий л мэдээллийг дахин сэргээгдэхгүйгээр устгана,

7.9.2.Серверийн хард зэрэг мэдээлэл агуулсан төхөөрөмжийг биет байдлаар эвдэж устгана.

7.9.3.Цаасан материал болон дискийн цаашид ашиглагдахгүй болсон хувийг тэр даруй цаас устгагчаар устгана.

Найм.Хяналтын тогтолцоо

8.1.Хууль тогтоомжийн нийцэл

8.1.1. БТХЭЗХ жил бүр болон холбогдох хууль шинээр батлагдсан, нэмэлт өөрчлөлт орсон даруй хуулийн нийцлийн үнэлгээг гаргана.

8.1.2. Ажлын албаны дарга хуулийн нийцлийн үнэлгээг үндэслэн хуулийн нийцлийн хэрэгжилтийг хангахыг холбогдох нэгжүүдэд үүрэг болгож, хяналт тавьж ажиллана.

8.1.3.Нэгжүүд хуулийн нийцлийг хангахдаа БТХЭЗХ ирүүлсэн зөвлөмж, дүгнэлтийг удирдлага болгон ажиллана.

8.1.Оюуны өмч

8.1.1.Бусдын оюуны өмчийн программ хангамж, үйлдлийн системийг албан ёсны эрхтэйгээр ашиглана.

8.1.2.Байгууллагын дотоодод хөгжүүлсэн программ хангамж болон бусад оюуны бүтээлийн зохиогчийн эрхийг байгууллагын өмчид тооцно.

8.1.3.Байгууллагын захиалгаар гэрээний дагуу хийгдэж буй бүхий л оюуны бүтээл, барааны тэмдэг байгууллагын өмч байна.

8.2.Нийлүүлэгч

8.2.1.Гэрээгээр ажил, үйлчилгээ үзүүлэх, бараа бүтээгдэхүүн нийлүүлэх зэрэг нийлүүлэгчтэй байгуулж буй гэрээнд КАБ-тай холбоотой дараах заалтууд тусгаж ажиллана. Үүнд :

- Хандах эрхтэй мэдээллүүд, тэдгээрт хандах аргууд;
- Талууд харилцан тохиролцсон үүрэг болон хяналт (хандалтыг хянах, гүйцэтгэлийг шалгах, мониторинг тайлагналт болон аудит);
- Мэдээллийн зохистой болон зохисгүй хэрэглээний заалтууд;
- Нийлүүлэгч талаас харилцах ажилтны мэдээлэл, тухайн ажилтны мэдээлэлд хандах, хүлээн авах эрхийн зөвшөөрөл олгох болон зөвшөөрөл цуцлах нөхцөл;
- КАБ-тай холбоотой тусгай шаардлагууд, тэдгээртэй холбоотой үүсэн гарах аливаа асуудлыг хоёр талаас хариуцах ажилтны мэдээлэл;
- Сүлжээний тоног төхөөрөмж, сервер тоног төхөөрөмж худалдан авах тохиолдолд Ажлын албаны даргад танилцуулна.

Ес.Бодит орчны аюулгүй байдал

9.1.Байгууллагын хамгаалагдах орон зайг “Хамгаалагдах орон зайн бүдүүвч зураг”-н дагуу тодорхойлно.

9.3.Хамгаалагдах орон зайд мэдээлэл технологи хөгжүүлэлт, хэрэгжүүлэлт хариуцсан албан хаагч нэвтрэх ба хяналт тавих чиг үүргийн хүрээнд БХИОХ-ийн ахлах мэргэжилтэн, нэгжийн дарга, Ажлын албаны дарга, Хурлын дарга нар тус тус нэвтэрнэ. Шаардлагатай тохиолдолд зочныг удирдлагын зөвшөөрлийн нэвтрүүлж болно.

9.4. Мэдээлэл технологи хөгжүүлэлт, хэрэгжүүлэлт хариуцсан ажилтан нь хамгаалагдах орон зайд нийт албан хаагч болон зочныг нэвтрүүлэхэд бүртгэлийг маягт-08 дагуу хөтөлж, хяналт тавина.

9.5.Нэвтрэх хаалга нь өөр дээрээ лог бүртгэдэг байж болно.

9.6.Орц, гарцыг камерын тугалд оруулсан байх ба камерын тасралтгүй ажиллагааг хангана.

9.7.Мэдээллийн хөрөнгө гадагш зөөвөрлөх

9.7.1.МАБХА мэдээллийн хөрөнгө зөөвөрлөх эрх бүхий албан хаагчдыг маягт-09 дагуу гарган Ажлын албаны даргаар батлуулна.

9.7.2.Албан хаагч нь мэдээллийн хөрөнгийг Ажлын албаны даргын зөвшөөрлийн дагуу зөөвөрлөнө. Зөвшөөрлийг маягт-10 дагуу гаргаж бүртгэлийг маягт-11 дагуу хөтлөнө.

9.7.3.Нууц мэдээлэл гадагш зөөвөрлөх, зөвшөөрөх асуудлыг аймгийн иргэдийн Төлөөлөгчдийн Хурлын “Төрийн болон албаны нууцын журам”-д заасан дагуу хэрэгжүүлнэ.

9.8.Гадны болон орчны аюулаас хамгаалах

9.8.1.Байгууллагын үндсэн байр байшинд учирч болох аюулаас хамгаалахын тулд ослын нөхцөлд ажиллах төхөөрөмжүүд болон нөөц хуулбар хадгалдаг тээгчийг аюулгүй өөр байрлалд байрлуулсан байна.

9.8.2.Гал түймэртэй тэмцэх тоног төхөөрөмж, хэрэгслүүдийг хангаж зохих газарт нь байрлуулсан байна.

9.9.Тоног төхөөрөмжийн аюулгүй байдал

9.9.1.Мэдээлэл технологи хөгжүүлэлт, хэрэгжүүлэлт хариуцсан ажилтан нь үйл ажиллагаа явуулахад ашиглагдаж буй тоног төхөөрөмжүүдийг зохих журмын дагуу унтраах, тасралтгүй ажиллуулахын тулд тасалдалгүй тэжээлийн аппарат (UPS – ТТА) ашигладаг байна.

9.9.2.Мэдээллийн технологи хөгжүүлэлт, хэрэгжүүлэлт хариуцсан ажилтан тохиолдлоор буруу кабель суурилуулах гэх мэт засвар, үйлчилгээний алдааг багасгахын тулд кабель бүрд тэмдэглэгээ хийж болно.

Арав .Хариуцлага

10.1.Энэхүү журам нь дагаж мөрдөх ерөнхий хэм хэмжээ бөгөөд журмаар хүлээсэн үүргээ гүйцэтгээгүй бүх тохиолдлыг зөрчил гэж үзэн ***“Хөдөлмөрийн дотоод журам”***-н дагуу шийдвэрлэнэ.

Арван нэг. Өөрчлөлтийн тэмдэглэл

Хувилбар	Өөрчлөлт оруулсан огноо	Өөрчлөлтийн утга	Өөрчлөлт оруулсан ажилтан
1	2	3	4
Хувилбар-1	Аймгийн ИТХ-ын даргын захирамж 2019.01.31 А/04	Батлагдсан хуулийн дагуу боловсруулсан.	Нарийн бичгийн дарга
Хувилбар-2	Аймгийн ИТХ-ын даргын захирамж 2023.09.06 №А/118	Шинэчлэгдэн батлагдсан хууль, ISO 27001:2013 стандартын дагуу боловсруулсан.	Төслийн баг
Хувилбар-3	Аймгийн ИТХ-ын даргын захирамж 2023.12.11 №А/183	Шинэчлэгдэн батлагдсан хууль, ISO 27001:2013 стандартын дагуу боловсруулсан.	Төслийн баг

Арван хоёр. Холбогдох маягтууд

Маягт- БҮЖ-08-01

МЭДЭЭЛЛИЙН СИСТЕМИЙН ХАНДАХ ЭРХ НЭЭХ,
ХААХ ЗӨВШӨӨРӨЛ ОЛГОХ ХУУДАС

20... он .... сар .... өдөр

..... овогтой ..... нь ..... байгууллагын .....хэлтэст ..... албан тушаалд ажиллах тул и-мэйл хаяг, шаардлагатай программ хангамж, эрхийг /нээх, хаах/ бэлэн болгож өгнө үү.

Хэлтэс/нэгжийн удирдлага /...../
ХНМенежер /...../

Д/д	Ангилал	Үндсэн программ хангамж, эрх нээх	Сонгоно уу
1	Системийн эрх нээлгэх	Eoffice.erdenet.mn	
		Orkhon.mlsp.mn	
2	Майл дотоод сүлжээ	И-мэйл хаяг	
		Gmail хаяг	
		Групп И-мэйл хаяг-т нэгтгэх	
		Дотоод сүлжээ	
		Facebook, youtube	
	Зургийн программ	Corel draw	
		Photoshop	
		Boria	
		Tak viewer	
		Autocad	
		3d max	
	MS	Хэрэглээний программ	
	Бусад		
Нийт нээлгэх эрхийн тоо			

Маягт- БҮЖ-08-02

МЭДЭЭЛЛИЙН СИСТЕМ, МЭДЭЭЛЛИЙН СҮЛЖЭЭНД
ХАНДАХ ЭРХИЙГ ОЛГОХ БҮРТГЭЛ

Д/д	Эрх нээлгэсэн, хаалгасан албан тушаалтан	Он сар өдөр	Эрх нээх	Эрх хаах	Хяналт тавих албан тушаалтны гарын үсэг	Эрх нээлгэсэн, хаалгасан албан тушаалтны гарын үсэг
1						

Маягт- БҮЖ-08-03

ӨӨРЧЛӨЛТ БҮРТГЭЛИЙН ХУУДАС

Д/д	Өөрчлөлтийн төрөл	Өөрчлөлт орсон процесс/систем	Агуулга	Өөрчлөлтийн огноо	Өөрчлөлт оруулах хүсэлт гаргасан нэгж	Өөрчлөлт оруулсан нэгж

Маягт- БҮЖ-08-04

МЭДЭЭЛЛИЙН ЖАГСААЛТ БОЛОН ДАМЖУУЛАХ МАТРИЦ

Д/д	Мэдээлэл	Ангилал	Хамрагдах нэгж	Дамжуулах суваг	Хадгалагдах байршил	Хандах эрхтэй ажилтан	Эрх олгох ажилтан

Маягт-БҮЖ-08-05

СИСТЕМИЙН ЖАГСААЛТ

№	Системийн нэр
Байгууллага	
Төрөл	
Систем хариуцагч	
Систем эзэмшигч	
Сервер	
Үйлдлийн систем	
Лиценз шаардлагатай эсэх	
IP хаяг	
Ач холбогдолын зэрэглэл	
Гадаад хандалттай эсэх	
VPN хандалттай эсэх	
Гарын авлага	
Энкрипшн шаардлагатай эсэх	
Backup авах хуваарь	
Redundant төхөөрөмж шаардлгатай эсэх	
Redundant төхөөрөмж байгаа эсэх	

Маягт-БҮЖ-08-06

ХАРИЛЦАА ХОЛБООНЫ МАТРИЦ

Төрөл	Юу мэдээллэх	Хэзээ мэдээллэх	Хэнд мэдээллэх	Хэн мэдээллэх	Хэрхэн мэдээллэх

Маягт- БҮЖ-08-07

ХЭРЭГЛЭЭНИЙ ПРОГРАММ ХАНГАМЖИЙН ЖАГСААЛТ

№	Программ хангамж нэр
Газар, нэгж:	
Албан тушаал:	
Заавал суулгах программ хангамж:	
Нэмэлтээр суулгаж болох программ хангамж:	
Суулгахыг хориглох программ хангамж:	

Маягт- БҮЖ-08-08

ХАМГААЛАГДСАН ОРОН ЗАЙД НЭВТРЭСЭН БҮРТГЭЛ

Д/д	Огноо	Нэвтрэсэн албан тушаалтан	Нэвтэрсэн зочины ово нэр	Шалтгаан	Зөвшөөрөл олгосон албан тушаалтан	Орсон цаг	Гарсан цаг

Маягт- БҮЖ-08-09

МЭДЭЭЛЛИЙН ХӨРӨНГӨ ЗӨӨВӨРЛӨХ ЭРХ БҮХИЙ АЖИЛТНУУДЫН ЖАГСААЛТ

№	Хэлтэс, нэгж	Албан тушаал	Овог нэр	Мэдээллийн хөрөнгө

Маягт- БҮЖ-08-10

МЭДЭЭЛЛИЙН ХӨРӨНГӨ ЗӨӨВӨРЛӨХ ЗӨВШӨӨРЛИЙН ХУУДАС

..... байгууллагын ..... хэлтэс ..... албан тушаалтан ..... ажилтан нь ..... шаардлагын улмаас .....-с ..... -ны хооронд

□Цахим мэдээлэл □Зөөврийн хард диск

□Цаасан мэдээлэл □Суурин компьютер

□CD/ DVD □Таблет

□Флаш □Бусад / /-г авч гарах зөвшөөрөл олгоно уу.

Хүсэлт гаргасан:
Хүсэлт баталгаажуулсан:
Мэдээлэл эзэмшигч:
Огноо:

Хүсэлт хянан шийдвэрлэсэн:
Ажлын албаны дарга:
Огноо:

Тайлбар:

Маягт- БҮЖ-08-11

МЭДЭЭЛЛИЙН ХӨРӨНГӨ ЗӨӨВӨРЛӨСӨН БҮРТГЭЛ

Д/д	Хэлтэс, нэгж	Албан тушаал	Овог нэр	Мэдээллийн хөрөнгө

Арван гурав. Хавсралт

Мэдээлэл технологийн аюулгүй байдлын ерөнхий шаардлага

	[redacted]	• Администратор бусдын мэйл рүү нэвтрэхэд хяналтын нэгжид мэдэгдэл ирдэг тохиргоотой байх • Газар нутгийн хувьд ялгаатай бүсэд log in хийхэд хязгаарлагдмал тохиргоотой байх • Мэйл энкрипшнтэй байх • 2 глобал администтай байх. Нэг админ Lockout болоход нөгөө администаар тохируулах
		• Имэйлийн хавсралт автоматаар шалгадаг байх • Зөөврийн мэдээлэл тээгч холбогдоход автоматаар шалгадаг байх • 7 хоног бүр Full scan хийдэг байх • Өдөр бүр Quick scan хийдэг байх
		• Маш чухал системийн back-up -ийг өдөр бүр авч тусдаа байршилд хадгалах • Сард нэг удаа back-up бүрэн авагдаж байгааг шалгах • Сард нэг удаа back-up -ийг сэргээх туршилт хийх • Жилд нэг удаа системийг бүрэн сэргээх туршилт хийх
		Sharing (SharePoint Online and OneDrive for Business) • Зөвхөн дотоод сүлжээнд ашигладаг байх • Байгууллагын Onedrive -с бусад сүлжээнд хуваалцах боломжгүй байх • Компанийн интранет sharepoint -д байрладаг байх
		• Хувийн хэрэгцээнд зөвхөн зочны сүлжээнд холбоно; • Албаны хэрэгцээнд ашиглах бол MDM, intune суулгасан байна • Нууц үгээр хамгаалдаг байх
		• Зөөврийн хэрэгсэл эсвэл төхөөрөмжийг нууц үгээр хамгаалах. • Бүх зөөврийн зөөврийн хэрэгсэл эсвэл төхөөрөмжүүдийн "Autorun" болон "Autoplay" функцийг идэвхгүй болгох • Зөөврийн мэдээлэл тээгчийг ашиглаж дууссан даруй тэр төхөөрөмж дээрх мэдээллийг устгадаг байх
		• Компьютер давхцахгүй нэршилтэй байх; • Үйлдлийн систем асаах нууц үгтэй байх; • Чухал файлуудыг нууц үгээр хамгаалах, нууц үг стандарт шаардлагыг хангасан байх • Файлуудыг үйлдлийн систем суугаагүй партишн дээр хадгалах • Антивирусийн програм суулгасан байх; • Файрвол нээлттэй байх; • Зөөврийн компьютерыг оффист болон гадуур ажиллаж байх үед зориулалт бүхий цоожлогчоор цоожилж байх; • Зөөврийн компьютерын хард дискт шифрлэлт хийсэн байх;
		• MAC хаяг бүртгэнэ • Байгууллагын тус бүрийн сүлжээ тусгаар байна

		• Сүлжээний үндсэн болон аюулгүй байдлын тохиргоонуудыг жил бүр шалгах • Зочны сүлжээ шууд интернэт хандалттай байх
		• Software update хийсэн байх; • 12 тэмдэгтээс дээш нууц үгээр хамгаалсан байх; •
		• • • •
		• Нууц үг хамгийн сүүлийн үеийн шифрийн алгоритм ашиглах (WPA2, 802.b.n.g.a) • 6 сард нэг удаа нууц үгийг солих • Зочны Wi-Fi тай байх
		• Нууц үгээр нэвтэрдэг байх
		• Системийн бүртгэлийн Log файлуудыг 7 хоног бүр шалгаж, алдаа бүртгэгдсэн тохиолдолд засварлах арга хэмжээ авах (System log Access, log Security log Cron, Log); • Лог файлуудыг шалгасан мөн засварласан арга хэмжээ авсан талаар бүртгэл хөтлөн, тайлагнах; • Файл болон фолдерт хандах эрхийн түвшинг хянах; • Лог файлыг үүсгэн 3 сараар хадгалах; • Вэб серверийн нэр болон хувилбарын дугаар, алдааны мэдээлэл зэргийг нуух; • Сүлжээний тохиргоонд TCP/IP түвшинд шүүлтүүр тавих; • Шаардлагагүй портуудыг хаах, iptables дээр сэжигтэй пакетуудыг оруулахгүй байх; • Вирусийн засваррам суулгаж, нэмэлт өөрчлөлт шинэчлэлтийг хийх.
		• Кабельд замаас нь холбогдох, кабель шугамыг гэмтээхээс хамгаална: • Кабелуудыг тэмдэгжүүлнэ;
		• Биет орчны аюулгүй байдлыг хангах; • Холболтын аюулгүй байдлыг хангах; • Хүчтэй нууц үг ашиглах; • Update тогтмол хийх; • Галт хана ашиглан хандалтыг хязгаарлах
		• Системийн цар хүрээнээс хамааруулан өгөгдлийн сан удирдах системийг тодорхойлох бөгөөд програм хангамж нь өгөгдлийн сантай холбогдох тусгай нэр, нууц үг ашигладаг байх • Системийн сангийн хүснэгтүүд болон хүснэгтийн баганууудын нэр нь түүнд агуулагдаж буй мэдээлэлтэй холбоотой англи үгээр тодорхойлогдсон байх • Системийн өгөгдлийн санд нэг мэдээллийг олон газар хадгалахаас зайлсхийсэн байх • Системд өгөгдлийн сангийн хүснэгт хоорондын хамаарлын холбоос /database relationship/-ыг тогтоож өгсөн байх

	[redacted]	• Системийн өгөгдлийн санд нэмэгдсэн мөр бүхэн нь хэзээ, хэн тухайн мэдээллийг нэмсэн, өөрчилсөн зэргийг хадгалдаг байх • Систем нь өгөгдлийн сангаас аль болох мэдээлэл устгахгүй байхаар зохион байгуулах
	[redacted]	• Зөвхөн баталгаажсан эх код бүхий програмыг үйл ажиллагаанд нэвтрүүлэх; • Програм зохиогч нь програм хангамжийн хөгжүүлэлт болон сайжруулалтын аливаа шатанд эх код нь ил биш буюу түүний сул талыг илрүүлэх боломжийг хаасан байх; • Програм хангамжийг зөвшөөрөгдсөн хэрэглээнээс өөрөөр ашиглахад буюу таах замаар мэдээлэлд хандах боломжгүй байхаар хөгжүүлсэн байх; • Програм хангамжид оруулж буй бүхий л өгөгдлийг шалгадаг байх; • Програм хангамжид гарсан системийн алдааны мэдээллийг хэрэглэгчид шууд харуулахгүй байхаар хөгжүүлсэн байх; • Програм хангамжийн хөгжүүлэлт, туршилт болон үндсэн үйл ажиллагааны орчин /өгөгдлийн сан, эх код, үйлдлийн систем зэрэг систем ажиллах орчин/-г тусгаарласан байх; • Програм хангамжид агуулагдах мэдээллийн ангиллыг тодорхойлж, хэрэглэгчийн мэдээлэлд хандах түвшинг тодорхойлсон байх; • Шаардлагатай мэдээлэлд нууцлал хийгдсэн байх; • Хэрэглэгчийн хандалт, мэдээллийн өөрчлөлт болон алдаа зэрэг лог бичдэг байх;

-000-