ИРГЭНИЙ НИСЭХИЙН ЕРӨНХИЙ ГАЗРЫН ДАРГЫН ТУШААЛ

2023 оны 04 сарын 18 өдөр Дугаар А/113 Улаанбаатар хот

Журам батлах тухай

Засгийн газрын агентлагийн эрх зүйн байдлын тухай хуулийн 8 дугаар зүйлийн 8.4 дэх хэсэг, Кибер аюулгүй байдлын тухай хуулийн 7 дугаар зүйлийн 7.2 дахь хэсэг, 19 дүгээр зүйлийн 19.2.1 дэх заалтыг тус тус үндэслэн ТУШААХ нь:

1.Иргэний нисэхийн ерөнхий газрын "Кибер аюулгүй байдлыг хангах үйл ажиллагааны дотоод журам"-ыг хавсралт ёсоор батлуулсугай.

2.Журмыг мөрдөн ажиллахыг Иргэний нисэхийн ерөнхий газар, түүний харьяа салбар, нэгжүүдэд үүрэг болгосугай.

3.Журмын хэрэгжилтэд хяналт тавьж ажиллахыг Дотоод аудитын алба (Б.Мөнх-Очир)-нд, Иргэний нисэхийн үндэсний төв (Н.Батсайхан)-д тус тус үүрэг болгосугай.

4.Энэхүү тушаал гарсантай холбогдуулан Иргэний нисэхийн ерөнхий газрын даргын 2015 оны 10 дугаар сарын 02-ны өдрийн "Журам батлах тухай" А/620 дугаартай тушаалыг хүчингүй болсонд тооцсугай.

ДАРГА Ч.МӨНХТУЯА

Иргэний нисэхийн ерөнхий газрын даргын
2023 оны 04 дүгээр сарын 18-ны өдрийн
А/113 дугаар тушаалын хавсралт

КИБЕР АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ҮЙЛ АЖИЛЛАГААНЫ ДОТООД ЖУРАМ

НЭГ. НИЙТЛЭГ ҮНДЭСЛЭЛ

1.1. Иргэний нисэхийн ерөнхий газрын мэдээллийн аюулгүй байдлын удирдлагын тогтолцоог бий болгох, нийтийн үйлчилгээний сүлжээ, мэдээллийн системийн найдвартай ажиллагаа, мэдээллийн сангийн нууцлал, аюулгүй байдлыг хангах, гаднаас болон дотоодоос учирч болох халдлага, аюул заналаас урьдчилан сэргийлэх, хор хохирол эрсдэл учирсан тохиолдолд нэн даруй шаардлагатай арга хэмжээг авахтай холбогдсон харилцааг энэхүү журмаар зохицуулна.

1.2. Энэхүү журмын зорилго нь мэдээллийн аюулгүй байдлын тогтолцоог бий болгохдоо дараах стандартуудыг мөрдөж, мэдээллийн аюулгүй байдлыг хангах, эрсдэлээс урьдчилан сэргийлэхэд оршино.

- Мэдээллийн технологи – Аюулгүй байдлын аргачлал – Мэдээллийн аюулгүй байдлын удирдлагын үйл ажиллагааны дүрэм – MNS 27002:2007
- Мэдээллийн технологи – Аюулгүй байдлын арга техник – Мэдээллийн ба холбооны технологийн аюулгүй байдлын удирдлага 1-р хэсэг: Мэдээлэл холбооны технологийн аюулгүй байдлын үндсэн ойлголтууд болон загварууд – MNS 13335-1:2009
- Мэдээллийн технологи – Аюулгүй байдлын арга техник – Мэдээллийн аюулгүй байдлын эрсдэлийн удирдлага – MNS 5969:2009
- Мэдээллийн технологи – Аюулгүй байдлын арга техник – Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоо шаардлага – MNS 27001:2009

1.3. Иргэний нисэхийн ерөнхий газрын мэдээллийн системд хандан ажиллаж байгаа бүх ажилтан, албан хаагч, гэрээт ажилтан энэхүү журмыг үйл ажиллагаандаа мөрдөж ажиллана.

1.4. Энэхүү журамд хэрэглэсэн дараах нэр томьёог дор дурдсан утгаар ойлгоно.

1.4.1 “**Байгууллагын мэдээлэл**” гэж ямар хэлбэрээр оршин байгаагаас үл хамааран уншиж ойлгож болох бүх төрлийн баримт бичиг, өгөгдлийг хэлнэ.

1.4.2. “**Эд хөрөнгө**” гэж байгууллага өөрөө мэдэж захиран зарцуулах эрхтэй, байгууллагад үнэ цэнэтэй биет болон биет бус эд зүйлийг хэлнэ.

1.4.3. “**Мэдээлэл эзэмшигч**” гэж албан ажлаа гүйцэтгэх явцдаа аливаа мэдээллийг олж мэдсэн, танилцсан, цуглуулсан, тухайн мэдээллийг эзэмшиж байгаа ажилтныг хэлнэ.

1.4.4. “**Мэдээлэл хариуцагч**” гэж мэдээллийг эзэмшиж байгаа ажилтан болон дээд албан тушаалтныг хэлнэ.

1.4.5. “**Мэдээллийн аюулгүй байдал хариуцсан нэгж**” гэж байгууллагын мэдээллийн аюулгүй байдал, мэдээллийн технологийн үйл ажиллагааны хэвийн нөхцөлийг хангах чиг үүрэг бүхий нэгжийг хэлнэ.

1.4.6. “**Мэдээллийн технологи хариуцсан нэгж**” гэж байгууллагын мэдээллийн технологийн үйл ажиллагааны хэвийн нөхцөлийг хангах чиг үүрэг бүхий нэгжийг хэлнэ.

1.4.7. “**Мэдээллийн технологи хариуцсан ажилтан**” гэж байгууллагын мэдээллийн технологи хариуцсан эрх, үүрэг бүхий албан тушаалтныг хэлнэ.

1.4.8. "**Мэдээллийн систем хариуцсан ажилтан**" гэж байгууллагын мэдээллийн систем болон сервер тоног төхөөрөмжүүдийг хариуцсан эрх, үүрэг бүхий албан тушаалтныг хэлнэ.

1.4.9. "**Мэдээллийн аюулгүй байдал**" гэж мэдээллийн нууцлал, бүрэн бүтэн, хүртээмжтэй байдлыг хадгалах болон хангах зорилгоор мэдээллийн бодит байдал, эх хувь, хариуцлагатай, тасралтгүй, найдвартай байдал зэрэг бусад шинжүүдийг хангахыг хэлнэ.

1.4.10. "**Мэдээллийн аюулгүй байдлын тогтолцоо**" гэж мэдээллийн аюулгүй байдлыг хангах, хэрэгжүүлэх, хянах, дэмжих, сайжруулахын тулд систем, програм хангамж, тоног төхөөрөмж, тэдгээртэй ажиллах дүрэм, журам, ажилтнуудын харилцан үйл ажиллагааны үр дүнд бий болсон цогцыг хэлнэ.

1.4.11. "**Мэдээллийн аюулгүй байдлын учрал**" гэж мэдээллийн аюулгүй байдлын бодлого, аюулгүй байдал зөрчигдсөн гэдгийг илэрхийлж буй систем, үйлчилгээ, сүлжээний байдлыг бий болгосон тохиолдол, будлиан эсхүл аюулгүй байдалтай холбоотой, өмнө нь тохиолдож байгаагүй нөхцөл байдлыг хэлнэ.

1.4.12. "**Аюул занал**" гэж байгууллагын үйл ажиллагааг алдагдуулах, мэдээллийн аюулгүй байдалд заналхийлэх бодит боломжтой, гэнэтийн эсвэл дэс дараалсан учралуудыг хэлнэ.

1.4.13. "**Эрсдэлийн үнэлгээ**" гэж эрсдэлийн ач холбогдлыг тодорхойлохын тулд байж болох эрсдэлийг өгөгдсөн шалгууруудтай харьцуулах үйл явцыг хэлнэ.

1.4.14. "**Лог файл**" мэдээллийн системд хандан ажиллаж буй хэрэглэгчийн үйлдлүүдийг тэмдэглэн авч баримтжуулдаг системийн файлыг хэлнэ.

1.4.15. **"Мэдээллийн нууцын зэрэглэл"** Байгууллагын мэдээллийн нууцын зэрэглэлийн дагуу мэдээлэлд тогтоох хамгаалалтын түвшинг хэлнэ.

1.4.16. **"VPN /Virtual Private Network/ холболт"** Интернэт сүлжээг ашиглан хувийн, нууцлалтай сүлжээг ашиглах боломжийг хэлнэ.

ХОЁР. ХАМРАХ ХҮРЭЭ

2.1. Мэдээлэл болон түүнтэй холбоотой үйл явц, мэдээллийн систем, сүлжээ нь байгууллагын эд хөрөнгө мөн бөгөөд хамгаалагдаж бүртгэгдсэн байна.

2.2. Байгууллагын мэдээлэл бүрэн бүтэн байх шаардлагын дагуу мэдээллийг дамжуулах, боловсруулах үеийн санамсаргүй болон санаатай өөрчлөлт нь хянагддаг байна.

2.3. Байгууллагын мэдээлэл, мэдээллийн системүүд нь нууцын зэрэглэлээр ангилагдаж эрх олгогдоогүй этгээдэд хаалттай, хандах боломжгүй бөгөөд нууцлалтай байна.

2.4. Байгууллагын мэдээлэл, мэдээллийн системүүд нь нууцын зэрэглэлээр ангилагдаж, эрх бүхий этгээд цаг алдалгүй хандах ашиглах боломжтой бөгөөд хүртээмжтэй байна.

2.5. Иргэний нисэхийн ерөнхий газрын мэдээллийн аюулгүй байдлыг хангах үйл ажиллагааны хүрээнд аюул ослын үед ажиллах төлөвлөгөөтэй байж аюул осол, эрсдэлээс урьдчилан сэргийлж ажиллана.

2.6. Энэхүү журмын биелэлт, техник технологийн дэвшлийг харгалзан шаардлагатай тохиолдолд нэмэлт өөрчлөлт оруулж, Иргэний нисэхийн ерөнийй газрын даргын тушаалаар батална.

ГУРАВ. БАЙГУУЛЛАГЫН МЭДЭЭЛЛИЙН АНГИЛАЛ, НУУЦЫН ЗЭРЭГЛЭЛ, ЭД ХӨРӨНГӨ

3.1. Байгууллагын мэдээллийг дараах байдлаар ангилна. Үүнд:

3.1.1. Биет мэдээлэл (Эрх зүйн баримт бичиг, үндсэн болон нэмэлт үйл ажиллагааны хүрээнд боловсруулсан болон цуглуулсан мэдээлэл, тайлан, төлөвлөгөө, төсөл хөтөлбөр, бүртгэлийн мэдээлэл, сургалтын материал, тараах хуудас, гарын авлага, хэвлэмэл зураг зэрэг бүх төрлийн цаасан суурьт мэдээллүүд);

3.1.2. Биет бус мэдээлэл (Биет мэдээллийн цахим хэлбэр, өгөгдлийн сан, файлын сан, цахим шуудан, дүрс бичлэг, дуу бичлэг зэрэг мэдээллүүд);

3.1.3. Бусад төрлийн цахим мэдээллүүд;

3.2. Байгууллагын хэмжээнд боловсруулагдан ашиглах болон хадгалах бичиг баримт, өгөгдлийг хэрэглээний зориулалт, нууцлалаас хамаарч мэдээллийн нууцын зэрэглэлийг дараах байдлаар тогтооно. Үүнд:

3.2.1. Маш нууц (Зэрэглэл4): Байгууллагын нууц мэдээллийг хадгалах бөгөөд зөвхөн тухайн мэдээллийг хариуцагч буюу нэвтрэх эрх бүхий албан тушаалтан нэвтрэх мэдээллүүд;

3.2.2. Нууц (Зэрэглэл3): Байгууллагын ажилтан тодорхой эрхийн хүрээнд хязгаарлалтайгаар ашиглах боломжтой, "Хувь хүний нууцын тухай" хуулиар хамгаалагдсан мэдээллүүд;

3.2.3. Дотоод хэрэгцээнд (Зэрэглэл2): Байгууллагын бүх ажилтанд зориулсан, байгууллагын үндсэн болон нэмэлт үйл ажиллагаатай холбоотой, байгууллага дотор нээлттэй, гадагш задруулахгүй мэдээллүүд;

3.2.4. Олон нийтэд зориулагдсан мэдээлэл (Зэрэглэл1): Хувилах, хадгалах дамжуулахад ямар нэгэн шаардлага тавихгүй нийтэд зориулагдсан, нууцлах шаардлагагүй, "Мэдээллийн ил тод байдал ба мэдээлэл авах эрхийн тухай" хуульд заасан мэдээллүүд;

3.3. Мэдээлэл, мэдээллийн системийн нууцын зэрэглэлийн жагсаалт

3.3.1. Байгууллагын эрх бүхий албан тушаалтнууд нь өөрийн хариуцсан алба нэгжийн маш нууц, нууц зэрэглэлд хамаарах бичиг баримтын нэрс, нууцад байх хугацаа тэдгээртэй танилцах эрх бүхий албан тушаалтны жагсаалтыг гарган мэдээллийн нууцын зэрэглэлийг тодорхойлж, Мэдээллийн аюулгүй байдал хариуцсан нэгжид хүргүүлэн батлуулж жил бүр шинэчлэл хийдэг байна.

3.3.2. Мэдээллийн систем бүрд "Хэрэглэгчийн мэдээллийн системд хандах хүсэлтийн маягт" боловсруулах бөгөөд систем хариуцсан ажилтан бүртгэж хадгална. Үүнд Мэдээллийн аюулгүй байдал хариуцсан нэгж хяналт тавьж ажиллана.

3.3.3. Байгууллагын алба нэгжийн удирдлага маш нууц болон нууц мэдээллийн хүчинтэй байх хугацааг тогтооно.

3.3.4. Байгууллагын компьютер дэх мэдээллийг устгахдаа Мэдээллийн аюулгүй байдал хариуцсан нэгж хатуу дискэн дэх мэдээллийг сэргээх боломжгүйгээр форматлан Хавсралт №2-д заасны дагуу тэмдэглэл хөтөлнө.

3.4. Байгууллагын мэдээллийн аюулгүй байдлын тогтолцоонд дараах эд хөрөнгийг хамааруулна. Үүнд:

3.4.1. Хэрэглээний болон тусгай зориулалтын программ хангамж, системүүд;

3.4.2. Өөрсдийн хөгжүүлсэн болон тусгай захиалгаар хөгжүүлэлт хийлгэсэн программ хангамж, системүүд;

3.4.3. Оффисын хэрэглээний компьютер тоног төхөөрөмжүүд (Процессор, дэлгэц, хэвлэгч, хувилагч, скайнер, зөөврийн компьютер, телефон аппарат, зөөврийн хард, флаш, диск гэх мэт);

3.4.4. Сүлжээний тоног төхөөрөмжүүд (галт хана, рутер, свич, сүлжээний кабель гэх мэт);

3.4.5. Сервер тоног төхөөрөмжүүд (сервер, хатуу диск, RAM, KVM switch, тог баригч);

ДӨРӨВ. БАЙГУУЛЛАГЫН МЭДЭЭЛЛИЙН НӨӨЦЛӨЛТ, ХАДГАЛАЛТ

4.1. Байгууллагын мэдээллийн систем бүрт аюул ослын үед сэргээх төлөвлөгөөг боловсруулж, нөөц хуулбар бэлтгэхэд шаардлагатай мэдээллийг тодорхойлсон байх ба нөөцийг бүрдүүлэх зорилгоор байгууллагын цахим мэдээллийн сантай байна.

4.2. Цахим мэдээллийг устгах эрсдэлээс сэргийлж заавал хуулбарыг нэр төрлөөр нь ангилж хавтас үүсгэн зөөврийн болон дундын хадгалах төхөөрөмж, цахим мэдээллийн санд байршуулна.

4.3. Хадгалагдаж буй байгууллагын цахим мэдээлэлд хандах эрхийг хязгаарласан байх ба Мэдээллийн аюулгүй байдал хариуцсан нэгж хяналт тавина.

4.4. Цахим бус байдлаар хадгалж байгаа мэдээллийг ангилж, ангиллын дагуу бичгийн хавтсанд хийн нууцын зэрэглэлийн дагуу цоожтой шүүгээ, шкаф, төмөр сейфэнд хадгална. Ангилсан хавтас бүр заавал мэдээллийн төрөл, ангилал болон төрлийн тухай агуулга бүхий хаягтай байна. Мэдээлэл хариуцагч, эзэмшигч нь тухайн мэдээллийн нөөцлөлт, хадгалалт, бүрэн бүтэн байдлыг хариуцна.

4.5. Байгууллагын сүлжээ болон сүлжээнд холбогдох дагалдах тоног төхөөрөмжүүдийн топологи зургийг сүлжээний бүтэц, зохион байгуулалт өөрчлөгдөх бүрт шинэчлэн хадгална.

4.6. Байгууллагын сүлжээний тоног төхөөрөмжүүдийн тохиргооны болон лог файлыг техник үйлчилгээ хийх, тохиргоог өөрчлөх бүрт нөөцлөн хадгалж, тэмдэглэл хөтөлнө.

4.7. Байгууллагын системүүдийн эх код, файлууд болон өгөгдлийн сангийн нөөцлөлтийг мэдээллийн систем хариуцсан ажилтан улирал тутам хадгална.

4.8. Байгууллагын системүүдийн лог файл болон бүх төрлийн өөрчлөлтүүдийг мэдээллийн систем хариуцсан ажилтан сервер дээр хадгалж тэмдэглэл хөтөлнө.

4.9. Байгууллагын үйл ажиллагаанд хэрэглэгддэг, худалдаж авсан, захиалгаар болон өөрсдийн хөгжүүлсэн тусгай зориулалтын программ хангамжийн эх хувийг болон хуулбаруудыг байгын хэрэгцээнд зориулан серверт байрлуулна.

4.10. Ажилтны албан цахим шуудангийн мэдээллийг сервер дээр 1 жилийн хугацаанд мэдээллийн аюулгүй байдал хариуцсан нэгж нөөцөлж хадгална. Жилээс илүү хугацааны цахим шуудангийн мэдээллийг мэдээлэл хариуцагч, эзэмшигч өөрөө хадгална.

ТАВ. БАЙГУУЛЛАГЫН МЭДЭЭЛЛИЙН ХАМГААЛАЛТ

5.1. Байгууллагын мэдээллийг бүрдүүлдэг, боловсруулдаг, дамжуулдаг, хадгалдаг ажилтан бүр мэдээллийг хамгаалах үүрэг хүлээнэ.

5.2. Байгууллага нь мэдээллийн аюулгүй байдлыг хангах чиглэлээр ажлыг тогтмол зохион байгуулж, зардлыг төлөвлөн жил бүрийн төсөвт суулгаж батлуулна.

5.3. Олон нийтэд зориулагдсан мэдээлэл(Зэрэглэл1)-ийг эзэмшигч, хариуцагч нь тухайн мэдээллийг авахыг хүссэн иргэн, аж ахуйн нэгжид саадгүй гаргаж өгөх ба байгууллагын мэдээллийн самбар, цахим хуудас бусад мэдээллийн сувгуудад ил тод байршуулна.

5.4. Дотоод хэрэгцээнд нээлттэй мэдээлэл(Зэрэглэл2)-ийг эзэмшигч, хариуцагч нь мэдээллийн хадгалалт, хамгаалалт, аюулгүй байдлыг бүрэн хариуцаж мэдээлж зөвхөн байгууллагын ажилтанд саадгүй гаргаж өгөх ба байгууллагын үйл ажиллагаанд харшлахгүй бол иргэд, аж ахуйн нэгж бусад төрийн байгууллагад харьяалах нэгжийн даргын зөвшөөрснөөр гаргаж өгнө.

5.5. Байгууллагын ажилтан тодорхой эрхийн хүрээнд хязгаарлалтайгаар ашиглах боломжтой нууц мэдээлэл(Зэрэглэл3)-ийг хариуцагч нь мэдээллийн хадгалалт, хамгаалалт, аюулгүй байдлыг бүрэн хариуцаж, мэдээллийг

байгууллагын ажилтанд харьяалах нэгжийн даргын зөвшөөрснөөр гаргаж өгнө. Байгууллага дотор хаалттай мэдээллийг удирдах албан тушаалтны зөвшөөрснөөр бусад төрийн байгууллага аж ахуйн нэгжид гаргаж өгнө.

5.6. Байгууллагын алба нэгжийн маш нууц мэдээллийн хадгалалт, хамгаалалт, дамжуулах үйл ажиллагаанд тухайн удирдах албан тушаалтан болон Мэдээллийн аюулгүй байдал хариуцсан нэгж хяналт тавьж ажиллана.

5.7. Байгууллагын мэдээллийг физик орчинд дараах байдлаар хамгаална.

5.7.1 Физик хамгаалалтыг 3 бүсэд ангилж үзнэ.

а/ Нээлттэй бүс – Зөвхөн нийтэд хүртээмжтэй мэдээллийг ил байршуулна. (цахим хуудас, мэдээллийн самбар)

б/ Нийтэд хаалттай бүс – Байгууллага дотор нээлттэй болон нууцлалтай мэдээллийг хадгална. Аюул занал учирч болох эрсдэлээс сэргийлж биет мэдээллийг цоож бүхий шүүгээ сейфэнд, биет бус мэдээллийг нууц үг бүхий компьютер, диск, зөөврийн хадгалах төхөөрөмжид байгаа мэдээллийг цоож бүхий шүүгээ сейфенд хадгална. Тухайн бүсийг хариуцсан ажилтны зөвшөөрлөөр түүний хяналт дор гадны этгээдийг нэвтрүүлнэ. (ажлын өрөө, эмчийн өрөө, цахилгааны өрөө зэрэг орно);

в/ Хаалттай бүс – Байгууллагын нууц мэдээллийг хадгалах бөгөөд зөвхөн тухайн мэдээллийг хариуцагч, эзэмшигч буюу нэвтрэх эрх бүхий албан тушаалтан нэвтэрнэ. (серверийн өрөө, нууцын өрөө гэх мэт).

5.7.2. Нээлттэй, нийтэд хаалттай, хаалттай бүсэд байршуулсан мэдээ мэдээлэл, тоног төхөөрөмж, бусад зүйлсийн аюулгүй байдлыг тухайн алба нэгжийн үүрэг бүхий албан тушаалтан энэхүү журмын дагуу хангаж ажиллана.

5.7.3. Серверийн өрөөнд нэвтрэх ажилтан албан тушаалтны жагсаалтыг Хавсралт №1-ын дагуу гаргаж харьяалах нэгжийн даргаар батлуулна. Мэдээллийн аюулгүй байдал хариуцсан нэгж хяналт тавина.

5.7.4. Серверийн өрөөнд байрлуулсан сервер, компьютер, сүлжээний тоног төхөөрөмж болон бусад тоног төхөөрөмжийн хэвийн үйл ажиллагаанд энэхүү журамд заасны дагуу мэдээллийн систем, технологи хариуцсан ажилтан тогтмол хяналт тавьж засвар үйлчилгээг хариуцан хийнэ. Засвар үйлчилгээг тогтмол хийх төлөвлөгөөг батлуулж, мөрдөж ажиллана.

ЗУРГАА. ТОНОГ ТӨХӨӨРӨМЖ, СҮЛЖЭЭНИЙ НУУЦЛАЛ, ХАМГААЛАЛ

6.1. Байгууллагын тоног төхөөрөмж, мэдээллийн сан, сүлжээг хариуцагч, нь тэдгээрийг аюул заналаас хамгаалах, эрсдэлээс урьдчилан сэргийлэх зорилгоор энэ журамд заасан болон бусад бүхий л шаардлагатай арга хэмжээг авч ажиллах үүрэгтэй.

6.2. Байгууллага нь өөрийн компьютер, техник хэрэгслийг заавал гэрчилгээжүүлсэн байна. Гэрчилгээг байгууллагын Мэдээллийн аюулгүй байдал хариуцсан нэгж хариуцан хөтлөх бөгөөд шинэчлэл, өөрчлөлт, засвар, үйлчилгээ хийсэн, шинэ програм хангамж суулгасан тохиолдолд тухайн ажлыг гүйцэтгэсэн мэдээллийн технологи хариуцсан ажилтан болон компьютер, техник хэрэгслийг эзэмшигч хоёул гарын үсэг зурж баталгаажуулна.

6.3. Программ хангамж, техник хангамжийг суурилуулах

6.3.1. Программ болон техник хангамжийн суурилуулалт түүний шинэчлэл, тохиргоог зөвхөн мэдээллийн технологи хариуцсан ажилтан хийж гүйцэтгэнэ.

6.3.2. Компьютер, тоног төхөөрөмж эзэмшигч нь Мэдээллийн аюулгүй байдал хариуцсан нэгжийн зөвшөөрөлгүйгээр дур мэдэн программ хангамж шинээр

суулгах, программ хангамжид өөрчлөлт, шинэчлэлт хийх, техник хангамжид өөрчлөлт, засвар, үйлчилгээ хийхийг хориглоно.

6.3.3. Мэдээллийн технологи хариуцсан ажилтан нь систем, техник хангамж суурилуулах, шинэчлэх, өөрчлөх, засвар үйлчилгээ хийхдээ тухайн систем, техник хангамжийн үндсэн үүрэг, үйл ажиллагааг алдагдуулахгүй байхаар чанартай гүйцэтгэнэ.

6.4. Компьютер, тоног төхөөрөмж ашиглах

6.4.1. Байгууллагын ажилтан нь өөрийн эзэмшиж буй компьютер, хэвлэгч, хувилагч болон бусад тоног төхөөрөмжийг зөвхөн зориулалтын дагуу албан ажлын хэрэгцээнд ашиглана. Гадны этгээдэд зөвшөөрөлгүйгээр компьютер, тоног төхөөрөмжийг ашиглуулахыг хориглоно.

6.4.2. Ширээний болон зөөврийн компьютер нь энэ журмын 6.8-д заасны дагуу заавал нэвтрэх нууц үгтэй байна.

6.4.3. Ширээний болон зөөврийн компьютерт зөвхөн албан хэрэгцээний мэдээллийг хадгалах бөгөөд хувийн мэдээллүүд/зураг, кино, дүрс бичлэг, дуу болон бусад файл гэх мэт/ хадгалахыг хориглоно.

6.4.4. Байгууллагын ажилтан нь өөрийн компьютерт мэдээллийн аюулгүй байдлын учрал, аюул занал учирч болзошгүй эсвэл учирсан гэж үзвэл мэдээллийн аюулгүй байдлын асуудал хариуцсан нэгжид энэ тухай нэн даруй мэдэгдэнэ.

6.4.5. Ажилтан нь түр хугацаагаар компьютероос холдох бол заавал түгжих буюу нууц үгээр хамгаалагдсан дэлгэцийн хамгаалалтыг ажиллуулна. Ажлын цаг дуусаж, явахдаа компьютер, тоног төхөөрөмжүүдийг унтрааж, цахилгааны хүчдэлээс салгана.

6.4.6. Байгууллагад дундаа ашигладаг хэвлэх төхөөрөмжийг хяналттай байлгаж, тэдгээрийг ашиглахад тодорхой эрхийн хязгаарлалт хийж өгнө.

6.4.7. Байгууллагын мэдээллийн сан, системүүд ажиллаж буй сервер компьютерыг хөргүүр, чийгшүүлэгч, хяналтын камер, нэмэлт цахилгааны үүсгүүр бүхий серверийн өрөөнд буюу хаалттай бүсэд байрлуулна.

6.5. Сүлжээ ашиглах

6.5.1. Байгууллагын ажилтан мэдээллийн технологи хариуцсан ажилтны зөвшөөрөлгүйгээр байгууллагын сүлжээг өөрчлөх, төхөөрөмжөөс салгах, гадны төхөөрөмж залгах, ажлын өрөө солих, байрлалаа шилжүүлэх тохиолдолд дур мэдэн сүлжээний утсаа солих, өөрийн компьютерт тохируулсан сүлжээний тохиргоог дур мэдэн өөрчлөхийг хориглоно.

6.5.2. Байгууллагын ажилтан нь өөрийн ашиглаж буй сүлжээнд мэдээллийн аюулгүй байдлын учрал, аюул занал учирч болзошгүй эсвэл учирсан гэж үзвэл Мэдээллийн аюулгүй байдал хариуцсан нэгжид энэ тухай нэн даруй мэдэгдэнэ.

6.5.3. Байгууллагын сүлжээний тоног төхөөрөмжүүдэд зөвхөн зөвшөөрөгдсөн албан тушаалтан хандаж тохиргоо хийх бөгөөд сүлжээг зохион байгуулахдаа сүлжээний порт, кабелийн 2 талын үзүүрт тэмдэглэгээ бүхий хаяг заавал хадна.

6.5.4. Сүлжээний зохион байгуулалтын болон сүлжээний хамгаалалтын төхөөрөмжүүдийг серверийн өрөөнд байрлуулж, тэдгээрт энэ журмын 6.8-д заасны дагуу заавал нэвтрэх нууц үгийг хийнэ. Нэвтрэх нууц үгийг ажил үүргийн хуваарийн дагуу сүлжээ, мэдээллийн систем болон мэдээллийн технологи хариуцсан ажилтан өөртөө хадгална.

6.5.5. Байгууллагын сүлжээ ашиглан нууцын зэрэглэл бүхий мэдээлэл дамжуулах, солилцох бол заавал нууцлал бүхий сүлжээ /VPN, төрийн сүлжээ/ ашиглан дамжуулна.

6.5.6. Байгууллагын мэдээллийн системүүд рүү зөвшөөрөгдсөн албан тушаалтан хандаж шаардлагагүй портуудыг хязгаарлана.

6.6. Зөөврийн хадгалах төхөөрөмжийг ашиглах

6.6.1. Зөөврийн хадгалах төхөөрөмж дээрх мэдээллийг ашиглаж дууссаны дараа шаардлагагүй бол мэдээллийг төхөөрөмжөөс тухай бүр арилгах үйлдэл хийнэ. Зөөврийн хадгалах төхөөрөмжийг албан бусаар ашиглах бусдад дамжуулахыг хориглоно.

6.6.2. Гаднаас зөөврийн хадгалах төхөөрөмж системд оруулах бол заавал вирусын эсрэг програм уншуулж, вирус илэрсэн тохиолдолд түүнийг устгасны дараа мэдээлэл авах, хадгалах үйлдлийг хийнэ.

6.7. Албан цахим шуудан ашиглах

6.7.1. Байгууллагын цахим шуудан хэрэглэгчдийн бүртгэл хөтлөх, шинээр хэрэглэгч нэмэх, өөрчлөх, хасах, хэрэглэгчийн бүртгэлийн нууцлал аюулгүй байдлыг хангах асуудлыг Мэдээллийн аюулгүй байдал хариуцсан нэгж зохион байгуулна.

6.7.2. Байгууллагын ажилтан нь албаны цахим шууданг зөвхөн албан ажлын хэрэгцээнд ашиглаж, өөрийн цахим шуудангийн нууцлал аюулгүй байдлыг хариуцах бөгөөд нэвтрэх нууц үгийг энэ журмын 6.8-д заасны дагуу зохион байгуулна.

6.8. Нууц үгийн бодлого

6.8.1. Нууц үгийг том, жижиг үсэг, тоо, тусгай тэмдэгт бүхий 8 ба түүнээс дээш тэмдэгт байхаар хийнэ. Нууц үгээ ил бичиж тэмдэглэх, бусдад дамжуулахыг хориглоно.

6.8.2. Анхдагч нууц үгийг заавал солих ба нууц үгийг цаашид улирал тутам солино. Ингэхдээ хуучин нууц үгийг дахин хэрэглэхээс зайлсхийж, хуучин тэмдэгтүүдийн ихэнхийг солино.

6.8.3. Хэрэв нууц үг илчлэгдсэн гэж үзвэл нэн даруй солино. Байгууллагын хэмжээний томоохон систем, тоног төхөөрөмжид нэвтрэх нууц үгийг сар тутам солино.

6.8.4. Байгууллагын мэдээллийн систем, өгөгдлийн сан, програм хангамжийн нууц үгийн сонголт, бүртгэл, ашиглах хугацааг мэдээллийн систем, технологи хариуцсан ажилтан хариуцан ажиллаж, мэдээллийн аюулгүй байдал хариуцсан нэгж хяналт тавина. Шинээр үүсгэх, өөрчлөх, устгах тохиолдолд баталгаажуулах ба улирал тутам системийн хэрэглэгчдийн жагсаалтыг хянана.

6.9. Хортой кодоос хамгаалах

6.9.1. Байгууллагын хэрэгцээнд хэрэглэгдэж байгаа компьютер, мэдээлэл хадгалагч зөөврийн хэрэгслүүдэд зөвшөөрөгдсөн хортой кодын /вирус/ эсрэг програм хангамжийг ашиглана.

6.9.2. Хортой кодын эсрэг программын шинэчлэлийг тогтмол хийнэ.

6.9.3. Тодорхой хугацаанд системийн хортой кодын эсрэг программыг уншуулж, илэрсэн тохиолдолд арилгах арга хэмжээг авна.

ДОЛОО. МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ЭРСДЭЛИЙН ҮНЭЛГЭЭ

7.1. Иргэний нисэхийн ерөнхий газар түүний харьяа салбар нэгжүүдийн мэдээллийн технологийн хөрөнгийг хамгаалж, эрсдэлийг бууруулах үүднээс аудит, эрсдэлийн үнэлгээг мэдээллийн технологийн чиглэлээр олон улсад мөрдөгдөж буй стандартуудын хүрээнд 2 жил тутамд 1 удаа хийлгэнэ.

7.2. Байгууллагын мэдээллийн технологи хариуцсан нэгжүүд нь өөрийн хариуцаж буй систем тоног төхөөрөмжүүдэд эрсдэлийн үнэлгээ хийх төлөвлөгөөг боловсруулж, нэгжийн даргаар батлуулан төлөвлөгөөний дагуу 1 жил тутамд аудит хийнэ.

7.3. Байгууллагын эрсдэлийн үнэлгээний тайлан дээр үндэслэн систем тоног төхөөрөмжүүдийн мэдээллийн аюулгүй байдлыг сайжруулах, эрсдэлийг бууруулах төлөвлөгөөг мэдээллийн технологи болон мэдээллийн аюулгүй байдал хариуцсан нэгж боловсруулж, Иргэний нисэхийн үндэсний төвийн даргаар батлуулна.

НАЙМ. БАЙГУУЛЛАГЫН МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДАЛ ХАРИУЦСАН НЭГЖ, АЖИЛТАНЫ ЭРХ, ҮҮРЭГ

8.1 Байгууллагын мэдээллийн аюулгүй байдал хариуцсан нэгжийн эрх, үүрэг:

8.1.1 Байгууллагын мэдээллийн аюулгүй байдлын бодлогыг тодорхойлох, мэдээллийн аюулгүй байдлын тогтолцоог бүрдүүлэх, холбогдох дүрэм, журмыг боловсруулж батлуулах, тэдгээрт нэмэлт өөрчлөлт оруулах санал боловсруулах;

8.1.2 Байгууллагын мэдээллийн аюулгүй байдлыг хангахад чиглэсэн арга хэмжээг төлөвлөх, хэрэгжүүлэх, тайлагнах, шаардагдах зардлыг төсөвт суулгах санал боловсруулах;

8.1.3 Байгууллагын мэдээллийн аюулгүй байдал хариуцсан нэгж нь мэдээллийн системд заналхийлж буй халдлагыг бүртгэх, илрүүлэх, таслан зогсоох болон эмзэг байдлыг тогтоох, түүнийг бууруулах, аюулгүй байдлын бодлого боловсруулах зорилгоор мэдээллийн аюулгүй байдлыг хангах мэргэжилтнийг ажиллуулна.

8.1.4 Мэдээллийн аюулгүй байдлын учрал, онц нөхцөл байдал тохиолдоход байгууллагын мэдээллийн системүүдийг сэргээх, хэвийн ажиллагааг хангах арга, гүйцэтгэх дараалал, хариуцах албан тушаалтныг тодорхойлсон төлөвлөгөөг боловсруулж, мөрдүүлж ажиллах;

8.1.5 Нэгжийн мэдээллийн аюулгүй байдлыг хариуцсан ажилтны мэргэжил, ур чадварыг дээшлүүлэх сургалтад байнга хамруулах;

8.1.6 Байгууллагын ажилтан албан хаагчдад мэдээллийн аюулгүй байдлыг хангаж ажиллах талаар жил бүр тогтмол сургалт зохион байгуулах.

8.2 Мэдээллийн технологи, систем хариуцсан ажилтны эрх:

8.2.1 Ажил үүргийн хуваарийн дагуу мэдээллийн аюулгүй байдлыг шалгах, эмзэг байдлыг бууруулах зорилгоор мэдээллийн систем, ажилтнуудын компьютерт нэвтрэх;

8.2.2 Мэдээллийн аюулгүй байдлын шаардлага зөрчиж буй хэрэглэгчийн мэдээллийн санд нэвтрэх эрхийг удирдах, тэдгээрийн ажиллагааг хэсэгчлэн болон бүрэн зогсоох;

8.2.3 Аюулгүй байдлын шаардлагыг зөрчигчдөд хариуцлага тооцох талаар байгууллагын удирдлагад санал оруулах;

8.2.4 Байгууллагад ашиглагдах мэдээллийн систем, техник технологи худалдан авах үйл ажиллагаанд оролцох, санал оруулах, нэвтрүүлэх үйл явцад хяналт тавих;

8.2.5 Нийтийн үйлчилгээний сүлжээ болон мэдээллийн системүүдэд эрсдэлийн үнэлгээг жил тутам хийж мэдээллийн аюулгүй байдлын эмзэг байдлыг тодорхойлох, хамгаалалтын түвшинг тогтоох, хөндлөнгийн хяналтыг хэрэгжүүлэх;

8.2.6 Нийтийн үйлчилгээний сүлжээний орчинд ажиллаж буй компьютер тоног төхөөрөмж болон систем, серверт нэмэлт өөрчлөлт, шинэчлэл, техникийн үйлчилгээг хийхэд гадны байгууллага, мэргэжилтнийг зайлшгүй ажиллуулах тохиолдолд тухайн ажлыг гүйцэтгэх байгууллагыг сонгох үйл явцад оролцох бөгөөд ажил гүйцэтгэх явц, гүйцэтгэлд нь хяналт тавих.

8.3 Мэдээллийн технологи, систем хариуцсан ажилтны үүрэг:

8.3.1 Нийтийн үйлчилгээний сүлжээ болон мэдээллийн системийг байгуулах, турших, ашиглах, засвар үйлчилгээг хийх, хэвийн үйл ажиллагааг хангах;

8.3.2 Нийтийн үйлчилгээний сүлжээний орчинд ажиллаж буй мэдээллийн сан, програм хангамж, компьютерийн мэдээллийн аюулгүй байдлыг хамгаалах;

8.3.3 Мэдээллийн аюулгүй байдлыг хангахад чиглэсэн сургалт, сурталчилгааг байгууллагад зохион байгуулах;

8.3.4 Нийтийн үйлчилгээний сүлжээ болон мэдээллийн системд нэвтэрсэн халдлагыг таслан зогсоож хариу үйлдэл хийх, хурдан хугацаанд системийг сэргээх арга хэмжээ авах;

8.3.5 Сүлжээний хамгаалалтын төхөөрөмж дээр шаардлагатай тохиргоог хийх;

8.3.6 Байгууллагын цахим шуудангийн ажиллагааг хянаж хэрэглэгчдийн бүртгэлийг тогтмол шинэчилж байх;

8.3.7 Тоног төхөөрөмжүүд дээр гарсан гэмтэл саатлын судалгаа, шинжилгээг улирал тутам гаргаж, найдвартай ажиллагааг хангах талаар техникийн шийдэл гаргах;

8.3.8 Мэдээллийн аюулгүй байдлыг хангах шаардлагад нийцүүлэн нийтийн үйлчилгээний сүлжээний орчинд байршиж буй сүлжээ болон мэдээллийн систем, түүний дагалдах тоног төхөөрөмжүүдийг сайжруулах, шинэчлэх, эмзэг байдал эрсдэлийг бууруулах ажлыг тогтмол зохион байгуулах;

8.3.9 Мэдээллийн технологи, систем хариуцсан ажилтан нь ажил үүргийн дагуу олгосон эрхээ бууруулаар ашиглахгүй байх;

ЕС. МЭДЭЭЛЛИЙН СИСТЕМИЙН ХЭРЭГЛЭГЧИЙН ҮҮРЭГ, ХАРИУЦЛАГА

9.1 Мэдээллийн аюулгүй байдлын учрал тохиолдсон, тохиолдож болзошгүй нөхцөл байдлыг илрүүлсэн бол мэдээллийн аюулгүй байдал хариуцсан нэгжид нэн даруй мэдэгдэх үүрэгтэй.

9.2 Компьютерын нэр, сүлжээний нэрийг солихгүй байх, шаардлага гарсан тохиолдолд мэдээллийн технологи хариуцсан ажилтанд мэдэгдэн зохих үйлчилгээг хийлгэх;

9.3 Ажлын өрөө болон хонгилд ил болон далд угсрагдсан сүлжээний кабель гэмтсэн, ороцолдсон, далд монтажаас сүлжээний утас ил гарсан тохиолдолд мэдээллийн аюулгүй байдал хариуцсан нэгжид утсаар болон цахимаар мэдэгдэх;

9.4 Мэдээллийн аюулгүй байдал хариуцсан нэгжээс мэдээллийн аюулгүй байдлын чиглэлээр зохион байгуулж буй сургалт, арга хэмжээнд хамрагдах, өгсөн заавар, зөвлөгөө, шаардлагуудыг биелүүлэх;

9.5 Гадны тоног төхөөрөмжийг компьютер болон сүлжээнд мэдээллийн систем, технологи хариуцсан ажилтны зөвшөөрөлгүй холбохгүй байх;

9.6 Мэдээллийн аюулгүй байдлын чиглэлээр мөрдөгдөж буй хууль, дүрэм, журамд тусгагдсан хориотой цахим хуудсанд нэвтрэхгүй байх, програм хангамжийг компьютер дээр суулгахгүй байх;

9.7 Ажилтны анхаарал болгоомжгүй үйлдлээс болж байгууллагын мэдээллийн систем, сүлжээ, мэдээллийн сангийн аюулгүй байдал алдагдах, мэдээллийн аюулгүй байдлын бодлого, журам зөрчигдөж, байгууллагын үйл ажиллагаанд хохирол учруулсан ба хохирч болзошгүй байдал үүсгэсэн нь эрүүгийн хариуцлага хүлээлгэхээргүй бол Зөрчлийн тухай хууль, Хөдөлмөрийн тухай хууль, Байгууллагын хөдөлмөрийн дотоод журамд заасны дагуу сахилгын арга хэмжээ авна.

9.8 Нууц мэдээллийг санаатай буюу санамсаргүй байдлаар бусдад задруулснаас үүсэх хохирлыг нөхөн төлүүлэх, бууртай этгээдэд хариуцлага оногдуулах асуудлыг Эрүүгийн хууль, Захиргааны ерөнхий хууль, Төрийн болон албаны нууцын тухай хууль, Байгууллагын нууцын тухай хууль, Хувь хүний нууцын тухай хуулийн холбогдох заалтыг баримтлан шүүхээр шийдвэрлүүлнэ.

---o0o---

“Кибер аюулгүй байдлыг хангах үйл ажиллагааны дотоод журам”-ын Хавсралт 1

НУУЦ АНГИЛЛЫН МЭДЭЭЛЭЛ, ТЭДГЭЭРИЙГ ХАРИУЦАГЧ, ЭЗЭМШИГЧ БОЛОН ХЭРЭГЛЭГЧИЙН ЖАГСААЛТ

№	Мэдээллийн нэр	Тайлбар	Нууцын зэрэглэл	Хариуцагч	Эзэмшигч	Хэрэглэгч
1.						
2.						

МЭДЭЭЛЛИЙН СИСТЕМИЙН БАЙР ӨРӨӨ ТАСАЛГААНЫ ХАМГААЛАЛТЫН ЗЭРЭГЛЭЛИЙН ЖАГСААЛТ

№	Өрөөний нэр	Тайлбар	Зэрэглэл	Хэрэглэгч
1.				
2.				

“Кибер аюулгүй байдлыг хангах үйл ажиллагааны
дотоод журам”-ын Хавсралт 2

КОМПЬЮТЕР ФОРМАТЛАХ ХУУДАС
№

1. Ажилтны мэдээлэл

Овог нэр: .....

Алба салбар: .....

Албан тушаал: .....

2. Компьютерийн мэдээлэл

Компьютерийн марк, сервис таг: .....

3. Форматлах шалтгаан

☐ Шинэ ажилтан .....

☐ Вирустсэн .....

☐ Үйлдлийн систем гэмтсэн, гацсан.....

☐ Үйлдлийн системийн хувилбар ахиулах .....

☐ Бусад .....

4. Нэмэлтээр суулгах программ хангамж: .....

5. Хүлээлцсэн мэдээлэл

Компьютер хүлээлгэн өгсөн: ..... / 2023 он ... сар ... өдөр ... цаг/

Компьютер форматалсан: ...../ 2023 он ... сар ... өдөр ... цаг/