МОНГОЛ УЛСЫН
ЕРӨНХИЙ АУДИТОРЫН ТУШААЛ

2015 оны 4 сарын 22 өдөр Дугаар 120 Улаанбаатар хот

Журам батлах тухай

Төрийн аудитын тухай хуулийн 13 дугаар зүйлийн 13.4.7 дахь заалт, Үндэсний аулгүй байдлын тухай хуулийн 3 дугаар зүйлийн 3.4.6 дахь заалт, 7 дугаар зүйлийн 7.1.8 дахь заалтуудыг тус тус үндэслэн ТУШААХ нь:

1. Төрийн аудитын байгууллагуудад мөрдөх “Мэдээллийн аюулгүй байдлыг хангах журам”, “Мэдээлэл, харилцаа холбоо, технологийн чиглэлийн үйл ажиллагааг зохицуулах журам”, “Компьютер техник, тоног төхөөрөмж болон дотоод сүлжээ, цахим шуудан ашиглалтын журам”-ыг тус тус хавсралтаар баталсугай.

4. Байгууллагын үйл ажиллагаандаа энэхүү журмыг мөрдлөг болгон ажиллахыг Үндэсний аудитын газар болон аймаг, нийслэлийн аудитын газрын тэргүүлэх аудиторууд болон нийт ажилчдад үүрэг болгосугай.

5. Дээрх журмыг хэрэгжүүлэхэд төрийн аудитын байгууллагуудад мэргэжил арга зүйн дэмжлэг үзүүлж, хяналт тавьж, хамтарч ажиллахыг Үндэсний аудитын газрын Тамгын газар /Л.Дулмаа/-д, тушаалын биелэлтэд хяналт тавьж, үр дүнг тооцож ажиллахыг Ерөнхий менежер /Э.Отгон/-д тус тус даалгасугай.

МОНГОЛ УЛСЫН
ЕРӨНХИЙ АУДИТОР А.ЗАНГАД

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ
/ЕРӨНХИЙ/ ЖУРАМ

Нэг. Ерөнхий зүйл

1.1.Энэхүү журмын зорилго нь Төрийн аудитын байгууллагуудад /цаашид газрууд гэх/ мэдээллийн аюулгүй байдлын удирдлагын тогтолцоог бий болгох, мэдээллийн сүлжээ, системийн найдвартай ажиллагаа, мэдээллийн сангийн нууцлал, аюулгүй байдлыг хангах, гаднаас болон дотоодоос учирч болох халдлага, аюул заналаас урьдчилан сэргийлэх, хор хохирол эрсдэл учирсан гэж үзвэл урьдчилан бэлтгэсэн заавар, журмын дагуу нэн даруй засаж, сэргээх, хариу арга хэмжээ авахад оршино.

1.2. Төрийн аудитын байгууллагууд, тэдгээрийн нийт ажилтан, албан хаагчид, мэдээллийн технологийн мэргэжилтнүүд ажил үүргээ гүйцэтгэхдээ энэхүү журмыг мөрдлөг болгон ажиллана.

1.3. Газрууд нь мэдээллийн системийг зохион байгуулахдаа холбогдох стандартууд /Мэдээллийн технологи - Аюулгүй байдлын аргууд - Мэдээллийн аюулгүй байдлын удирдлагын үйл ажиллагааны дүрэм - MNS 17799.2007, Мэдээллийн технологи- Аюулгүй байдлын арга техник - Мэдээллийн ба холбооны технологийн аюулгүй байдлын удирдлага1-р хэсэг: Мэдээлэл холбооны технологийн аюулгүй байдлын үндсэн ойлголтууд болон загварууд-MNS ISO/IEC 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 ISO/IEC 27001:2009/-ыг мөрдсөн байна.

1.4.Мэдээллийн технологийн арга техник өөрчлөгдсөн тохиолдолд энэхүү журмыг нягтлан зохих өөрчлөлт, сайжруулалтыг хийнэ.

Хоёр. Нэр томьёо

2.1.Мэдээлэл - гэдэг нь эзэмшиж, хадгалж байгаа төхөөрөмжөөс үл хамааран боломжит бүх л хэлбэрээр оршин байгаа уншиж ойлгож болох бүх төрлийн баримт бичиг, мэдээ, мэдээлэл, биет зүйлсийг;

2.2.Нийтэд хүртээмжтэй мэдээлэл - гэж хуулиар болон энэхүү журмаар нууц мэдээлэл гэж үзээгүй, эрх бүхий этгээдийн зөвшөөрлийн дагуу олон нийтэд тараагдсан, задруулбал байгууллагад болон бусад этгээдэд илтэд хохирол учруулахааргүй мэдээллийг;

2.3.Нууц ангиллын мэдээлэл- гэж хууль тогтоомжид нийцүүлэн нууцалсан бөгөөд задруулбал байгууллага болон хувь хүний эрх, хууль ёсны ашиг сонирхол, нэр төр, алдар хүндэд илтэд хохирол учруулж болзошгүй мэдээллийг

2.4.Ажилтан - гэж Байгууллага хөдөлмөрийн болон нэгээс дээш сарын хугацаатай байгуулсан хөдөлмөрийн гэрээтэй адилтгах бусад аливаа гэрээгээр ажиллаж байгаа этгээдийг;

2.5.Мэдээлэл эзэмшигч - гэж, албан үүрэг, ажил мэргэжлийн үйл ажиллагааны хүрээнд аливаа мэдээллийг олж мэдсэн, танилцсан, тухайн мэдээллийг эзэмшиж байгаа ажилтныг;

2.6.Мэдээлэл хариуцагч - гэж мэдээллийг эзэмшиж байгаа ажилтны удирдах дээд албан тушаалтныг ойлгоно.

2.7.Мэдээллийн аюулгүй байдал - гэж мэдээлэл, мэдээлэл боловсруулах хэрэгсэл, холбогдох дэд бүтцийн нууцлал, бүрэн бүтэн байдал, хүртээмжтэй байдал, тасралтгүй

ажиллагаа, найдвартай байдлыг тодорхойлох, бий болгох, хадгалж байхтай холбоотой бүх асуудлууд.

2.8.Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоо - МАБУТ- Мэдээллийн аюулгүй байдлыг хангах, хэрэгжүүлэх, ажиллуулах, хянах, нягтлан шалгах, дэмжих, сайжруулахын тулд хэрэгжүүлсэн байгууллагын удирдлагын тогтолцооны нэг хэсэг (эрсдэлийн удирдлагын хандлага дээр суурилсан);

2.9.Аюул занал - гэж систем болон байгууллагад хор учруулж болох мэдээллийн аюулгүй байдлыг ямар нэг байдлаар зөрчиж болох боломж, үйлдэл, үйл явдлыг;

2.10.Өмч хөрөнгө - гэж байгууллагад ямар нэг ач холбогдолтой аливаа биет болон биет бусюмс, эд зүйл. МХТ- ийн талаас нь авч үзвэл мэдээлэл, түүнтэй холбоотой аливаа юмс, эд зүйл;

2.11.Мэдээллийн аюулгүй байдлын учрал - гэж мэдээллийн аюулгүй байдлын зөрчил гарсан, аюулгүй байдлын арга хэмжээ үр дүнгүй болсон, ажиллахгүй байгаа, эсхүл аюулгүй байдалтай холбоотой ямар нэг нөхцөл байдал үүссэн гэдгийг илтгэж буй систем, үйлчилгээ, сүлжээний хэвийн байдалд нөлөөлөх аливаа тохиолдол, үйл явдал;

2.12.Эрсдэлийн үнэлгээ - гэж эрсдэлийн хэмжээ, ач холбогдлыг тодорхойлохын тулд байж болох эрсдэлийг өгөгдсөн шалгууруудтай харьцуулах үйл явц;

2.13.Нэгж - гэж байгууллагын мэдээллийн аюулгүй байдал, мэдээллийн технологийн үйл ажиллагааны хэвийн нөхцөлийг хангах чиг үүрэгтэй албан хаагч, нэгж бүтцийг;

2.14.Зохицуулагч - гэж байгууллагын мэдээллийн технологи хариуцсан эрх, үүрэг бүхий мэргэжилтэн, администыг;

2.15.Хэрэглэгч -гэж байгууллагын мэдээллийн системтэй харьцдаг бүхий л шатны ажилтан,албан хаагчдыг;

Гурав. Байгууллагын мэдээллийн өмч хөрөнгө, ангилал

3.1 Мэдээллийн өмч хөрөнгийн ангилал

3.1.1.Биет мэдээллийн хөрөнгө гэдэг нь судалгааны материалууд, үйл ажиллагааны төлөвлөгөө, төсөл хөтөлбөрүүд, бүртгэлийн мэдээллүүд, сургалтын материал, тараах хуудсууд, гарын авлага, хяналт шалгалтын тайлан, хэвлэмэл зургууд зэрэг бүх төрлийн хэвлэмэл мэдээллийг;

3.1.2.Цахим мэдээллийн хөрөнгө гэдэг нь биет мэдээллийн, цахим хэлбэрүүд, өгөгдлийн сангийн өгөгдлүүд болон бусад төрлийн цахим мэдээллийг;

3.1.3.Програм хангамжийн хөрөнгө гэдэг нь зөвшөөрөлтэй хэрэглээний, мэргэжлийн болон системийн програм хангамж, өөрсдийн боловсруулсан болон тусгай захиалгаар хийлгэсэн програм хангамжууд, системүүд

3.1.4.Техник хангамжийн хөрөнгө гэдэг нь сервер, компьютерын ба харилцаа холбооны төхөөрөмжүүд (процессор, дэлгэц, зөөврийн компьютер, телефон, факсын аппарат), зөөврийн төхөөрөмжүүд (зөөврийн хард, флаш, диск, хуурцаг), сүлжээний тоног төхөөрөмжүүд (рутер, свич, салаалагч, сүлжээний утас, толгой) зэрэг бүх төрлийн мэдээлэл боловсруулах, дамжуулах, хадгалах хэрэгслүүдийг;

3.2. Мэдээллийн нууцлал, ангилал

3.2.1.Байгууллагын мэдээллийг хэрэглээний зориулалтаар нь дараах байдлаар ангилна. Нийтэд хүртээмжтэй: Нийтэд зориулагдсан, нууцлах шаардлагагүй мэдээллүүд-

хэрэглэгчдэд зориулсан гарын авлага, зөвшөөрөл авахад бүрдүүлэх материалууд, ил тод байдлыг илэрхийлсэн материалууд- байгууллагын төлөвлөгөө, тайлан, төсөв, санхүүгийн мэдээ, буруугаар ашиглан байгууллагад ямар нэгэн хохирол учруулах боломжгүй материалууд

а/ Хувилах, хадгалах, дамжуулахад ямар нэгэн шаардлага тавихгүй мэдээллүүд

б/ Энэ нь хууль тогтоомжийн дагуу төрийн нууцад хамаарах, улсын аюулгүй байдлыг хангах тусгайлсан чиг үүрэг бүхий байгууллагын үйл ажиллагаанд хамаарахгүй.

3.2.2.Байгууллага дотор нээлттэй: Байгууллагын ажилтан албан хаагчдад зориулагдсан мэдээ, мэдээллүүд, даргын тушаал, үүрэг даалгавар, ажилтан, албан хаагчдын хувийн хэрэг, өдөр тутмын үйл ажиллагааны мэдээллүүд,

а/ Байгууллага дотроо хувилж, олшруулж, тараахад хязгаарлалт тавихгүй

б/ Байгууллага дотор нээлттэй мэдээллийг гадагш гаргасан тохиолдолд хариуцлага тооцно.

3.2.3.Нууц мэдээлэл: Хуулинд заагдсан болон тухайн байгууллагын нууцын тухай журамд тусгагдсан мэдээллүүд хамаарна. Нууц мэдээллийг дараах зэрэглэлд ангилна. Үүнд:

3.2.1.1 Онц нууц
3.2.1.2 Маш нууц
3.2.1.3 Нууц

3.2.4.Ажилтнууд нууц ангиллын мэдээллийг энэхүү журамд заасан арга хэлбэрээр эзэмших, ашиглах, хадгалах, хамгаалах, дамжуулах үүрэг хүлээнэ.

3.2.5.Байгууллагын нууцын зэрэглэл бүхий мэдээлэл, баримт бичиг, үйл ажиллагаатай холбоотой нууц, харилцагчийн мэдээллийн нууц зэрэг мэдээллүүдийн нууцыг хадгалах хамгаалахтай холбоотой ажилтантай хийх “НУУЦЫГ ХАДГАЛАХ БАТАЛГАА”-ний загварыг Маягт №1-ээр батална.

3.2.6.Байгууллага нь нууц ангиллын мэдээллийн жагсаалт болон уг мэдээллийг хариуцах, эзэмших, хэрэглэх ажилтан, албан тушаалтныг Маягт №2 –оор батална.

3.2.7.Хадгалагдах мэдээллийн зэрэглэлээс хамаарч өрөө тасалгааг дараах байдлаар зэрэглэн ангилна:

Зэрэглэл I: Нээлттэй бүс
Зэрэглэл II: Нийтэд хаалттай бүс
Зэрэглэл III: Хаалттай бүс

3.2.8.Тухайн өрөө тасалгааны зэрэглэл болон түүнд нэвтрэх эрхийг олгох хариуцагчийг Маягт № 2–оор зохицуулна.

Дөрөв. Байгууллагын мэдээллийн хамгаалалт

4.1.Эрх зүйн орчин, зохион байгуулалтын хувьд

4.1.1.Байгууллагын мэдээлэл гаргадаг, хүлээн авдаг, боловсруулдаг, дамжуулдаг, хадгалдаг албан хаагч бүр мэдээллийг хамгаалах үүрэг хүлээнэ.

4.1.2.Байгууллагын үйл ажиллагааны онцлог, байрлал, өмч хөрөнгө, технологийн дагуу МАБУТ- ны хүрээ хил хязгаарыг тогтоосон байна.

4.1.3.Мэдээллийн аюулгүй байдлын талаар баримтлах бодлого боловсруулан мөрдөж ажиллах, нууцын зэрэглэлд хамаарах мэдээллийг тодорхойлон, хадгалах хамгаалах асуудлыг зохицуулсан дүрэм, журамтай байна.

4.1.4.Мэдээллийн аюулгүй байдлын бодлогыг агуулсан албан ёсны баримт бичиг нь байгууллагын өөрийн онцлогт тохирсон, мэдээллийн аюулгүй байдлыг хангах үүрэгтэй бүх албан хаагчдад хүртээмжтэй байх шаардлагатай.

4.1.5.Онц чухал дэд бүтцийн болон онцгой нөхцөл үүссэн үед мэдээллийн системээ нөхөн сэргээх, нүүлгэн шилжүүлэх төлөвлөгөөтэй байна.

4.1.6.Мэдээллийн аюулгүй байдлын бодлогыг боловсруулах, хяналт, дотоод аудит хийх, мэдээллийн санд нэвтрэх хандалтын удирдлагыг хэрэгжүүлэх үүрэг бүхий бүтэц, орон тоог бий болгоно.

4.1.7.Мэдээллийн системийг шинээр байгуулахдаа мэдээллийн аюулгүй байдлын бодлогод нийцүүлэн төлөвлөж, хамгаалалтыг зохицуулна.

4.1.8.Мэдээллийн аюулгүй байдлын чиглэлээр төсөв төлөвлөн, төлөвлөгөө гаргадаг байна.

4.2.Физик орчны хувьд

4.2.1.Сервер болон мэдээллийн сан, мэдээлэл хадгалагддаг компьютеруудыг орчны нөлөөнөөс хамгаалах шаардлагатай.

4.2.2.Орчны хамгаалалт: Физик хамгаалалт нь сервер болон ажлын компьютерууд, өрөөг орчны аюулаас сэргийлэх зорилготой. Физик хамгаалалтын дараах 3 бүсэд ангилж үзнэ.

а/ Нээлттэй бүс – нийтэд мэдээллээр үйлчлэх хэсэг (лавлагаа, мэдээлэл, зөвшөөрөл өгөх өрөө, нэг цэгийн үйлчилгээ, уулзалтын өрөө зэрэг орно)

б/ Нийтэд хаалттай бүс – зөвхөн тухайн байгууллагын ажилтнууд орох эрхтэй хэсэг

в/ Хаалттай бүс – зөвхөн эрх бүхий албан хаагчид нэвтрэх эрхтэй хэсэг (серверийн өрөө) Серверийн өрөөнд ажиллахдаа ”Серверийн өрөөнд ажиллах журам”-ыг мөрдлөг болгоно.

Хаалттай бүсэд нэвтрэх

- Зөвхөн орох эрх бүхий зөвшөөрөлтэй хүмүүс тусгай картаар нэвтэрнэ.
- Зөвшөөрөлгүй хүн орох тохиолдолд эрх бүхий албан тушаалтнаас зөвшөөрөл авч, бүртгүүлж орно.

4.2.3.Тоног төхөөрөмжийн нууцлал, хамгаалалт

4.2.3.1.Байгууллага нь өөрийн байгууллагын компьютер, техник хэрэгслийг заавал гэрчилгээжүүлсэн байна. Гэрчилгээг байгууллагын мэдээллийн технологийн мэргэжилтэн хөтлөх бөгөөд засвар үйлчилгээ хийсэн шинэ програм хангамж суулгасан тохиолдолд МТ-ийн мэргэжилтэн болон тухайн компьютер техник хэрэгслийг эзэмшигч хоёул гарын үсэг зурж баталгаажуулна.

4.2.3.2.Компьютерт програм хангамж, техник хангамжийг суурилуулах

а/ Програм болон техник хангамжийн суурилуулалт түүний шинэчлэл, тохиргоог зөвхөн мэдээллийн технологийн мэргэжилтэн хийнэ

б/ Ажилтны компьютерыг форматлан үйлдлийн системийг дахин суулгах тохиолдолд хэрэгцээт файлуудыг өөр дискэнд хуулж, үйлдлийн системийг суулгаж тохируулга хийсний дараа файлын вирусийг шалган, арилгаад буцааж хуулна.

в/ Систем суулгах, өөрчлөлт оруулах бүрд гэрчилгээнд тэмдэглэл хийн эзэмшигч, мэдээллийн технологийн ажилтан хоёул гарын үсэг зурж баталгаажуулна.

4.2.3.3.Зөөврийн компьютер ашиглахад анхаарах зүйлс

а/ Хулгайд алдах, эвдэрч гэмтсэний улмаас мэдээлэл алдагдахаас сэргийлэх үүднээс хадгалж хамгаалах

б/ Зөөврийн компьютерт хадгалагдаж байгаа мэдээллийг зохих ёсоор заавал хамгаалах – аль болох бага мэдээллийг зөөврийн компьютерт байршуулах

в/ Зөөврийн компьютерыг албан хэрэгцээнээс бусад зориулалтаар ашиглахыг хориглох

г/ Зөөврийн компьютертай гадуур ажлаар болон албан томилолтоор явахдаа мэдээллийн нууцлалт хамгаалалтын асуудлыг судалж мэдсэн байх

д/ Зөөврийн компьютерт хулгайгаас сэргийлэх зориулалтын цоожлогч ашиглах

е/ Нууц зэрэглэлийн мэдээллийг шифрлэх, кодлох байдлаар хамгаалах шаардлагатай

4.2.3.4.Сүлжээний кабел

а/ Байгууллагын сүлжээний байнгын ажиллагааг мэдээллийн технологийн ажилтан шалгаж, хариуцна.

б/ Сүлжээний кабелийн үзүүрт хаяг хадан, ашиглагдаагүй гаралтуудыг тэмдэглэж сүлжээний зохицуулагчаас өөр хүн ашиглах боломжийг хаана.

4.2.3.5.Тоног төхөөрөмжийн байрлал

а/ Ажилтан, албан хаагчдын ажлын компьютерын дэлгэцийг бусдад шууд харагдахгүйгээр байрлуулсан байх

б/ Хэвлэгч, олшруулагч хэрэгслүүдийг удирдлагын хараа хяналттай өрөөнд байрлуулах.

в/ Нууц бичиг баримт боловсруулахдаа гадаад, дотоод сүлжээнд холбогдоогүй компьютер ашиглах

4.2.3.6.Хэвлэх, олшруулах төхөөрөмжийг ашиглах

а/ Хэвлэх төхөөрөмжийг үйл ажиллагаандаа өргөнөөр хэрэглэдэг газрууд ашиглалтаа хяналттай байлгах;

б/ Дундын хэвлэх төхөөрөмж рүү холбогдохдоо эрхээр ордог байх;

в/ Олшруулагчаар хийгдсэн ажлыг тэмдэглэж гүйцэтгэлийг дүгнэдэг байх;

4.2.3.7.Зөөврийн хадгалах төхөөрөмжийг ашиглах

а/ Зөөврийн хадгалах төхөөрөмж дээрх мэдээллийг ашиглаж дууссаны дараа мэдээллийг арилгах

б/ Зориулалтын сав, хайрцагт хийж зөөвөрлөдөг байх

в/ Гаднаас зөөврийн хадгалах төхөөрөмж системд оруулах бол заавал хортой кодын эсрэг програм уншуулах

г/ Зөөврийн хадгалах төхөөрөмжийг албан бусаар ашиглах бусдад дамжуулахыг хориглоно.

4.3.Програм, техникийн хувьд

4.3.1.Цахим мэдээллийн архив бүртгэлийн автоматжуулсан системтэй байна.

4.3.2.Сүлжээний хамгаалалтыг зохион байгуулах, мэдээллийн системийг хууль бус гадны халдлагаас хамгаалах.

4.3.3.Мэдээллийн аюулгүй байдлыг хангах, мэдээлэлд зөвшөөрөлгүй нэвтрэх оролдлогыг таслан зогсоох, илрүүлэх зориулалтаар хамгаалалт, хяналтын техникийн систем, програм хэрэгслийг сонгох, нэвтрүүлэх, байнгын ажиллагаанд оруулах.

4.3.4.Техник програмд мэдээ дамжуулах хэрэгсэл байгаа эсэхийг хэрэглээнд нэвтрүүлэхээс өмнө шалгах харилцаа холбооны нууцлал хамгаалалтыг хангах.

4.3.5.Харилцаа холбооны нууцлал хамгаалалтыг хангах

4.2.6.Хамгаалалтын шаардлагатай түвшинг хангахуйц техникийн шийдлийг боловсруулах.

Тав. Байгууллагын мэдээллийн систем, сүлжээ, мэдээллийн сангийн нууцлалт, хамгаалалт

5.1.Биет хамгаалалт

5.1.1.Мэдээллийн системд холбогдсон компьютер, техник хэрэгслүүд нь газардуулгатай өрөөнд байрласан, тэжээлийн нөөц эх үүсвэрт холбогдсон байна.

5.1.2.Байгууллагын ажилтан, албан хаагчид өөрийн, компьютер дээр шууд харьяалах албан тушаалтны зөвшөөрөлгүйгээр гадны этгээдийг ажиллуулах, компьютерыг түгжилгүйгээр /screen lock, log off хийлгүйгээр/ орхиж явахыг хориглоно.

5.2.Нууц үгийн бодлого

5.2.1.Бодлогын хүрээнд байгууллагын бүх ажилтан, албан хаагчид багтах бөгөөд байгууллагын мэдээллийн системд нууц үгээр хандах аргачлалыг тодорхойлж өгнө.

5.2.2.Нууц үгээ сонгох

а/ Нууц үгээ ил бичиж тэмдэглэхийг хориглоно.
б/ Анхдагч нууц үгийг заавал солих.
в/ Нууц үгийг бусдад дамжуулахгүй байх, илчлэгдсэн гэж үзвэл даруй солих.
г/ Зохицуулагчийн нууц үгийг дундаа хэрэглэхгүй байх.

5.2.3.Нууц үгийн бүрдэл

а/ Том, бага үсэг, тоо, тусгай тэмдэгтийг хослуулсан байх.
б/ Үүсмэл үг үүсгэх.
в/ Аюулгүй байдлын шаардлага хангасан нууц үгийг эргэн санахад хялбар байхаар логик дараалалтай үүсгэх.

5.2.4.Нууц үг үүсгэхдээ ашиглахад хориглох зүйлс

а/ Өөрийн болон гэр бүл, төрөл төрөгсөд, ойр дотны хүмүүсийн нэр, төрсөн он сар өдөр, утас, машины дугаар, зэрэг таныг таньдаг болон судалсан хүн мэдэж болох мэдээлэл,түүнийурвуулсан хэлбэрийг хэрэглэх.
б/ Хэрэглэгчийн нэрийг давтах, түлхүүр үгээ адил өгөх.
в/ Нууц үгээ дахин хэрэглэх, хуучин нууц үгээ эргүүлэн өгөх
г/ Нүдэндил харагдах зүйлс/ширээ, ном, компьютер гэхмэт/ таах боломжтой үгс
д/ Гарын хөдөлгөөнөөр амархан илрүүлж болох үгс, тоо /asd, aabbcc, 1234 гэх мэт/
е/ Дан буюу дараалсан тоо, үсэг /1111, 123456, ааа/
ё Тэгш хэмтэй үг, тоо

5.3.Нууц үгийн хамгаалалт

5.3.1.Байгууллагын системийн хэрэглэгчид нууц үгээ хамгаалах үүрэгтэй бөгөөд, бусдад дамжуулахыг хориглоно.

5.3.2.Өрөөнд байгаа компьютерыг 2 минут болон түүнээс дээш хугацаагаар орхиж явахдаа заавал түгжих буюу нууц үгээр хамгаалагдсан дэлгэцийн хамгаалалтыг ажиллуулна.

5.3.3.Нууц үгийг тодорхой хугацаанд буюу улиралд заавал сольдог байх үүрэгтэй.

5.3.4.Нууц үг илэрсэн гэж үзвэл даруй солих. Ингэхдээ хуучин нууц үгийг дахин хэрэглэхээс зайлсхийж, хуучин тэмдэгтүүдийн ихэнхийг солих.

5.3.5.Байгууллагын мэдээллийн систем, програм хангамжийн нууц үгийн сонголт, бүртгэл, ашиглах хугацааг системийн зохицуулагч хариуцан ажиллаж, хяналт тавина. Шинээр үүсгэх, өөрчлөх, устгах тохиолдолд Маягт №3-аар баталгаажуулах ба улирал тутам системүүдийн хэрэглэгчийн жагсаалтыг хянах үүрэг хүлээнэ.

5.4.Лог файлын бүртгэл

5.4.1.Мэдээллийн системд ажиллаж байгаа хэрэглэгчийн хийсэн үйлдлүүд, хэзээ, хаашаа нэвтэрсэн, ямар үйлдэл хийсэн зэрэг нь системд бүртгэгдэж байхаар тохируулна.

5.4.2.Лог файлын бүртгэл, үнэн зөв, бүрэн бүтэн байдлыг системийн зохицуулагч хариуцна.

5.4.3.Лог мэдээллийг 6 сар тутам нөөцөлж, 2 жилийн дараа нягтлан шинжилсний дараа системийн зохицуулагч устгана. Байгууллага нь өөрийн онцлогт нийцүүлэн уялдах тусгай дүрэм журамтай байж энэхүү хугацааг өөрчлөн тогтоож болно.

5.5.Хандалтын удирдлага

5.5.1.Системийн зохицуулагчаас хэрэглэгчдэд хандах эрхийг олгохдоо зөвшөөрөгдсөнөөс бусад мэдээлэлд хандах боломжгүй байхаар зохион байгуулна.

5.5.2.Системийн зохицуулагч өөрийн чиг үүргийн дагуу системд нэвтрэх хандалтын эрхийг эдэлнэ.

5.5.3.Ажилтнуудын мэдээллийн санд нэвтрэх эрхийг тухайн нэгжийн удирдлагын албан бичгээр ирүүлсэн зөвшөөрлийг үндэслэн системийн зохицуулагч нээж өгнө.

5.6.Хортой кодоос хамгаалах

5.6.1.Байгууллагын хэрэгцээнд хэрэглэгдэж байгаа компьютер, мэдээлэл хадгалагч болон тээгч зөөврийн хэрэгслүүдэд зөвшөөрөгдсөн хортой кодын эсрэг програм хангамжийг ашиглана.

5.6.2.Хортой кодын эсрэг програмын шинэчлэлтийг тогтмол хийнэ.

5.6.3.Тодорхой хугацаанд системийн хортой кодын эсрэг програмыг уншуулж, илэрсэн тохиолдолд арилгах арга хэмжээг авна.

5.6.4.Гаднаас мэдээлэл системд оруулах бол сүлжээнд холбогдоогүй компьютерт эхэлж хортой кодын шинжилгээг заавал хийсний дараа системд нэвтрүүлнэ.

5.7.Мэдээллийн санд нэвтрэх эрхийн түвшин

5.7.1.Тухайн байгууллагын ажилтан, албан хаагчид ажлын чиг үүргийнхээ дагуу мэдээллийн санд эрхийн өөр өөр түвшинд хандана.

5.7.2.**Админ эрх** /Admin/ - Систем шинээр суулгах, тохируулга хийх, нэмэлт, өөрчлөлт оруулах, системд хэрэглэгч нэмэх, хасах эрхтэй байна.

5.7.3.**Бичих эрх** /Writing/ - Мэдээллийн санд шинэ бичлэг нэмэх, өөрчлөх, хадгалах эрхтэй.

5.7.4.**Зөвхөн харах эрх** /Read only/ - Зөвхөн харах, унших эрхтэй байна.

5.8.Нэвтрэх эрхийг цуцлах

5.8.1.Мэдээллийн сан, мэдээллийн системд хандах эрх бүхий албан хаагч ажлаас гарсан, халагдсан, өөр ажилд шилжсэн тохиолдолд нэвтрэх эрхийг цуцална. Байгууллагын хүний

нөөцийн нэгж, мэргэжилтэн тухайн ажилтанг ажлаас чөлөөлөх тухай системийн зохицуулагчид мэдэгдсэн байна.

5.8.2.Мэдээллийн систем, мэдээллийн санд нэвтрэх эрх бүхий ажилтан мэдээллийн аюулгүй байдлын бодлого, журмыг зөрчсөн байвал системд нэвтрэх эрхийг системийн зохицуулагчийн зүгээс түдгэлзүүлж болно.

5.9.Цахим баримт бичиг боловсруулах, хадгалах

5.9.1.Хэрэглэгч нь цахим баримт бичиг боловсруулахдаа холбогдох стандартуудыг мөрдлөг болгоно.

5.9.2.Хэрэглэгч нь тухайн ажлын байртай холбогдох бичиг баримтыг төрөлжүүлж өөрийн компьютерын нөөцөд хадгалах. Шаардлагатай бол зөвшөөрөгдсөн бусад санд хадгална.

5.9.3.Хэрэглэгч нь албан хэрэгцээний файлаа нэр төрлөөр нь ангилж хавтас үүсгэн хадгална. Шаардлагатай бол дэд хавтас үүсгэн хадгалж, хэрэглэж хэвшинэ.

5.9.4.Хэрэглэгч нь жил тутмын эхний улиралд нууцын эрхлэгч, архивын ажилтанд өмнөх оны хадгалагдсан файл, хавтсаа байгууллагын мэдээллийн цахим сан хөмрөгт хадгалуулах зорилгоор хүлээлгэн өгнө.

5.9.5.Нууцын эрхлэгч, архивын ажилтан нь хүлээн авснаас долоо хоногийн дотор байгууллагын мэдээллийн цахим архивд хадгална. Ингэхдээ холбогдох тэмдэглэлийг заавал хөтөлнө.

5.9.6.Файлд нэр өгөхдөө “Монгол кирилл цагаан толгойн үсгүүдийг романчлах” MNS 5217:2003 стандартыг мөрдлөг болгоно.

Зургаа. Байгууллагын мэдээллийн нөөцлөлт, хадгалалт

6.1.Байгууллагын үйл ажиллагаанд хэрэглэгддэг худалдаж авсан, захиалан хийлгэсэн, өөрсдийн зохиосон, тусгай зориулалтын програм хангамжийн эх хувийг болон хувилбаруудыг байнгын хэрэгцээнд зориулан серверт байрлуулна.

6.2.Байнгын өөрчлөгддөг мэдээллийн баазын шинэчлэлтийг тогтмол хугацаанд серверт байрлуулна.

6.3.Серверт хадгалагдах өгөгдлийн нэрийг латин үсгээр галиглан бичсэн байна.

6.4.Серверт хадгалагдах өгөгдөл, мэдээллийг юникод ашиглан оруулах.

6.5.Серверт хадгалагдах мэдээллийг байнгын болон түр хадгалах гэж 2 ангилж үзнэ.

а/ Байнгын хадгалах нь байнгын хэрэгцээнд зориулагдсан шаардлагын дагуу боловсруулагдсан байнга хадгалах өгөгдлийн сан, мэдээллийг серверт тусгай хавтаст хадгална. Мөн заавал нөөц хувь үүсгэн хадгал

б/ Түр хадгалах нь түр хадгалагдах мэдээллийг хадгалах хугацаа дууссан тохиолдолд нэгжийн даргын зөвшөөрлөөр устгаж серверийг чөлөөлнө.

6.6.Мэдээллийн системээс мэдээллийг устгахдаа дахин сэргээгдэхгүй байдлаар устгана.

Долоо. Байгууллагын мэдээллийн аюулгүй байдлын мэргэжилтний эрх, үүрэг

7.1.Байгууллагын мэдээллийн системд заналхийлж буй халдлагыг бүртгэх, илрүүлэх, таслан зогсоох болон эмзэг байдлыг тогтоох, бууруулах, аюулгүй байдлын бодлого боловсруулах зорилгоор мэдээллийн аюулгүй байдлыг хангах чиглэлээр Үндэсний аудитын

газрын Тамгын газрын мэдээлэл технологийн баг /системийн зохицуулагч/ ажиллана. Байгууллагын мэдээлэл, дүн шинжилгээний болон захиргаа удирдлагын нэгжүүд эсвэл хариуцсан албан хаагчдын чиг үүргийн дагуу мэдээллийн аюулгүй байдлыг хангахад дэмжиж ажиллана.

7.2.Системийн зохицуулагчийн эрх

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

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

7.2.3.Аюулгүй байдлын шаардлагыг зөрчигчдөд хариуцлага тооцох талаар байгууллагын удирдлагад санал оруулах.

7.2.4.Байгууллагад ашиглагдах мэдээллийн систем, техник технологи худалдан авах болон шинээр нэвтрүүлэх үйл явцад хяналт тавих.

7.2.5.Эрсдэлийн үнэлгээг жил тутам хийж мэдээллийн аюулгүй байдлын эмзэг байдлыг тодорхойлох, хамгаалалтын түвшинг тогтоох, хөндлөнгийн хяналтыг хэрэгжүүлэх.

7.2.6.Мэдээллийн систем, сангийн бүрэн бүтэн байдалд хяналт тавих, мэдээллийн сангийн нөөц хувийг хувилж хадгалах нөхцөлийг хангах.

7.2.7.Байгууллагын компьютерын систем, серверт нэмэлт өөрчлөлт, шинэчлэлт, 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.

7.2.8.Худалдан авах, захиалан хийлгэх програм хангамжийн даалгаварт зөвлөгөө, санал өгөх, худалдан авах үйл ажиллагаанд мэргэжлийн зүгээс зөвлөгөө өгөх.

7.3.Системийн зохицуулагчийн үүрэг

7.3.1.Мэдээллийн системийг байгуулах, турших, ашиглах, засвар үйлчилгээг хийх, хэвийн үйл ажиллагааг хангах.

7.3.2.Мэдээллийн сан, програм хангамж, компьютерыг хортой кодоос хамгаалах.

7.3.3.Мэдээллийн аюулгүй байдлыг хангахад чиглэсэн сургалт, сурталчилгааг зохион байгуулах.

7.3.4.Байгууллагын сүлжээ, системд нэвтэрсэн халдлагыг таслан зогсоож хариу үйлдэл хийх, хурдан хугацаанд системийг сэргээх арга хэмжээ авах.

7.3.5.Мэдээллийн системд ашиглах техник хэрэгсэл, програм хангамжийн гарал үүслийг бүртгэх, шаардлагатай тохиолдолд техникийн үзлэг хийх.

7.3.6.Хамгаалагдсан мэдээлэлд зөвшөөрөлгүй хандах оролдлогыг тухайн цагт нь илрүүлэх, таслан зогсоох зорилготой аюулгүй байдлын хяналтыг тасралтгүй зохион байгуулах.

7.3.7.Байгууллагын компьютерууд, дагалдах тоног төхөөрөмж, хэрэгслүүдийн ажиллагаа, шинэ тоног төхөөрөмжийн суурилуулалтыг хариуцах.

7.3.8.Компьютер, техник хэрэгслүүдийн битүүмжлэлийг хариуцаж, хяналт тавьж ажиллах.

7.3.9.Мэдээллийн аюулгүй байдлыг хангах шаардлагад нийцүүлэн мэдээллийг хамгаалах системийг бий болгох, түүний ажлын горимыг боловсруулах.

7.3.10.Мэдээллийн аюулын байдлыг хангахад шаардагдах мэргэжил дээшлүүлэх сургалтад байнга хамрагдаж байх

7.3.11.Мэдээллийн аюулгүй байдлын аудитыг 3 жил тутамд хийж тайлан мэдээг тогтмол гаргадаг байх

7.3.13.Аюулгүй байдлын горимыг мөрдөж ажиллахыг шаардах, зөрчигдсөн үед зөрчлийг арилгахыг шаардах.

7.3.14.Шинээр гарсан хөтөлбөр, төлөвлөгөө, дүрэм, журмыг харьяа газруудад сурталчлан таниулах, гүйцэтгэлийн тайлан мэдээг гаргаж нэгтгэх.

Найм. Мэдээллийн системийн хэрэглэгчийн үүрэг

8.1.Төрийн аудитын байгууллагуудын мэдээллийн системд ажиллаж байгаа бүх ажилтан, албан хаагчид, гэрээт ажилтан нар энэхүү журмыг өдөр тутмын ажилдаа мөрдлөг болгон ажиллана.

8.2.Мэдээллийн аюулгүй байдалтай холбоотой учрал гарсан тохиолдолд системийн зохицуулагчид тухай бүрд нь мэдэгдэнэ.

8.3.Систем болон үйлчилгээнд ажиглагдсан, байж болох сул талд анхаарлаа хандуулах, түүний тухай мэдээлэх,

8.4.Компьютерын нэр, сүлжээний нэрийг солихгүй байх. Шаардлага гарсан тохиолдолд системийн зохицуулагчид мэдэгдэн зохих үйлчилгээг хийлгэх.

8.5.Ажлын өрөө болон хонгилд ил болон далд угсрагдсан сүлжээний утсууд гэмтсэн, ороцолдсон, далд монтажаас утас ил гарсан тохиолдолд мэдээлэл, технологийн асуудал хариуцсан ажилтанд мэдэгдэх,

8.6.Мэдээллийн аюулгүй байдлыг хангах талаар өгсөн системийн зохицуулагчийн шаардлагыг биелүүлэх,

8.7.Өөрийн компьютерт түр холбосон гадны төхөөрөмжийг сүлжээнд нээж өгөхгүй байх. Хэрэв сүлжээнд нээж ажиллуулж байгаад салгасан бол сүлжээнээс хассан байх шаардлагатай.

Ес. Хориглох зүйл

10.1.Албан хэрэгцээнээс бусад зөвшөөрөлгүй програм хангамжийг суулгаж ажиллуулах.

10.2.Интернетээс албан ажилтай холбогдолгүй програм, дуу, кино, зураг, тоглоом зэрэг мэдээлэл татах.

10.3.Байгууллагын бус компьютер, зөөврийн хэрэгслийг сүлжээнд зөвшөөрөлгүй холбох, мэдээлэл авах, солилцох

10.4.Хариуцаж буй компьютер техник хэрэгсэлд засвар, үйлчилгээг зөвшөөрөлгүй гадны хүнээр хийлгэх.

10.5.Ажлын өрөө солих, байрлалаа шилжүүлэх тохиолдолд дур мэдэн сүлжээний утсаа солих. Өөрийн компьютерт тохируулсан сүлжээний тохиргоог дур мэдэн өөрчлөх.

10.6.Өөрийн компьютерт шаардлагагүй дундын хавтас сүлжээнд нээхгүй байх. Сүлжээнд нээсэн дундын хавтас дотор чухал мэдээ материал, өгөгдлийг удаан хугацаагаар хадгалахгүй байх.

10.7.Мэдээлэл хадгалсан мэдээлэл хадгалах, тээх хэрэгслийг буруу хадгалах, гэмтээх, хаяж үрэгдүүлэх.

10.8.Сүлжээнд холбогдсон бусад компьютер доторх дундын хавтас дахь материалыг устгах.

10.9.Мэдээлэл тээгчийг өөр зориулалтаар ашиглахыг хориглох ба актлагдсан үед физик устгал хийж, устгасан тухай нотломж үйлдэх.

10.10.Системийн зохицуулагч нь ажил үүргийн дагуу олгосон эрхээ бусдаар ашиглах.

Арван нэг. Хариуцлага

11.1. Албан хаагчдын анхаарал болгоомжгүй үйлдлээс болж мэдээллийн систем, мэдээллийн сангийн аюулгүй байдал алдагдах, мэдээллийн аюулгүй байдлын бодлого, журам зөрчигдөж, байгууллагын үйл ажиллагаанд хохирол учруулсан ба эмзэг байдал үүсгэсэн бол холбогдох хууль, дүрэмд заасан шийтгэл ноогдуулна.

11.2.Нууц мэдээллийг санаатай буюу санамсаргүй байдлаар бусдад задруулснаас учрах хохирлыг нөхөн төлүүлэх түүнчлэн хууль зүйн зохих заалтын дагуу асуудлыг шийдвэрлэнэ.

Арван хоёр. Бусад

12.1.Нууц ангиллын мэдээллийн хадгалалт, хамгаалалт, дамжуулах үйл ажиллагаанд мэдээллийн хариуцагч болон системийн зохицуулагч хяналт тавьж ажиллах бөгөөд нууцын журам зөрчсөн, алдаа дутагдал илэрсэн тохиолдолд заавар зөвлөмж өгөх, засаж сайжруулах талаар арга хэмжээ авч байгууллагын удирдлагад мэдэгдэж байна.

12.2.Нууц ангиллын мэдээлэлтэй шууд харьцах, нуущад зэрэглэл хамаарахгүйгээр нэвтрэх албан тушаалтныг Монгол Улсын Ерөнхий аудиторын тушаалаар томилох бөгөөд шаардлагатай тохиолдолд өөрчлөлт оруулж болно.

12.3.Журмыг хэрэгжүүлэхтэй холбоотой хавсралт болох маягтууд нь журмын хүрээнд хүчин төгөлдөр үйлчилнэ.

Маягт №1

НУУЦЫН БАТАЛГАА

Газар, алба:

Албан тушаал:

Овог:
Нэр:

Би өөрийн албан үүргээ гүйцэтгэх явцад олж мэдсэн, хадгалж байсан, үйл ажиллагаандаа ашиглаж байсан Байгууллагын нууцад хамаарах зүйлсийг цаашид задруулахгүй байх үүргийг хүлээн зөвшөөрч байна.

Байгууллагын нууцыг задруулсан тохиолдолд Монгол Улсын холбогдох хууль болон Мэдээллийн аюулгүй байдлыг хангах журам, Дотоод журмын дагуу хариуцлага хүлээхэд бэлэн байна гэдгээ энэ хүү баталгаагаар хүлээн зөвшөөрч байна.

БАТАЛГАА ГАРГАСАН:

_____ .....

(Ажилтны нэр) (Гарын үсэг)

**ТАЙЛБАР: Нууц мэдээлэлд хандах эрхийн баталгааг заавал биеэр төлөөлүүлэн авах маягт /*3.2.5*./*

Маягт №2

НУУЦ АНГИЛЛЫН МЭДЭЭЛЭЛ, ТЭДГЭЭРИЙГ ХАРИУЦАГЧ, ЭЗЭМШИГЧ БОЛОН ХЭРЭГЛЭГЧИЙН ЖАГСААЛТ

№	Мэдээллийн нэр	Тайлбар	Нууцын зэрэглэл	Хариуцагч	Эзэмшигч	Хэрэглэгч
1						
2						

**ТАЙЛБАР: Уг ангилалыг нууцийн тухай журмаар зохицуулагдана /*3.2.6*./*

МЭДЭЭЛЛИЙН СИСТЕМИЙН БАЙР ӨРӨӨ ТАСАЛГААНЫ ХАМГААЛАЛТЫН ЗЭРЭГЛЭЛИЙН ЖАГСААЛТ

№	Өрөөний нэр	Тайлбар	Зэрэглэл	Хариуцагч
1				
2				

**ТАЙЛБАР: Уг зэрэглэлийг Үндэсний аудитын Тамгын газрын мэдээлэл, технологийн баг, нууцийн асуудал хариуцсан албан хаагчид тогтооно.*

Маягт №3

Хүсэлтийн дугаар №.....
Хүсэлтийн төрөл:
❑Шинэ хэрэглэгч үүсгэх
❑Хандах эрхийг өөрчлөх
❑Хэрэглэгчийг устгах
Эрх хүсэж буй ажилтнымэдээлэл:
Хэрэглэгчийн нэр: .....
Алба /Хэлтэс/ Албан тушаал: .....
Холбогдох хаяг: .....

Хандах эрх нэмэх			
№	Хандах эрхийн төвшин, төрөл, хэлбэр	Хандах эх үүсвэр	Хандах эрх нэмэх шалтгаан, тайлбар
1			
Хандах эрх өөрчлөх			
№	Хандах эрхийн төвшин, төрөл, хэлбэр	Хандах эх үүсвэр	Хандах эрхийн өөрчлөлт хийлгэх шалтгаан, тайлбар
1			
Хандах эрх устгах			
№	Хандахэрхийнтөвшин, төрөл, хэлбэр	Хандах эх үүсвэр	Хандах эрх устгах шалтгаан, тайлбар
1			

Хүсэлт гаргасан ажилтны менежер	**Хүсэлтийг зөвшөөрсөн хариуцсан дарга**
Гарын үсэг: / /	Гарын үсэг: / Дарга /
Он / сар / өдөр: 20..../.../....	Он / сар / өдөр:20..../.../...

**ТАЙЛБАР: Систем, өгөгдлийн сан, сүлжээ, компьютер болон бусад нууц гэх мэдээлэлд хандах эрхийг шинээр үүсгэх, устгах, өөрчлөх хүсэлтийг авах маягт*