ОНЦГОЙ БАЙДЛЫН ЕРӨНХИЙ ГАЗРЫН ДАРГЫН ТУШААЛ

2020 оны 10 сарын 26 өдөр Дугаар А/234 Улаанбаатар хот

Журам батлах тухай

Онцгой байдлын ерөнхий газрын даргын зөвлөлийн 2020 оны 8 дугаар хуралдааны шийдвэрийг хэрэгжүүлэхийн тулд Засгийн газрын агентлагийн эрх зүйн байдлын тухай хуулийн 8 дугаар зүйлийн 8.4, Гамшгаас хамгаалах тухай хуулийн 30 дугаар зүйлийн 30.1.4-ийг тус тус үндэслэн ТУШААХ нь:

1. "Онцгой байдлын байгууллагын цахим мэдээллийн аюулгүй байдлыг хангах журам"-ыг хавсралтаар батлалсугай.

2. Батлагдсан журмыг мөрдөж ажиллахыг төв, орон нутгийн Онцгой байдлын байгууллагын дарга, захирагч нарт үүрэг болгосугай.

3. Тушаалын хэрэгжилтэд хяналт тавьж ажиллахыг Гамшгийн шуурхай удирдлагын газар (хурандаа Б.Мандахгэрэл)-т даалгасугай.

4. Энэ тушаал батлагдсантай холбогдуулан Онцгой байдлын ерөнхий газрын даргын 2015 оны 6 дугаар сарын 12-ны өдрийн А/182 дугаар тушаалыг хүчингүй болсонд тооцсугай.

ДАРГА,
БРИГАДЫН ГЕНЕРАЛ Г.АРИУНБУЯН

00002426

Онцгой байдлын ерөнхий газрын даргын
2020 оны .. дугаар сарын ..-ны өдрийн
../.. дүгээр тушаалын хавсралт

ОНЦГОЙ БАЙДЛЫН БАЙГУУЛЛАГЫН ЦАХИМ МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ЖУРАМ

Нэг. Нийтлэг үндэслэл

1.1. Энэхүү журмын зорилго нь Онцгой байдлын байгууллагын цахим мэдээллийн сан, мэдээлэл, түүнийг дэмжих дэд бүтцийн цахим аюулгүй байдлыг хангахтай холбогдсон харилцааг зохицуулахад оршино.

1.2. Онцгой байдлын байгууллагын мэдээллийн аюулгүй байдлын удирдлага, хяналтын тогтолцоог бүрдүүлэх, мэдээллийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй байдлыг дээшлүүлэх, мэдээллийн сүлжээ, системийн найдвартай ажиллагааг хангах, цахим аюул заналаас урьдчилан сэргийлэх, эрсдэлийг бууруулах, нэн даруй хариу арга хэмжээ авах, интернэтийн зохистой хэрэглээг бий болгоход энэхүү журмыг дагаж мөрдөнө.

1.3. Мэдээллийн аюулгүй байдлыг хангахтай холбоотой эрх зүйн баримт бичиг, арга хэрэгсэл, технологи өөрчлөгдсөн тохиолдолд энэхүү журамд өөрчлөлт оруулж болно.

1.4. Энэхүү журам нь Онцгой байдлын байгууллагын мэдээллийн аюулгүй байдлыг хангах бодлогын нэг хэсэг байна.

1.5. Энэ журамд хэрэглэсэн дараах нэр томьёог дор дурдсан утгаар ойлгоно.

1.5.1. “Хэрэглэгч” гэж байгууллагын мэдээллийн системтэй харьцдаг бүх шатны албан хаагчийг;

1.5.2. “Системийн зохицуулагч” гэж байгууллагын цахим мэдээллийн аюулгүй байдал хариуцсан албан тушаалтныг;

1.5.3. “Удирдлага, хяналтын систем /Active Directory domain controller/” гэж дотоод сүлжээнд холбогдсон нийт компьютерийг хэрэглэгчийн эрхээр нь зохион байгуулан нэгдсэн удирдлагаар хангах системийг;

1.5.4. “Мэдээллийн сан” гэж мэдээллийн нэгдсэн ангилал код, индекс, арга зүй, стандартаар ижилсүүлсэн баримт бичгийг шаардлагын дагуу цуглуулж, боловсруулж хадгалсан мэдээлэл, өгөгдлийн бүрдлийг;

1.5.5. “Мэдээллийн систем” гэж мэдээ мэдээллийг боловсруулах, түүний алдааг хянах, найдвартай хадгалах, шаардлагатай мэдээллийг цаг тухайд нь түргэн шуурхай, төрөл бүрийн /дуу авиа, цаасан, хальсан, эд зүйлс, цахилгаан соронзон/ байдлаар гаргах, тэдгээрт ашиглагдах техник болон программ хангамжийн бүрдлийг;

1.5.6. “Дэд бүтэц” гэж мэдээлэл үүсгэх, хүлээн авах, боловсруулах, хадгалах, дамжуулах, үйл ажиллагааг хангаж буй хоорондоо уялдаа холбоо бүхий холболтын систем, техник хэрэгсэл, тоног төхөөрөмжийн бүрдлийг;

1.5.7. “Хамгаалалтын төхөөрөмж” гэж мэдээллийн нууцлал хамгаалалтыг сүлжээний түвшинд зохицуулах хэрэгсэл, тоног төхөөрөмжийг;

1.5.8. “Сүлжээний чиглүүлэгч” гэж байгууллага хоорондын сүлжээг чиглүүлэх, удирдах зориулалтын программ болон техник хангамжийг;

1.5.9. “Хувийн хамгаалагдсан сүлжээ-/VPN-Virtual Private Network/” гэж нууцлалын алгоритм болон түлхүүрээр үүсгэсэн, мэдээллийг нууцлан дамжуулах сувгийг;

1.5.10. “Утасгүй сүлжээ” гэж долгионы тархалт ашиглан ойрын зайд мэдээлэл дамжуулах утасгүй холболтын сүлжээг;

1.5.11. “Нэгдсэн сүлжээ” гэж анги, байгууллага хооронд мэдээлэл солилцох үйл явцыг шуурхай болгох, интернэтийн зохистой хэрэглээг бий болгох зорилгоор үүсгэсэн мэдээллийн аюулгүй байдал хангагдсан нэгдсэн дэд бүтцийг;

1.5.12. “Хорт код” гэж мэдээлэл устгах, хулгайлах, хуулах, өөрчлөх, эвдэх мэт хорлон сүйтгэх зориулалттай хөнөөлт программыг;

1.5.13. “Зөөврийн мэдээлэл тээгч” гэж флаш диск, зөөврийн хатуу диск, компакт диск, зургийн аппарат болон ухаалаг утасны бичил карт гэх мэт зүйлсийг.

Хоёр. Мэдээллийн аюулгүй байдлыг хангах удирдлага, зохион байгуулалт

2.1. Албаны суурин болон зөөврийн компьютерийн нууцлал, аюулгүй байдлыг хангахад дараах арга хэмжээг авч хэрэгжүүлнэ**.** Үүнд:

2.1.1. Төрийн болон албаны нууцад хамаарах мэдээ, мэдээлэл боловсруулах, хадгалах, хамгаалах зөөврийн болон суурин компьютерийг интернэт сүлжээнд холбохгүй, зөвшөөрөгдсөнөөс бусад эх үүсвэр, оролтуудыг хааж, хатуу диск, компьютерийн гадна хэсэгт лац, тэмдэг тэмдэглэгээ, зориулалтын хамгаалалтыг хийсэн байна.

2.1.2. Ажлын шаардлагаар албаны компьютерийг байгууллагаас гадагш гаргах тохиолдолд Холбоо, техник, цахим мэдээллийн аюулгүй байдал хариуцсан бүтцийн нэгжээс зөвшөөрөл авах ба нэвтрэх эрх бүхий хамгаалагдсан программ хангамж ашиглан, мэдээлэлд нууцлал хийнэ.

2.1.3. Алба хаагч нь компьютер, бусад техник хэрэгсэл алдагдсан бол системийн зохицуулагч, эд хөрөнгө хариуцсан мэргэжилтэнд яаралтай мэдэгдэнэ. Энэхүү мэдээллийг авснаар хэрэглэгчийн дотоод системд нэвтрэх эрхийг цуцална.

2.1.4. Байгууллагын компьютер, техник хэрэгсэл тус бүрд техник ашиглалтын паспортыг “Хавсралт 1”-д заасны дагуу хөтлөх ба системийн зохицуулагч эзэмшигч өөрчлөгдсөн тухай бүртгэлийг хийнэ.

2.1.5. Компьютерийн эдэлгээний хугацаа дууссан, техникийн гэмтэл гарч, засварлах боломжгүй тохиолдолд “Хавсралт 2”-т заасны дагуу техникийн гэмтлийн тодорхойлолтыг үйлдэж, саналыг хүргүүлнэ.

2.1.6. Онцгой байдлын байгууллагын мэдээллийн сан, халдлага илрүүлэх, урьдчилан сэргийлэх хяналтын систем, бусад сервер, хэрэглэгчийн компьютерт албан ёсны эрхтэй үйлдлийн систем, хорт кодын эсрэг, хэрэглээний программ хангамжийг худалдан авах, ашиглах хугацааг сунгах зардлыг жил бүрийн төсөвт тусгана.

2.1.7. Программ хангамж нь нийтэд хүлээн зөвшөөрөгдсөн, холбогдох стандартын шаардлагыг хангасан байх ба албан хэрэглээний программ хангамжийн эх код, технологийн шийдэл, гарал үүсэл нь нууц байна.

2.2. Сүлжээний хяналт, зохион байгуулалтад дараах ерөнхий шаардлага тавигдана. Үүнд:

2.2.1. Онцгой байдлын байгууллагын сүлжээний нэгдсэн топологи зурагтай байна.

2.2.2. Аймаг, нийслэлийн Онцгой байдлын байгууллага, түүний салбар, нэгжид харилцаа холбооны үйлчилгээ үзүүлэгч байгууллагатай холбогдож буй шугамын төгсгөл, байгууллагын сүлжээний оролт дээр сүлжээний чиглүүлэгч суурилуулж, тохируулсан байна.

2.2.3. Онцгой байдлын байгууллагын сүлжээг гуравдагч талтай холбоход хамтран ажиллах гэрээг Холбоо, техник, цахим мэдээллийн аюулгүй байдал хариуцсан бүтцийн нэгж байгуулна.

2.2.4. Онцгой байдлын байгууллагын мэдээллийн сүлжээг Монгол Улсын Засгийн газрын 2012 оны 5 дугаар тогтоолын дагуу зохион байгуулна.

2.3. Удирдлага, хяналтын систем, цахим шуудангийн зохион байгуулалтыг хангахад дараах арга хэмжээг авч хэрэгжүүлнэ. Үүнд:

2.3.1. Байгууллагын мэдээллийн системийн тасралтгүй үйл ажиллагааг хангах, мэдээллийн нууцлал, аюулгүй байдлыг дээшлүүлэх зорилгоор компьютер тус бүрийн тохиргоог төвлөрүүлэн зохион байгуулна.

2.3.2. Албаны компьютер нь байгууллагын мэдээллийн нэгдсэн системд нийцсэн Windows үйлдлийн системтэй байх бөгөөд системийн зохицуулагч нь удирдлага, хяналтын систем ашиглан нэгдсэн удирдлагад оруулна.

2.3.3. Системийн зохицуулагч нь хэрэглэгчийн ажил үүргээс хамааруулан “тусгай”, “онцгой”, “энгийн” гэсэн ангиллаар удирдлага, хяналтын системд домэйнд хандах эрхийн хязгаарлалтыг үүсгэнэ.

2.3.4. Байгууллагын хэмжээнд компьютер ашиглаж буй хэрэглэгч бүр нэр@nema.gov.mn, нэр@gmail.com домэйн нэр бүхий албаны цахим шуудангийн хаягтай байна.

2.3.5. Алба хаагч цахим шуудангийн хаяг үүсгэх, устгах, тохиргоо хийх, багтаамжийг нэмэгдүүлэх асуудлыг системийн зохицуулагчид цахим шуудангаар хандан шийдвэрлүүлнэ.

2.4. Дараах тохиолдолд мэдээллийн системд хандах эрхийг цуцална. Үүнд:

2.4.1. Ажлаас чөлөөлөгдсөн;

2.4.2. Урт хугацааны чөлөө авсан;

2.4.3. Жирэмсний амралттай;

2.4.4. Мэдээллийн системд нэвтрэх эрх шаардлагагүй болсон;

2.4.5. Хэрэглэгч өөр ажил, албан тушаалд шилжин томилогдсон;

2.4.6. Хууль, хяналтын байгууллагаас ажиллах эрхийг нь түдгэлзүүлсэн;

2.4.7. Мэдээллийн систем, мэдээллийн санд нэвтрэх эрх бүхий хэрэглэгч мэдээллийн аюулгүй байдлын журмыг зөрчсөн.

2.4.8. Дээрх тохиолдол бүрд байгууллагын хүний нөөцийн мэргэжилтэн нь системийн зохицуулагчид нэн даруй мэдэгдэнэ.

2.5. Цахим мэдээллийн санг зохион байгуулахад дараах арга хэмжээг авч хэрэгжүүлнэ. Үүнд:

2.5.1. Их багтаамж бүхий файлыг түргэн шуурхай солилцох зорилгоор дотоод сүлжээнд үүсгэсэн цахим мэдээллийн санг ашиглах ба аймаг, нийслэлийн Онцгой байдлын байгууллага нууцлал, хамгаалалтын шаардлага хангасан төвлөрсөн мэдээллийн сан үүсгэх зориулалтын төхөөрөмжтэй байна.

2.5.2. Мэдээллийн санд хандах хэрэглэгчдийг ажил үүргийн байдлаас хамааруулан системийн зохицуулагчийн, хяналтын, хэрэглэгчийн гэсэн бүлэгт ангилан нэвтрэх эрхийг тогтооно.

2.5.3. Нууцтай танилцах эрх бүхий албан тушаалтан нь тогтоосон эрхийн дагуу төрийн болон албаны нууцад хамаарах мэдээллийн санд ажлын цагаар нэвтэрнэ.

2.5.4. Ажлын байранд шилжилт хөдөлгөөн хийгдсэн тохиолдолд холбогдох баримт, бичгийн цахим хэлбэрийг ажил хүлээлцэх комисст өгч, хүлээлцсэн акт үйлдэж баталгаажуулна.

2.5.5. Төрийн болон албаны нууцад хамаарах мэдээлэлтэй танилцах, түүнийг агуулсан, тээсэн компьютер, техник хэрэгслийг засварлахад нууцын эрхлэгч нь нууцын баталгааг гаргуулж, системийн зохицуулагч нь хяналт тавьж ажиллана.

2.5.6. Системийн зохицуулагч нь цахим мэдээллийн сан устсан тохиолдолд шалтгаан нөхцөлийг тодорхойлох, нөөц архивлалтыг ашиглан мэдээллийн санг сэргээх ба засварлах боломжгүй тохиолдолд системийг нөөц серверт түр хугацаанд үүсгэн хэвийн ажиллагааг хангана.

2.6. Сервер компьютерийн нууцлал аюулгүй байдлыг хангахад дараах арга хэмжээг авч хэрэгжүүлнэ. Үүнд:

2.6.1. Системийн зохицуулагч шилжин томилогдох үед сервер компьютерийн тохиргоо, дүрэм, нууц үг, бусад зааврыг Холбоо, техник, цахим мэдээллийн аюулгүй байдал хариуцсан бүтцийн нэгжийн даргад бичгээр хүлээлгэн өгнө.

2.6.2. Мэдээллийн санг зориулалтын сервер компьютерт үүсгэн, байгууллагын үйл ажиллагаатай холбоотой цахим мэдээллийг байршуулан улирал тутамд шинэчилж, “Хавсралт 4”-т заасны дагуу бүртгэл хөтлөлтийг системийн зохицуулагч, аюулгүй байдлыг хангахыг зохион байгуулалтын бүтцийн нэгж тус бүр хариуцна.

2.6.3. Серверийн өрөөнд нэвтрэх эрх бүхий албан тушаалтны жагсаалтыг Гамшгийн шуурхай удирдлагын асуудал хариуцсан зохион байгуулалтын бүтцийн нэгжийн дарга баталгаажуулна.

2.6.4. Гамшгийн шуурхай удирдлага, зарлан мэдээллийн төвийн техникийн бэлэн байдал хариуцсан инженер эрх бүхий албан тушаалтныг серверийн өрөөнд нэвтрүүлэн бүртгэл хөтөлнө.

Гурав. Мэдээллийн аюулгүй байдлыг хангахад тоног төхөөрөмж, сүлжээ, программ хангамжийн ашиглалт

3.1. Албаны суурин болон зөөврийн компьютерийг ашиглахдаа дараах зүйлсийг анхаарна. Үүнд:

3.1.1. Компьютерт файлыг “С”-ээс бусад дискэнд, шаардлагатай тохиолдолд зөвшөөрөгдсөн нөөц санд хадгална.

3.1.2. Хэрэглэгчийн буруутай үйлдлээс албаны компьютерт гарсан системийн болон техникийн эвдрэл, гэмтлийг тухайн хэрэглэгч өөрөө хариуцан засварлана.

3.1.3. Хэрэглэгч албаны зөөврийн компьютерийг Холбоо, техник, цахим мэдээллийн аюулгүй байдал хариуцсан бүтцийн нэгжийн зөвшөөрлөөр ашиглана.

3.1.4. Алба хаагч гадаад томилолтоор ажиллахдаа албаны зөөврийн компьютерийг ашигласан бол холбогдох файлыг хуулбарлан авч, тухайн компьютероос устгана.

3.2. Хорт кодын эсрэг болон бусад программ хангамжийг ашиглахдаа дараах зүйлсийг анхаарна. Үүнд:

3.2.1. Хэрэглэгч өөрийн компьютерийн хорт кодын эсрэг программ хангамжийг тогтмол хугацаанд уншуулан, хорт код илэрсэн тохиолдолд устгах арга хэмжээг авч,

Холбоо, техник, цахим мэдээллийн аюулгүй байдал хариуцсан бүтцийн нэгжид мэдэгдэнэ.

3.2.2. Программ, техник хангамжийн туршилтыг Холбоо, техник, цахим мэдээллийн аюулгүй байдал хариуцсан бүтцийн нэгж хийх бөгөөд энэ хугацаанд хорт кодыг дамжуулж болзошгүй хэрэглээний программ хангамжийг ажиллуулж болохгүй.

3.2.3. MNS ISO/IEC 17799 (Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоо-шаардлага) стандартад заасны дагуу мэдээллийн системд хууль бусаар нэвтрэх, өөрчлөх эрсдэлийг бууруулахын тулд программ хангамж хөгжүүлэх, турших, түүнд ашиглагдах техник хэрэгсэл, тоног төхөөрөмжийг үндсэн сүлжээнээс тусгаарлана.

3.2.4. Дүрст хурал зохион байгуулахад нууцлал, аюулгүй байдлын шаардлага хангасан албан ёсны эрх бүхий программ хангамж ашиглана.

3.3. Интернэт болон дотоод сүлжээг ашиглахдаа дараах арга хэмжээг авч хэрэгжүүлнэ. Үүнд:

3.3.1. Байгууллагын дотоод сүлжээнд зөвхөн албаны компьютерийг холбох бөгөөд тэдгээрийг физик /MAC/ хаягаар бүртгэнэ.

3.3.2. Нэгдсэн сүлжээг нууцлалын алгоритм, түлхүүр ашиглан зохион байгуулж, сүлжээний хамгаалалт, чиглүүлэгч төхөөрөмжийн тохиргоог хагас жил тутамд шалган бүртгэл хөтөлнө.

3.3.3. Байгууллагын хэмжээнд интернэт сүлжээг дотоод сүлжээнээс тусгаарлаж, нийгмийн сүлжээ болон зүй зохисгүй сайт, холбоосууд (Facebook, Twitter, Wechat, Instagram, Hi5, Youtube, Restricted site гэх мэт)-ыг нэгдсэн удирдлагаар тохируулж хязгаарлана.

3.3.4. Аймаг, нийслэлийн Онцгой байдлын байгууллагын гамшгаас урьдчилан сэргийлэх асуудал хариуцсан алба хаагчийн компьютерт нийгмийн сүлжээний албан ёсны нэг хаяг бүхий сайтыг ашиглах эрхийг Гамшгийн шуурхай удирдлагын асуудал хариуцсан зохион байгуулалтын бүтцийн нэгжийн даргын зөвшөөрлөөр нээнэ.

3.3.5. Интернэт сүлжээнд төрийн болон албаны нууцад хамаарах мэдээлэл, удирдлагын байранд авахуулсан албаны дүрэмт хувцастай фото зураг, дүрс бичлэгийг байршуулах, цахим шуудангаар бусдад илгээх, интернэт орчны “cloud storage”-д хадгалж болохгүй.

3.3.6. Албан хэрэгцээнд шаардлагагүй веб сайтуудад хандах, их хэмжээтэй файл болон баталгаагүй, сэжигтэй эх сурвалжаас файл татах, байгууллагын сүлжээг ашиглан зүй зохисгүй сэтгэгдэл үлдээж болохгүй.

3.3.7. Компьютерт Dial-up, DSL, модем, гар утас холбох, сүлжээнд утсан болон утасгүй сүлжээний төхөөрөмжийг системийн зохицуулагчийн зөвшөөрлөөр залгаж болно.

3.3.8. Утасгүй сүлжээг зөвхөн утсан сүлжээ татах боломжгүй, алслагдсан газарт ашиглах зайлшгүй нөхцөлд зохион байгуулна.

3.4. Сүлжээний чиглүүлэгчийг ашиглахдаа дараах зүйлсийг анхаарна. Үүнд:

3.4.1. Сүлжээний чиглүүлэгчийг ашиглахдаа үйлдвэрээс заасан анхны хандалтын IP хаяг, нууц үгийг өөрчилж, ашиглагдахгүй байгаа портуудыг программ хангамжийн түвшинд хааж, зориулалтын тагаар таглаж, лацадсан байна.

3.4.2. Сүлжээний холболтын аюулгүй хамгаалагдсан сувагчлал үүсгэсэн тохиолдолд зайлшгүй шаардлагын дагуу “Telnet” ашиглах ба удирдахад SSH протокол ашиглана.

3.5. Онцгой байдлын байгууллага тусгай зориулалтын тоноглогдсон серверийн өрөөтэй байх ба дараах шаардлагыг хангасан байна. Үүнд:

3.5.1.Тоос, шороо орохоос хамгаалагдсан битүүмжлэл сайтай байх;

3.5.2. Чийгшил, дулаан тодорхойлогч, агааржуулагчтай байх;

3.5.3. Серверийн өрөөний талбай болон тоног төхөөрөмжийн тоо хэмжээнээс хамаарч хөргөлтийн төхөөрөмжийг суурилуулах;

3.5.4. Болзошгүй гадны халдлага, цахилгаан соронзон долгионы нөлөөллөөс хамгаалагдсан байх;

3.5.5.Техник, тоног төхөөрөмж нь газардуулгатай байх;

3.5.6. Хаалгандаа электрон /код/, био өгөгдлөөр нээгддэг цоож, хяналтын камертай байх;

3.5.7. Хөдөлгөөн мэдрэгч гэрэлтүүлэгтэй байх;

3.5.8. Тоног төхөөрөмж 24/7 цагийн асаалттай горимоор ажиллах зарчмыг алдагдуулахгүй цахилгааны үндсэн болон нөөц эх үүсвэртэй байх;

3.5.9. Ухаалаг цахилгаан нөөц эх үүсвэр нь хамгийн багадаа нэг цаг ажиллах бөгөөд хүчин чадал нь 30 хувиас доош орсон тохиолдолд автоматаар унтраахаар тохируулагдсан байх;

3.5.10. Кабел тараагч сувагчлал, цахилгаан тэжээлийн самбартай байх;

3.5.11. Галын аюулгүй байдлыг бүрэн хангасан, хяналтын болон автомат унтраах системтэй байх;

3.5.12. Серверийн өрөөн дэх тоног төхөөрөмжүүдийн цахилгаан эрчим хүчний нийт зарцуулалтыг тооцсон байх;

3.5.13. Серверийн өрөөнд шаардлагатай анхааруулах тэмдэг, холбоо барих утасны жагсаалтыг байршуулсан байх;

3.5.14. Тоног төхөөрөмжүүдийн кабел шугамын холболтыг эмх цэгцтэй татаж, хаяглан, тоног төхөөрөмжийг зориулалтын цоожтой зогсуурт нэг эгнээгээр байрлуулна.

3.5.15. Серверийн өрөөнд зориулалтын бус тоног төхөөрөмж, эд хогшил болон шатамхай бодис, тэсэрч дэлбэрэх зүйлсийг байрлуулахгүй.

3.6. Хэрэглэгч цахим шууданг ашиглахдаа дараах зүйлсийг анхаарна. Үүнд:

3.6.1. Цахим шуудангийн хаягт нэвтрэх нэр, нууц үгийн нууцлал, аюулгүй байдлыг хариуцна.

3.6.2. Цахим шуудангийн хаягт нэвтрэх нэр, нууц үгийг мартсан эсвэл солих шаардлагатай тохиолдолд Холбоо, техник, цахим мэдээллийн аюулгүй байдал хариуцсан бүтцийн нэгжид хүсэлт гаргана.

3.6.3. Цахим шуудангаар илгээх файлын хэмжээ 25 мегабайтаас хэтрэхгүй байна.

3.6.4. Суртал ухуулгын шинжтэй, үргэлжилсэн бичвэртэй, хорт код агуулсан мэдээллийг цахим шуудангаар хүлээн авч, илгээхгүй.

3.7. Зөөврийн мэдээлэл тээгчийг ашиглахдаа дараах зүйлсийг анхаарна.

Үүнд:

3.7.1. Төрийн болон албаны нууцад хамаарах мэдээллийг нууцлалын программ хангамж ашиглан тусгай зориулалтын төхөөрөмжид улирал тутамд хадгалан нууцын өрөөнд байршуулна.

3.7.2. Холбоо, техник, цахим мэдээллийн аюулгүй байдал хариуцсан бүтцийн нэгж нь “Хавсралт 3”-т заасны дагуу зөөврийн мэдээлэл тээгчийг бүртгэлжүүлнэ.

3.7.3. Хэрэглэгч зөөврийн мэдээлэл тээгчийг ашиглахын өмнө программ хангамжийг уншуулан хорт кодыг шалгана.

3.7.4. Зайлшгүй шаардлагаар цахим мэдээллийг хуулбарлан хүргүүлэх тохиолдолд зөөврийн мэдээлэл тээгчийг ашиглана.

3.7.5. Ашиглалтын шаардлага хангахгүй болсон зөөврийн мэдээлэл тээгчийг Холбоо, техник, цахим мэдээллийн аюулгүй байдал хариуцсан бүтцийн нэгжийн даргын зөвшөөрлөөр дахин сэргээгдэхгүйгээр устгана.

3.7.6. Албаны холбогдолтой цахим мэдээллийг хадгалах, дамжуулахад гар утсыг зөөврийн мэдээлэл тээгч хэлбэрээр ашиглахгүй.

3.8. Нууц үгийг ашиглахдаа дараах зүйлсийг анхаарна. Үүнд:

3.8.1. Нууц үг нь том, жижиг үсэг, тоо, тусгай тэмдэгт (a-z,A-Z, 0-9,!@#$%^&*()_+|~-=\`{}[]:";'<>?,./;)-ээс бүрдсэн байна.

3.8.2. Нууц үгийг хялбар биш, амархан тогтоож болохоор үүсгэх ба сүлжээ, сервер компьютер, мэдээллийн сан, удирдлагын программ хангамжийн нууц үг 12 тэмдэгтээс багагүй, бусад тоног төхөөрөмжид хандах нууц үг 8 тэмдэгтээс багагүй байна.

3.8.3. Системийн зохицуулагч өөр ажил, албан тушаалд томилогдох, чөлөөлөгдөхөд нууц үгийг цаасан дугтуйнд битүүмжилж, Холбоо, техник, цахим мэдээллийн аюулгүй байдал хариуцсан бүтцийн нэгжийн даргад хүлээлгэн өгнө.

3.8.4. Удирдлагын системийн нууц үгийг 6 сар, хэрэглэгчийн түвшний нууц үгийг 3 сар тутам солино.

Дөрөв. Системийн зохицуулагч, удирдлага, нэгж, хэрэглэгчийн эрх, үүрэг

4.1. Системийн зохицуулагч дараах эрх, үүрэгтэй байна. Үүнд:

4.1.1. Байгууллагын мэдээллийн аюулгүй байдлыг хангахад шаардагдах хамгаалалтын системийг бий болгох, ажлын горимыг боловсруулах;

4.1.2. Албан хэрэгцээнээс бусад зөвшөөрөлгүй программ хангамж болон веб сайтын жагсаалтыг жил бүр Онцгой байдлын ерөнхий газрын даргаар батлуулах, жагсаалтын дагуу хязгаарлалт хийх;

4.1.3. Мэдээллийн систем, хэрэглэгчийн компьютерт нэвтрэх, шалгах үйл ажиллагаа явуулах, бүрэн бүтэн байдалд хяналт тавих, мэдээллийн сангийн нөөц хувийг үүсгэн хадгалах нөхцөлийг хангах;

4.1.4. Байгууллагын сервер компьютерийн системд техникийн үйлчилгээ үзүүлэгчийг сонгоход оролцох, ажлын гүйцэтгэлд хяналт тавих;

4.1.5. Байгууллагын сүлжээ, системд нэвтэрсэн халдлагыг таслан зогсоож, хариу арга хэмжээ авах, системийг сэргээх арга хэмжээг яаралтай зохион байгуулах;

4.1.6. Байгууллагын мэдээллийн системд ашиглах техник болон программ хангамжийн гарал үүслийг бүртгэх, шаардлагатай тохиолдолд техникийн үзлэг хийх;

4.1.7. Байгууллагын мэдээллийн аюулгүй байдлыг хангах чиглэлээр сургалт, сурталчилгаа хийх;

4.1.8. Мэдээллийн аюулгүй байдлыг хангахад шаардагдах мэргэжил дээшлүүлэх сургалтад хамрагдах;

4.1.9. Шинээр гарч буй мэдээллийн аюулгүй байдлыг хангах техник, технологийг судлан байгууллагын үйл ажиллагаанд нэвтрүүлэх;

4.2. Байгууллагын удирдлага дараах эрх, үүрэгтэй байна. Үүнд:

4.2.1. Цахим мэдээллийн аюулгүй байдлын талаар хүлээх үүргийг хуваарилж, байгууллагын хэмжээнд мэдээллийн аюулгүй байдлыг хэрэгжүүлэх үйл ажиллагааг уялдуулах, алба хаагчдын оролцоог нэмэгдүүлэх;

4.2.2. Цахим мэдээллийн аюулгүй байдлыг хангах санал санаачилга, үйл ажиллагааг бүхий л талаар дэмжиж ажиллах;

4.2.3. Техник болон программ хангамжийн хэвийн ажиллагаа, мэдээллийн сүлжээний нууцлал хамгаалалтыг хангахад дэмжлэг үзүүлэх;

4.2.4. Үйл ажиллагааны үндсэн чиг үүргийн хүрээнд мэдээллийн аюулгүй байдлын бодлого, журмыг мөрдөн, алба хаагчдын мэдээллийн аюулгүй байдлыг хангаж байгаа эсэхэд хяналт тавих.

4.3. Холбоо, техник, цахим мэдээллийн аюулгүй байдал хариуцсан бүтцийн нэгж нь дараах эрх, үүрэгтэй байна. Үүнд:

4.3.1. Мэдээллийн системийн бүтцийг зураглах, систем хоорондын нийцлийг зохицуулах, нэгдсэн удирдлагаар хангах;

4.3.2. Мэдээллийн системийг зохион байгуулах, турших, ашиглах, засвар үйлчилгээ хийх, хэвийн ажиллагааг хангах;

4.3.3. Байгууллагад шинээр нэвтрүүлэх техник технологийн шийдлийг боловсруулах, худалдан авах үйл ажиллагаанд оролцох.

4.4. Хэрэглэгч нь дараах эрх, үүрэгтэй байна. Үүнд:

4.4.1. Албан хэрэгцээнд ашиглаж буй зөөврийн болон суурин компьютерийг зүй зохистой ашиглаж, мэдээллийн аюулгүй байдлыг хангах;

4.4.2. Өөр ажил, албан тушаалд томилогдох, чөлөөлөгдөх тохиолдолд хариуцсан төрийн болон албаны нууцад хамаарах мэдээллийг нууцын эрхлэгчид хүлээлгэн өгч, мэдээллийн системд хандах эрхээ хаалгах;

4.4.3. Мэдээллийн сан, системд нэвтрэх нууц үгийг бусдад дамжуулахгүй байх ба нууц үг задарсан гэж үзвэл системийн зохицуулагчид мэдэгдэн солиулах;

4.4.4. Төрийн болон албаны нууцад хамаарах мэдээлэл алдагдаж болзошгүй нөхцөл байдал үүссэн бол нэн даруй Холбоо, техник, цахим мэдээллийн аюулгүй байдал хариуцсан бүтцийн нэгжид мэдэгдэх.

Тав. Программ хангамж, тоног төхөөрөмжийг худалдан авах, эрсдэлийн үнэлгээ хийх

5.1. Мэдээллийн аюулгүй байдлыг хангах программ хангамж, тоног төхөөрөмж худалдан авахад дараах зүйлсийг анхаарна. Үүнд:

5.1.1. Байгууллагын үйл ажиллагаанд нийцсэн, тавигдах шаардлагыг хангасан программ хангамж, тоног төхөөрөмж худалдан авахад Холбоо, техник, цахим мэдээллийн аюулгүй байдал хариуцсан бүтцийн нэгжээр баталгаажуулах;

5.1.2. Мэдээллийн системийн зохион байгуулалт, программ хангамжийн хөгжүүлэлт хийж буй байгууллагатай нууцын гэрээ байгуулах.

5.2. Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээ хийх байгууллага нь дараах шаардлагыг хангасан байна. Үүнд:

5.2.1. Хууль эрх зүйн зөвшөөрөлтэй байх бөгөөд энэхүү журмыг үндэслэн гэрээ байгуулна.

5.2.2. Мэдээллийн систем, сүлжээг шинжлэхдээ мэргэжлийн программ хангамж болон олон улсад хүлээн зөвшөөрөгдсөн аргуудыг ашиглана.

5.3. Эрсдэлийн үнэлгээ хийхэд дараах арга хэмжээг авч хэрэгжүүлнэ. Үүнд:

5.3.1. Байгууллагын мэдээллийн аюулгүй байдлын удирдлага, хяналтын хэрэгжилт, сүлжээний дэд бүтэц, мэдээллийн сангийн бүрэн бүтэн, халдашгүй нууцлагдсан болон хүртээмжтэй байдлыг баталгаажуулах;

5.3.2. Мэдээллийн аюулгүй байдлын зөрчил гарч болзошгүй эмзэг байдлыг тодорхойлох;

5.3.3. Байгууллагын цахим мэдээллийн дэд бүтцийн зохион байгуулалт мэдээллийн аюулгүй байдлын бодлоготой нийцэж буй эсэхийг тогтоох;

5.3.4. Гадны халдлага нэвтрэн орох цоорхой байгаа эсэхийг тодорхойлох;

5.3.5. Хэрэглэгч болон мэдээллийн системийн үйл ажиллагааг шалгах.

5.4. Эрсдэлийн үнэлгээ хийх байгууллагад мэдээллийн орчинд хандах дараах эрхийг системийн зохицуулагчийн хяналтан дор олгоно. Үүнд:

5.4.1. Хэрэглэгчийн болон үйлдлийн системийн түвшний хандалтын эрх;

5.4.2. Байгууллагын цахим мэдээллийн санд хандах эрх;

5.4.3. Ажлын талбарт хандах эрх (серверийн өрөө, албаны өрөөнүүд г.м);

5.4.4. Шаардлагатай лог /бүртгэл/-ийн файлуудад хандах эрх.

5.5. Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээг мэргэжлийн байгууллагаар 2 жилд нэг удаа, шаардлагатай тохиолдолд тухай бүр хийлгэх ба холбогдох зардлыг төсөвт тусгана.

5.6. Аймаг, нийслэлийн Онцгой байдлын байгууллага цахим мэдээллийн аюулгүй байдалд бие даан эрсдэлийн үнэлгээ хийж болно.

5.7. Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээнд үндэслэн эрсдэлийг бууруулах арга хэмжээнд зарцуулах хөрөнгийг жил бүрийн төсөвт тусгана.

Зургаа. Хяналт, хариуцлага

6.1. Журмыг зөрчсөн албан тушаалтанд эрүүгийн хариуцлага хүлээлгэхээргүй бол Төрийн болон албаны нууцын тухай хууль, Төрийн албаны тухай хууль, Цэргийн нийтлэг дүрмийн дагуу сахилгын шийтгэл ноогдуулна.

6.2. Хэрэглэгч хуулийн хариуцлага хүлээлгэсэн эсэхээс үл хамаарч учирсан хохирлыг бүрэн барагдуулна.

..... o O o .....

Хавсралт 1

ТЕХНИК АШИГЛАЛТЫН ПАСПОРТ

1. ТОНОГ ТӨХӨӨРӨМЖИЙН ТЕХНИКИЙН ҮЗҮҮЛЭЛТ, ЗОРИУЛАЛТ

1. Тоног төхөөрөмжийн нэр _____
2. Тоног төхөөрөмжийн марк, сериал_____
3. Үйлдвэрлэсэн орны нэр_____
4. Үйлдвэрлэсэн огноо_____
5. Ашиглалтад оруулсан огноо_____
6. Хаана суурилагдсан _____

Үндсэн үзүүлэлт

№	Үзүүлэлтийн төрөл	Үзүүлэлт

2. ТОНОГ ТӨХӨӨРӨМЖИЙН ДАГАЛДАХ ХЭРЭГСЛҮҮД

№	Дагалдах хэрэгслийн нэр	Тоо хэмжээ

3. ТЕХНИК ҮЗЛЭГ, ҮЙЛЧИЛГЭЭНИЙ ТЭМДЭГЛЭЛ

№	Огноо	Ямар үйлчилгээ хийсэн эсэх	Эвдрэл гэмтэл, засварын тухай	Үзлэг, үйлчилгээ хийсэн хүний нэр, албан тушаал

4. ЭЗЭМШИГЧ СОЛИГДСОН ТУХАЙ МЭДЭЭЛЭЛ

Эзэмшигчийн мэдээлэл	
Нэгжийн нэр	
Цол	
Албан тушаал	
Овог, нэр	
Тоног төхөөрөмжийн үзүүлэлт	
Төрөл	
Марк, загвар	
Техникийн үзүүлэлт	
Сериал дугаар	
Ашиглалтад орсон огноо	
Бусад	
Эзэмшигч солигдсон мэдээлэл	

Хавсралт 2

Дугаар:20-…	ТЕХНИКИЙН ГЭМТЛИЙН ТОДОРХОЙЛОЛТ

Тоног төхөөрөмжийн нэр:

Загвар, сериал дугаар:

Ашиглалтад орсон огноо:

Гэмтлийн шалтгаан:

Санал:

Шийдвэр

Техникийн тодорхойлолт гаргасан:

Эзэмшигч :

20.. оны…….сарын ……өдөр

Хавсралт 3

ЗӨӨВРИЙН МЭДЭЭЛЭЛ ТЭЭГЧ ЭЗЭМШИГЧИЙН БҮРТГЭЛИЙН КАРТ

Байгууллагын нэр:……
Бүтгэл хийсэн огноо:……

Эзэмшигчийн мэдээлэл	
Нэгжийн нэр	
Цол	
Албан тушаал	
Овог, нэр	
Тоног төхөөрөмжийн үзүүлэлт	
Төрөл	
Марк, загвар	
Техникийн үзүүлэлт	
Сериал дугаар	
Ашиглалтад орсон огноо	
Бусад	
Шилжилт хөдөлгөөний мэдээлэл	

Эзэмшигчийн гарын үсэг: ……../ /
Бүртгэгчийн гарын үсэг: ……./ /

Хавсралт 4

МЭДЭЭЛЛИЙН САНГ НӨӨЦӨЛСӨН БҮРТГЭЛ

д/д	Мэдээллийн сангийн нэр	Нөөцөлсөн огноо	Мэдээллийн сангийн хэмжээ	Мэдээллийн санг нөөцөлсөн сервер, зөөврийн мэдээлэл тээгч, хатуу дискний нэр	Мэдээллийн санг нөөцөлсөн хавтасны нэр	Нөөцөлсөн алба хаагчийн албан тушаал	Нөөцөлсөн алба хаагчийн нэр	Нөөцөлсөн алба хаагчийн гарын үсэг	Тайлбар

Бүртгэл хүлээлгэн өгсөн алба хаагчийн гарын үсэг ……../ /

Бүртгэл хүлээн авсан алба хаагчийн гарын үсэг: ……/ /