Хавсралт

ТӨР, ЗАСГИЙН ҮЙЛЧИЛГЭЭГ ЭРХЛЭХ ГАЗРЫН МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ЖУРАМ

Нэг. Нийтлэг үндэслэл

1.1.Газрын мэдээллийн аюулгүй байдлын тогтолцоог бий болгох, гадаад болон дотоод сүлжээ, системийн найдвартай ажиллагаа, мэдээллийн сангийн нууцлал, аюулгүй байдлыг хангах, гаднаас болон дотоодоос учирч болох халдлага, аюул занал эрсдэлээс урьдчилан сэргийлэх, учирсан хор хохирлыг нэн даруй засаж сэргээх, хариу арга хэмжээ авахад энэхүү журам мөрдөгдөнө.

Хоёр. Нэр томъёо

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,

2.7.Мэдээллийн аюулгүй байдал – гэж мэдээлэл, мэдээлэл боловсруулах хэрэгсэл, холбогдох дэд бүтцийн нууцлал, бүрэн бүтэн халдашгүй, хүртээмжтэй байдал, тасралтгүй, найдвартай ажиллагаа байдлыг тодорхойлох, бий болгох, хадгалахтай холбоотой бүх асуудлууд;

2.8.Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоо /МАБУТ/ - Байгууллагын удирдлагын тогтолцооны Мэдээллийн аюулгүй байдлыг хангах, хэрэгжүүлэх, ажиллуулах, хянах, нягтлан шалгах, дэмжих, сайжруулахын тулд хэрэгжүүлсэн 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 бус юмс, эд зүйл. Мэдээлэл харилцааны тогтолцооны 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 системийн үйлчилгээ, 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.Зохицуулагч /administrator/–гэж байгууллагын мэдээллийн технологи хариуцсан эрх, үүрэг бүхий мэргэжилтэн;

2.14.Хэрэглэгч – гэж байгууллагын мэдээллийн системтэй харьцдаг бүхий л шатны ажилтнуудыг;

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, санхүү болон 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, компьютерийн 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 нийтлэг мэдээ, мэдээллүүд, зөвлөлөөс гаргасан нийтэд мэдээлэх шаардлагатай мэдээлэл, үүрэг даалгавар, ажилтан, 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.

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

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

3.2.6.Хадгалах мэдээллийн зэрэглэлээс хамаарч өрөө тасалгааг дараах байдлаар зэрэглэн ангилна.

Зэрэглэл I: Нээлттэй бүс
Зэрэглэл II: Хаалттай бүс

Дөрөв. Физик орчны хувьд

4.1.1.Сервер болон мэдээллийн сан, мэдээлэл хадгалдаг компьютерүүдийг орчны нөлөөнөөс хамгаалах шаардлагатай.

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

а) Нээлттэй бүс – нийтэд мэдээллээр үйлчлэх хэсэг (ажилтны өрөө тасалгаа, заал болон уулзалтын өрөө зэрэг орно);

б) Хаалттай бүс – зөвхөн эрх бүхий албан хаагчид нэвтрэх эрхтэй хэсэг (серверийн өрөө)

Хаалттай бүсэд нэвтрэх

а) Зөвхөн орох эрх бүхий зөвшөөрөлтэй ажилтан нэвтэрнэ;.

б) Зөвшөөрөлгүй хүн орох тохиолдолд эрх бүхий албан тушаалтнаас зөвшөөрөл авч, мэдэгдэж орно.

4.1.3.Тоног төхөөрөмжийн нууцлал, хамгаалалт

4.1.3.1.Байгууллага нь өөрийн байгууллагын компьютер, техник хэрэгслийг заавал бүртгэл хөтөлсөн байна. Бүртгэлийг байгууллагын компьютерийн инженер болон техникч хөтлөх бөгөөд засвар үйлчилгээ хийсэн, шинэ програм хангамж суулгасан тохиолдолд тухайн компьютер техник хэрэгслийг эзэмшигч болон инженер, техникч нар гарын үсэг зурж баталгаажуулна.

4.1.3.2.Компьютерт програм хангамж, техник хангамжийг суурилуулах

а) Програм болон техник хангамжийн суурилуулалт түүний шинэчлэл, тохиргоог зөвхөн мэдээллийн технологийн мэргэжилтнүүд болон програм хангамжийн инженер хийнэ;

б) Ажилтны компьютерийг форматлан /шуурхай санах ойг цэвэрлэх/ үйлдлийн системийг дахин суулгах тохиолдолд хэрэгцээт файлуудыг өөр дискэнд хуулж, үйлдлийн системийг суулгаж тохируулга хийсний дараа файлын вирусыг шалган, ажилд бэлэн болгож ажилтанд хүлээлгэн өгнө.

4.1.3.3.Байгууллагаас албан хэрэгцээний зориулалтаар тавьж олгосон зөөврийн компьютер ашиглахад анхаарах зүйлс

а) Хулгайд алдах, эвдэрч гэмтсэний улмаас мэдээлэл алдагдахаас сэргийлэх үүднээс хадгалж хамгаалах зааварчилгаа эзэмшигч ажилтанд өгнө;

б) Зөөврийн компьютерт хадгалагдаж байгаа мэдээллийг зохих ёсоор заавал хамгаалах. Аль болох бага мэдээллийг зөөврийн компьютерт байршуулна;

в) Зөөврийн компьютерийг албан хэрэгцээнээс бусад зориулалтаар ашиглахыг хориглоно;

г) Албаны мэдээлэл бүхий зөөврийн компьютертэй ажлын байрнаас гадуур ажлаар болон албан томилолтоор явахдаа мэдээллийн нууцлалт, хамгаалалтын асуудлыг судалж мэдсэн байна;
д) Нууц зэрэглэлийн мэдээллийг шифрлэх, кодлох байдлаар хамгаалах шаардлагатай.

4.1.3.4.Сүлжээний кабель

а) Байгууллагын сүлжээний байнгын ажиллагааг мэдээллийн технологийн мэргэжилтэн шалгаж, хариуцна;
б) Сүлжээний кабелийн үзүүрт хаяг хадаж, ашиглагдаагүй гаралтуудыг тэмдэглэж сүлжээний зохицуулагчаас өөр хүн ашиглах боломжийг хааж байрлуулна.

4.1.3.5.Тоног төхөөрөмжийн байрлал

а) Ажилтан, албан хаагчдын ажлын компьютерийн дэлгэцийг бусдад шууд харагдахгүйгээр байрлуулсан байна;
б) Хэвлэгч, олшруулагч хэрэгслүүдийг удирдлагын хараа хяналттай өрөөнд байрлуулна;
в) Нууц бичиг баримт боловсруулахдаа гадаад, дотоод сүлжээнд холбогдоогүй компьютер ашиглана.

4.1.3.6.Зөөврийн хадгалах төхөөрөмжийг ашиглах

а) Зөөврийн хадгалах төхөөрөмж дээрх мэдээллийг ашиглаж дууссаны дараа мэдээллийг арилгана;
б) Зориулалтын сав, хайрцагт хийж зөөвөрлөдөг байна;
в) Гадны зөөврийн хадгалах төхөөрөмж системд оруулах бол заавал вирусын эсрэг програм уншуулна;
г) Зөөврийн хадгалах төхөөрөмжийг албан бусаар ашиглах бусдад дамжуулахыг хориглоно.

4.2.Програм, техникийн хувьд

4.2.1.Цахим мэдээллийн архив бүртгэлийн автоматжуулсан системтэй байна.

4.2.2.Сүлжээний хамгаалалтыг зохион байгуулж, мэдээллийн системийг хууль бус гадны халдлагаас хамгаална.

4.2.3.Мэдээллийн аюулгүй байдлыг хангах, мэдээлэлд зөвшөөрөлгүй нэвтрэх оролдлогыг таслан зогсоох, илрүүлэх зориулалтаар хамгаалалт, хяналтын техникийн систем, програм хэрэгслийг сонгон нэвтрүүлж байнгын ажиллагаанд оруулна.

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 байрласан, тэжээлийн нөөц эх үүсвэрт холбогдсон байна.

5.1.2.Байгууллагын ажилтан, албан хаагчид өөрийн компьютер дээр шууд харъяалах албан тушаалтны зөвшөөрөлгүйгээр гадны этгээдийг ажиллуулах, компьютерийг 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 дотоод 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 солино;
в) Нууц үгийг бусдад дамжуулахгүй байх, илчлэгдсэн гэж үзвэл даруй солино;
г) Зохицуулагчийн нууц үгийг дундаа хэрэглэхгүй байна.

5.2.3.Нууц үгийн бүрдэл

а) Том, бага үсэг, тоо, тусгай тэмдэгтийг хослуулсан байна;
б) Үүсмэл үг үүсгэнэ;
в) Аюулгүй байдлын шаардлага хангасан нууц үгийг эргэн санахад хялбар байхаар логик дараалалтай үүсгэнэ.

5.2.4.Нууц үгийн хамгаалалт

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

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

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

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

5.2.9.Байгууллагын мэдээллийн систем, програм хангамжийн нууц үгийн сонголт, бүртгэл, ашиглах хугацааг мэдээллийн технологийн мэргэжилтнүүд болон компьтерийн инженер хариуцан ажиллаж, хяналт тавина. Шинээр үүсгэх, өөрчлөх, устгах тохиолдолд баталгаажуулах ба улирал тутам системүүдийн хэрэглэгчийн жагсаалтыг хянах үүрэг хүлээнэ.

5.3.Лог файлын бүртгэл /Бүртгэл/тэмдэглэл файл (log file) гэж нэрлэх файл/

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

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

5.3.3.Лог мэдээллийг 6 сар тутам нөөцөлж, 2 жилийн дараа шинжилсний дараа мэдээллийн технологийн мэргэжилтэн устгана. Байгууллага нь өөрийн онцлогт нийцүүлэн уялдах тусгай дүрэм журамтай байж энэхүү хугацааг өөрчлөн тогтоож болно.

5.4.Хандалтын удирдлага

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

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

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

5.5.Хортой код /вирус/-ээс хамгаалах

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

5.5.2.Хортой кодын эсрэг програмын шинэчлэлтийг тогтмол хийнэ.

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

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

5.6.Мэдээллийн санд нэвтрэх эрхийн түвшин

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

5.6.2.Удирдах 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.

5.6.4.Зөвхөн харах эрх /Read only/ - Зөвхөн 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. Байгууллагын хүний нөөцийн нэгж, мэргэжилтэн тухайн ажилтанг ажлаас чөлөөлөх тухай системийн зохицуулагчид мэдэгдсэн байна.

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

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 системийг 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. Заавал нөөц хувь үүсгэн тусгайлан хадгална;

б) Түр хадгалах хугацаа дууссан тохиолдолд Албаны даргын зөвшөөрлөөр устгаж серверийг чөлөөлнө.

6.6.Мэдээллийн системээс мэдээллийг дахин сэргээгдэхгүй байдлаар устгана.

Долоо. Байгууллагын мэдээллийн аюулгүй байдлын нэгж, 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 мэдээллийн технологийн мэргэжилтнийг /системийн зохицуулагч/ ажиллуулна. Байгууллагын мэдээлэл, дүн шинжилгээний болон захиргаа удирдлагын нэгжүүд эсвэл хариуцсан мэргэжилтнүүд 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, эрсдэлтэй байдлыг бууруулах зорилгоор мэдээллийн систем, ажилтнуудын компьютерт нэвтэрнэ.

7.2.2.Мэдээллийн аюулгүй байдлын шаардлага зөрчиж буй хэрэглэгчийн мэдээллийн санд нэвтрэх эрхийг удирдах, тэдгээрийн ажиллагааг хэсэгчлэн болон бүрэн зогсоож, зорилгыг судлах, удирдлагад мэдэгдэнэ.

7.2.3.Байгууллагад ашиглагдах мэдээллийн систем, техник технологи худалдан авах болон шинээр нэвтрүүлэх үйл явцад санал оруулах, хяналт тавина.

7.2.4.Эрсдэлийн үнэлгээг жил тутам хийж мэдээллийн аюулгүй байдлын эмзэг байдлыг тодорхойлон, хамгаалалтын түвшинг тогтоож, хөндлөнгийн хяналтыг хэрэгжүүлнэ.

7.2.5.Мэдээллийн систем, сангийн бүрэн бүтэн байдалд хяналт тавих, мэдээллийн сангийн нөөц хувийг хувилж хадгалах нөхцлийг хангана.

7.2.6.Байгууллагын компьютерийн 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 тавина.

7.3.Системийн зохицуулагчийн үүрэг.

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

7.3.2.Мэдээллийн сан, програм хангамж, компьютерийг хортой кодоос хамгаална.

7.3.3.Мэдээллийн аюулгүй байдлыг хангахад чиглэсэн сургалт, сурталчилгааг байгууллагад зохион байгуулна.

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

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

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

7.3.7.Байгууллагын компьютерүүд, дагалдах тоног төхөөрөмж, хэрэгслүүдийн ажиллагаа, шинэ тоног төхөөрөмжийн суурилуулалтыг хариуцана.

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

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

7.3.10.Мэдээллийн аюулгүй байдлыг хангахад шаардагдах мэргэжил дээшлүүлэх сургалтад байнга хамрагдаж байна.

Найм. Мэдээллийн системийн хэрэглэгчийн үүрэг, хариуцлага

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

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

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

8.4.Компьютерийн нэр, сүлжээний нэрийг солихгүй байх. Шаардлага гарсан тохиолдолд системийн зохицуулагчид мэдэгдэж зохих үйлчилгээг хийлгэнэ.

8.5.Ажлын өрөө болон хонгилд ил болон далд угсрагдан сүлжээний утсууд гэмтсэн, ороцолдсон, далд монтажаас утас ил гарсан тохиолдолд байгууллагын холбогдох нэгж, мэргэжилтэнд мэдэгдэнэ.

8.6.Мэдээллийн аюулгүй байдлыг хангах талаар өгсөн системийн зохицуулагчийн шаардлагыг биелүүлэнэ.

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

Маягт №1

ТӨР, ЗАСГИЙН ҮЙЛЧИЛГЭЭГ ЭРХЛЭХ ГАЗАР

НУУЦЫН БАТАЛГАА №

Алба:
Овог:
Нэр:
Албан тушаал:

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 энэхүү баталгаагаар хүлээн зөвшөөрч байна.

БАТАЛГАА ГАРГАСАН:

_____
……
(Ажилтны нэр) (Гарын үсэг)

Журам батлах тухай

Засгийн газрын 2013 оны 212 дугаар тогтоол, Газрын дүрмийн 4 дүгээр бүлгийн 4.4.4 дэх заалтыг тус тус үндэслэн ТУШААХ нь:

1.“Төр, засгийн үйлчилгээг эрхлэх газрын мэдээллийн аюулгүй байдлыг хангах журам“-ыг хавсралтаар баталсугай.

2.Энэхүү журамд хяналт тавьж хэрэгжүүлж ажиллахыг Зохион байгуулалтын алба /Д.Адъяахүү/-д үүрэг болгосугай.

ЗАХИРАЛ Д.НЯМЖАВ