Нийслэлийн Үйлдвэр, хөдөө аж ахуйн газрын даргын 2015 оны ... дугаар сарын .... –ны өдрийн .... дүгээр тушаалын хавсралт

НИЙСЛЭЛИЙН ҮЙЛДВЭР, ХӨДӨӨ АЖ АХУЙН ГАЗРЫН МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ЖУРАМ

Нэг. Ерөнхий зүйл

1.1. Байгууллагын 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 эрсдэлээс урьдчилан сэргийлэх, эрсдэл учирсан, хохирол гарсан тохиолдолд урьдчилан бэлтгэсэн заавар, журмын дагуу холбогдох арга хэмжээг шуурхай авч хэрэгжүүлэх нөхцөлийг бүрдүүлэхэд энэхүү журмын зорилго оршино.

1.2. Нийслэлийн Үйлдвэр, хөдөө аж ахуйн газрын мэдээллийн технологийн мэргэжилтэн ажил үүргээ гүйцэтгэхдээ энэхүү журмыг мөрдлөг болгоно.

Хоёр. Нэр томьёо

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

2.5.Мэдээлэл хариуцагч Мэдээллийг эзэмшиж байгаа ажилтны удирдах дээд албан тушаалтныг;

2.6.Мэдээллийн аюулгүй байдал Аливаа хэлбэрээр илэрхийлэгдсэн мэдээлэл алдагдалд орохгүй байх, үүнээс урьдчилан сэргийлэх арга хэмжээг хэлнэ

2.7.Аюул занал Мэдээллийн систем болон байгууллагад хор хохирол учруулж болох боломж, үйлдэл, үйл явдлыг;

2.9.Нэгж Байгууллагын мэдээллийн аюулгүй байдал, мэдээллийн технологийн үйл ажиллагааны хэвийн нөхцлийг хангах чиг үүрэгтэй албан хаагч, нэгж бүтцийг;

2.10.Зохицуулагч Байгууллагын мэдээллийн технологи хариуцсан эрх, үүрэг бүхий мэргэжилтэн;

2.11.Хэрэглэгч Байгууллагын мэдээллийн системтэй харьцдаг бүх шатны ажилтан, албан хаагчдыг хэлнэ.

Гурав. Байгууллагын мэдээллийн өмч хөрөнгө, ангилал

3.1. Мэдээллийн өмч хөрөнгийн ангилал

Мэдээллийн өмч хөрөнгийг биет мэдээллийн, цахим мэдээллийн, программ хангамжийн болон техник хангамжийн мэдээлэл гэж ангилна.

3.1.1.Биет мэдээллийн өмч хөрөнгөд судалгааны материалууд, үйл ажиллагааны төлөвлөгөө, төсөл хөтөлбөрүүд, бүртгэлийн мэдээллүүд, сургалтын материал, гарын авлага, хяналт шалгалтын тайлан, хэвлэмэл зургууд зэрэг бүх төрлийн хэвлэмэл мэдээлэл багтана.

3.1.2.Цахим мэдээллийн өмч хөрөнгөнд биет мэдээллийн цахим хэлбэрүүд, мэдээллийн сангийн өгөгдлүүд болон бусад төрлийн цахим мэдээлэл орно.

3.1.3.Программ хангамжийн өмч хөрөнгөнд албан ёсны зөвшөөрөлтэй хэрэглээний программ хангамж, мэргэжлийн болон системийн программ хангамж, байгууллагын бие даан боловсруулсан болон тусгай захиалгаар хийлгэсэн программ хангамж, системүүд хамаарна.

3.1.4.Техник хангамжийн өмч хөрөнгөнд 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 хэрэгслүүд багтана.

3.2. Мэдээллийн нууцлал, ангилал

Байгууллагын мэдээллийг хэрэглээний зориулалтаар нь дараах байдлаар ангилна.

3.2.1. Нийтэд хүртээмжтэй мэдээлэл

Нийтэд зориулагдсан, холбогдох хууль тогтоомж, журмаар нууцлаагүй бөгөөд буруугаар ашиглахад байгууллагад ямар нэгэн хохирол учруулахгүй мэдээллүүд үүнд багтана.

Эдгээр мэдээллийг хувилах, хадгалах, дамжуулахад ямар нэгэн шаардлага тавихгүй бөгөөд зөвшөөрөл авахад бүрдүүлэх материал, байгууллагын санхүүгийн үйл ажиллагааны төлөвлөгөө, тайлан, нийтэд хандсан зөвлөмж, сэрэмжлүүлэг зэрэг байгууллагын үйл ажиллагааны ил тод байдлыг илтгэсэн, нийтийг мэдлэг мэдээллээр хангахад чиглэсэн мэдээллүүд байна.

3.2.2.Байгууллага доторх нээлттэй мэдээлэл

Энэхүү мэдээлэлд байгууллагын нийт албан хаагчдад танилцуулах, хувилж тараах мэдээ, мэдээлэл хамаарна.

3.2.3.Нууц мэдээлэл

Хууль тогтоомж болон байгууллагын дотоод дүрэм журамд нууц байхаар заасан 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

Дөрөв. Байгууллагын мэдээллийн хамгаалалт

4.1.Физик орчны хувьд

4.1.1. Сервер болон мэдээллийн сан, мэдээлэл хадгалагддаг компьютерууд орчны нөлөөнөөс хамгаалагдсан байна.

Физик хамгаалалтыг дараах 3 бүсэд ангилна.

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

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

в/ Хориотой бүс – зөвхөн эрх бүхий албан хаагчид нэвтрэх эрхтэй хэсэг

4.2.3.Тоног төхөөрөмжийн нууцлал, хамгаалалт

4.2.3.1.Байгууллага компьютер, техник хэрэгслийг заавал гэрчилгээжүүлнэ.

Гэрчилгээг байгууллагын мэдээллийн технологийн мэргэжилтэн хөтлөх бөгөөд засвар үйлчилгээ хийсэн, шинэ программ хангамж суулгасан тохиолдол бүрийг баримтжуулна.

4.2.3.2.Компьютерт программ хангамж, техник хангамжийг суурилуулах

Программ болон техник хангамжийн суурилуулалт, түүний шинэчлэл, тохиргоог зөвхөн мэдээллийн технологийн мэргэжилтэн хийж гүйцэтгэх бөгөөд дараах журмыг баримталж ажиллана.

а/ Компьютерыг форматлах болон үйлдлийн системийг дахин суулгах тохиолдолд бүх файлуудыг өөр дискэнд хуулж авах, мэдээлэл бүрэн гүйцэт хуулагдсан эсэхийг файлын хэмжээ болон тоо ширхэгээр нь нягтлан тулгана.

б/ Үйлдлийн системийг суулгаж, тохируулга хийсний дараа файлын вирусийг шалган арилгаад буцааж хуулна.

в/ Систем суулгах, өөрчлөлт оруулах бүрд гэрчилгээнд тэмдэглэл хийж эзэмшигч, мэдээллийн технологийн ажилтан гарын үсэг зурж баталгаажуулах.

4.2.3.3.Зөөврийн компьютерийн мэдээллийн аюулгүй байдлыг хангах

Албан хэрэгцээнд ашиглаж байгаа зөөврийн компьютерийн эзэмшигч нь түүнд хадгалагдаж байгаа мэдээлийн аюулгүй байдлыг хангах талаар дараах арга хэмжээг авна. Үүнд:

а/ Хулгайд алдах, эвдэрч гэмтэх зэргээс шалтгаалан мэдээлэл алдагдахаас сэргийлэх үүднээс зөөврийн компьютерын мэдээллийг суурин компьютер, серверт байнга хуулбарлаж, аль болох бага мэдээлэлтэй байлгах;

б/ Зөөврийн компьютерт системийн болон хэрэглэгчийн нууцлалын кодыг заавал суурилулах;

в/ Зөөврийн компьютерыг албан хэрэгцээнээс бусад зориулалтаар ашиглахгүй байх;

г/ Зөөврийн компьютерт хулгайгаас сэргийлэх зориулалтын цоожлогч ашиглах;

д/ Нууцын зэрэглэлтэй мэдээллийг шифрлэх, кодлох байдлаар хамгаалах.

4.2.3.4.Сүлжээний кабель

Байгууллагын сүлжээний байнгын ажиллагааг мэдээллийн технологийн ажилтан хариуцна.

Сүлжээний кабелийн үзүүрт хаяг хадан, ашиглагдаагүй гаралтуудыг тэмдэглэж, сүлжээний зохицуулагчаас өөр хүн ашиглахгүй байх нөхцөлийг бүрдүүлнэ. Хэрэглэгчдийн ашиглахгүй байгаа сүлжээний сул кабелийг хурааж авна.

4.2.3.5.Техник хэрэгслийг байрлуулах

Хэрэглэгчид ажил үүргээ гүйцэтгэх явцад хэрэглэж байгаа техник, тоног төхөөрөмжөөс мэдээлэл алдахгүй байх үүднээс дараах байдлаар байрлуулна.

а/ Ажлын компьютерын дэлгэцийг бусдад шууд харагдахгүй байхаар байрлуулах;

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

в/ Дундын хэвлэх төхөөрөмж рүү холбогдохдоо зөвшөөрөгдсөн эрхээр ордог байх;

г/ Олшруулагчаар хувилсан бичиг баримтын талаар тэмдэглэл хөтөлж, гүйцэтгэлийг дүгнэдэг байх;

4.2.3.6.Зөөврийн хадгалах төхөөрөмж ашиглах

а/ Зөөврийн хадгалах төхөөрөмж дээрх мэдээллийг ашиглаж дууссаны дараа уг мэдээллийг устгана;

б/ Зориулалтын сав, хайрцагт хийж зөөвөрлөдөг байх;

в/ Зөөврийн хадгалах төхөөрөмжөөс байгууллагын мэдээллийн системд мэдээлэл оруулах тохиолдолд вирусны эсрэг программыг заавал уншуулж байна;

г/ Нууцын зэрэглэл бүхий мэдээлэл агуулсан зөөврийн хадгалах төхөөрөмжийг албан бусаар ашиглах, бусдад дамжуулахыг хориглоно.

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

5.1.Биет хамгаалалт

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

5.1.2.Байгууллагын албан хаагчид өөрийн компьютерт гадны этгээдийг ажиллуулах, компьютерээ түгжихгүй /screen lock, log off хийхгүй/-ээр орхиж явахыг хориглоно.

5.2.Нууц үг

5.2.1. Мэдээллийн нууцлалыг хангах ажлын хүрээнд хэрэглэгч бүр нууц үгээр байгууллагын мэдээллийн системд хандах ба нууц үгийг сонгохдоо дараах арга хэмжээг авсан байна.

5.2.1.1.Нууц үгээ сонгох

а/ Том, жижиг үсэг, тоо, тусгай тэмдэгтийг хослуулсан байх;

б/ Үүсмэл үг үүсгэх;

в/ Нууц үгийг эргэн санахад хялбар байхаар логик дараалалтай үүсгэх.

5.2.2.2. Нууц үг үүсгэхэд хориглох зүйлс

а/ Өөрийн болон гэр бүл, төрөл төрөгсөд, ойр дотны хүмүүсийн нэр, төрсөн он сар өдөр, утас, машины дугаар, түүний урвуулсан хэлбэр зэрэг таныг таньдаг болон судалсан хүн мэдэх, таамаглах боломжтой мэдээллийг хэрэглэх;

б/ Хэрэглэгчийн нэрийг давтах, түлхүүр үгээ адилхан байдлаар өгөх;

в/ Өмнө нь хэрэглэж байсан нууц үгээ дахин хэрэглэх;

г/ Нүдэнд ил харагдах эд зүйл /ширээ, ном, компьютер/ зэрэг тааж олоход хялбар үгс хэрэглэх;

д/ Гарын хөдөлгөөнөөр амархан илрүүлж болох үсэг, тоо /asd, aabbcc, 1234 гэх мэт/ хэрэглэх;

е/ Дан буюу дараалсан, эсвэл тэгш хэмтэй тоо, үсэг /1111, 123456, aaa/ хэрэглэх.

5.3.Нууц үгийн хамгаалалт

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

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

5.3.3.Хэрэглэгч нууц үгийг тодорхой хугацаанд буюу улирал бүр заавал сольж байна.

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

5.3.5.Байгууллагын мэдээллийн систем, программ хангамжийн нууц үгийн сонголт, бүртгэл, ашиглах хугацааг мэдээллийн технологийн мэргэжилтэн хариуцан ажиллаж, хяналт тавина.

5.3.6. Нууц үгээ ил бичиж тэмдэглэхийг хориглоно.

5.3.7. Зохицуулагчийн нууц үгийг дундаа хэрэглэхийг хориглоно.

5.3.8. Мэдээллийн системээс олгогдсон анхдагч нууц үгийг заавал солих

5.4.Мэдээллийн системийн хандалтын удирдлага

5.4.1. Мэдээллийн технологийн мэргэжилтнээс хэрэглэгчдэд хандах эрхийг олгохдоо зөвшөөрөгдсөнөөс бусад мэдээлэлд хандах боломжгүй байхаар зохион байгуулна.

5.4.2. Мэдээллийн технологийн мэргэжилтэн өөрийн чиг үүргийн дагуу системд нэвтрэх хандалтын эрхийг эдэлнэ.

5.4.3. Хэрэглэгчдийн мэдээллийн санд нэвтрэх эрхийг тухайн нэгжийн удирдлагын албан бичгээр ирүүлсэн зөвшөөрлийг үндэслэн мэдээллийн технологийн мэргэжилтэн нээж өгнө.

5.5. Хортой код /Вирус/ -оос хамгаалах

5.5.1.Байгууллагын хэрэгцээнд хэрэглэгдэж байгаа компьютер, мэдээлэл хадгалагч болон мэдээлэл тээгч зөөврийн хэрэгслүүдэд хортой кодын эсрэг албан ёсны зөвшөөрөлтэй программ хангамжийг ашиглана. Хортой кодын эсрэг албан ёсны зөвшөөрөлтэй программ хангамж худалдан авах санхүүжилтийг байгууллага хариуцна.

5.5.2.Системийн зохицуулагч нь хортой кодын эсрэг программын шинэчлэлтийг хэрэглэгчдийн компьютерт тогтмол хийх боломж нөхцөлөөр хангана.

5.5.3. Системийн хортой кодын эсрэг программыг тодорхой давтамжтайгаар уншуулж, хортой код илэрсэн тохиолдолд түүнийг арилгах арга хэмжээ авна.

5.5.4. Гаднаас мэдээллийн системд мэдээлэл хуулбарлан оруулах бол эхлээд сүлжээнд холбогдоогүй компьютерт хуулбарлан хортой кодын шинжилгээ хийж, аюулгүй болгосны дараа системд нэвтрүүлнэ.

5.6.Мэдээллийн санд нэвтрэх эрхийн түвшин

5.6.1. Албан ажлын чиг үүргээс хамаарч хэрэглэгчид мэдээллийн санд эрхийн өөр өөр түвшинд хандана.

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

5.6.3. Бичих эрх /Writing/ - Мэдээллийн санд шинэ бичлэг нэмэх, өөрчлөх, хадгалах эрхтэй байна.

5.6.4. Зөвхөн харах эрх /Read only/ - Мэдээллийг харах, унших эрхтэй байна.

5.7.Нэвтрэх эрхийг цуцлах

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

Албан хаагч ажлаас гарсан тохиолдолд байгууллагын хүний нөөцийн нэгж, мэргэжилтэн энэ тухай мэдээллийн технологийн мэргэжилтэнд заавал мэдэгдэнэ.

5.7.2. Мэдээллийн систем, мэдээллийн санд нэвтрэх эрх бүхий албан хаагч мэдээллийн аюулгүй байдлын бодлого, журмыг зөрчсөн нь тогтоогдвол системд нэвтрэх эрхийг системийн зохицуулагчийн зүгээс түдгэлзүүлж болно.

Зургаа. Сүлжээний орчинд баримтлах зарчим

6.1 Сүлжээний тоног төхөөрөмжийн сонголт

Сүлжээний тоног төхөөрөмжийг сонгоход дараах шалгууруудыг тавина.

- CAT-6 технологийн кабелаас дээд шатны UTP кабель
- L2 төрлийн менежмент свитч, түүнээс дээш свитч
- Cisco, Mikrotek брэндийн нууцлал өндөр роутер

- Cisco, D-Link төрлийн firewall /галт хана
- Сүлжээний тоног төхөөрөмж, сервер байрлуулах боломж бүхий РАК
- 1000 Вт –аас дээш чадал бүхий, РАК-д байрлах сүлжээний тоног төхөөрөмж, сервер компьютерыг цахилгаанаар хангах чадвартай тог баригч.

6.2 Сүлжээний топологи

Дотоод сүлжээний топологийг одон эсвэл одон салаа холболтоор холбох ба сүлжээний аль нэг хэсэгт гэмтэл гарсан тохиолдолд бусад сүлжээнд саад болохгүй байхаар сүлжээг зохион байгуулна.

Сүлжээний бүх төхөөрөмжийг хаягжуулж, тэмдэглэл хөтлөн топологи зураглалд тусгасан байна.

6.3 Сүлжээний нууцлал хамгаалал

- Дотоод сүлжээнд нэвтрэх хэрэглэгч нь мэдээллийн технологийн мэргэжилтэн өгсөн эрхийн дагуу нэвтрэн ордог байх;
- Хэрэглэгчдийн нэвтрэх эрх хяналттай байх;
- Сүлжээнд холбогдсон, сүлжээнээс гарсан бүх тоног төхөөрөмжүүдийн үйлдэл бүр тэмдэглэгээ файлд тэмдэглэгдэн үлддэг байх;
- Хандалтын хяналтын жагсаалтыг хагас жил тутамд хянаж байх;
- Дотоод сүлжээг нээлттэй, хязгаарлагдсан, өндөр түвшинд хязгаарлагдсан хэсэгт хуваж хамгаалсан байх;
- Хязгаарлагдсан хэсэгт ашиглаж байгаа сүлжээний кабелыг нийтийн бүсэд ил татахгүй байх;
- Сүлжээнд холбогдсон бүх тоног төхөөрөмжүүдэд шошго зүүж сүлжээн дэх нэр, IP хаяг, MAC хаяг, кабелын дугаарыг бичиж баримтжуулж байх.

6.4 Сүлжээний тасралтгүй ажиллагаа, найдвартай байдал

- Дотоод сүлжээ 24 цагаар ажиллах бөгөөд жилд 1 удаа бүрэн хэмжээний засвар үйлчилгээ хийнэ.
- Сүлжээнд гарсан гэмтэл, ачааллын хяналтыг тогтмол мэдээлж байна.
- Сүлжээнд хийгдсэн өөрчлөлт, шинэчлэлт, засвар үйлчилгээг тэмдэглэл хөтлөн баримтжуулна.
- Дотоод, гадаад сүлжээний аюулгүй байдал, хэвийн ажиллагааг хянах мониторингийн системийг бүрэн нэвтрүүлсэн байна.

Долоо. Байгууллагын мэдээллийн аюулгүй байдлын нэгж, мэргэжилтний эрх, үүрэг

7.1.Системийн зохицуулагчийн эрх

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

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

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

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

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

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

7.1.7. 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.Системийн зохицуулагчийн үүрэг

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

7.2.2.Мэдээллийн сан, программ хангамж, компьютерыг хортой кодоос хамгаалах.

7.2.3.Мэдээллийн аюулгүй байдлыг хангахад чиглэсэн сургалт, сурталчилгааг байгууллагын хэмжээнд зохион байгуулах.

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

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

7.2.6.Хамгаалагдсан мэдээлэлд зөвшөөрөлгүй хандах оролдлогыг илрүүлэх, таслан зогсоох зорилготой аюулгүй байдлын хяналтыг тасралтгүй зохион байгуулах.

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

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

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

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

Найм. Мэдээллийн системийн хэрэглэгчийн үүрэг, хариуцлага

8.1. Байгууллагуудын мэдээллийн системд ажиллаж байгаа бүх ажилтан, албан хаагчид нар энэхүү журмыг өдөр тутмын ажилдаа мөрдлөг болгон ажиллах.

8.2.Систем болон үйлчилгээнд ажиглагдсан, байж болох доголдолд анхаарлаа хандуулах, түүний тухай мэдээлж байх.

8.3.Компьютерын нэр, сүлжээний нэрийг солихгүй байх, зайлшгүй шаардлага гарсан тохиолдолд системийн зохицуулагчид мэдэгдэн зохих үйлчилгээг хийлгэх.

8.4.Ажлын өрөө, хонгилд ил болон далд угсрагдсан сүлжээний утсууд гэмтсэн, ороолдсон, далд монтажаас утас ил гарсан тохиолдолд байгууллагын холбогдох нэгж, мэргэжилтэнд мэдэгдэх.

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

8.6.Өөрийн компьютерт түр холбосон гадны төхөөрөмжийг сүлжээнд нэвтрүүлэхгүй байх, сүлжээнд нээж ажиллуулсан бол сүлжээнээс хассан байх шаардлагатай.

Ес. Хэрэглэгчид хориглох зүйл

9.1. Зөвшөөрөлгүй программ хангамжийг суулгаж ажиллуулах.

9.2. Албан ажилтай холбогдолгүй програм, дуу, кино, зураг, тоглоом зэрэг мэдээллийг интернет, бусад эх үүсвэрээс татах.

9.3. Гадны компьютер, зөөврийн хэрэгслийг сүлжээнд зөвшөөрөлгүй холбох, мэдээлэл авах, солилцох.

9.4. Хариуцаж байгаа компьютер, техник хэрэгсэлд зөвшөөрөл авахгүйгээр гадны хүнээр засвар, үйлчилгээ хийлгэх.

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

9.6. Чухал мэдээ материал, өгөгдлийг сүлжээнд нээсэн дундын хавтаст удаан хугацаагаар хадгалахгүй байх.

9.7. Албан мэдээлэл бүхий мэдээлэл хадгалах, тээх хэрэгслийг буруу хадгалах, гэмтээх, хаяж үрэгдүүлэх.

9.8.Сүлжээнд холбогдсон бусад компьютерийн дундын хавтас дахь материалыг устгах.

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

9.10. Системийн зохицуулагч нь ажил үүргийн дагуу олгосон эрхээ буруугаар ашиглах.

Арав. Хариуцлага

10.1. Ажилтны анхаарал болгоомжгүй үйлдлээс болж мэдээллийн системийн сүлжээний мэдээллийн сангийн аюулгүй байдал алдагдсан, мэдээллийн аюулгүй байдлын журам зөрчигдөж, байгууллагын үйл ажиллагаанд хохирол учруулсан, эмзэг байдал үүсгэсэн бол Төрийн албаны тухай, Хөдөлмөрийн тухай хуулийн дагуу холбогдох ажилтанд сахилгын шийтгэл ногдуулна.