ИРГЭНИЙ НИСЭХИЙН
ЕРӨНХИЙ ГАЗРЫН ДАРГЫН
ТУШААЛ

2024 оны 08 сарын 20 өдөр Дугаар А/404 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 “Мэдээллийн аюулгүй байдал, технологийн үйл ажиллагааны чиглэлээр баримтлах журам”-ыг хавсралтаар батлалсугай.

2.“Мэдээллийн аюулгүй байдал, технологийн үйл ажиллагааны чиглэлээр баримтлах журам”-ыг мөрдөн ажиллахыг Иргэний нисэхийн ерөнхий газар, түүний харьяа салбар, нэгжүүдэд, журмын хэрэгжилтэд хяналт тавьж ажиллахыг Бодлогын хэрэгжилтийн хэлтэс (Ч.Одгэрэл), Хяналт-шинжилгээ, үнэлгээ, дотоод аудитын алба (Б.Мөнх-Очир)-нд тус тус үүрэг болгосугай.

3.Энэхүү тушаал гарсантай холбогдуулан Иргэний нисэхийн ерөнхий газрын даргын 2023 оны 04 дүгээр сарын 18-ны өдрийн “Журам батлах тухай ” А/113 дугаартай тушаалыг хүчингүй болсонд тооцсугай.

ДАРГА Ч.МӨНХТУЯА

17120 2374

Иргэний нисэхийн ерөнхий газрын даргын
2024 оны 12 дугаар сарын 20-ны өдрийн
А/604 дугаар тушаалын хавсралт

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДАЛ, ТЕХНОЛОГИ ҮЙЛ АЖИЛЛАГААНЫ ЧИГЛЭЛЭЭР БАРИМТЛАХ ЖУРАМ

НЭГ. НИЙТЛЭГ ҮНДЭСЛЭЛ

1.1.Монгол Улсын Кибер аюулгүй байдлын тухай хуулийн 16.1, 17.1, 19.1-д заасан хуулийн этгээд болох Иргэний нисэхийн ерөнхий газар (цаашид "байгууллага" гэх)-ын үйл ажиллагаанд ашиглагдаж буй мэдээлэл, мэдээллийн систем, дэд бүтэц, өгөгдлийн сан, мэдээллийн сүлжээний кибер аюулгүй байдлыг хангах, кибер халдлага, мэдээллийн аюулгүй байдлын зөрчлийг илрүүлэх, хариу арга хэмжээ авах, урьдчилан сэргийлэх, нөхөн сэргээх болон Олон улсын иргэний нисэхийн тухай Чикагогийн конвенцын Хавсралт-19 (Аюулгүй байдлын удирдлагын тогтолцоо)-ийн стандарт шаардлага, Олон улсын иргэний нисэхийн байгууллага (ICAO)-аас боловсруулан гаргасан Нисэхийн кибер аюулгүй байдлын стратеги, холбогдох зөвлөмж, шаардлагыг бүрэн хангахуйц *АЮУЛГҮЙ, ҮР АШИГТАЙ, ТОГТВОРТОЙ* үйлчилгээг үзүүлэхтэй холбоотой үйл ажиллагаанд дагаж мөрдөх нийтлэг харилцааг зохицуулахад энэхүү журмын зорилго оршино.

1.2.Мэдээллийн аюулгүй байдал, технологи үйл ажиллагааны чиглэлээр баримтлах журам нь байгууллагын мэдээлэл болон мэдээллийн хөрөнгийн бүрэн бүтэн, хүртээмжтэй нууцлалтай байдлыг ханган ажиллах, түүнд үүсэх эрсдэлийг бууруулах замаар байгууллагад учирч болох хохирлыг хамгийн бага түвшинд хүргэхэд чиглэгдэнэ.

1.3.Иргэний нисэхийн ерөнхий газар, түүний харьяа салбар, нэгжүүд нь өөрийн үйл ажиллагааны онцлог, цар хүрээг харгалзан мэдээллийн аюулгүй байдлыг хангах үйл ажиллагааны дотоод журмыг мөрдөнө.

1.4.Байгууллагын нэвтрүүлсэн ISO27001:2023 (Мэдээллийн аюулгүй байдал, кибер аюулгүй байдал, нууцлалын хамгаалалт) олон улсын стандарт, холбогдох хууль, дүрэм, журмын хүрээнд тавигдах шаардлага нь хоорондоо давхацсан тохиолдолд өндөр шаардлага тогтоосон шаардлагыг дагаж мөрдөнө.

1.5.Энэхүү журмын 1.3-т заасан журамд жил бүр тогтмол хугацаанд, эсхүл холбогдох хууль тогтоомж, байгууллагын дотоод бүтэц, мэдээллийн систем, мэдээллийн сүлжээнд өөрчлөлт орсон тухай бүр шаардлагатай өөрчлөлтийг оруулна.

1.6.Төрийн болон албаны нууцад хамаарах мэдээллийн аюулгүй байдлыг хангахад Төрийн болон албаны нууцын тухай хууль, журмыг дагаж мөрдөнө.

1.7.Энэхүү журамд хэрэглэсэн дараах нэр томьёог дор дурдсан утгаар ойлгоно.Үүнд:

1.7.1.Байгууллагын *"ӨГӨГДӨЛ"* гэж боловсруулагдаагүй мэдээлэл, баримтуудын цуглуулгыг хэлнэ.

1.7.2.Байгууллагын *"МЭДЭЭЛЭЛ"* гэж ямар хэлбэрээр оршин байгаагаас үл хамааран уншиж, ойлгож болохуйц боловсруулагдсан бүх төрлийн баримт бичгийг хэлнэ.

1.7.3.Байгууллагын *"ЭД ХӨРӨНГӨ"* гэж байгууллага өөрөө мэдэж захиран зарцуулах эрхтэй, байгууллагад үнэ цэнтэй биет болон биет бус эд зүйлийг хэлнэ.

1.7.4.Байгууллагын *"МЭДЭЭЛЭЛ ЭЗЭМШИГЧ"* гэж албан ажлаа гүйцэтгэх явцдаа аливаа мэдээллийг олж мэдсэн, танилцсан, цуглуулсан, тухайн мэдээллийг эзэмшиж байгаа ажилтныг хэлнэ.

1.7.5.Байгууллагын *"МЭДЭЭЛЭЛ ХАРИУЦАГЧ"* гэж мэдээллийг эзэмшиж байгаа ажилтан, албан тушаалтныг хэлнэ.

1.7.6.Байгууллагын *"МЭДЭЭЛЛИЙН ТЕХНОЛОГИ ХАРИУЦСАН НЭГЖ"* гэж байгууллагын мэдээллийн аюулгүй байдал, мэдээллийн технологийн үйл ажиллагааны хэвийн нөхцөлийг хангах чиг үүрэг бүхий нэгжийг хэлнэ.

1.7.7.Байгууллагын *"МЭДЭЭЛЛИЙН ТЕХНОЛОГИ ХАРИУЦСАН АЖИЛТАН"* гэж байгууллагын мэдээллийн технологи хариуцсан эрх, үүрэг бүхий албан тушаалтныг хэлнэ.

1.7.8.Байгууллагын *"МЭДЭЭЛЛИЙН СИСТЕМ ХАРИУЦСАН АЖИЛТАН"* гэж байгууллагын мэдээллийн систем болон сервер тоног төхөөрөмжүүдийг хариуцсан эрх, үүрэг бүхий албан тушаалтныг хэлнэ.

1.7.9.Байгууллагын *"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.

1.7.10.*"МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ТОГТОЛЦОО"* гэж мэдээллийн аюулгүй байдлыг хангах, хэрэгжүүлэх, хянах, дэмжих, сайжруулахын тулд мэдээллийн систем, дэд бүтэц, программ хангамж, тоног төхөөрөмж, тэдгээртэй ажиллах дүрэм, журам, ажилтнуудын харилцан үйл ажиллагааны үр дүнд бий болсон цогцыг хэлнэ.

1.7.11.*"МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ТОХИОЛДОЛ"* гэж мэдээллийн аюулгүй байдлын бодлого, аюулгүй байдал зөрчигдсөн гэдгийг илэрхийлж буй систем, үйлчилгээ, сүлжээний байдлыг бий болгосон тохиолдол, ойлгомжгүй эсхүл аюулгүй байдалтай холбоотой, өмнө нь тохиолдож байгаагүй нөхцөл байдлыг хэлнэ.

1.7.12.“*АЮУЛ ЗАНАЛ*” гэж байгууллагын үйл ажиллагааг алдагдуулах, мэдээллийн аюулгүй байдалд заналхийлэх бодит боломжтой, гэнэтийн эсвэл дэс дараалсан тохиолдлуудыг хэлнэ.

1.7.13.“*ЭРСДЭЛИЙН ҮНЭЛГЭЭ*” гэж эрсдэлийн ач холбогдлыг тодорхойлохын тулд байж болох эрсдэлийг өгөгдсөн шалгууруудтай харьцуулах үйл явцыг хэлнэ.

1.7.14.“*ЛОГ ФАЙЛ*” гэж мэдээллийн системд хандан ажиллаж буй хэрэглэгчийн үйлдлүүдийг тэмдэглэн авч баримтжуулдаг системийн файлыг хэлнэ.

1.7.15.Байгууллагын *“МЭДЭЭЛЛИЙН НУУЦЫН ЗЭРЭГЛЭЛ”* гэж мэдээллийн нууцын зэрэглэлийн дагуу мэдээлэлд тогтоох хамгаалалтын түвшинг хэлнэ.

1.7.16.“*VPN /VIRTUAL PRIVATE NETWORK/ ХОЛБОЛТ*” гэж интернэт сүлжээг ашиглан хувийн, нууцлалтай сүлжээг ашиглах боломжийг хэлнэ.

ХОЁР. УДИРДЛАГЫН МАНЛАЙЛАЛ

2.1.Иргэний нисэхийн ерөнхий газар, түүний харьяа салбар, нэгжийн удирдлагууд мэдээллийн аюулгүй байдлын удирдлагын тогтолцоог тогтолцоог нэвтрүүлэх, хэрэгжүүлэх, тогтвортой байлгах, тасралтгүй сайжруулах үйл ажиллагааг хэрэгжүүлэхэд бүх талаар дэмжиж, үр дүнтэй байдлыг хангахад манлайлал үзүүлэн, шаардагдах нөөцөөр тогтмол хангаж, нийт ажилтнуудыг уриална.

2.2.Мэдээллийн аюулгүй байдлын бодлого, зорилтуудыг байгууллагын стратеги төлөвлөгөө, нөхцөл байдалтай нийцүүлж, боловсруулж батална.

2.3.Байгууллагын мэдээллийн аюулгүй байдлыг хангах нь ажилтан бүрийн үүрэг, хариуцлага байна.

ГУРАВ. ҮЙЛ АЖИЛЛАГААНД ХЭРЭГЖҮҮЛЭХ БОДЛОГО

3.1.Иргэний нисэхийн ерөнхий газар, түүний харьяа салбар, нэгжийн удирдлагууд мэдээллийн аюулгүй байдал, технологи үйл ажиллагааны чиглэлээр баримтлах журмын хэрэгжилтийг хангах үйл ажиллагааг байгууллагын мэдээллийн технологи хариуцсан нэгж, эсхүл албан тушаалтны дэмжлэгтэйгээр удирдан чиглүүлж, зохион байгуулна.

3.2.Байгууллага нь Кибер аюулгүй байдлын тухай хуулийн 19 дүгээр зүйлийн 19.2.3-т заасны дагуу мэдээллийн аюулгүй байдлыг хангах талаар стандартыг нэвтрүүлсэн байна.

3.3.Байгууллага нь Кибер аюулгүй байдлын тухай хуулийн 19 дүгээр зүйлийн 19.2.4-т заасны дагуу мэдээллийн технологи хариуцсан нэгж, эсхүл мэдээллийн аюулгүй байдлын албан тушаалтантай байна.

3.4.Байгууллага нь мэдээллийн аюулгүй байдлын аудит хариуцсан нэгж эсхүл албан тушаалтантай байна.

3.5.Иргэний нисэхийн ерөнхий газар, түүний харьяа салбар, нэгжийн удирдлагууд, хариуцсан нэгж эсхүл албан тушаалтан нь мэдээллийн аюулгүй байдлын зорилго, зорилтыг энэхүү журамд нийцүүлэн харьяа салбар нэгжүүдийг хамруулан дэвшүүлж, хэрэгжилтийг тогтмол хугацаанд хянаж, үнэлэн үнэлгээнд тулгуурлан сайжруулалт хийнэ.

3.6.Байгууллага нь сүлжээ, мэдээллийн системүүдийн хэвийн найдвартай, тасралтгүй ажиллагааг хангахын нөөц систем болон тоног төхөөрөмжүүдтэй байна.

3.7.Байгууллага нь сүлжээ, мэдээллийн системүүдийн хэвийн найдвартай, тасралтгүй ажиллагаа болон мэдээллийн аюулгүй байдлыг тус тус хангах зорилгоор жил бүр төсөв батлан зарцуулна.

3.8.Кибер аюулгүй байдлын тухай холбогдох хууль, тогтоомж, стандарт, эрх бүхий байгууллагаас өгсөн зөвлөмж, шаардлагыг үйл ажиллагаандаа нийцүүлэн хэрэгжүүлнэ.

3.9.Иргэний нисэхийн ерөнхий газар, түүний харьяа салбар, нэгжийн удирдлагууд мэдээллийн аюулгүй байдал, технологи үйл ажиллагааны чиглэлээр холбогдох журмуудад тусгасан үйл ажиллагааны төлөвлөгөөг хэлэлцэж, шаардлагатай шийдвэрийг гаргаж мөрдүүлнэ.

3.10.Байгууллага нь ажилтнуудын албан хэрэгцээнд ашиглагдаж буй мэдээллийн технологийн тоног төхөөрөмж, мэдээллийн систем, өгөгдлийн сан болон сервер тоног төхөөрөмжүүдийн ашиглалт, нэвтрүүлэлт, хөгжүүлэлтийг зохицуулсан журамтай байна.

3.11.Мэдээллийн аюулгүй байдлын учирч болзошгүй эрсдэлийг тодорхойлж, үнэлэлт дүгнэлт өгөх, урьдчилан сэргийлэх, бууруулах зорилгоор эрсдэлийн удирдлага, байнгын сайжруулалтын тогтолцоог хэрэгжүүлнэ.

3.12.Байгууллагын 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.

3.13.Байгууллагын эрсдэлийн үнэлгээний тайлан дээр үндэслэн систем тоног төхөөрөмжүүдийн мэдээллийн аюулгүй байдлыг сайжруулах, эрсдэлийг бууруулах төлөвлөгөөг мэдээллийн технологи хариуцсан нэгж боловсруулан батлуулна

3.14.Байгууллагын цахим мэдээллийн нууцлал, хамгаалалт, нөөцлөлт, хүртээмжтэй болон бүрэн бүтэн байдал, программ хангамжийн бүтээгдэхүүн, системийн орчин, сүлжээний орчны тасралтгүй хэвийн ажиллагаа, аюулгүй байдлыг мэдээллийн технологи хариуцсан нэгж хангаж ажиллана.

3.15.Байгууллага нь Кибер аюулгүй байдлын тухай хуулийн 19 дүгээр зүйлийн 19.2.2, 19.2.13-т тус тус заасны дагуу кибер халдлага, зөрчлийн үед дагаж мөрдөх болон гэмтэл саатлын үед сэргээн ажиллуулах төлөвлөгөөтэй байна.

3.16.Байгууллага нь Кибер аюулгүй байдлыг хангах нийтлэг журмын 2.1.3-т заасны дагуу кибер аюулгүй байдал хариуцсан ИТА-нуудын мэдлэг, ур чадварыг тогтмол сайжруулах чиглэлээр холбогдох арга хэмжээнүүдийг авна.

3.17.Байгууллага нь сүлжээ болон мэдээллийн системүүдийн тоног төхөөрөмжүүдийг стандарт шаардлага хангасан тусгай зориулалтын тоног төхөөрөмжийн өрөөнд байршуулж, түүний аюулгүй байдал, хяналтыг хийнэ.

3.18.Байгууллага нь Кибер аюулгүй байдлыг хангах нийтлэг журмын 4.7-т заасан шаардлагуудыг хангасан үүлэн технологид суурилсан үйлчилгээг ашиглах журамтай байна.

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

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

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

ДӨРӨВ. МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ, ЗОХИОН БАЙГУУЛАХ

4.1.Байгууллага нь мэдээллийн аюулгүй байдлыг хангах чиглэлээр дараах зохион байгуулалтын арга хэмжээг авч хэрэгжүүлнэ:

4.1.1.Мэдээллийн аюулгүй байдлыг хангах стратеги төлөвлөгөөг байгууллагын стратеги төлөвлөгөөтэй уялдуулан боловсруулах;

4.1.2.Хүний нөөцийн чадавхыг бүрдүүлж, эрсдэлийн үнэлгээний үр дүнд үндэслэн эрсдэлийг бууруулахад чиглэсэн арга хэмжээг төлөвлөж, мэдээллийн аюулгүй байдлын стратеги төлөвлөгөөг хэрэгжүүлэх;

4.1.3.Мэдээллийн аюулгүй байдлын аудит, аюулгүй байдлын эрсдэлийн үнэлгээг холбогдох стандарт, эсхүл хуульд заасан хугацаанд хийлгэж, тайланг кибер халдлага, зөрчилтэй тэмцэх холбогдох төвд хүргүүлэх;

4.1.4.Мэдээллийн аюулгүй байдлыг хангахтай холбоотой энэ журмын 1.3-т заасан холбогдох баримт бичгийг боловсруулж, Иргэний нисэхийн ерөнхий газар, түүний харьяа салбар, нэгжийн удирдлагуудад тухай бүр танилцуулах.

4.2.Байгууллага нь мэдээллийн аюулгүй байдлыг хангах чиглэлээр дараах хүний нөөцийн арга хэмжээг авч хэрэгжүүлнэ. Үүнд:

4.2.1.Мэдээллийн аюулгүй байдлын удирдах болон гүйцэтгэх чиг үүргийг

ажлын байрны, эсхүл албан тушаалын тодорхойлолтод тусгаж, орон тооны, эсхүл хавсран гүйцэтгэх ажилтныг томилох;

4.2.2.Мэдээллийн аюулгүй байдлын мэдлэг олгох дараах сургалтыг зохион байгуулах:

4.2.2.1.Жил бүр тогтмол хугацаанд, нийт ажилтнуудыг хамруулах;

4.2.2.2.Ажилтныг томилогдсоноос хойш 1 сарын дотор;

4.2.2.3.Гэрээгээр хамтран ажиллаж байгаа гуравдагч талын ажилтныг тухай бүр.

4.2.3.Кибер, цахим орчинд хандаж, мэдээлэлтэй ажиллах ажилтан, албан хаагч, бусад этгээдтэй мэдээллийн нууц хадгалах болон мэдээллийн аюулгүй байдлыг хангах талаар үүрэг, хариуцлагыг тусгасан гэрээ байгуулах, эсхүл нууцын баталгаа үйлдэх.

4.2.4.Ажилтан, албан хаагч бүрд кибер халдлага, зөрчилтэй тэмцэх, мэдээллийн аюулгүй байдал, технологи үйл ажиллагааны чиглэлээр баримтлах журмын зөрчлийн үед авах арга хэмжээний талаар мэдлэг олгох.

ТАВ. МЭДЭЭЛЛИЙН АНГИЛАЛ, ТҮҮНИЙГ АГУУЛЖ БАЙГАА МЭДЭЭЛЛИЙН СИСТЕМ, НУУЦЫН ЗЭРЭГЛЭЛ, ЭД ХӨРӨНГӨ, МЭДЭЭЛЛИЙН СҮЛЖЭЭГ ТОДОРХОЙЛОХ

5.1.Байгууллага нь хамгаалбал зохих мэдээлэл, түүнийг агуулж байгаа мэдээллийн систем, мэдээллийн сүлжээний нууцын зэрэглэл, мэдээлэл хариуцагчийг тодорхойлсон жагсаалтыг гаргаж, тогтмол шинэчилнэ.

5.2.Байгууллага нь энэ журмын 5.1-д заасан жагсаалтад дурдсан мэдээлэл, мэдээллийн систем, мэдээллийн сүлжээнд учирч болзошгүй аюул занал, үр дагавар, нөлөөллийг үнэлэх зорилгоор эрсдэлийн үнэлгээг хийхдээ ISO27001:2023 (Мэдээллийн аюулгүй байдал, кибер аюулгүй байдал, нууцлалын хамгаалалт) стандартыг баримтална.

5.3.Байгууллага нь мэдээллийн нууцын зэрэглэлээс хамаарч, танилцах, ашиглах, дамжуулах, хадгалахтай холбоотой үйл ажиллагааг зохицуулсан тусгайлсан журмыг батлан, мөрдөж болно.

5.4.Байгууллагын мэдээллийг дараах байдлаар ангилна. Үүнд:

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

5.4.2.Биет бус мэдээлэл (Биет мэдээллийн цахим хэлбэр, өгөгдөл болон файлын сан, цахим шуудан, дүрс бичлэг, дуу бичлэг зэрэг мэдээллүүд);

5.4.3.Бусад төрлийн цахим мэдээллүүд;

5.5.Байгууллагын хэмжээнд боловсруулагдан ашиглах болон хадгалах баримт бичиг, өгөгдөл болон файлын хэрэглээний зориулалт, шууцлалаас хамаарч мэдээллийн нууцын зэрэглэлийг дараах байдлаар тогтооно. Үүнд:

5.5.1.Маш нууц (Зэрэглэл 4): Байгууллагын нууц мэдээллийг хадгалах бөгөөд зөвхөн тухайн мэдээллийг хариуцагч буюу нэвтрэх эрх бүхий албан тушаалтан нэвтрэх мэдээллүүд багтана.

5.5.2.Нууц (Зэрэглэл 3): Байгууллагын ажилтан тодорхой эрхийн хүрээнд хязгаарлалтайгаар ашиглах боломжтой, "Хувь хүний нууцын тухай" хуулиар хамгаалагдсан мэдээллүүд багтана.

5.5.3.Дотоод хэрэгцээнд (Зэрэглэл 2): Байгууллагын бүх ажилтанд зориулсан, байгууллагын үндсэн болон нэмэлт үйл ажиллагаатай холбоотой, байгууллага дотор нээлттэй, гадагш задруулахгүй мэдээллүүд багтана.

5.5.4.Олон нийтэд зориулагдсан мэдээлэл (Зэрэглэл 1): Хувилах, хадгалах дамжуулахад ямар нэгэн шаардлага тавихгүй нийтэд зориулагдсан, нууцлах шаардлагагүй, "Мэдээллийн ил тод байдал ба мэдээлэл авах эрхийн тухай" хуульд заасан мэдээллүүд багтана.

5.6.Мэдээлэл, мэдээллийн системийн нууцын зэрэглэлийн жагсаалт:

5.6.1.Байгууллагын эрх бүхий албан тушаалтнууд нь өөрийн хариуцсан алба нэгжийн маш нууц, нууц зэрэглэлд хамаарах баримт бичгийн нэрс, нуущад байх хугацаа, тэдгээртэй танилцах эрх бүхий албан тушаалтны жагсаалтыг гарган мэдээллийн нууцын зэрэглэлийг тодорхойлж, мэдээллийн технологи хариуцсан нэгжид хүргүүлэн батлуулж, жил бүр шинэчлэнэ.

5.6.2.Мэдээллийн систем бүрд "Хэрэглэгчийн мэдээллийн системд хандах хүсэлтийн маягт" боловсруулах бөгөөд мэдээллийн технологи хариуцсан нэгж, систем хариуцсан ажилтан бүртгэж хяналт тавин хадгална.

5.6.3.Байгууллагын удирдлага маш нууц болон нууц мэдээллийн хүчинтэй байх хугацааг тогтооно.

5.6.4.Байгууллагын компьютер дэх мэдээллийг устгахдаа мэдээллийн технологи хариуцсан нэгж хатуу диск дэх мэдээллийг сэргээх боломжгүйгээр форматлан Хавсралт 1-т заасны дагуу бүртгэл, тэмдэглэл хөтөлнө.

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

5.7.1.Хэрэглээний болон тусгай зориулалтын программ хангамж, өөрсдийн хөгжүүлсэн болон тусгай захиалгаар хөгжүүлэлт хийлгэсэн программ хангамж, системүүд;

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

5.7.3.Сервер сүлжээний тоног төхөөрөмжүүд (галт хана, сервер, рутер, свич, хатуу диск, RAM, KVM switch, тог баригч сүлжээний кабель гэх мэт);

ЗУРГАА. КИБЕР ХАЛДЛАГА, ЗӨРЧЛӨӨС ХАМГААЛАХ АРГА ХЭМЖЭЭ

6.1.Байгууллага нь мэдээлэл, түүнийг агуулж байгаа мэдээллийн систем, мэдээллийн сүлжээнд зөвшөөрөлгүй хандах, дамжуулах, өөрчлөх, устгахаас хамгаалж хандалтын удирдлагыг мэдээллийн технологи хариуцсан нэгж тодорхойлно.

6.2.Байгууллага нь хандалтын удирдлагад тодорхойлсны дагуу мэдээлэл, түүнийг агуулж байгаа мэдээллийн систем, мэдээллийн сүлжээнд хандах эрхийг олгож, энэ талаар бүртгэл хөтлөн, хяналт тавьж ажиллах бөгөөд тухай бүр шаардлагатай өөрчлөлтийг оруулан тохиолдлыг шинжилж, кибер халдлага, зөрчилд тооцох шалгуур үзүүлэлтийг мэдээллийн технологи хариуцсан нэгж гаргана.

6.3.Байгууллагын удирдлага мэдээллийн систем, мэдээллийн сүлжээнд давуу эрхтэй (*ADMIN, ROOT*) хандах этгээдийг тухай бүр тогтоож, хандах эрхийн ашиглалтад мэдээллийн технологи хариуцсан нэгж хяналт тавьж ажиллана.

6.4.Байгууллагын мэдээллийн систем, мэдээллийн сүлжээний тоног төхөөрөмж байрлаж байгаа зориулалтын өрөөнд зөвшөөрөлгүй нэвтрэхийг хориглоно.

6.5.Байгууллага нь мэдээллийн систем, мэдээллийн сүлжээний тоног төхөөрөмж байршуулах зориулалтын өрөөгүй бол энэ журмын 6.4-т заасан шаардлагад дүйцэх, тоног төхөөрөмжид зөвшөөрөлгүй этгээд хандахаас сэргийлсэн цоож, шүүгээ бүхий өрөөнд байршуулж болно.

6.6.Байгууллага нь үүлэн технологид суурилсан үйлчилгээ (цаашид "үйлчилгээ" гэх) ашиглах, ажилтан, албан хаагч бүр хэрэглэгчийн эцсийн төхөөрөмж (компьютер зэрэг)-гээ ажиллахад аюулгүй байдлыг хангах талаар энэ журмын 1.3-т заасан журамд, эсхүл тусгайлсан журам баталж, холбогдох мэдээллийг тусгана.

6.7.Байгууллага нь үүлэн технологид суурилсан үйлчилгээ авах бол холбогдох хууль тогтоомжид нийцүүлэн ажил гүйцэтгэгчтэй байгуулах гэрээг байгуулна.

6.8.Үйлчилгээтэй холбоотой өөрчлөлтийн үед ажил гүйцэтгэгч байгууллагад урьдчилан мэдэгдэл хүргэнэ.

6.9.Байгууллага нь мэдээлэл, түүнийг агуулж байгаа мэдээллийн систем, мэдээллийн сүлжээ, компьютер, мэдээлэл хадгалагч зөөврийн хэрэгслүүдэд зөвшөөрөгдсөн хортой кодын /вирус/ эсрэг программ хангамжийг ашиглана.

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

6.11.Байгууллага нь өөрийн мэдээллийн системийн хөгжүүлэлтийг бусдаар гүйцэтгүүлэх тохиолдолд оюуны өмчийн эрхийг хамгаалах талаар арга хэмжээг авч хэрэгжүүлнэ.

6.12.Байгууллага нь зохиогчийн эрхийн зөрчилгүй программ хангамж, хөгжүүлэлтийн санг худалдан авч, ашиглана.

6.13.Байгууллага нь мэдээллийн систем, мэдээллийн сүлжээний үйлдлийн бүртгэлийг доор дурдсан хугацаанд хадгална:

6.13.1.Кибер аюулгүй байдлын тухай хуулийн 19.1-д заасан байгууллага 1 жил буюу түүнээс дээш хугацаагаар;

ДОЛОО. КИБЕР ХАЛДЛАГА, ЗӨРЧЛИЙГ ИЛРҮҮЛЭХ, ХАРИУ АРГА ХЭМЖЭЭ АВАХ

7.1.Мэдээллийн систем, мэдээллийн сүлжээний хэвийн бус үйл ажиллагааг илрүүлэх, мэдээллийн систем, мэдээллийн сүлжээг хянахад энэ журмын 1.3-т заасан журамд, эсхүл тусгайлсан журам баталж, холбогдох мэдээллийг тусгана.

7.2.Кибер халдлага, зөрчлийг илрүүлэх ажиллагааг туршин шалгаж тогтмол сайжруулалт хийж кибер халдлага, зөрчлийн үед хариу арга хэмжээ авах төлөвлөгөөг баталж хэрэгжүүлэх бөгөөд төлөвлөгөөнд дараах мэдээллүүдийг тусгасан байна. Үүнд:

7.2.1.Байгууллага дотор кибер халдлага, зөрчлийг мэдэгдэх албан тушаалтан;

7.2.2.Тохиолдлыг шинжилж, кибер халдлага, зөрчилд тооцох шалгуур үзүүлэлт;

7.2.3.Халдлага, зөрчлийн талаарх мэдээллийг илгээх, хүлээн авах суваг.

7.3.Мэдээллийн технологи хариуцсан нэгж эсхүл албан тушаалтан нь энэ журмын 6.2-т заасан шалгуур үзүүлэлтийн дагуу кибер халдлага, зөрчлийн тохиолдол бүрд үнэлгээ хийж, халдлага, зөрчлийг тодорхойлно.

7.4.Байгууллага жилд нэгээс доошгүй удаа кибер халдлага, зөрчилд хариу арга хэмжээ авах төлөвлөгөөний дагуу дадлага, туршилт хийж, төлөвлөгөөг тогтмол шинэчилж сайжруулна.

НАЙМ. МЭДЭЭЛЛИЙН СИСТЕМ, МЭДЭЭЛЛИЙН СҮЛЖЭЭГ НӨХӨН СЭРГЭЭХ, МЭДЭЭЛЛИЙН НӨӨЦЛӨЛТ, ХАДГАЛАХ АРГА ХЭМЖЭЭ

8.1.Байгууллага нь кибер халдлага, зөрчилд өртсөн мэдээллийн систем, мэдээллийн сүлжээг нөхөн сэргээх үйл ажиллагааг хариуцах албан тушаалтан эсхүл мэдээллийн технологи хариуцсан нэгж үйл ажиллагааны дараалаллыг тодорхойлсон нөхөн сэргээх төлөвлөгөөг баталж, хэрэгжүүлнэ.

8.2.Байгууллагын мэдээллийн систем бүрд аюул ослын үед сэргээх төлөвлөгөөг боловсруулж, нөөц хуулбар бэлтгэхэд шаардлагатай мэдээллийг тодорхойлсон байх ба нөөцийг бүрдүүлэх зорилгоор байгууллагын цахим мэдээллийн сантай байна. Үүнийг мэдээллийн технологи хариуцсан нэгж хийнэ.

8.3.Цахим мэдээллийг устгах эрсдэлээс сэргийлж заавал хуулбарыг нэр төрлөөр нь ангилж хавтас үүсгэн зөөврийн болон дундын хадгалах төхөөрөмж, цахим мэдээллийн санд байршуулан хадгалагдаж буй байгууллагын цахим мэдээлэлд хандах эрхийг хязгаарлаж, хяналт тавина.

8.4.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.

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

8.6.Байгууллагын сүлжээний тоног төхөөрөмжүүдийн тохиргооны лог файлыг техник үйлчилгээ хийх, тохиргоог өөрчлөх бүрд нөөцлөн хадгалж, тэмдэглэл хөтлөн системүүдийн эх код, лог файлууд болон өгөгдлийн сан, бүх төрлийн өөрчлөлтүүдийн нөөцлөлтийг мэдээллийн систем хариуцсан ажилтан улирал тутам хадгална.

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

8.8.Ажилтны албан цахим шуудангийн мэдээллийг сервер дээр 1 жилийн хугацаанд мэдээллийн технологи хариуцсан нэгж нөөцөлж хадгална. 1 жилээс илүү хугацаан дах цахим шуудангийн мэдээллийг мэдээлэл хариуцагч, эзэмшигч өөрөө хадгална.

8.9.Байгууллага нь энэ журмын 8.1-д заасан төлөвлөгөөнд тусгагдсан үйл ажиллагааг жилд нэгээс доошгүй удаа шалган туршиж, шаардлагатай өөрчлөлтийг оруулан сайжруулалтыг мэдээллийн технологи хариуцсан нэгж хийнэ.

ЕС. БАЙГУУЛЛАГЫН МЭДЭЭЛЛИЙН ХАМГААЛАЛТ

9.1.Байгууллагын мэдээллийг бүрдүүлдэг, боловсруулдаг, дамжуулдаг, хадгалдаг ажилтан, албан хаагч бүр тухайн мэдээллийг хамгаалах үүрэг хүлээнэ.

9.2.Олон нийтэд зориулагдсан мэдээлэл (Зэрэглэл 1)-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.

9.3.Дотоод хэрэгцээнд нээлттэй мэдээлэл (Зэрэглэл 2)-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.

9.4.Байгууллагын ажилтан тодорхой эрхийн хүрээнд хязгаарлалтайгаар ашиглах боломжтой нууц мэдээлэл (Зэрэглэл 3)-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.

9.5.Байгууллагын алба нэгжийн маш нууц мэдээллийн хадгалалт, хамгаалалт, дамжуулах үйл ажиллагаанд тухайн удирдах албан тушаалтан болон мэдээллийн технологи хариуцсан нэгж хяналт тавьж ажиллана.

9.6.Байгууллагын мэдээллийг физик орчинд дараах байдлаар хамгаална.

9.6.1.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 болон биет бус мэдээллийг нууц үг бүхий компьютер, диск, зөөврийн хадгалах төхөөрөмжид байгаа мэдээллүүдийг 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. (тоног төхөөрөмжийн өрөө, нууцын өрөө гэх мэт).

9.7.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.

9.8.Тоног төхөөрөмжийн 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.

АРВАН. ТОНОГ ТӨХӨӨРӨМЖ, СҮЛЖЭЭНИЙ НУУЦЛАЛ, ХАМГААЛАЛТ

10.1.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.

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

10.3.Программ хангамж, техник хангамжийг суурилуулах ажлыг дараах байдлаар хийнэ. Үүнд:

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

10.3.2.Компьютер, тоног төхөөрөмж эзэмшигч нь мэдээллийн технологи хариуцсан нэгжийн зөвшөөрөлгүйгээр дур мэдэн программ хангамж шинээр суулгах, программ хангамжид өөрчлөлт, шинэчлэлт хийх, техник хангамжид өөрчлөлт, засвар, үйлчилгээ хийхийг хориглоно.

10.3.3.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.

10.4.Компьютер, тоног төхөөрөмжийг дараах байдлаар ашиглана. Үүнд:

10.4.1.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.

10.4.2.Ширээний болон зөөврийн компьютер нь энэ журмын 10.9-д заасны дагуу заавал нэвтрэх нууц үгтэй байна.

10.4.3.Ширээний болон зөөврийн компьютерт зөвхөн албан хэрэгцээний

мэдээллийг хадгалах бөгөөд хувийн мэдээллүүд /зураг, кино, дүрс бичлэг, дуу болон бусад файл гэх мэт/ хадгалахыг хориглоно.

10.4.4.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.

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

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

10.5.Сүлжээг дараах байдлаар ашиглана. Үүнд:

10.5.1.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.

10.5.2.Байгууллагын ажилтан нь өөрийн ашиглаж буй сүлжээнд мэдээллийн аюулгүй байдлын тохиолдол, аюул занал учирч болзошгүй эсвэл учирсан гэж үзвэл мэдээллийн технологи хариуцсан нэгжид энэ тухай нэн даруй мэдэгдэнэ.

10.5.3.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.

10.5.4.Сүлжээний зохион байгуулалтын болон сүлжээний хамгаалалтын төхөөрөмжүүдийг тоног төхөөрөмжийн өрөөнд байрлуулж, тэдгээрт энэ журмын 10.9-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.

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

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

10.6.Зөөврийн хадгалах төхөөрөмжийг дараах байдлаар ашиглана. Үүнд:

10.6.1.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.

10.6.2.Гаднаас зөөврийн хадгалах төхөөрөмж системд оруулах бол заавал

вирусийн эсрэг программ уншуулж, вирус илэрсэн тохиолдолд түүнийг устгасны дараа мэдээлэл авах, хадгалах үйлдлийг хийнэ.

10.7.Албан цахим шууданг дараах байдлаар ашиглана. Үүнд:

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

10.7.2.Байгууллагын ажилтан нь албаны цахим шууданг зөвхөн албан ажлын хэрэгцээнд ашиглаж, өөрийн цахим шуудангийн нууцлал аюулгүй байдлыг хариуцах бөгөөд нэвтрэх нууц үгийг энэ журмын 10.9-д заасны дагуу зохион байгуулна.

10.8.Үүлэн технологид суурилсан үйлчилгээг дараах байдлаар ашиглана. Үүнд:

10.8.1.Байгууллага нь үүлэн технологид суурилсан үйлчилгээ авах бол холбогдох хууль тогтоомжид нийцүүлэн ажил гүйцэтгэгчтэй гэрээ байгуулна.

10.8.2.Байгууллага нь үүлэн технологид суурилсан үйлчилгээтэй холбоотой өөрчлөлтийн үед ажил гүйцэтгэгч байгууллагад урьдчилан мэдэгдэл хүргэнэ.

10.9.Нууц үгийн бодлого, хориглох зүйл. Үүнд:

10.9.1.Нууц үгийг том, жижиг үсэг, тоо, тусгай тэмдэгт бүхий 8 ба түүнээс дээш тэмдэгт байх ба нууц үгээ ил бичиж тэмдэглэх, бусдад дамжуулахыг хориглоно.

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

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

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

АРВАН НЭГ. ҮҮРЭГ, ХАРИУЦЛАГА

11.1.Байгууллагын дарга нь мэдээллийн аюулгүй байдлыг хангах чиглэлээр дараах үүрэгтэй:

11.1.1.Байгууллагын мэдээллийн аюулгүй байдлыг хангах үйл ажиллагааг нэгдсэн удирдлагаар хангах, уялдуулан зохион байгуулах, байгууллагыг төлөөлөх;

11.1.2.Мэдээллийн аюулгүй байдлыг хангах дүрэм, журам батлах;

11.1.3.Мэдээллийн аюулгүй байдлыг хангах төлөвлөгөө гаргах ба түүнийг хэрэгжүүлэхэд шаардагдах төсвийг байгууллагын жил бүрийн төсөв, төлөвлөгөөнд тусгах.

11.2.Байгууллагын мэдээллийн технологи хариуцсан албан тушаалтан дараах үүрэгтэй:

11.2.1.Байгууллагын мэдээллийн аюулгүй байдлыг хангах өдөр тутмын үйл ажиллагааг хариуцан гүйцэтгэх;

11.2.2.Холбогдох дүрэм, журмыг боловсруулах, шинэчлэх санал боловсруулах;

11.2.3.Мэдээллийн аюулгүй байдлыг хангахад шаардлагатай үйл ажиллагаа, нөөцийг төлөвлөх;

11.2.4.Мэдээллийн аюулгүй байдлыг хангах мэргэшүүлэх сургалтад хамрагдах.

11.3.Байгууллагын нийт ажилтан мэдээллийн аюулгүй байдлыг хангах чиглэлээр дараах үүрэгтэй:

11.3.1.Энэ журам болон мэдээллийн аюулгүй байдлыг хангахтай холбоотой бусад дүрэм, журмыг дагаж мөрдөх;

11.3.2.Илэрсэн халдлага, зөрчил, сэжигтэй тохиолдол бүрийг мэдээллийн технологи хариуцсан ажилтан, албан тушаалтанд мэдэгдэх;

11.3.3.Байгууллагын мэдээлэл, мэдээллийн систем, мэдээллийн сүлжээг зөвхөн албан хэрэгцээнд, заасан журам, зааврын дагуу хэрэглэх;

11.3.4.Байгууллагаас зохион байгуулж буй мэдээллийн аюулгүй байдлын мэдлэг олгох сургалтад хамрагдах.

11.4.Байгууллагын мэдээллийн систем, сүлжээ, мэдээллийн сангийн аюулгүй байдал алдагдах, журам зөрчигдөж, байгууллагын үйл ажиллагаанд хохирол учруулсан ба учруулж болохуйц нөхцөл байдал үүсгэсэн ажилтан, албан тушаалтанд хууль тогтоомжид заасан хариуцлага хүлээлгэнэ.

----o0o---

Хавсралт 1

КОМПЬЮТЕР ФОРМАТЛАХ ХУУДАС

№ ...

1. Ажилтны мэдээлэл

   Овог нэр: .....

   Алба салбар: .....

   Албан тушаал: .....

2. Компьютерын мэдээлэл, үзүүлэлт

   Компьютерын 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: ..... / 20 ... он ... сар ... өдөр ... цаг/

   Компьютер форматалсан: ...../ 20 ... он ... сар ... өдөр ... цаг/