МОНГОЛ УЛСЫН ИХ СУРГУУЛИЙН
РЕКТОРЫН ТУШААЛ

2026 оны 04 сарын 08 өдөр Дугаар А/151 Улаанбаатар хот

Мэдээллийн аюулгүй байдлын журам
батлах тухай

Дээд боловсролын тухай хуулийн 31 дүгээр зүйлийн 31.1.2 дахь заалт, МУИС-ийн Дүрмийн 5.4.1, 5.4.8.5 дахь заалт, МУИС-ийн Ректорын зөвлөлийн 2026 оны 03 дугаар сарын 24-ний өдрийн хурлын тэмдэглэл, шийдвэрийг тус тус үндэслэн ТУШААХ нь:

1. "Мэдээллийн аюулгүй байдлын журам"-ыг хавсралтаар баталж, 2026 оны 04 дүгээр сарын 01-ний өдрөөс эхлэн мөрдсүгэй.

2. Мэдээллийн аюулгүй байдлын журмыг үйл ажиллагаандаа мөрдөж ажиллахыг проректор, бүрэлдэхүүн/салбар сургуулийн захирал, захиргааны нэгжийн удирдлагуудад тус тус үүрэг болгосугай.

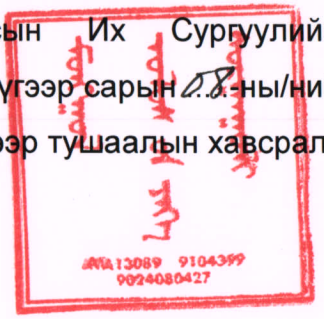
3. Журмыг нийтэд танилцуулж, хэрэгжилтэд хяналт тавьж ажиллахыг Цахим шилжилтийн газрын дарга (А.Баатарбилэг)-д даалгасугай.

РЕКТОР Б.ОЧИРХУЯГ

АТА13089 9104399
9024080427

1426131274

Монгол Улсын Их Сургуулийн
ректорын 2026 оны 04 дүгээр сарын 08-ны/ний
өдрийн А/151 дугаар/дүгээр тушаалын хавсралт



МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ЖУРАМ

НЭГ. НИЙТЛЭГ ҮНДЭСЛЭЛ

1.1. Энэхүү журам нь Монгол Улсын Их Сургууль (цаашид “МУИС” гэх)–ийн мэдээллийн аюулгүй байдлын үндсэн баримт бичиг бөгөөд мэдээлэл, мэдээллийн систем, программ хангамж, мэдээллийн технологийн дэд бүтэц, өгөгдлийн сангийн нууцлал, бүрэн бүтэн байдал, хүртээмжтэй байдлыг хангахтай холбоотой үйл ажиллагааг зохицуулна.

1.2. Монгол Улсын Кибер аюулгүй байдлын тухай хууль, Хүний хувийн мэдээлэл хамгаалах тухай хууль, холбогдох хууль тогтоомжийн хүрээнд энэхүү журмыг нийцүүлэн мөрдөнө.

1.3. МУИС-ийн багш, ажилтан, суралцагчид болон гадаад, дотоод сонирхогч, оролцогч тал, нийлүүлэгч байгууллага энэхүү журмыг дагаж мөрдөнө.

1.4. Энэхүү журам нь мэдээллийн хөрөнгийн аюулгүй байдлыг зохицуулах бөгөөд хөрөнгийн удирдлага, бүртгэлтэй холбоотой асуудалд хамаарахгүй.

ХОЁР. НЭР ТОМЬЁОНЫ ТОДОРХОЙЛОЛТ

2.1. Энэхүү журамд хэрэглэсэн нэр томьёог доор дурдсан утгаар ойлгоно:

2.1.1. “Мэдээллийн хөрөнгө” гэж байгууллагын үйл ажиллагаанд үнэ цэн бүхий мэдээлэл, түүнийг үүсгэх, боловсруулах, хадгалах, дамжуулахад ашиглагдах программ хангамж, техник хангамж, мэдээллийн систем, хүний нөөц болон мэдээллийн технологийн дэд бүтцийг;

2.1.2. “Мэдээллийн хөрөнгийн эзэмшигч” гэж мэдээллийн хөрөнгийн үнэ цэнэ, ашиглалт, хамгаалалтад хариуцлага хүлээж, тухайн хөрөнгийн ангилал тогтоох, хандалтын эрхийг баталгаажуулах, аюулгүй байдлын шаардлагыг тодорхойлох нэгж эсхүл албан тушаалтныг;

2.1.3. “Мэдээллийн хөрөнгийн хариуцагч” гэж мэдээллийн хөрөнгийг эзэмшигчийн тогтоосон эрх үүргийн хүрээнд мэдээллийн хөрөнгийн нууцлал, бүрэн бүтэн байдал, хүртээмжтэй байдлыг хангах, мэдээлэлтэй танилцах, цуглуулах, боловсруулах, хадгалахтай холбоотой өдөр тутмын ажиллагааг хариуцсан нэгж эсхүл албан тушаалтныг;

2.1.4. “Мэдээлэл хэрэглэгч” гэж албан үүргийн хүрээнд мэдээллийг ашиглах, олгогдсон эрхийн дагуу мэдээлэлтэй танилцах, цуглуулах, боловсруулах, хадгалах эрх бүхий этгээдийг;

2.1.5. “Мэдээллийн эзэн” гэж тухайн мэдээллээр тодорхойлогдож буй хувь хүн, түүний хууль ёсны төлөөлөгчийг;

2.1.6. “Мэдээллийн аюулгүй байдал” гэж мэдээллийн нууцлагдсан байдал, бүрэн бүтэн байдал, хүртээмжтэй байдал хангагдсан байхыг;

2.1.7. “Мэдээллийн аюулгүй байдлын мэргэжилтэн” гэж МУИС-ийн мэдээллийн аюулгүй байдал болон мэдээллийн технологийн үйл ажиллагааны аюулгүй, тасралтгүй байдлыг хангах чиг үүрэгтэй ажилтныг;

2.1.8. “Администратор” гэж мэдээллийн технологийн сервер, сүлжээ, тоног төхөөрөмжид нэвтрэх, тохиргоо хийх, өөрчлөх эрх бүхий ажилтныг;

2.1.9. “Мэдээллийн аюулгүй байдлын тохиол” (event) гэж мэдээллийн хөрөнгө, мэдээллийн систем, сүлжээ, программ хангамж, техник хангамж, эсхүл тэдгээрийн орчинд мэдээллийн аюулгүй байдлын бодлого, хяналтын хэрэгсэл алдагдсан, доголдсон, зөрчигдсөн байж болзошгүйг илтгэх, эсхүл мэдээллийн аюулгүй байдалд сөргөөр нөлөөлж болзошгүй ажиглагдсан хэвийн бус үйл явдлыг;

2.1.10. “Мэдээллийн аюулгүй байдлын зөрчил” (incident) гэж нэг буюу хэд хэдэн мэдээллийн аюулгүй байдлын тохиолын улмаас мэдээллийн хөрөнгө, мэдээллийн систем, сүлжээ, эсхүл тэдгээрийн орчинд мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмж алдагдсан эсхүл алдагдаж болзошгүй нөхцөл байдлыг;

2.1.11. “Аюул занал” гэж МУИС-ийн үйл ажиллагааг алдагдуулах, мэдээллийн хөрөнгө болон мэдээллийн аюулгүй байдалд заналхийлэх бодит боломж бүхий нөхцөл байдал, гэнэтийн эсвэл дэс дараалсан тохиолдлуудыг;

2.1.12. “Эрсдэлийн үнэлгээ” гэж мэдээллийн хөрөнгөнд учирч болзошгүй аюул занал, эмзэг байдлыг тодорхойлж, эрсдэлийн түвшнийг үнэлэх, бууруулах арга хэмжээг тодорхойлох үйл ажиллагааг;

2.1.13. “Лог файл” гэж мэдээллийн системд хандан ажиллаж буй хэрэглэгч болон системийн үйлдлийг бүртгэн хадгалдаг системийн файлыг;

2.1.14. “Нууцлалтай байдал” гэж эрх олгогдоогүй этгээд, процессын зүгээс мэдээлэлд хандах боломжгүй, хаалттай байх шинж чанарыг;

2.1.15. “Бүрэн бүтэн байдал” гэж мэдээллийн үнэн зөв, нийцтэй, бүрэн дүүрэн байдлыг хангаж буй шинж чанарыг;

2.1.16. “Хүртээмжтэй байдал” гэж эрх бүхий этгээд нь олгогдсон зөвшөөрлийн дагуу шаардлагатай үед мэдээлэлд хандаж, ашиглах боломжтой байх шинж чанарыг;

2.1.17. “Цахим мэдээлэл” гэж мэдээллийн систем, программ хангамж, өгөгдлийн сан, файл, сүлжээ болон бусад цахим орчинд үүсгэгдэж, хадгалагдаж, боловсруулагдаж, дамжуулагдаж буй мэдээллийг;

2.1.18. “Цаасан мэдээлэл” гэж баримт бичиг, хэвлэмэл материал, гар бичмэл зэрэг цаасан хэлбэрээр үүсгэгдэж, хадгалагдаж, ашиглагдаж буй мэдээллийг;

ГУРАВ. МЭДЭЭЛЛИЙН ХӨРӨНГӨ, ТҮҮНИЙ АНГИЛАЛ

3.1. Мэдээллийн технологи хариуцсан нэгж нь мэдээллийн хөрөнгийн эзэмшигчтэй хамтран мэдээллийн аюулгүй байдалд хамаарах мэдээллийн хөрөнгийн жагсаалтыг бүрдүүлж, жилд нэг удаа, эсвэл мэдээллийн хөрөнгийн эзэмшигчийн хүсэлтээр тухай бүр өөрчилж шинэчилнэ. Бүртгэлд дараах агуулга хамаарна. Үүнд:

3.1.1. Мэдээллийн хөрөнгийн нэр;
3.1.2. Мэдээллийн хөрөнгийн төрөл;
3.1.3. Мэдээллийн хөрөнгийг хариуцагч;
3.1.4. Мэдээллийн хөрөнгийн ангилал;
3.1.5. Мэдээллийн хөрөнгийн байршил;

3.2. Мэдээллийн хөрөнгийн бүртгэлд цахим болон цаасан хэлбэрийн мэдээллүүд, мэдээллийн технологи хариуцсан нэгжийн эзэмшилд буй технологийн хөрөнгүүдээс хамруулна.

3.2.1. Цахим мэдээлэлд өгөгдлийн сан, файлын сан, хандалтын эрхийн мэдээлэл, цахим шуудан, нөөцөлсөн мэдээлэл, лог бүртгэл, хяналтын камерын бичлэг зэрэг мэдээллийн аюулгүй байдлыг хангах шаардлагатай цахим хэлбэрийн мэдээллийг хамруулж ойлгоно.

3.2.2. Цаасан мэдээлэлд эрх зүйн үр дагавар бүхий баримт бичиг, байгууллагын үндсэн болон нэмэлт үйл ажиллагааны хүрээнд боловсруулсан, цуглуулсан бүртгэл, мэдээлэл, тайлан, төлөвлөгөө, төсөл, хөтөлбөр, сургалтын материал зэрэг мэдээллийн аюулгүй байдлыг хангах шаардлагатай цаасан хэлбэрийн мэдээллийг хамруулж ойлгоно.

3.2.3. Технологийн хөрөнгөд дараах төрлийн хөрөнгүүдийг хамааруулж ойлгоно. Үүнд:

3.2.3.1. Хэрэглээний болон тусгай зориулалтын программ хангамж, системүүдийн лиценз;

3.2.3.2. Дотооддоо болон гуравдагч этгээдээр захиалгаар хөгжүүлсэн мэдээллийн систем, программ хангамж, эх код, системийн өгөгдөл;

3.2.3.3. Сервер, компьютер, хадгалах болон дамжуулах тоног төхөөрөмжүүд;

3.2.3.4. Сүлжээний тоног төхөөрөмжүүд (галт хана, чиглүүлэгч, холбогч, ачаалал тэнцвэржүүлэгч, утасгүй сүлжээний төхөөрөмж);

3.2.3.5. Серверийн хэвийн үйл ажиллагааг дэмжих туслах тоног төхөөрөмжүүд;

3.3. Мэдээллийн хөрөнгийг түүний ач холбогдол, нууцлал, эрсдэлийн түвшинд үндэслэн дараах төрлөөр ангилна. Үүнд:

3.3.1. Нээлттэй: Нийтэд чөлөөтэй түгээх боломжтой, ил тод байхаар зориулагдсан, хувилах, хадгалах, дамжуулах, гарган өгөхөд ямар нэгэн шаардлага тавигдахгүй, мөн Монгол Улсын хууль тогтоомжоор нийтэд ил болгосон мэдээлэл.

3.3.2. Дотоод хэрэгцээнд: МУИС-ийн дотоод үйл ажиллагаанд ашиглахад зориулагдсан, зөвшөөрөлгүйгээр гадагш задруулахгүй байх мэдээлэл.

3.3.3. Хязгаарлагдмал: МУИС-ийн үндсэн болон нэмэлт үйл ажиллагаатай холбоотой, холбогдох журам, шийдвэрийн дагуу зөвхөн эрх этгээд ашиглах бөгөөд ректор болон эрх бүхий албан тушаалтны шийдвэрээр, хууль тогтоомжид нийцүүлэн гадагш задруулж болох мэдээлэл.

3.4. Төрийн болон албаны нууцын тухай хуулиар тогтоосон төрийн болон байгууллагын нууцад хамаарах мэдээллийн ангилал, тэмдэглэгээ, хадгалалт, дамжуулалт, танилцах, ашиглах, хамгаалахтай холбоотой харилцааг МУИС-ийн Нууцын журам болон холбогдох хууль тогтоомжийн дагуу зохицуулна.

3.5. Мэдээллийн хөрөнгийн ангиллыг мэдээллийн хөрөнгийн эзэмшигчийн санал, мэдээллийн аюулгүй байдлын мэргэжилтний дүгнэлтэд үндэслэн мэдээллийн технологи хариуцсан нэгжийн удирдлага тогтоож, өөрчилнө.

ДӨРӨВ. МЭДЭЭЛЛИЙН ХӨРӨНГИЙН ХЯНАЛТ, ХАМГААЛАЛТ

4.1. МУИС-ийн мэдээллийг үүсгэх, бүрдүүлэх, боловсруулах, дамжуулах, хадгалах, эзэмших үйл ажиллагаанд оролцож буй багш, ажилтан болон харилцагч байгууллагын ажилтан бүр мэдээллийг хамгаалах үүрэг хүлээнэ.

4.2. МУИС-ийн мэдээллийн хөрөнгө бүр нь мэдээллийн хөрөнгийн эзэмшигчийн тодорхойлсон хариуцагчтай байх бөгөөд тухайн хөрөнгийн ашиглалт, хамгаалалт, аюулгүй байдал, хяналтыг хариуцна.

4.3. Мэдээллийн технологи хариуцсан нэгж нь мэдээллийн хөрөнгийн эзэмшигчийг оролцуулан эрсдэлийн үнэлгээг жилд дор хаяж нэг удаа хийж, үнэлгээний үр дүнд үндэслэн шаардлагатай хяналт, хамгаалалтын арга хэмжээг тогтооно.

4.4. Мэдээллийг дамжуулахад тавигдах шаардлага:

4.4.1. Мэдээллийг хууль тогтоомж болон байгууллагын дотоод журамд заасан үндэслэл, зориулалтын дагуу дамжуулна.

4.4.2. Шаардлагаас илүү мэдээлэл дамжуулахыг хориглоно.

4.4.3. Мэдээлэл дамжуулахдаа нууцлал, бүрэн бүтэн байдал, хүртээмжийг хангах зарчмыг мөрдөнө.

4.4.4. Хүний хувийн мэдээлэл дамжуулах тохиолдолд мэдээллийн аюулгүй байдлыг хангах нөхцөл, хариуцлагыг тодорхой тусгана

4.4.5. Нээлттэйгээс бусад зэрэглэлийн мэдээллийг цаасан баримт, зөөврийн төхөөрөмж (USB, HDD гэх мэт) болон бусад биет хэлбэрээр дамжуулах үед зөвшөөрөлгүй хандалт, алдагдлаас хамгаалах арга хэмжээг мэдээллийн хөрөнгийн эзэмшигч хариуцан хэрэгжүүлнэ.

4.4.6. Цахим мэдээлэл дамжуулах нэмэлт шаардлага:

4.4.6.1. Мэдээллийг зөвхөн мэдээллийн аюулгүй байдлын шаардлага хангасан орчин, хамгаалагдсан сувгаар дамжуулна.

4.4.6.2. Албан ёсны бус цахим шуудан, хувийн чатаар нээлттэйгээс бусад мэдээлэл дамжуулахыг хориглоно.

4.5. Хязгаарлагдмал ангилалтай мэдээллийн хөрөнгийг цахим шуудангаар илгээх үед нууцлалын тодорхой зааж, зөвхөн эрх бүхий этгээдэд дамжуулах нөхцөлийг хангана.

4.6. Хязгаарлагдмал ангилалтай мэдээллийн хөрөнгийг файл хэлбэрээр дамжуулах тохиолдолд хүлээн авагчид урьдчилан нууцын зэрэглэлийг мэдэгдэж, зохих тэмдэглэгээ болон хамгаалалтын арга хэмжээг хэрэгжүүлнэ.

4.7. Хязгаарлагдмал ангилалтай мэдээллийн хөрөнгийн хандалт, ашиглалт, дамжуулалтыг дараах байдлаар зохицуулна:

4.7.1. Эрх бүхий хэрэглэгч мэдээлэлд хандах үед зохих анхааруулга харуулж, мэдээллийг хэвлэх, татаж авах үйлдэл бүрийн хэрэглэгчийг тодорхойлон бүртгэл хөтөлнө.

4.7.2. Мэдээлэлд хандах, боловсруулах, дамжуулахтай холбоотой үйлдлийн лог бүртгэлийг мэдээллийн хөрөнгийн эзэмшигч нь дотоод журмын дагуу бүртгэн хөтөлж, хадгална. Мэдээллийн хөрөнгийг зохих тусгай тэмдэглэгээтэй байна.

4.7.3. Мэдээллийг цахим шуудангаар илгээх үед мэдээллийн ангиллыг тодорхой зааж, зөвхөн эрх бүхий этгээдэд дамжуулах нөхцөлийг хангана.

4.7.4. Мэдээллийг файл хэлбэрээр дамжуулах тохиолдолд хүлээн авагчид мэдээллийн ангиллыг урьдчилан мэдэгдэж, зохих тэмдэглэгээ болон хамгаалалтын арга хэмжээг хэрэгжүүлнэ.

ТАВ. ХАНДАЛТЫН УДИРДЛАГА

5.1. Хандах эрхийг “боломжит хамгийн бага эрх” зарчмыг үндэслэн олгоно.

5.2. Мэдээллийн системд үүрэгт суурилсан хандалтын удирдлага аргачлалыг ашиглана.

5.3. Шинэ багш, ажилтанд эрх олгохдоо албан тушаал, гүйцэтгэх үүрэгт тохируулж хүний нөөцийн мэдээллийн системд тулгуурлан олгоно.

5.4. Суралцагчид эрх олгохдоо холбогдох сургалт удирдлагын мэдээллийн системд тулгуурлан олгоно.

5.5. Багш, ажилтан ажлаас гарах, гэрээ дуусах, албан тушаал шилжих үед хандах эрхийг хүний нөөц хариуцсан нэгж ажлын 3 (гурван) өдрийн дотор хаах эсвэл өөрчилнө.

5.6. Суралцагчийн хандах эрхийг холбогдох шийдвэр, тушаалд үндэслэн хариуцсан нэгж ажлын 3 (гурван) өдрийн дотор хаана.

5.7. Мэдээллийн системийн давуу эрхтэй хэрэглэгчийн бүртгэлийг мэдээллийн технологи хариуцсан нэгж хөтлөх бөгөөд мэдээллийн аюулгүй байдлын мэргэжилтэн хяналт тавьж, улирал тутам удирдлагад тайлагнан баталгаажуулна.

5.7.1. Түр хугацаанд давуу эрх олговол хугацаа, эрхийн хүрээ, хариуцагчийг заавал тэмдэглэж, хугацаа дуусмагц хандах эрхийг цуцлах ба хэрэгжилтэд мэдээллийн аюулгүй байдлын мэргэжилтэн хяналт тавина.

5.8. Гадаад сүлжээнээс МУИС-ийн дотоод сүлжээ, системд хандах тохиолдолд эрсдэл өндөртэй систем, давуу эрхтэй хэрэглэгчид VPN болон олон хүчин зүйлийн баталгаажуулалт (MFA) ашиглана.

5.9. Мэдээллийн системд нэвтрэх бүх үйлдэл лог файлд бүртгэгдэнэ.

ЗУРГАА. НУУЦ ҮГИЙН ШААРДЛАГА

6.1. МУИС-ийн мэдээллийн системд нэвтрэх багш, ажилтан, суралцагч болон эрх бүхий бусад этгээд нь нууц үгийн дараах шаардлагыг мөрдөнө.

6.1.1. Хэрэглэгчийн түвшний нууц үг нь том үсэг, жижиг үсэг, тоо, тусгай тэмдэгт бүхий 10 ба түүнээс дээш тэмдэгт орсон байна.

6.1.2. Давуу эрхтэй хэрэглэгчийн түвшний нууц үг нь том үсэг, жижиг үсэг, тоо, тусгай тэмдэгт бүхий 18 ба түүнээс дээш тэмдэгт орсон байна.

6.1.3. Нууц үгийг бусдад хялбар таагдахуйц үг, хувийн мэдээлэл, нийтлэг дараалал ашиглалгүйгээр үүсгэнэ.

6.1.4. Мэдээллийн системүүдэд нэвтрэх нууц үгийг ижил байдлаар үүсгэхгүй байна.

6.1.5. Нууц үг солих шаардлага:

6.1.5.1. Системээс олгогдсон анхдагч нууц үгийг заавал солих;

6.1.5.2. Тухайн системд ашигласан сүүлийн 3 нууц үгийг дахин хэрэглэхээс зайлсхийх;

6.1.5.3. Хэрэглэгчийн түвшний нууц үгийн хүчинтэй хугацаа дууссан үед;

6.1.5.4. Өөрийн эзэмшлийн төхөөрөмжөөс бусад төхөөрөмжид нууц үгийг сануулсан, холболтыг салгалгүй үлдээсэн тохиолдолд нэн даруй солих;

6.1.5.5. Хэрэв нууц үг илчлэгдсэн эсвэл алдсан гэж үзвэл нэн даруй солих;

6.1.6. Давуу эрхтэй хэрэглэгчийн түвшний нууц үгийн хүчинтэй хугацаа 90 хоногоос ихгүй байна. Бусад хэрэглэгчийн түвшний нууц үгийн хүчинтэй хугацааг системийн ашиглалт онцлогт нийцүүлэн тогтооно.

6.1.7. Нууц үгийн аюулгүй байдлыг хангахтай холбоотой хориглолт:

6.1.7.1. Нууц үгийг бусдад дамжуулах;

6.1.7.2. Нууц үгийг бусдад ил харагдах байдлаар бичиж тэмдэглэх, дамжуулах, түр хэрэглүүлэх;

6.1.7.3. Нууц үгийг хамгаалагдаагүй сувгаар дамжуулах, бусадтай хуваалцах;

6.1.7.4. Олон хүчин зүйлийн баталгаажуулалт (MFA) ашиглах боломжтой системд олон хүчин зүйлийн баталгаажуулалт ашиглахгүй байх;

6.1.7.5. Бусад ажилтны нууц үгийг тогтоох, ямар нэг аргаар тааж мэдэж авах, таахыг оролдох;

6.1.8. Нууц үгийн аюулгүй байдлыг хангахтай холбоотой арга хэмжээ:

6.1.8.1. Хэн нэгэн ил задгай тэмдэглэсэн, дамжуулсан бол даруй хэлж сануулна.

6.1.8.2. Илэрсэн зөрчлийг холбогдох нэгжид мэдээлнэ.

6.1.8.3. Нууц үг алдагдсан гэж үзсэн бол цаг алдалгүй холбогдох журмын дагуу мэдээлж, шаардлагатай хамгаалалтын арга хэмжээг авна.

ДОЛОО. ТЕХНИК ХАНГАМЖИЙН АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ

7.1. Техник хангамж гэдэгт мэдээлэл үүсгэх, боловсруулах, хадгалах, дамжуулах, ашиглахад хэрэглэгдэж буй компьютер, сервер, сүлжээний болон хадгалах төхөөрөмж, хэвлэх, хувилах төхөөрөмж, хяналт болон нэвтрэх систем зэргийн тоног төхөөрөмж хамаарна.

7.2. МУИС-ийн багш, ажилтан нь өөрийн эзэмшиж буй техник хангамжийг зөвхөн албан ажлын хэрэгцээнд, байгууллагын холбогдох журам, бодлогын дагуу ашиглана.

7.2.1. Техник хангамжийг ажлын байрнаас гадагш гаргах тохиолдолд холбогдох журмын дагуу урьдчилан зөвшөөрөл авч, гаргалт, буцаалтыг бүртгэлээр баталгаажуулна.

7.2.2. Компьютер нь нууц үгээр хамгаалагдсан байх бөгөөд ажлын байрнаас холдох үед компьютерыг заавал түгжих, эсхүл тодорхой хугацаанд идэвхгүй үед автоматаар түгжигдэх тохиргоог идэвхжүүлсэн байна.

7.3. МУИС-ийн мэдээллийн технологи хариуцсан нэгж, удирдлага болон хязгаарлагдмал мэдээлэлд ашиглаж байсан аливаа тоног төхөөрөмжийг шилжүүлэх, дахин ашиглуулах, устгах эсхүл актлах тохиолдолд техник хангамжийн хадгалах, санах ойг дахин сэргээх боломжгүй байдлаар цэвэрлэх (wipe) ба шаардлагатай тохиолдолд физик устгал хийж, тэмдэглэл үйлдэнэ.

7.4. Нээлттэйгээс бусад мэдээллийг үзүүлдэг дэлгэц, самбар гэх мэтийг техник хангамжийг зөвшөөрөлгүй этгээд үзэхээс сэргийлэх бүхий л арга хэмжээг авна.

7.5. Серверийг зориулалтын, аюулгүй байдал болон тасралтгүй ажиллагааны шаардлага хангасан орчинд байршуулна.

7.6. Серверийн өрөөн дэх тоног төхөөрөмжүүдийн хэвийн ажиллагаа доголдсон үед мэдэгдэх боломжтой шийдэлтэй байна.

7.7. Сервер болон сүлжээний тоног төхөөрөмжийг тоос, чийг, доргилт, цахилгаан соронзон орон, химийн бодисын нөлөөллөөс хамгаалах зохих арга хэмжээ авна.

7.8. Серверийн болон тоног төхөөрөмж байрлах орчинд хооллох, ундлах, тамхи татах, гал гаргахыг хатуу хориглоно.

7.9. Сервер компьютер болон бусад тоног төхөөрөмжийг үйлдвэрээс болон нийлүүлэгчээс дагалдан ирсэн техникийн болон аюулгүй ажиллагааны нөхцөл шаардлагын дагуу ашиглах ба анхны нэвтрэх нууц үгийг заавал солино.

7.10. Сервер компьютер нь заавал нэвтрэх нууц үгтэй байна. Нэвтрэх нууц үгийг ажил үүргийн хуваарийн дагуу хариуцсан ажилтан өөртөө хадгалах, мөн гамшгийн нөхцөлд нэвтрэх зорилгоор серверт нэвтрэх нэр, нууц үгийг тусгай лац бүхий дугтуйнд хийн аюулгүй газар хадгалж мэдээллийн технологи хариуцсан нэгжийн удирдлагын шийдвэрээр ашиглана.

7.11. Хортой кодоос хамгаалах шаардлага:

7.11.1. Мэдээллийн аюулгүй байдлыг хангах шаардлагатай мэдээллийн хөрөнгийг агуулж буй сервер, компьютер, мэдээлэл хадгалагч болон зөөврийн хэрэгслүүдэд зөвшөөрөгдсөн хортой кодын эсрэг программ хангамжийг ашиглаж шинэчлэлтийг тогтмол хийх.

7.11.2. Хортой кодын эсрэг программ хангамжийн бодит хугацааны хамгаалалт тохиргоо идэвхтэй байлгах.

7.11.3. Тогтмол хугацаанд хортой кодын эсрэг программыг уншуулж, хортой код илэрсэн тохиолдолд арилгах арга хэмжээг авна.

7.11.4. Давуу эрхтэй хэрэглэгчээр гаднаас мэдээлэл оруулах тохиолдолд сүлжээнд холбогдоогүй төхөөрөмжид эхэлж хортой кодын шинжилгээг заавал хийж аюулгүй тохиолдолд нэвтрүүлэх.

НАЙМ. СҮЛЖЭЭНИЙ АШИГЛАЛТ, НУУЦЛАЛ, ХАМГААЛАЛТ

8.1. Мэдээллийн технологи хариуцсан нэгжийн зөвшөөрөлгүйгээр МУИС-ийн сүлжээг өөрчлөх, төхөөрөмжийг салгах, залгах, сүлжээний тохиргоог дур мэдэн өөрчлөхийг хориглоно.

8.2. Сүлжээний кабелийг гадна цахилгаан соронзон орон болон цахилгаан дамжуулах утаснаас зайтай байрлуулна. Зайлшгүй тохиолдолд хамгаалалтын давхаргатай кабель ашиглана.

8.3. Сүлжээний утас, сувагчлалыг ил задгай болон олон нийтийн хэсгээр байрлуулахаас зайлсхийнэ.

8.4. Сүлжээний зохион байгуулалтыг мэдээллийн технологи хариуцсан нэгжийн удирдлагаар баталгаажуулж, сүлжээ хариуцсан администратор хэрэгжүүлнэ.

8.5. Сүлжээ хариуцсан администратор нь сүлжээ хооронд хандах хандалтын аюулгүй байдлын тохиргоог хийж мэдээллийн аюулгүй байдлын мэргэжилтэн тогтмол хяналт тавина.

8.6. Сүлжээ хариуцсан администратор нь сүлжээний ашиглаагүй төгсгөлийн цэгүүд, портыг хамгаалж идэвхгүй болгох эсхүл унтраана.

8.7. Гуравдагч талын холболтыг үндсэн сүлжээнээс бүрэн тусгаарлах шийдлийг сүлжээ хариуцсан администратор хэрэгжүүлэх ба мэдээллийн аюулгүй байдлын мэргэжилтэн хяналт тавин ажиллана.

ЕС. СИСТЕМД НЭВТРЭХ, ЛОГ БҮРТГЭЛ, ХАМГААЛАЛТ

9.1. Мэдээллийн систем, программ хангамж, техник хангамжийг суурилуулахад тавигдах шаардлага:

9.1.1. МУИС-ийн үйл ажиллагаанд шинээр мэдээллийн систем, программ хангамж, тоног төхөөрөмж нэвтрүүлэх, ашиглалтад оруулах тохиолдолд мэдээллийн технологи хариуцсан нэгжтэй урьдчилан зөвшилцөнө.

9.1.2. МУИС нь үйл ажиллагаандаа оюуны өмчийн зөрчилгүй мэдээллийн систем, программ хангамж ашиглана.

9.1.3. Мэдээллийн систем, программ хангамжийг худалдаж авахдаа зөвхөн албан ёсны нийлүүлэгч, түүний итгэмжлэгдсэн төлөөлөгчөөс худалдаж авахыг зорино.

9.2. Нэвтрэлтийн аюулгүй байдлын шаардлага:

9.2.1. Нэвтрэх нууц үг нь тус журмын 6-р бүлэгт заасан нууц үгийн шаардлагыг хангасан байна.

9.2.2. Шаардлагатай тохиолдолд мэдээллийн системд тусгагдсан шаардлагын дагуу хэрэглэгч заавал олон хүчин зүйлийн баталгаажуулалт ашиглана.

9.2.3. Нэвтрэх нууц үгийг таах оролдлогоос хамгаалж амжилтгүй 5 оролдлогын дараа 30 минутын турш нэвтрэх эрхийг автоматаар хязгаарлах тохиргоо, шийдлийг нэвтрүүлсэн байна.

9.2.4. Системд тодорхой хугацаанд үйлдэл хийгдэхгүй, идэвхгүй байгаа тохиолдолд автоматаар системээс гарч, холболтын мэдээллийг устгах тохиргоог хийсэн байна.

9.3. Системийн лог бүртгэлийн шаардлага:

9.3.1. Мэдээллийн системд администратор, давуу эрхтэй хэрэглэгч болон энгийн хэрэглэгчийн нэвтрэлт, хандалт, системийн үйл ажиллагааны бүх үйлдлийг лог бүртгэлийн системд автомат хэлбэрээр бүртгэж, логийн бүрэн бүтэн байдлыг хангах техникийн шийдэл ашиглана.

9.3.2. Галт хана, сервер, өгөгдлийн сан, веб сервер, цахим шуудан, VPN, домэйн болон дотоод, гадаад хөгжүүлэлттэй мэдээллийн системүүдийн үйл ажиллагааны логийг боломжит бүх түвшинд бүртгэнэ.

9.3.3. Лог бүртгэлд хэрэглэгчийг таних мэдээлэл, төхөөрөмжийг таних мэдээлэл, огноо, хийсэн үйлдэл, өөрчлөлт зэргийг заавал агуулна.

9.3.4. Хэрэглэгчийн эрх нээх, өөрчлөх, хаах, устгах бүх үйлдэл лог бүртгэлд заавал бүртгэгдэнэ.

9.3.5. Системд амжилттай болон амжилтгүй нэвтрэх оролдлого бүрийг лог бүртгэнэ.

9.3.6. Мэдээллийн систем, сүлжээ болон серверийн тоног төхөөрөмжийн лог бүртгэлийг хариуцсан ажилтан хөтлөн хэрэгжүүлж, логийн бүрэн бүтэн байдал, хүртээмжтэй байдал болон хамгаалалтыг хангана. Логийг устгах, өөрчлөхөөс сэргийлэх техникийн болон зохион байгуулалтын арга хэмжээг хэрэгжүүлнэ.

9.3.7. Мэдээллийн аюулгүй байдлын мэргэжилтэн лог бүртгэлд тогтмол хяналт тавьж, түүнийг системийн эрсдэлийн үнэлгээнд үндэслэн тогтоосон хугацаанд хадгалах, архивлах нөхцөлийг баталгаажуулна.

9.3.8. Нэгдсэн лог бүртгэлд мэдээллийн технологи хариуцсан нэгжийн удирдлага, мэдээллийн аюулгүй байдлын мэргэжилтэн болон эрх бүхий администратораас бусад этгээд хандахыг хориглоно.

9.3.9. Лог бүртгэлийн статистик мэдээллийг тогтмол давтамжаар мэдээллийн аюулгүй байдлын мэргэжилтэн нэгжийн удирдлагад тайлагнана.

АРАВ. ҮҮЛЭН ОРЧНЫ КРИПТОГРАФ, ХАМГААЛАЛТ, ХЯНАЛТ

10.1. Шифрлэлт ба өгөгдлийн хамгаалалт

10.1.1. Үүлэн орчин болон мэдээллийн системд хадгалагдаж буй мэдээллийг олон улсад хүлээн зөвшөөрөгдсөн, шифрлэлтийн болон хэшийн алгоритм ашиглан хамгаална. Нууц үгийг эх текст хэлбэрээр хадгалахыг хориглоно.

10.1.2. Өгөгдлийн санд нууц үг болон хүний хувийн мэдээллийг шифрлэж хадгална.

10.1.3. Хүний хувийн болон нууц мэдээлэл агуулсан сүлжээний урсгал болон логийг хамгаалалттай (шифрлэгдсэн) хэлбэрээр хадгална.

10.1.4. Шифрлэлтийн түлхүүрийн нууцлалыг мэдээллийн аюулгүй байдлын мэргэжилтэн хариуцна.Түлхүүрийг шинэчлэх хугацаа 12 сараас ихгүй байна.

10.2. Үүлэн тооцооллын системд мэдээллийн аюулгүй байдлын шаардлагад нийцсэн хамгаалалтын тохиргоог ашиглана.

10.2.1. Хүний хувийн мэдээлэл, санхүүгийн мэдээллийг үүлэн тооцооллын системд байршуулах тохиолдолд зөвхөн олон улсын стандарт, шаардлагад нийцсэн үүлэн үйлчилгээ ашиглана.

10.2.2. Мэдээллийг зөвхөн Монгол улсад ашиглахаар хуульд заасан бол тухайн өгөгдлийг ашиглаж боловсруулах систем нь холбогдох хууль, зохицуулалтын шаардлагыг зөрчихгүй байна.

10.2.3. Үүлэн тооцооллын орчинд алдаатай тохиргооноос сэргийлэх хамгаалалтын шийдлийг ашиглаж, тогтмол хяналт хийнэ.

10.3. Үүлэн орчны сүлжээний хуваалтыг дотоод сүлжээний хамгаалалтын түвшнээс доогуургүйгээр тохируулж ашиглах ба мэдээллийн аюулгүй байдлын мэргэжилтэн хяналт тавина.

10.4. Өгөгдөл дамжуулалт ба интеграцид тавигдах шаардлага:

10.4.1. Үүлэн тооцооллын систем болон дотоод систем хооронд өгөгдөл дамжуулах үед нууцлалтай сүлжээ ашиглах ба өгөгдлийн аюулгүй байдлыг хангах.

10.4.2. API хандалтад хүсэлтийн давтамжийн хязгаарлалт (rate limit) болон хамгаалалтын тохиргоо ашиглах.

10.4.3. Webhook ашиглах тохиолдолд заавал нууцлалтай холболт ашиглах.

10.5. Үүлэн тооцооллын системийн хэрэглэгч заавал олон хүчин зүйлийн баталгаажуулалт ашиглана.

10.6. Үүлэн тооцооллын системийн логийг мэдээллийн аюулгүй байдлын мэргэжилтэн тогтоосон давтамжаар шалгаж тайланг нэгжийн удирдлагад хүргүүлнэ.

10.7. Үүлэн тооцооллын системд зөрчил илэрсэн тохиолдолд холбогдох журмын дагуу нэн даруй шийдвэрлэнэ.

АРВАН НЭГ. ЦАХИМ МЭДЭЭЛЭЛ, ӨГӨГДЛИЙН САНГИЙН НӨӨЦЛӨЛТ, ХАДГАЛАЛТ

11.1. Албан ажлын хэрэгцээний чухал шаардлагатай мэдээллийг устах эрсдэлээс сэргийлж нөөцлөлт хуулбарыг үүсгэн байгууллагын үүлэн хадгалалтын системд хадгалах тохиргоог заавал хийсэн байна.

11.2. Цахим мэдээллийн нөөцлөлтийг мэдээллийн системийн ач холбогдол, эрсдэлийн түвшинд үндэслэн тодорхойлсон хуваарийн дагуу хийж, жилд дор хаяж нэг удаа бүрэн нөөцлөлт хийнэ.

11.3. Мэдээллийн технологийн хариуцсан нэгж нь өөрийн хариуцсан мэдээллийн систем, программ хангамжийн өгөгдлийн сангийн нөөцлөлтийг нэгжийн удирдлагаас баталсан хуваарийн дагуу хэрэгжүүлнэ.

11.4. Нөөцлөлт болон архивын өгөгдөл хадгалагдаж буй сервер, хадгалах төхөөрөмжийг аюулгүй байдлыг хангасан орчинд байршуулна.

АРВАН ХОЁР. МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХАД ХҮЛЭЭХ ҮҮРЭГ

12.1. Багш, ажилтны нийтлэг үүрэг:

12.1.1. Мэдээллийн аюулгүй байдлын журам болон бусад холбогдох журмуудыг дагаж мөрдөх.

12.1.2. Мэдээллийн хөрөнгө, өөрийн ашиглаж буй компьютер, сүлжээ, системд мэдээллийн аюулгүй байдлын зөрчил, тохиол, эсхүл аюул занал илэрсэн, эсхүл сэжиглэгдсэн тохиолдолд мэдээллийн технологийн хариуцсан нэгжид нэн даруй мэдэгдэх.

12.1.3. Ажлын байр, орчинд байрлах мэдээллийн технологийн дэд бүтэц, сүлжээний утас гэмтсэн, доголдсон, ил гарсан, эсхүл мэдээллийн аюулгүй байдалд сөргөөр нөлөөлж болзошгүй нөхцөл илэрсэн тохиолдолд мэдээллийн технологийн хариуцсан нэгжид мэдэгдэх.

12.1.4. Мэдээллийн хөрөнгийн эзэмшигч эсвэл хариуцагч ажлаас гарах, албан тушаал өөрчлөгдөх үед өөрийн ашиглаж, үүсгэсэн болон хариуцаж байсан бүх мэдээллийн хөрөнгө, тоног төхөөрөмжийг эрх бүхий албан тушаалтанд бүрэн, албан ёсоор шилжүүлэх.

12.1.5. Байгууллагын мэдээллийн хөрөнгөнд эрх бүхий хяналт, шалгалт хийх үед саад учруулахгүй, шаардлагатай нөхцөл, мэдээлэл, оролцоог бүрэн хангах.

12.1.6. Харилцагч, иргэн, гэрээт болон хамтран ажиллагч байгууллагад байгууллагын мэдээллийн аюулгүй байдлын бодлого, журам, шаардлагыг танилцуулж, мөрдүүлэх болон хэрэгжилтэд хяналт тавих.

12.2. Мэдээллийн хөрөнгө эзэмшигчийн эрх, үүрэг:

12.2.1. Мэдээллийн хөрөнгийн бүрэн бүтэн байдал, хүртээмж, нууцлалын шаардлагыг хангах зорилгоор зохион байгуулалтын арга хэмжээг хэрэгжүүлэх.

12.2.2. Мэдээллийн хөрөнгийн хандалтын бодлогыг тодорхойлж, хэрэгжилтэд хяналт тавих.

12.2.3. Хандалтын эрхийг “шаардлагатай доод эрхийн зарчим”-д үндэслэн олгох, өөрчлөх, цуцлах үйл ажиллагааг зохицуулах.

12.2.4. Нөөц хуулбарын хадгалалт, сэргээх ажиллагааны найдвартай байдлыг хангах.

12.2.5. Мэдээллийн хөрөнгийн ашиглалт, хөдөлгөөнд дотоод хяналт тавих.

12.2.6. Мэдээллийн аюулгүй байдлын бодлого, журам, стандартын хэрэгжилтэд нийцлийг хангах.

12.2.7. Мэдээллийн хөрөнгийг шилжүүлэх, өөрчлөх, устгах, актлах үйл ажиллагааг батлагдсан журмын дагуу гүйцэтгэх.

12.2.8. Мэдээллийн аюулгүй байдлын зөрчил, тохиолдол болон онцгой нөхцөл байдал үүссэн үед системийг сэргээх, хэвийн ажиллагааг хангах арга хэмжээ, гүйцэтгэх дараалал, хариуцах нэгж, ажилтныг тодорхойлсон сэргээн ажиллагааны төлөвлөгөөг боловсруулж мөрдүүлэх.

12.3. Мэдээллийн технологи хариуцсан нэгжийн эрх, үүрэг:

12.3.1. Мэдээллийн систем, сүлжээ, мэдээллийн технологийн дэд бүтэц болон мэдээллийн аюулгүй байдлын эсрэг заналхийлэл, халдлагыг илрүүлэх, бүртгэх, таслан зогсоох, эмзэг байдлыг тодорхойлох болон бууруулах арга хэмжээг хэрэгжүүлэх.

12.3.2. Мэдээллийн аюулгүй байдлыг хангах техникийн болон зохион байгуулалтын шийдлийг боловсруулж, хэрэгжүүлэх, дэмжлэг үзүүлэх.

12.3.3. Нэгжийн хариуцсан мэдээллийн хөрөнгөд мэдээллийн аюулгүй байдлын зөрчил, тохиолдол болон онцгой нөхцөл байдал үүссэн үед системийг сэргээх, хэвийн ажиллагааг хангах арга хэмжээ, гүйцэтгэх дараалал, хариуцах нэгж, ажилтныг тодорхойлсон сэргээн ажиллагааны төлөвлөгөөг боловсруулж мөрдүүлэх.

12.3.4. МУИС-ийн үйл ажиллагаанд ашиглаж буй мэдээллийн системийн талаарх бүртгэлийг хөтлөх бөгөөд шинэчлэл, өөрчлөлт, засвар үйлчилгээ бүртгэх.

12.3.5. МУИС-ийн мэдээллийн технологийн дэд бүтэц, сүлжээний төхөөрөмжийн хэвийн ажиллагааг хангах зорилгоор шаардлагатай тоног төхөөрөмжийн хүчин чадал, нөөцийн ашиглалтад тогтмол хяналт тавьж, шаардлагатай тохиолдолд хүчин чадлыг нэмэгдүүлэх, сайжруулах арга хэмжээг төлөвлөн хэрэгжүүлнэ.

12.3.6. Мэдээллийн технологи хариуцсан нэгжийн удирдлагын эрх, үүрэг:

12.3.6.1. МУИС-ийн мэдээллийн аюулгүй байдлын чиглэлээр үйл ажиллагааг удирдан зохион байгуулах, стратегийн болон үйл ажиллагааны түвшний чиглэл, зөвлөмж өгөх.

12.3.6.2. Мэдээллийн аюулгүй байдлын асуудлаар шууд удирдлагыг тогтмол болон шаардлагатай үед мэдээллээр хангах.

12.3.6.3. Байгууллагыг төлөөлөн мэдээллийн аюулгүй байдлын чиглэлээр гадаад болон дотоод сонирхогч талуудтай харилцах эрхийг хэрэгжүүлэх.

12.3.6.4. Мэдээллийн аюулгүй байдлын бодлого, журам, стандарт боловсруулах, шинэчлэх, сайжруулах үйл ажиллагаанд оролцож, батлуулах ажлыг зохион байгуулах.

12.3.6.5. Мэдээллийн аюулгүй байдлын бодлого, журам, стандартын хэрэгжилтэд хяналт тавих.

12.3.6.6. Мэдээллийн аюулгүй байдлын стратеги төлөвлөлтийг боловсруулж, байгууллагын стратеги болон холбогдох төлөвлөгөөнд тусгуулах.

12.3.6.7. Мэдээллийн аюулгүй байдлын шаардлага зөрчсөн тохиолдолд хариуцлага тооцох санал боловсруулж удирдлагад хүргүүлэх.

12.3.6.8. Бусад холбогдох журамд заасан эрх, үүргийг хэрэгжүүлнэ.

12.3.7. Мэдээллийн аюулгүй байдлын мэргэжилтний эрх, үүрэг:

12.3.7.1. Мэдээллийн аюулгүй байдлын бодлого, журам, стандартын хэрэгжилтийг хангах, хяналт тавих, сайжруулах санал боловсруулах.

12.3.7.2. Мэдээллийн хөрөнгө, системийн эрсдэлийг үнэлэх, эмзэг байдлыг тодорхойлох, бууруулах арга хэмжээг төлөвлөх, хамгаалалтын түвшнийг тогтоох, сайжруулах санал боловсруулах, хөндлөнгийн хяналтыг хэрэгжүүлэх.

12.3.7.3. Мэдээллийн аюулгүй байдлын зөрчил, тохиолдлыг илрүүлэх, бүртгэх, үр дагаврыг үнэлэх, шаардлагатай хариу арга хэмжээ авах, оролцох.

12.3.7.4. Хамгаалалтын системүүд, дотоод болон гадаад сүлжээ, зайнаас ажиллах орчны ажиллагаа, тохиргоо, мэдээллийн аюулгүй байдлын хэрэгжилтэд хяналт тавих.

12.3.7.5. Үйлдлийн бүртгэл (log) болон мэдээллийн аюулгүй байдлын хяналт хийх, бүртгэлд шинжилгээ хийх, зөрчлийг илрүүлэх, дүнг нэгжийн удирдлагад тайлагнах.

12.3.7.6. Мэдээллийн аюулгүй байдлын мэдлэг, ойлголтыг нэмэгдүүлэх сургалт, таниулгын ажлыг зохион байгуулах.

12.3.7.7. Мэдээллийн аюулгүй байдлын шалгалт, үнэлгээний дүн, илэрсэн зөрчил болон хэрэгжүүлсэн арга хэмжээний тайланг тогтоосон хугацаанд удирдлагад танилцуулах.

12.3.8. Администраторын эрх, үүрэг:

12.3.8.1. Мэдээллийн аюулгүй байдлын шаардлагад нийцүүлэн хэрэглэгчийн хандалтын эрхийг удирдах, зөрчил илэрсэн тохиолдолд түр хугацаанд хязгаарлах эсвэл хаах арга хэмжээ авах.

12.3.8.2. Мэдээллийн систем, дэд бүтэц, өгөгдлийн сангийн хэвийн ажиллагаа, бүрэн бүтэн байдал, хүртээмжийг хангах, нөөцлөлт болон сэргээх ажиллагааг гүйцэтгэх.

12.3.8.3. Сервер, систем, сүлжээний засвар үйлчилгээ, шинэчлэл, өөрчлөлтийг гүйцэтгэх болон гүйцэтгэлд хяналт тавих.

12.3.8.4. Мэдээллийн системийг суурилуулах, тохируулах, турших, хэвийн ажиллагаанд оруулах болон тасралтгүй ажиллагааг хангах.

12.3.8.5. Сервер, өгөгдлийн сан, сүлжээний төхөөрөмжүүдийг хортой код, зөвшөөрөлгүй хандалтаас хамгаалах техникийн хамгаалалтын тохиргоог хэрэгжүүлэх.

12.3.8.6. Мэдээллийн систем, сүлжээний ажиллагаа, хандалт, аюулгүй байдлын үндсэн лог, мониторингийн ажиллагааг техникийн түвшинд хангах.

12.3.8.7. Мэдээллийн систем, сүлжээний тасалдал, халдлага, доголдлын үед анхан шатны хариу арга хэмжээ авч, системийн хэвийн ажиллагааг сэргээх үйл ажиллагааг хэрэгжүүлэх.

12.3.8.8. Мэдээллийн хамгаалалтын техникийн шийдлүүдийг хэрэгжүүлэх, ажиллагааг тогтмол хэвийн байлгах.

АРВАН ГУРАВ. ХАРИУЦЛАГА

13.1 МУИС-ийн мэдээллийн аюулгүй байдлын журам зөрчигдсөн тохиолдолд нөхцөл байдал, зөрчлийн шинж чанарыг харгалзан МУИС-ийн Хөдөлмөрийн дотоод журам болон холбогдох хууль тогтоомжийн дагуу зохих арга хэмжээ авна.

--ooOoo--