МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ЖУРАМ

Нэг. Зорилго

1.1.Байгууллагын мэдээллийн аюулгүй байдлыг хангах чиг үүргийг ажилтаны ажлын байрны тодорхойлолтонд бий болгох, мэдээллийн сүлжээ, системийн найдвартай ажиллагаа, мэдээллийн сангийн 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.

Хоёр. Хамрах хүрээ

2.1.Байгууллагын нийт ажилтан албан хаагчид, мэдээллийн технологийн мэргэжилтэн ажил үүргээ гүйцэтгэхдээ энэхүү журмыг мөрдлөг болгон ажиллана.

Гурав. Нэр томьѐо

3.1.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;

3.2.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;

3.3.Хадгалагдах мэдээлэл – Даргын тушаал, шийдвэр, мэдээлэл судалгаа, санхүүгийн мэдээлэл, тайлан мэдээ

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

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

3.6.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.

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

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

3.9.Нөөц – гэж тухайн ажилтны локал “Д” диск

3.10.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;

3.11.Зохицуулагч - гэж байгууллагын мэдээллийн сангийн дотоод үйл ажиллагааг хариуцсан эрх, үүрэг бүхий нэг буюу хэд хэдэн мэргэжилтэнг;

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

3.13. Хэрэглэгчийн эрх - гэж хэрэглэгчийн мэдээллийн системд хандаж хийх үйлдлийг тодорхойолсон хэм хэмжээг;

3.14 Хэрэглэгчийн эрхийн бүлэг - гэж хэрэглэгчийн ажлын байрын тодорхойлолтонд тулгуурлан хийх үйлдлийг нэгтгэж тодорхойлсон бүлгийг;

3.15 “CISA гэрчилгээ /CISA certificate/ ” гэж Мэдээллийн системийн аудит болон хяналтын холбоо /ISACA/-оос олгодог мэдээллийн системийн аудиторын гэрчилгээг;

3.16 “COBIT тогтолцоо / COBIT framework/ ” гэж Мэдээллийн технологийн засаглалын институт /ITGI/ болон Мэдээллийн системийн аудит болон хяналтын холбоо /ISACA/ -оос гаргасан Мэдээллийн технологийн ерөнхий хяналт, удирдлагын тогтолцоог;

3.17 Мэдээллийн систем - гэж мэдээллийн сангийн үйл ажиллагааг хэрэгжүүлж байгаа програм хангамж, техник хангамж, сүлжээний төхөөрөмжүүдийг хэлнэ.

Дөрөв. Мэдээлэл, мэдээллийн систем, хэрэглэгчийн эрхийн хяналт

4.1 Мэдээллийн өмч хөрөнгийн ангилал

4.1.1.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;

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

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

4.1.4.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;

4.2 Мэдээлэл хадгалалт

4.2.1.Хэрэглэгч нь тухайн ажлын байртай холбогдох баримт төрөлжүүлж бичигийг өөрийн компьютерийн нөөцөд хадгална. Шаардлагатай бол зохицуулагчид өгч хадгалуулна.

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

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

4.2.4 Хадгалагдах мэдээллийг зохицуулагч хагас жил болон жилд архивлана.

4.3.Мэдээллийн хамгаалалт

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

4.3.2.Байгууллагын ажилтан, албан хаагчид өөрийн, компьютер дээр шууд харьяалах албан тушаалтны зөвшөөрөлгүйгээр гадны этгээдийг ажиллуулахыг хориглоно.

4.3.3 Байгууллагын ажилтан бүр өөрийн комьютер дээрээ нэвтрэх нууц үгийг нээнэ

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

4.3.5.Нууц үгийг 3 сард заавал нэг удаа сольдог байна.

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

4.3.7. Мэдээллийн сангийн даатгалын гэрээ, нөхөн төлбөр, даатгуулагчын мэдээлэл нь мэдээллийн сангийн хамгаалалтай хэсэгт байх ба гадагш гарах боломжгүй байна.

4.4.Хортой кодоос хамгаалах

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

4.4.2.Хортой кодын эсрэг програмын шинэчлэлтийг тогтмол жил бүр хийнэ.

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

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

4.5.Нууц

4.5.1 Нууц мэдээлэл гэж хуулинд заагдсан болон байгууллагын нууцын журамд тусгагдсан мэдээллүүд хамаарна.

4.6 Мэдээллийн системийн биет байршил

4.6.1 Үндсэн болон нөөц төвүүд нь Монгол улсын нутаг дэвсгэрт байрлана.

4.6.2 Үндсэн төвд нөлөөлөх боломжтой онцгой нөхцөлд өртөхөөргүй газар зүйн алслагдмал байршилд нөөц төв нь байна.

4.6.3 Мэдээллийн сантай холбогдох гуравдагч этгээдийн аливаа мэдээллийн систем нь үндсэн төвийн тусгай бүсд байрлах ба үндсэн МИИС системээс тусдаа байна.

4.6.3.1 Гадны буюу гуравдагч этгээдийн мэдээллийн систем нь мэдээллийн сантай холбогдохдоо хамгаалттай сүлжээг ашиглах ба мэдээллийн сангийн дэд сүлжээ байдлаар зохион байгуулагдана.

4.6.3.2 Гадны буюу гуравдагч этгээдийн мэдээллийн системд ашиглагдах бүх програм хангамж нь албан ёсны лицензтэй байна.

4.6.3.3 Гадны буюу гуравдагч этгээдийн мэдээллийн систем суулгах, өөрчлөлт оруулах бүрд гэрчилгээнд тэмдэглэл хийн эзэмшигч, зохицуулагч хоёул гарын үсэг зурж баталгаажуулна.

4.6.3.4 Гадны буюу гуравдагч этгээдийн мэдээллийн систем нь мэдээллийн санд хандахдаа тусгай бүртгэл хяналтын системээр дамжин мэдээлэл солилцоно.

4.6.3.4.1 Тусгай бүртгэл хяналтын систем нь хэн хэзээ ямар мэдээлэл авсан, өгсөн, эрхийн хяналт, бүртгэлийг хийх ба давхар нөөц бүртгэлтэй байна.

4.6.4 Үндсэн төвийн тасралтгүй, найдвартай ажиллагаанд дараах шаардлагыг тавина.

4.6.4.1 Үндсэн төвийн тоног төхөөрөмж, мэдээллийн систем, програм хангамжийн засвар, үйлчилгээ, шинэчлэлийг тогтмол хийх;

4.6.4.2 Үндсэн төвийн тоног төхөөрөмж, мэдээллийн систем, програм хангамжийн тохиргоо, түүнд орсон өөрчлөлт бүрийг баримтжуулж, хадгалах;

4.6.4.3 Үндсэн төвд зөвхөн эрх бүхий ажилтан нэвтрэх бөгөөд нэвтрэх бүрд бүртгэл хөтлөх;

4.6.4.4 Үндсэн төв нь цахилгааны нэмэлт эх үүсвэр болох тог баригч (UPS), эрчим хүчний нэмэлт шугам, генератортай байх;

4.6.4.5 Үндсэн төвийн сервер, сүлжээний тоног төхөөрөмж, хөргөлтийн систем, агаарын чийгшил тохируулагч систем, гал унтраах систем, серверийн өрөөний мэдрэгчийг цахилгааны нэмэлт эх үүсвэрт холбосон байх;

4.6.4.6 Үндсэн төвийг, нөөц төвтэй үндсэн ба нөөц шугамаар шууд холбосон байх;

4.6.5 Нөөц төвийн тасралтгүй, найдвартай ажиллагаанд дараах шаардлагыг тавина. Үүнд:

4.6.4.1 Нөөц төвд зөвхөн эрх бүхий ажилтан нэвтрэх бөгөөд нэвтрэх бүрт бүртгэл хөтлөх;

4.6.4.2 Нөөц төвийн тоног төхөөрөмж, мэдээллийн систем, програм хангамжийн засвар, үйлчилгээ, шинэчлэлийг тогтмол хийх;

4.6.4.3 Нөөц төвийн тоног төхөөрөмж, мэдээллийн систем, програм хангамжийн тохиргоо, түүнд орсон өөрчлөлт бүрийг баримтжуулж, хадгалах;

4.6.4.4 Нөөц төв нь цахилгааны нэмэлт эх үүсвэр болох тог баригч (UPS), эрчим хүчний нэмэлт шугам, генератортай байх;

4.6.4.5 Нөөц төвийн сервер, сүлжээний тоног төхөөрөмж, хөргөлтийн систем, агаарын чийгшил тохируулагч систем, гал унтраах систем, серверийн өрөөний мэдрэгчийг цахилгааны нэмэлт эх үүсвэрт холбосон байх;

4.6.4.6 Нөөц төвийг үндсэн төвтэй сүлжээний үндсэн ба нөөц шугамаар холбосон байх;

4.6.4.7 Нөөц төвийн санд байх мэдээлэл нь үндсэн төвийн санд байх мэдээлэлтэй адилхан байна.

4.7 Хэрэглэгчийн эрхийн хяналт

4.7.1 Мэдээллийн сан нь аюулгүй байдлын хяналтын үйл ажиллагааг хэрэгжүүлэн тогтмол хянаж ажиллах бөгөөд зөвхөн хэрэглэгчийн эрх, эрхийн хүснэгт, хэрэглэгчийн эрхийн бүлэгт тулгуурласан хандалтыг зөвшөөрдөг байхын зэрэгцээ мэдээллийг эзэмшигч баталгаажуулснаар ажилтанд тухайн мэдээлэлд хандах эрхийг олгоно.

4.7.1.1 Хэрэглэгчийн эрх

4.7.1.1.1 Хянах эрх - тухай мэдээллийн үнэн зөвийг хянаж шалгах, бүртгэх, өөрчлөх, өөрчлөлийн бүртгэл хөтлөх

4.7.1.1.2 Харах эрх - тухай мэдээллийг харах ба ямар нэг өөрчлөлт хийх боломжгүй.

4.7.1.1.3 Оруулах, засварлах эрх - шинээр мэдээлэл оруулах боломжтой ба зөвхөн өөрийн оруулсан мэдээллээ харах, түүнийг засварлах боломжтой.

4.7.1.1.4 Эрхгүй - тухай мэлээллийг харах болон ямар нэг өөрчлөлт хийх боломжгүй байна.

4.7.1.2 Эрхийн хүснэгт

	Даатгалын гэрээ	Даатгалын нөхөн төлбөр	Даатгалын дуудлага, тохиолдол
Мэдээллийн сан	Хянах эрх	Хянах эрх	Хянах эрх
Шуурхай алба	Харах эрх	Харах эрх	Оруулах, засварлах эрх
Даатгалын сан	Харах эрх	Оруулах, засварлах эрх	Харах эрх
Даатгалын компани	Оруулах, засварлах эрх	Оруулах, засварлах эрх	Оруулах, засварлах
Даатгалын зуучлагч	Оруулах, засварлах эрх	Эрхгүй	Эрхгүй
Төрийн байгууллага	Харах эрх	Харах эрх	Харах эрх

4.7.1.3 Хэрэглэгч зөвхөн өөрийн оруулсан, засварласан мэдээллийг харах эрхтэй.

4.7.2 Хэрэглэгч бүр өөрийн гэсэн дахин давтагдашгүй хэрэглэгчийн нэр, нууц үгтэй байх бөгөөд зөвхөн өөрийн хэрэглэгчийн нэр, нууц үгийг ашиглан зөвшөөрөгдсөн мэдээллийн систем болон мэдээлэлд хандана. Админ эрхээр нэвтрэхдээ мэдээллийн санд бүртгэлтэй цахим гарын үсгийг ашиглана.

4.7.3 Нийтийн сүлжээгээр дамжуулан мэдээллийн системд хандах тохиолдолд хэрэглэгчийг таних хоёроос доошгүй шаттай баталгаажуулалтыг ашиглах бөгөөд мэдээллийг дамжуулахад нууцлалтай холболт ашиглана.

4.7.4 Хэрэглэгчийн эрхийг зөвхөн тухайн ажилтны ажил үүргийн хуваарийн дагуу хандах шаардлагатай мэдээллийн систем, мэдээлэлд хандах хязгаарлалттай олгоно. Мөн нэг хэрэглэгчид бүх эрхийг олгохыг хориглох ба шат дараалсан хяналттай байна.

4.7.5 Хэрэглэгчийн эрхийн бүлгийг тухайн хэрэглэгчийн эрхийн бүлэгт хамаатай мэдээллийн систем болон мэдээлэлд хандах байдлаар тодорхойлно. Энэхүү хэрэглэгчийн эрхийн бүлгийг ажил үүргийн зөв зохистой хуваарилалт, тусгаарлалтыг дэмжсэн байдлаар тодорхойлж ялгана.

4.7.6 Хэрэглэгчийн эрх болон хэрэглэгчийн эрхийн бүлгүүдийг тогтмол хянан шалгаж, Холбооны бүтэц зохион байгуулалт, мэдээллийн технологи болон мэдээллийн системийн өөрчлөлтөд нийцүүлэн тухай бүр шинэчилнэ.

Тав. Тоног төхөөрөмж

5.1 Байгууллагын компьютер, техник хэрэгслийг заавал гэрчилгээжүүлсэн байна. Гэрчилгээг байгууллагын зохицуулагч хөтлөх бөгөөд засвар үйлчилгээ хийсэн шинэ програм хангамж суулгасан тохиолдолд зохицуулагч болон тухайн компьютер техник хэрэгслийг эзэмшигч хоёул гарын үсэг зурж баталгаажуулна.

5.2.Компьютерын програм хангамж, техник хангамжийн хамгаалалт

5.2.1. Програм болон техник хангамжийн суурилуулалт түүний шинэчлэл, тохиргоог зөвхөн зохицуулагч хийнэ.

5.2.2. 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.

5.2.3. Систем суулгах, өөрчлөлт оруулах бүрд гэрчилгээнд тэмдэглэл хийн эзэмшигч, зохицуулагч хоёул гарын үсэг зурж баталгаажуулна.

5.2.4. Мэдээллийн санд байгаа бүх програм хангамж нь албан ёсны лицензтэй суурилуулагдсан байна.

5.2.5. Мэдээллийн сантай холбогдож ажиллах гадны програм хангамж нь эх кодны түвшинд зохицуулагчаар хянагдаж зөвшөөрөгдсөн байна.

5.2.6. Зөвхөн зөвшөөрөгдсөн програм хангамжийг ашиглана.

5.3 Сүлжээ

5.2.1. Байгууллагын сүлжээний байнгын ажиллагааг мэдээллийн технологийн ажилтан шалгаж, хариуцна.

5.2.2. Мэдээллийн сангийн хэрэглэгч зөвхөн Монгол улсын нутаг дэвсэрт байгаа сүлжээнээс хандана.

5.2.3. Сүлжээнд холбоотой бүх төхөөрөмжийн MAC хаяг, IP хаягаар бүртгэл хөтлөж хяналт тавьна.

5.2.4. Сүлжээнд холбогдох бүх төхөөрөмжийн аюулгүй байдалд үзлэг хийж тэмдэглэл хөтлөж аюулгүй тохиолдолд холболт хийнэ.

5.4 Хэвлэх, олшруулах төхөөрөмжийг ашиглах

5.4.1 Олшруулагчаар хийгдсэн ажлыг тэмдэглэж гүйцэтгэлд тухай эд хариуцагч ажилтан

хяналт тавьна;

5.5 Зөөврийн хадгалах төхөөрөмжийг ашиглах

5.5.1 Зөөврийн хадгалах төхөөрөмж дээрх мэдээллийг ашиглаж дууссаны дараа мэдээллийг арилгах

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

5.5 Цахим шуудан ашиглах

5.5.1 Цахим шуудангаар ирсэн захиаг 1 жил тутам архивлан авч хадгална.

5.5.2 Албаны бус цахим шуудангаар албаны файл зөөхийг хориглоно.

5.5.3 Албаны цахим хаягаар ирсэн захиаг устгахыг хориглоно.

Зургаа. Эрх, үүрэг

6.1.Мэдээллийн сангийн эрх

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

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

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

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

6.1.5.Эрсдэлийн үнэлгээг жил тутам хөндлөнгийн CISA гэрчилгээ эсхүл дүйцэх түвшний гэрчилгээ бүхий аудитороор COBIT тогтолцоонд суурилсан мэдээллийн технологийн тусгайлсан хяналт, аудитыг хийлгэх ба мэдээллийн аюулгүй байдлын эмзэг байдлыг тодорхойлох, хамгаалалтын түвшинг тогтоох, хөндлөнгийн хяналтыг хэрэгжүүлэх.

6.1.6.Мэдээллийн систем, сангийн бүрэн бүтэн, аюулгүй байдалд хяналт тавих, мэдээллийн сангийн нөөц хувийг хувилж хадгалах.

6.1.7.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.

6.2.Мэдээллийн сангийн үүрэг

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

6.2.2.Мэдээллийн сангийн програм хангамж, компьютерыг хортой кодоос хамгаалах.

6.2.3.Мэдээллийн аюулгүй байдлыг хангахад чиглэсэн сургалт, сурталчилгааг байгууллагад зохион байгуулах.

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

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

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

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

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

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

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

6.2.11.Мэдээллийн сантай холбогдож байгаа програм хангамж болон мэдээллийн системд ажиллаж байгаа хэрэглэгчийн хийсэн үйлдлүүд, хэзээ, хаашаа нэвтэрсэн, ямар үйлдэл хийсэн, дамжуулсан мэдээлэл зэрэг нь системд бүртгэгдэж байхаар тохируулах.

6.2.12. Даатгалын гэрээ, дуудлага, үзлэг, даатгуулагч, нөхөн төлбөрийн мэдээллийг 10 жил хадгалах ба лог мэдээллийг 3 сар тутам нөөцөлж, 2 жилийн дараа нягтлан шинжилсний дараа мэдээллийн технологийн мэргэжилтэн устгана.

6.2.13 Мэдээллийн технологийн үйлчилгээг үйлчилгээ үзүүлэгчээс авах тохиолдолд эрсдлийн удирдлагад болон үйлчилгээ үзүүлэгчид хяналт тавих ба дараах хяналтийн арга хэмжээнүүдийг хэрэгжүүлнэ.

6.2.13.1 Үйлчилгээ үзүүлэгчээс үйлчилгээ авах тохиолдолд үүдэн гарах дэд бүтцийн эсдслийн хянах.

6.2.13.2 Мэдээллийн технологийн үйлчилгээ авах гэрээ байгуулахаас өмнө үйлчилгээ үзүүлэгчийг магадлан шалгах.

6.2.13.3 Мэдээллийн технологийн үйлчилгээ авах гэрээ болон үүсэх харилцаа нь мэдээллийн аюулгүй байдал, даатгуулагчийн мэдээллийн нууцлал болон холбогдох бусад бичиг баримтуудтай нийцүүлэх.

6.2.14 Мэдээллийн сангийн веб, апликешин, баазын хандалтын лог бүртгэл хөтлөх.

6.2.15 Мэдээллийн санд ашиглагдаж байгаа системд өөрчлөлт хийх бүрт холбогдох өөрчлөлтийн бүртгэл хөтлөх, хяналт тавих.

6.3 Хэрэглэгчийн үүрэг, хариуцлага

6.3.1.Мэдээллийн аюулгүй байдлын холбоотой учрал гарсан тохиолдолд системийн зохицуулагчид тухай бүрд нь мэдэгдэнэ.

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

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

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

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

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

6.3.7 Мэдээллийн системийн нууц үгсийг мэдээллийн сангийн дарга болон гүйцэтгэх захирал хадгалах ба алдагдсан тохиолдолд хариуцлагыг хамтран тэгш хүлээнэ.

Долоо. Хориглох зүйл

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

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

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

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

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

7.6 Лицензгүй, интернетээс татсан, үнэгүй, тодорхой хугацаанд үнэгүй ашигдагддаг болон батлагдаагүй програм хангажийг хэрэглэхийг хориглоно.

7.7 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.

Найм. Хариуцлага

8.1.Ажилтны анхаарал болгоомжгүй үйлдлээс болж мэдээллийн системийн сүлжээний мэдээллийн сангийн аюулгүй байдал алдагдах, мэдээллийн аюулгүй байдлын бодлого, журам зөрчигдөж, байгууллагын үйл ажиллагаанд хохирол учруулсан ба эмзэг байдал үүсгэсэн нь эрүүгийн хариуцлага хүлээлгэхээргүй бол дотоод журамд заасны дагуу хариуцлага тооцно.

***