ЭРҮҮЛ МЭНДИЙН ХӨГЖЛИЙН ТӨВИЙН ЗАХИРЛЫН ТУШААЛ

2023 оны 11 сарын 13 өдөр Дугаар А/113 Улаанбаатар хот

Журам шинэчлэн батлах тухай

Монгол Улсын “Кибер аюулгүй байдлын тухай” хуулийн 16.1.1, Кибер аюулгүй байдлыг хангах нийтлэг журмын 1.2 дах заалт, Эрүүл мэндийн хөгжлийн төвийн Удирдлагын зөвлөлийн 2023 оны 08 дугаар хурлын тэмдэглэлийг тус тус үндэслэн ТУШААХ НЬ:

1. “Эрүүл мэндийн хөгжлийн төвийн кибер аюулгүй байдлыг хангах журам”-ыг нэгдүгээр, “Төрийн болон албаны нууцыг задруулахгүй байх баталгааны маягт”-ыг хоёрдугаар, “Нууц ангиллын мэдээлэл, тэдгээрийг хариуцагч, эзэмшигч болон хэрэглэгчийн жагсаалт”-ыг гуравдугаар, “Мэдээллийн системийн байр өрөө тасалгаачы хамгаалалтын зэрэглэлийн жагсаалт”-ыг дөрөвдүгээр, “Хандалтын эрхийн хүсэлтийн маягт”-ыг тавдугаар, “Эрүүл мэндийн хөгжлийн төвийн үйл ажиллагаанд ашиглагдах цахим систем, программ хангамжуудын хэрэглэгчдийн хандах эрхийн жагсаалт”-ыг зургаадугаар хавсралтаар тус тус баталсугай.

2. Журмын хэрэгжилтийг хангаж ажиллахыг нийт албан хаагчдад үүрэг болгосугай.

3. Тушаалын хэрэгжилтэд хяналт тавьж ажиллахыг Хяналт-шинжилгээ, үнэлгээ, дотоод аудитын алба (Ш.Алтанцэцэг)-д даалгасугай.

4. Энэхүү тушаал гарсантай холбогдуулан Эрүүл мэндийн хөгжлийн төвийн ерөнхий захирлын 2019 оны 09 дүгээр сарын 26-ны өдрийн “Эрүүл мэндийн хөгжлийн төвийн мэдээллийн технологийн журам” А/139 дугаар тушаалыг хүчингүй болсонд тооцсугай.

ЗАХИРАЛ Б.НАРАНТУЯА

13230000506

Эрүүл мэндийн хөгжлийн төвийн захирлын
2023 оны .11. дугаар сарын 13. өдрийн
А/113 дугаар тушаалын нэгдүгээр хавсралт

ЭРҮҮЛ МЭНДИЙН ХӨГЖЛИЙН ТӨВИЙН КИБЕР АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ЖУРАМ

Нэг. Нийтлэг үндэслэл

1.1 Энэхүү журмын зорилго нь Эрүүл мэндийн хөгжлийн төвийн /цаашид ЭМХТ 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 Төвийн нийт ажилтан, албан хаагчид, мэдээллийн технологи хариуцсан ажилтан нь ажил үүргээ гүйцэтгэхдээ энэхүү журмыг мөрдлөг болгон ажиллана.

1.3 Төвийн мэдээллийн аюулгүй байдлын тогтолцоог бий болгохдоо доорхи холбогдох хууль, журам, стандартуудыг мөрдлөг болгоно. Үүнд:

- Монгол улсын “Төрийн болон албаны нууцын тухай” хууль;
- Монгол улсын “Нийтийн мэдээллийн ил тод байдлын тухай” хууль;
- Монгол улсын “Хүний хувийн мэдээлэл хамгаалах тухай” хууль;
- Монгол улсын “Кибер аюулгүй байдлын тухай” хууль;
- Монгол улсын "Монгол кирилл цагаан толгойн үсгүүдийг романчлах” MNS 5217:2012 стандарт;
- Олон улсын мэдээллийн аюулгүй байдлын ISO27001:2013 стандарт;
- Кибер аюулгүй байдлыг хангах нийтлэг журам;
- Эрүүл мэндийн сайдын 2013 оны 140 тоот “Эрүүл мэндийн салбарт мэдээллийн технологийн талаар мөрдөх журам”;
- Эрүүл мэндийн сайдын 2019 оны 396 дугаар тушаалаар батлагдсан “Мэдээллийн нууцлал аюулгүй байдлын журам”.

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;

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 асуудлуудыг;

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 бус юмс, эд зүйл, мэдээллийн технологийн талаас нь авч үзвэл мэдээлэл, түүнтэй холбоотой аливаа юмс, эд зүйл;

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

2.12 Мэдээллийн технологи хариуцсан нэгж - гэж байгууллагын мэдээллийн аюулгүй байдал, мэдээллийн технологийн үйл ажиллагааны хэвийн нөхцөлийг хангах чиг үүрэгтэй албан хаагч, нэгж бүтцийг;

2.13 Мэдээлэл технологи хариуцсан ажилтан - гэж байгууллагын мэдээллийн технологи хариуцсан эрх, үүрэг бүхий мэргэжилтэн, администыг;

2.14 Систем хариуцсан мэргэжилтэн - гэж мэдээлэл технологийн тоног төхөөрөмжүүд болон серверүүдийг хариуцан ажиллуулдаг мэргэжилтэнг;

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

2.16 Зөөврийн хэрэгсэл- гэж зөөврийн хард, флаш диск, төрөл бүрийн компакт диск, хуурцаг гэх мэтийг;

2.17 Биет мэдээллийн хөрөнгө гэж 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;

2.18 Цахим мэдээллийн хөрөнгө гэж биет мэдээллийн цахим хэлбэрүүд, өгөгдлийн сангийн өгөгдлүүд болон бусад төрлийн цахим мэдээллийг;

2.19 Програм хангамжийн хөрөнгө гэж зөвшөөрөлтэй хэрэглээний, мэргэжлийн болон системийн програм хангамж, өөрсдийн боловсруулсан болон тусгай захиалгаар хийлгэсэн програм хангамжууд, системүүд;

2.20 Техник хангамжийн хөрөнгө гэж 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;

Гурав. Байгууллагын мэдээллийн өмч хөрөнгө, ангилал

3.1 Мэдээллийн өмч хөрөнгийн удирдлага зохион байгуулалтыг дараах байдлаар тодорхойлно. Үүнд:

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

3.1.2 төв нь энэ журмын 3.1.1-д заасан мэдээллийн нууцын зэрэглэлийг холбогдох хууль, журамд нийцүүлж тогтооно.

3.1.3 төв нь энэ журмын 3.1.1-д заасан жагсаалтад дурдсан мэдээлэл, мэдээллийн систем, мэдээллийн сүлжээнд учирч болзошгүй аюул занал, үр дагавар, нөлөөллийг үнэлэх зорилгоор эрсдэлийн үнэлгээг хийхдээ ISO 27005 стандартыг баримтална.

3.1.4 төв нь мэдээллийн нууцын зэрэглэлээс хамаарч, танилцах, ашиглах, дамжуулах, хадгалахтай холбоотой үйл ажиллагааг зохицуулсан тусгайлсан

журмыг батлан, мөрдөж болно.

3.2 Мэдээллийн нууцлал, ангиллыг дараах байдлаар тодорхойлно. Үүнд:

3.2.1 Төвийн мэдээллийг хэрэглээний зориулалт, нууцлалаас хамаарч дараах байдлаар ангилна. Үүнд:

3.2.1.1 нийтэд хүртээмжтэй мэдээлэл: Хувилах, хадгалах, дамжуулахад ямар нэгэн шаардлага тавихгүй нийтэд зориулагдсан, нууцлах шаардлагагүй, "Нийтийн мэдээллийн ил тод байдлыг тухай" хуульд зааснаар иргэн, аж ахуйн нэгжид саадгүй олгох мэдээллүүд;

3.2.1.2 төвийн дотор нээлттэй мэдээлэл: бүх ажилтан, албан хаагчдад зориулагдсан, төвийн үндсэн болон нэмэлт үйл ажиллагаатай холбоотой, байгууллага дотор нээлттэй, гадагш задруулахгүй мэдээллүүд;

3.2.1.3 төвийн дотор хаалттай мэдээлэл: Байгууллагын ажилтан тодорхой эрхийн хүрээнд хязгаарлалттайгаар ашиглах боломжтой, байгууллагын үндсэн болон нэмэлт үйл ажиллагаатай холбоотой, гадагш задруулахгүй, "Хүний хувийн мэдээлэл хамгаалах тухай", "Кибер аюулгүй байдлын тухай хууль", "Төрийн болон албаны нууц тухай" болон "Байгууллагын нууцын тухай" хуулиар хамгаалсан мэдээллүүд;

3.2.1.4 нууц мэдээлэл: Хуульд заагдсан болон тухайн байгууллагын нууцын тухай журамд тусгагдсан мэдээллүүд хамаарна. Нууц мэдээллийг дараах зэрэглэлд ангилна. Үүнд:

- онц нууц
- маш нууц
- нууц

ажилтан нь нууц ангиллын мэдээллийг энэхүү журамд заасан арга хэлбэрээр эзэмших, ашиглах, хадгалах, хамгаалах, дамжуулах үүргийг хүлээнэ.

3.2.1.5 албадууд тухайн байгууллагын нууцын зэрэглэл бүхий мэдээлэл, баримт бичиг, үйл ажиллагаатай холбоотой нууц, харилцагчийн мэдээллийн нууц зэрэг мэдээллүүдийн нууцыг хадгалах хамгаалах баталгааг тус журмын төрийн болон албаны нууцийг задруулахгүй байх баталгааны маягтын дагуу хийж гүйцэтгэнэ.

3.2.2 Физик орчинд мэдээллийг дараах байдлаар хамгаална. Үүнд:

3.2.2.1 Физик хамгаалалтыг 3 бүсэд ангилж үзнэ:

а/ нээлттэй бүс - нийтэд мэдээллээр үйлчлэх хэсэг (лавлагаа, мэдээлэл, зөвшөөрөл өгөх өрөө, хурлын заал, уулзалтын өрөө зэрэг орно);

б/ нийтэд хаалттай бүс - зөвхөн тухайн байгууллагын ажилтнууд орох эрхтэй хэсэг (ажлын өрөө, агуулах өрөө, цахилгааны өрөө зэрэг орно);

в/ хаалттай бүс - зөвхөн эрх бүхий албан хаагчид нэвтрэх эрхтэй хэсэг (серверийн өрөө, нууцын өрөө, архивын өрөө зэрэг орно).

3.2.2.2 нээлттэй, нийтэд хаалттай, хаалттай бүсэд байршуулсан мэдээ, мэдээлэл, тоног төхөөрөмж, бусад зүйлсийн аюулгүй байдлыг тухайн бүсийг хариуцах үүрэг бүхий албан тушаалтан энэ журмын дагуу хангаж ажиллана.

3.2.2.3 нээлттэй бүсэд зөвхөн нийтэд хүртээмжтэй мэдээллийг ил байршуулна.

3.2.2.4 нийтэд хаалттай бүсэд байгууллага дотор нээлттэй болон нууцлалтай мэдээллийг хадгална. Аюул занал, халдлага, учирч болох эрсдэлээс сэргийлж биет мэдээллийг цоож бүхий шүүгээ, сейфэнд, биет бус мэдээллийг нууц үг бүхий компьютерт, диск, зөөврийн хадгалах төхөөрөмжид байгаа мэдээллийг цоож бүхий шүүгээ, сейфэнд хадгална. Тухайн бүсийг хариуцсан ажилтны зөвшөөрлөөр түүний хяналт дор гадны

этгээдийг нэвтрүүлнэ.

3.2.2.5 хаалттай бүсэд албаны нууц мэдээллийг хадгалах бөгөөд зөвхөн тухайн мэдээллийг хариуцагч, эзэмшигч буюу нэвтрэх эрх бүхий албан тушаалтан нэвтэрнэ. Аюул занал, халдлага, учирч болох эрсдэлээс сэргийлж албаны нууц мэдээллийг гадны нөлөөллөөс хол тусгай зориулалтын өрөөнд хадгалах бөгөөд биет нууц мэдээллийг цоож бүхий шүүгээ, сейфэнд, биет бус нууц мэдээллийг нууц үгтэй, сүлжээнд холбоогүй эсвэл нууцлалтай сүлжээ бүхий компьютерт хадгална.

3.2.2.6 серверийн өрөөнд нэвтрэх ажилтан албан хаагчдын жагсаалтыг тус журмын гуравдугаар хавсралтын дагуу гаргаж, мэдээллийн технологийн асуудал хариуцсан нэгжийн дарга батална.

3.2.2.7 серверийн өрөөнд байрлуулсан сервер компьютер, сүлжээний тоног төхөөрөмж болон бусад тоног төхөөрөмжийн хэвийн үйл ажиллагаанд энэ журмын 4.8.6-д заасан албан хаагч тогтмол хяналт тавьж, засвар үйлчилгээг бүрэн хариуцан хийнэ. Засвар, үйлчилгээг тогтмол хийх төлөвлөгөөг баталж мөрдөж ажиллана.

Дөрөв. Төвийн мэдээллийн системийн ашиглалт

4. Компьютер, принтер, техник хэрэгсэл болон програм хангамжийн ашиглалтыг дараах байдлаар тодорхойлно. Үүнд:

4.1 Техник хэрэгслийн ашиглалтад дараах зарчмыг баримтална. Үүнд:

4.1.1 албан хаагч нь өөрийн эзэмшиж буй компьютер, хэвлэгч, хувилагч болон бусад тоног төхөөрөмжийг зөвхөн зориулалтын дагуу албан ажлын хэрэгцээнд ашиглана. Гадны этгээдэд дур мэдэн компьютер, тоног төхөөрөмжийг ашиглуулахыг хориглоно;

4.1.2 ширээний болон зөөврийн компьютер нь энэ журмын 5.5.1-д заасны дагуу заавал нэвтрэх нууц үгтэй байх;

4.1.3 ширээний болон зөөврийн компьютерт зөвхөн албан ажлын хэрэгцээний мэдээллийг хадгалах бөгөөд хувийн мэдээллүүд/зураг, кино, дүрс бичлэг, дуу, бусад файл гэх мэт/хадгалахыг хориглоно. Албан ажлын хэрэгцээнд чухал шаардлагатай мэдээллийг устах эрсдэлээс сэргийлж заавал хуулбарыг үүсгэн дундын хадгалах төхөөрөмжид байршуулах;

4.1.4 албан хаагч нь нь өөрийн компьютерт мэдээллийн аюулгүй байдлын учрал, аюул занал учирч болзошгүй эсвэл учирсан гэж үзвэл мэдээллийн аюулгүй байдал хариуцсан мэргэжилтэнд энэ тухай нэн даруй мэдэгдэх;

4.1.5 албан хаагч нь түр хугацаагаар гарах бол компьютерыг заавал түгжих буюу нууц үгээр хамгаалагдсан дэлгэцийн хамгаалалтыг ажиллуулна. Ажлын цаг дуусаж, ажилтан явахдаа компьютер, тоног төхөөрөмжүүдийг унтрааж, цахилгааны хүчдэлээс салгах;

4.1.6 албан хаагчдын дундаа ашигладаг хэвлэх, хувилах төхөөрөмжийг хяналттай байлгаж, тэдгээрийг ашиглахад тодорхой эрхийн хязгаарлалт хийж өгөх;

4.1.7 төвийн мэдээллийн сан, системүүд ажиллаж буй сервер компьютерыг хөргүүр, чийгшүүлэгч, хяналтын камер, нэмэлт цахилгааны үүсгүүр зэрэг серверийн өрөөний стандартад нийцсэн серверийн өрөөнд буюу хаалттай бүсэд байрлуулах;

4.1.8 сервер компьютер нь энэ журмын 5.9-д заасны дагуу заавал нэвтрэх нууц үгтэй байна. Нэвтрэх нууц үгийг ажил үүргийн хуваарийн дагуу мэдээллийн сан, мэдээллийн системийн чиглэлийн мэдээллийн технологи хариуцсан албан хаагч өөртөө хадгалах бөгөөд нууцлалыг өндөр түвшинд хамгаалж, журмын төрийн болон албаны нууцийг задруулахгүй байх баталгааны маягтын дагуу баталгаа гаргах;

4.1.9 төвийн мэдээллийн систем, мэдээллийн сүлжээний тоног төхөөрөмж байрлаж байгаа зориулалтын өрөөнд зөвшөөрөлгүй нэвтрэхийг хориглох бөгөөд өрөө нь дараах шаардлагыг хангана: Үүнд:

4.1.9.1. өрөөний хаалга цоожтой байх;

4.1.9.2. дохиоллын системтэй байх;

4.1.9.3. цонхны хамгаалалттай байх;

4.1.9.4. орох хаалганы дэргэд дүрст хяналтын системтэй байх;

4.1.9.5. температур, чийгшил зэрэг орчны нөхцөлийг хянах, бүрдүүлэх хэрэгсэлтэй байх;

4.1.9.6. хаалганы түлхүүр, эрхийг зөвхөн эрх бүхий ажилтан хадгалах;

4.1.10 төвийн мэдээллийн систем, мэдээллийн сүлжээний тоног төхөөрөмж байршуулах зориулалтын өрөөгүй бол энэ журмын 4.4-т заасан шаардлагад дүйцэх, тоног төхөөрөмжид зөвшөөрөлгүй этгээд хандахаас сэргийлсэн цоож, шүүгээ бүхий өрөөнд байршуулна.

4.2. Програм хангамжийн ашиглалтад дараах зарчмыг баримтална. Үүнд:

4.2.1 програм болон техник хангамжийн суурилуулалт түүний шинэчлэл, тохиргоог зөвхөн мэдээллийн технологи хариуцсан ажилтан хийж гүйцэтгэнэ;

4.2.2 албан хаагч нь мэдээллийн технологи хариуцсан ажилтны зөвшөөрөлгүйгээр дур мэдэн програм хангамж шинээр суулгах, програм хангамжид өөрчлөлт, шинэчлэлт хийх, техник хангамжид өөрчлөлт, засвар, үйлчилгээ хийхийг хориглоно;

4.2.3 албан хаагч нь нь аливаа компьютерыг форматлан үйлдлийн системийг дахин суулгах тохиолдолд өөрийн хэрэгцээт файлуудыг өөр дискэнд хуулж, үйлдлийн системийг суулгаж тохируулга хийсний дараа файлын вирусийг шалган, устгаж буцааж хуулна;

4.2.4 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;

4.3 Сүлжээ болон сүлжээний тоног төхөөрөмжийн ашиглалтад дараах зарчмыг баримтална. Үүнд:

4.3.1 албан хаагч нь 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.

4.3.2 албан хаагч нь өөрийн ашиглаж буй сүлжээнд мэдээллийн аюулгүй байдлын учрал, аюул занал учирч болзошгүй эсвэл учирсан гэж үзвэл мэдээллийн аюулгүй байдлын асуудал хариуцсан мэргэжилтэнд энэ тухай нэн даруй мэдэгдэнэ;

4.3.3 төвийн сүлжээний зохион байгуулалт, байнгын ажиллагаа, сүлжээний тоног төхөөрөмжийн тохиргоо, тэдгээрийн хяналтыг мэдээллийн технологи хариуцсан ажилтан хариуцан гүйцэтгэнэ;

4.3.4 төвийн сүлжээг зохион байгуулахдаа сүлжээний порт, сүлжээний кабелийн 2 талын үзүүрт тэмдэглэгээ бүхий хаяг заавал хадна;

4.3.5 сүлжээний зохион байгуулалтын болон сүлжээний хамгаалалтын төхөөрөмжүүдийг серверийн өрөөнд байрлуулж, тэдгээрт энэ журмын 6.9-д заасны дагуу заавал нэвтрэх нууц үгийг хийнэ. Нэвтрэх нууц үгийг ажил үүргийн хуваарийн дагуу сүлжээ, мэдээллийн системийн чиглэлийн мэдээллийн технологи хариуцсан албан хаагч өөртөө хадгалах бөгөөд нууцлалыг өндөр түвшинд хамгаалж, журмын төрийн болон албаны нууцийг задруулахгүй байх баталгааны маягтын дагуу баталгаа гаргаж өгнө;

4.3.6 сүлжээ ашиглан байгууллага хооронд нууцлалын зэрэглэл бүхий мэдээлэл

дамжуулах, солилцох бол заавал нууцлал бүхий сүлжээ/VPN, төрийн сүлжээ/ ашиглан дамжуулна.

4.4 Цахим шуудан ашиглалтад дараах зарчмыг баримтална. Үүнд:

4.4.1 төвийн албаны цахим шуудан хэрэглэгчдийн бүртгэл хөтлөх, шинээр хэрэглэгч нэмэх, өөрчлөх, хасах, хэрэглэгчдийн бүртгэлийн нууцлал аюулгүй байдлыг хангах асуудлыг Мэдээллийн технологийн асуудал хариуцсан нэгж зохион байгуулна;

4.4.2 албан хаагч нь албаны цахим шууданг зөвхөн албан ажлын хэрэгцээнд ашиглаж, өөрийн цахим шуудангийн нууцлал аюулгүй байдлыг хариуцна;

4.4.3 албаны цахим шуудангийн нэвтрэх нууц үгийг энэ журмын 5.5.1-д заасны дагуу зохион байгуулна.

4.4.4 эх үүсвэр нь тодорхойгүй, сэжиг бүхий хаягнаас ирсэн url: цахим холбоос болон файл агуулсан цахим шууданд орохыг болон татаж авахыг хориглоно. Шаардлагатай тохиолдолд мэдээллийн аюулгүй байдлын мэргэжилтэнд мэдэгдэнэ.

4.5 Цахим хуудас ашиглалтад дараах зарчмыг баримтална. Үүнд:

4.5.1 төвийн цахим хуудсыг Үндэсний дата төвд байршуулан аюулгүй байдал, хэвийн үйл ажиллагаа, шинэчлэлт хөгжүүлэлтийг мэдээллийн технологийн асуудал хариуцсан мэргэжилтэн ханган ажиллана;

4.5.2 цахим хуудас нь өгөгдлийн сангуудыг өргөтгөх, цэс нэмэх, засварлах, устгах боломжтой динамик бүтэцтэй, гар утас, таблет веб хөтөч дээр харагдах дэлгэцийн зохиомжтой байна. (FTP болон Өгөгдлийн сангийн хэрэглэгчийн нэвтрэх эрхүүдийг үүсгэж хадгална);

4.5.3 цахим хуудасны мэдээ, мэдээлэл түгээх хэл нь Монгол, Англи хэл байна. Цахим хуудасны Монгол, Англи хувилбар бүтэц агуулгын хувьд ялгаатай байж болно;

4.5.4 олон нийттэй харилцах асуудал хариуцсан ажилтан цахим хуудсанд мэдээ, мэдээллийг оруулах, мэдээллийг шинэчлэх ажлыг хийнэ;

4.5.5 цахим хуудаст хуулийн дагуу олон нийтэд ил тод байх ёстой мэдээ, мэдээлэл заавал байршуулсан байна;

4.5.6 мэдээлэл оруулах эрх бүхий ажилтан нь цахим хуудаст мэдээллийг оруулахдаа тухайн газар, хэлтэс, албадын даргын зөвшөөрлөөр мэдээллийг оруулна;

4.5.7 цахим хуудсанд тавигдсан мэдээний үнэн бодит байдлыг тухайн газар, хэлтэс, албадын дарга хариуцна;

4.5.8 цахим хуудас нь гадны довтолгоонд өртөх (вирустэх, хакердах гэх мэт) үед үүсэх сүлжээний урсгал, серверийн ачаалал нь хэт ихэсч системийн хэвийн ажиллагааг алдагдсан тохиолдолд мэдээллийн технологи хариуцсан ажилтан нь цахим хуудсыг түр хаах эрхтэй;

4.6 Сервер, дагалдах тоног төхөөрөмжүүдийн ашиглалтад дараах зарчмыг баримтална. Үүнд:

4.6.1 мэдээлэл, технологи хариуцсан нэгж нь серверийн өрөөнд байрлах серверүүд, тоног төхөөрөмжүүдийн бэлэн байдлыг хангах, гэмтэл саатал гарсан тохиолдолд засвар үйлчилгээг хийж ажиллана;

4.6.2 тоног төхөөрөмжийн өрөөнд шинээр сервер байрлуулах, ашиглагдаж буй серверийн үйлдлийн систем болон программ хангамжийг шинэчлэх тохиолдолд албан хүсэлтээр шийдвэрлүүлнэ;

4.6.3 мэдээлэл, технологи хариуцсан нэгж нь техникийн өргөтгөл болон холболтын шинэчлэлт хийх зайлшгүй шаардлага гарсан үед хэрэглэгчдэд урьдчилан мэдэгдэнэ;

4.6.4 мэдээлэл, технологи хариуцсан нэгж нь техник ашиглалтын зааврын дагуу серверүүдэд тогтмол хугацаанд техник үйлчилгээ хийж, өгөгдлийн сан болон эх кодуудыг тогтмол хугацаанд хуулан авч хадгалах үүрэгтэй;

4.6.5 серверт хадгалагдах мэдээллийн санг байнга болон түр хадгалах гэж 2 ангилж үзнэ;

4.6.6 байнга хадгалах өгөгдлийн сан, мэдээллийг серверт тусгай хавтас үүсгэн хадгална. Тухайн өгөгдөл, мэдээллийн хүртээмж, ашиглалт, нууцлалын байдлыг харгалзан минут, цаг, өдрийн давтамжтайгаар мэдээллийн сангийн зохицуулагч хугацааг тохируулан заавал нөөц хувийг үүсгэж хадгална;

4.6.7 байнга хадгалах өгөгдлийн сан, мэдээллийг хадгалах хугацаа дууссан тохиолдолд цахим архивд шилжүүлнэ;

4.6.8 түр хадгалах өгөгдлийн сан, мэдээллийг шаардлагатай тохиолдолд нөөцийг үүсгэж серверт хадгална. Хадгалах хугацаа дууссан тохиолдолд нэгжийн даргын зөвшөөрлөөр устгаж серверийг чөлөөлнө. Мэдээллийн системээс мэдээллийг устгахдаа дахин сэргээгдэхгүй байдлаар устгана;

4.6.9 байгууллага нь мэдээллийн систем, өгөгдөл, мэдээллийг өөрийн серверийн өрөөнд байршуулахаас гадна газарзүйн байршлын хувьд өөр газарт нөөц дата төвд хуулбарыг заавал байршуулна;

4.6.10 нөөц дата төвд мэдээллийн систем, өгөгдөл, мэдээллийг байршуулах, тэдгээрт хяналт тавих, нөөц сервер компьютер, тоног төхөөрөмж, сүлжээний тохиргоог хийх, үндсэн мэдээллийн систем доголдох, аюул занал учрахад нөөц систем нөхөж ажилладаг байхаар тохируулах ажлыг Мэдээллийн технологийн асуудал хариуцсан нэгж зохион байгуулна.

Тав. Кибер аюулгүй байдлыг хангах зохион байгуулалтын арга хэмжээ

5.1 Эрх зүйн орчин, зохион байгуулалтын хувьд дараах үйл ажиллагааг хэрэгжүүлнэ. Үүнд:

5.1.1 мэдээллийн аюулгүй байдлыг хангах стратеги төлөвлөгөөг төвийн стратеги төлөвлөгөөтэй уялдуулан боловсруулах;

5.1.2 шаардлагатай удирдлага, санхүү, хүний нөөцийн чадавхыг бүрдүүлж кибер аюулгүй байдлын стратеги төлөвлөгөөг хэрэгжүүлэх;

5.1.2 мэдээллийн аюулгүй байдлын удирдах болон гүйцэтгэх чиг үүргийг ажлын байрны, эсхүл албан тушаалын тодорхойлолтод тусгаж, орон тооны, эсхүл хавсран гүйцэтгэх ажилтныг томилох;

5.1.4 мэдээллийн технологи, мэдээллийн аюулгүй байдал хариуцсан ажилтан, албан хаагчийн мэдлэг, ур чадварыг тогтмол дээшлүүлэх арга хэмжээг авах;

5.1.5 мэдээллийн аюулгүй байдлын аудит, мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээг холбогдох стандарт, эсхүл хуульд заасан хугацаанд хийлгэж, тайланг кибер халдлага, зөрчилтэй тэмцэх газарт хүргүүлэх;

5.1.6 эрсдэлийн үнэлгээний үр дүнд үндэслэн эрсдэлийг бууруулахад чиглэсэн арга хэмжээг төлөвлөж, хэрэгжүүлэх;

5.1.7 кибер халдлага, зөрчилтэй тэмцэх төвөөс хүргүүлсэн зөвлөмж, шаардлагыг тогтоосон хугацаанд, эсхүл ажлын 10 өдрийн дотор хэрэгжүүлж хариу мэдэгдэх;

5.1.8 мэдээллийн аюулгүй байдлын бодлогыг агуулсан албан ёсны баримт бичиг нь төвийн өөрийн онцлогт тохирсон, мэдээллийн аюулгүй байдлыг хангах үүрэгтэй бүх ажилтнуудад хүртээмжтэй байх шаардлагатай;

5.1.9 онцгой нөхцөл үүссэн үед мэдээллийн системээ нөхөн сэргээх, нүүлгэн шилжүүлэх төлөвлөгөөтэй байна;

5.2 Физик орчны хувьд дараах үйл ажиллагааг хэрэгжүүлнэ. Үүнд:

5.2.1 Сервер болон мэдээллийн сан, мэдээлэл хадгалагддаг компьютеруудыг орчны нөлөөнөөс хамгаалах;

5.2.2 Тоног төхөөрөмжийн нууцлал, хамгаалалтын аюулгүй байдлыг хангахдаа анхаарах зүйлс. Үүнд:

5.2.3.1 компьютер, техник хэрэгслийг заавал бүртгэлийн картаар (Техник хэрэгслийн бүртгэлийн карт) бүртгэсэн байна. Бүртгэлийн картыг мэдээллийн технологи хариуцсан ажилтан хөтлөх бөгөөд засвар үйлчилгээ хийсэн эсвэл шинэ програм хангамж суулгасан тохиолдолд мэдээллийн технологи хариуцсан ажилтан болон тухайн компьютер, техник хэрэгслийг

эзэмшигч хоёул гарын үсэг зурж баталгаажуулна;

5.2.3.2 компьютерт программ хангамж, техник хангамжийг суурилуулахдаа дараах зарчмыг биримтална. Үүнд:

- програм болон техник хангамжийн суурилуулалт түүний шинэчлэл, тохиргоог зөвхөн мэдээллийн технологи хариуцсан ажилтан хийнэ;
- 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;
- систем суулгах, өөрчлөлт оруулах бүрд бүртгэлийн карт дээр тэмдэглэл хийн эзэмшигч, мэдээллийн технологийн ажилтан хоёул гарын үсэг зурж баталгаажуулна;

5.2.3.3 зөөврийн компьютер ашиглахад анхаарах зүйлс. Үүнд:

- зөөврийн компьютерт хулгайд алдахаас сэргийлж зориулалтын цоожлогч ашиглах;
- зөөврийн компьютерыг албан хэрэгцээнээс бусад зориулалтаар ашиглахыг хориглох;
- зөөврийн компьютертэй гадуур ажлаар болон албан томилолтоор явахдаа нууц зэрэглэлийн мэдээллийг шифрлэх, кодлох байдлаар хамгаална;
- гаднаас зөөврийн хадгалах төхөөрөмж ашиглах бол заавал хортой код илрүүлэх програм уншуулна.

5.2.3.4 сүлжээний орчинд ажиллахад анхаарах зүйлс. Үүнд:

- байгууллагын сүлжээний байнгын бэлэн байдлыг мэдээлэл технологи хариуцсан нэгж хариуцна.
- сүлжээний шинэчлэлийг хийх төсвийг жил бүрийн төсөвт тогтмол суулгах.
- сүлжээний кабель бүрт хаягчлал хийж, сүлжээний тоног төхөөрөмжүүдийн ашиглагдаагүй гаралтууд дээр лац, ломбо тавих ажлыг мэдээлэл технологи хариуцсан нэгж хийх бөгөөд өөр хүн ашиглах боломжийг хаана.
- төв нь мэдээллийн систем, мэдээллийн сүлжээнд тохирсон аюулгүй байдлыг хангах систем (IDS/IPS, antimalware, WAF, Email filter, SIEM)-ийг хэрэглэнэ.

5.3 Програм, техник хангамжийн хувьд дараах үйл ажиллагааг хэрэгжүүлнэ. Үүнд:

5.3.1 цахим мэдээллийн архив, бүртгэлийн автоматжуулсан системтэй байх.

5.3.2 сүлжээний хамгаалалтыг зохион байгуулах, мэдээллийн системийг хууль бус гадны халдлагаас хамгаалах шийдлийг нэвтрүүлсэн байх.

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

- сүлжээний хамгаалалтын тоног төхөөрөмж нь албан ёсны лицензтэй, нөөцтэй, IPS, IDS, access control, content filter гэх мэт үндсэн модуль, бусад нэмэлт модультай байх;
- сүлжээний үндсэн (core) свич нь албан ёсны лиценз бүхий програм хангамжтай, Layer 3 буюу түүнээс дээш үзүүлэлт бүхий свичтэй байх;
- сүлжээний үндсэн свич нь нөөцтэй байх;
- серверүүд нөөцтэй байх шаардлагатай бөгөөд программ хангамжууд нь албан ёсны лицензтэй байх.

5.3.4 сервер болон програм хангамж шинээр нэвтрүүлэхийн өмнө хортой код байгаа эсэхийг мэдээлэл технологи хариуцсан нэгжээр шалгуулах;

5.3.5 хамгаалалтын түвшинг байнгын шинэчлэн сайжруулж байх;

5.4 Биет хамгаалалтын хувьд дараах үйл ажиллагааг хэрэгжүүлнэ. Үүнд:

5.4.1 албан хаагчид нь өөрийн, компьютер дээр шууд харьяалах албан тушаалтны зөвшөөрөлгүйгээр гадны этгээдийг ажиллуулах, компьютерыг түгжилгүйгээр /screen lock, log off, shut down хийлгүйгээр/ орхиж явахыг хориглоно;

5.4.1 мэдээллийн систем, програм хангамж, сервер болон тоног төхөөрөмжүүд нь харуул хамгаалалттай тусгай зориулалтын өрөөнд байрлуулна;

5.4.1 сервер болон сүлжээний тоног төхөөрөмжүүдийн сул портуудыг програмын түвшинд хааж хамгаалах. Програмын төвшинд хаах боломжгүй портуудтай тоног төхөөрөмжүүдийн портыг лац тавьж баталгаажуулна;

5.5 Мэдээллийн систем, сүлжээ, мэдээллийн сангийн нууцлалын хувьд дараах үйл ажиллагааг хэрэгжүүлнэ. Үүнд:

5.5.1 Нууц үгийн бодлогод дараах зарчмыг баримтална. Үүнд:

5.5.1.1 нууц үгийг том, жижиг үсэг, тоо, тусгай тэмдэг бүхий 8 ба түүнээс дээш тэмдэгт байхаар хийнэ. Нууц үгээ ил бичиж тэмдэглэх, бусдад дамжуулахыг хориглоно;

5.5.1.2 анхдагч нууц үгийг заавал солих ба нууц үгийг цаашид улирал тутам солино. Ингэхдээ хуучин нууц үгийг дахин хэрэглэхээс зайлсхийж, хуучин тэмдэгтүүдийн ихэнхийг солино;

5.5.1.3 хэрэв нууц үг илчлэгдсэн гэж үзвэл нэн даруй солино. Төвийн хэмжээний томоохон систем, тоног төхөөрөмжид нэвтрэх нууц үгийг сар тутам солино;

5.5.1.4 мэдээллийн систем, өгөгдлийн сан, програм хангамжийн нууц үгийн сонголт, бүртгэл, ашиглах хугацааг мэдээллийн технологийн мэргэжилтэн, системийн зохицуулагч, мэдээллийн аюулгүй байдлын мэргэжилтэн нар хариуцан ажиллаж, хяналт тавина. Шинээр үүсгэх, өөрчлөх, устгах тохиолдолд Маягт №3-аар баталгаажуулах ба улирал тутам системийн хэрэглэгчдийн жагсаалтыг хянана;

5.5.2 Нууц үгийн хамгаалалтыг дараах байдлаар зохион байгуулна. Үүнд:

5.5.2.1 төвийн системийн хэрэглэгчид нууц үгээ хамгаалах үүрэгтэй бөгөөд, бусдад дамжуулахыг хориглоно;

5.5.2.2 өрөөнд байгаа компьютерыг түр болон удаан хугацаагаар орхиж явахдаа заавал түгжих буюу нууц үгээр хамгаалагдсан дэлгэцийн хамгаалалтыг ажиллуулна /screen lock, log off/;

5.5.2.3 нууц үгээ ажлын шаардлагаар бусдад ашиглуулсан эсвэл нууц үгээ алдсан байх магадлалтай бол нууц үгээ заавал солих. Ингэхдээ хуучин нууц үгийг дахин хэрэглэхээс зайлсхийж, хуучин тэмдэгтүүдийн ихэнхийг солих шаардлагатай;

5.5.2.4 албан хаагчдын ажлын компьютерын дэлгэцийг бусдад шууд харагдахгүйгээр байрлуулсан байх;

5.5.3 Төвийн мэдээллийн систем, програм хангамж, сервер болон тоног төхөөрөмжийн нууц үгийн хамгаалалт

5.5.3.1 мэдээллийн систем, програм хангамж, сервер болон тоног төхөөрөмжийн нууц үгийн сонголт, бүртгэл, ашиглах хугацааг систем хариуцсан инженер, мэдээллийн аюулгүй байдлын мэргэжилтэн нар хариуцан ажиллаж, хяналт тавина;

5.5.3.2 нууц үгийг цаасан дээр хэвлэмэл хэлбэрээр үл гэрэлтэх дугтуйнд битүүмжлэн тусгай зориулалтын сейфэнд лацдаж хадгална. Сейф нь серверийн өрөөнд байрлах бөгөөд бүрэн бүтэн байдлыг мэдээллийн технологийн мэргэжилтэн бүр хариуцна;

5.5.3.3 сейфийг нээх, хаах, лацдах, нууц үгтэй дугтуйны өөрчлөлт зэрэг нь Бүртгэлийн дэвтэрт байнга хөтлөгдөж байна. Бүртгэлийн дэвтрийг мэдээлэл, технологи хариуцсан нэгж хөтөлнө;

5.5.3.4 нууц үгтэй дугтуйг задалж нууц үг ашигласан тохиолдолд тухайн нууц үгийг

шинэчлэн дуттуйд хийж битүүмжлэн сейфэнд лацдаж хадгална;

5.5.3.6 төвийн мэдээллийн систем, програм хангамж, сервер тоног төхөөрөмжийн нууц үг агуулсан файл нь нууц үгээр хамгаалагдсан байх ба тухайн нууц үгийг тухайн систем хариуцсан мэргэжилтнүүд мэднэ;

5.5.3.7 нууц үг агуулсан файлын нууц үгийг системийн нууц үгтэй дуттуйнд хамт хадгалах ба мартсан тохиолдолд систем хариуцсан нэгжээс зөвшөөрөл авч нууц үгийг сэргээнэ;

5.6 Хандалтын удирдлагыг тогтооход дараах үйл ажиллагааг хэрэгжүүлнэ. Үүнд:

5.6.1 систем хариуцсан хэрэглэгчдэд хандах эрхийг олгохдоо зөвшөөрөгдсөнөөс бусад мэдээлэлд хандах боломжгүй байхаар зохион байгуулна;

5.6.2 систем хариуцсан мэргэжилтэн өөрийн чиг үүргийн дагуу системд нэвтрэх хандалтын эрхийг эдэлнэ;

5.6.3 албан хаагч нь мэдээллийн санд нэвтрэх эрхийг тухайн алба нэгжийн удирдлагаас ирүүлсэн хандах тус журмын эрх хүсэлтийн маягтыг үндэслэн зөвшөөрлийг үндэслэн систем хариуцсан мэргэжилтэн нээж өгнө;

5.7 Мэдээллийн санд нэвтрэх эрхийн түвшинг дараах байдлаар зохион байгуулна. Үүнд:

5.7.1 албан хаагч нь чиг үүргийнхээ дагуу мэдээллийн санд эрхийн өөр өөр түвшинд хандана;

5.7.2 админ, /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 цуцлахдаа дараах үйл ажиллагааг хэрэгжүүлнэ. Үүнд:

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

5.8.2 хүний нөөцийн мэргэжилтэн ажилтанг ажлаас чөлөөлсөн тухай систем хариуцсан инженерт заавал мэдэгдсэн байна;

5.8.3 мэдээллийн систем, мэдээллийн санд нэвтрэх эрх бүхий ажилтан мэдээллийн аюулгүй байдлын бодлого, журмыг зөрчсөн байвал системд нэвтрэх эрхийг систем хариуцсан инженер түдгэлзүүлж болно;

5.9 Лог файлын бүртгэлийг үүсгэхэд дараах үйл ажиллагааг хэрэгжүүлнэ. Үүнд:

5.9.1 мэдээллийн системд ажиллаж байгаа хэрэглэгчийн хийсэн үйлдлүүд, хэзээ, хаашаа нэвтэрсэн, ямар үйлдэл хийсэн зэрэг нь системд бүртгэгдэж байхаар тохируулна;

5.9.2 лог файлын бүртгэл, үнэн зөв, бүрэн бүтэн байдлыг системийн зохицуулагч хариуцна;

5.9.3 лог мэдээллийг сар бүр нөөцөлж, 3 жил тутам нягтлан шинжилсний дараа системийн зохицуулагч устгана.

5.9.4 төвийн мэдээллийн системд хөгжүүлэлт хийсэн аж ахуй нэгж нь гэрээний хугацаа болон засвар үйлчилгээний хугацаандаа Лог мэдээллийн үнэн зөв, бүрэн бүтэн байдлыг хариуцна;

5.9.5 мэдээллийн систем, програм хангамж, сервер тоног төхөөрөмжүүд нь тусдаа бие даасан лог бүртгэлийн програм хангамжтай байна;

5.9.6 мэдээллийн систем, програм хангамж, сервер тоног төхөөрөмжүүдийн програм хангамж дээр гарсан өөрчлөлт, гэмтэл саатлын мэдээлэл болон мэдээллийн системд ажиллаж байгаа хэрэглэгчийн хийсэн үйлдлүүд, хэзээ, хаашаа нэвтэрсэн, ямар үйлдэл хийсэн зэргийг бүртгэгдэж байхаар тохиргоо хийнэ. Үүнд:

5.9.6.1 хэрэглэгчийн нэр, системд нэвтрэх нэр буюу ID;

5.9.6.2 огноо;

5.9.6.3 хандсан хаяг, төхөөрөмжийн мэдээлэл;
5.9.6.4 хандалтын үргэлжлэх хугацаа;
5.9.6.5 гүйцэтгэсэн үйлдэл;
5.9.6.6 гүйцэтгэсэн үйлдлийн үр дүн.

5.10 Хортой кодоос хамгаалахад дараах үйл ажиллагааг хэрэгжүүлнэ. Үүнд:

5.10.1 төвийн хэрэгцээнд хэрэглэгдэж байгаа компьютер, мэдээлэл хадгалагч болон тээгч зөөврийн хэрэгслүүдэд зөвшөөрөгдсөн хортой кодын/вирус/ эсрэг програм хангамжийг ашиглана.
5.10.2 хортой кодын эсрэг програмын шинэчлэлтийг тогтмол хийнэ.
5.10.3 тодорхой хугацаанд системийн хортой кодын эсрэг програмыг уншуулж, илэрсэн тохиолдолд арилгах арга хэмжээг авна.
5.10.4 системд гаднаас мэдээлэл оруулах бол сүлжээнд холбогдоогүй компьютерт эхэлж хортой кодын шинжилгээг заавал хийсний дараа системд нэвтрүүлнэ.
5.10.5 цахим хөтчөөс хортой кодын эсрэг програм хориглосон, хаасан цахим хуудас болон контентруу нэвтрэхийг хориглоно.

5.11 Төвийн цахим баримт бичиг, мэдээллийн сангийн нөөцлөлт, хадгалалтыг хийхэд дараах үйл ажиллагааг хэрэгжүүлнэ. Үүнд:

5.11.1 мэдээллийн цахим сан хөмрөгийг бүрдүүлэх зорилгоор байгууллагын цахим архивын сантай байна.
5.11.2 цахим архивын сангийн компьютер, тоног төхөөрөмжийг серверийн өрөөнд байрлуулж, цахим архивын бүрдүүлэлт, хадгалалт, хамгаалалт, нууцлалыг архивын асуудал хариуцсан албан хаагч Мэдээллийн технологийн асуудал хариуцсан нэгжтэй хамтран зохион байгуулна.
5.11.3 албан хаагч нь цахим баримт бичиг боловсруулахдаа Төрийн албан хэрэг хөтлөлтийн заавар болон бусад холбогдох стандартуудыг мөрдлөг болгоно.
5.11.4 хэрэглэгч тухайн ажлын байртай холбогдох бичиг баримтыг төрөлжүүлж өөрийн компьютерт хадгалах ба шаардлагатай бол хуулбарыг нөөц мэдээллийн санд хадгална.
5.11.5 хэрэглэгч нь албан хэрэгцээний файлаа нэр төрлөөр нь ангилж хавтас үүсгэн хадгална. Шаардлагатай бол дэд хавтас үүсгэн хадгалж, жил тутмын эхний улиралд архивын ажилтанд өмнөх оны файл, хавтсаа байгууллагын мэдээллийн цахим сан хөмрөгт хадгалуулах зорилгоор хүлээлгэн өгнө.
5.11.6 архивын ажилтан цахим мэдээллийг хүлээн авч байгууллагын мэдээллийн цахим архивд хадгална. Ингэхдээ холбогдох тэмдэглэлийг заавал хөтөлнө. Файлд нэр өгөхдөө "Монгол кирилл цагаан толгойн үсгүүдийг романчлах" MNS 5217:2012 стандартыг мөрдлөг болгоно.
5.11.7 байгууллагын үйл ажиллагаанд хэрэглэгддэг худалдаж авсан, захиалгаар хөгжүүлсэн, өөрсдийн хөгжүүлсэн, тусгай зориулалтын програм хангамжийн эх хувийг болон хувилбаруудыг байнгын хэрэгцээнд зориулан серверт байрлуулна.

5.12 Төв нь үүлэн технологид суурилсан үйлчилгээ (цаашид "үйлчилгээ" гэх) ашиглах бол дараах мэдээллийг тусгана. Үүнд:

5.12.1 үйлчилгээг ашиглахад тавигдах кибер аюулгүй байдлын шаардлага;
5.12.2 үйлчилгээг сонгох шалгуур үзүүлэлт, хэрэглээний хамрах хүрээ;
5.12.3 албан хаагчийн үүрэг, хариуцлага;
5.12.4 үүлэн технологид суурилсан үйлчилгээ үзүүлэгч этгээдийн хэрэгжүүлж болох кибер аюулгүй байдлыг хангах үйл ажиллагаа;
5.12.5 үйлчилгээтэй холбоотой байгууллагын хэрэгжүүлж болох кибер аюулгүй байдлын арга хэмжээ;
5.12.6 олон үйлчилгээг зэрэг ашиглах үед тэдгээрийн аюулгүй байдлыг уялдуулан зохион байгуулах арга хэмжээ;

5.12.7 үйлчилгээ ашиглах үед тохиолдсон халдлага, зөрчлийн эсрэг авах хариу арга хэмжээ;
5.12.8 эрсдэлийг бууруулах арга хэмжээ;
5.12.9 үйлчилгээнд өөрчлөлт орсон эсхүл зогсоох үед хэрэгжүүлэх аюулгүй байдлын арга хэмжээ.

5.13 Төв нь үүлэн технологид суурилсан үйлчилгээ авах бол холбогдох хууль тогтоомжид нийцүүлэн ажил гүйцэтгэгчтэй байгуулах гэрээнд дараах шаардлагыг тусгана. Үүнд:
5.13.1 үйлдвэрлэгчээс тогтоосон стандартын дагуу технологийн шийдэл хэрэгжүүлэх талаар;
5.13.2 байгууллагын аюулгүй байдлын шаардлагад нийцсэн хандалтын удирдлага хэрэгжүүлэх талаар;
5.13.3 хортой кодын хяналт болон хамгаалалтын шийдлийг хэрэгжүүлэх талаар;
5.13.4 харилцан зөвшөөрсөн байршилд мэдээллийг хадгалах, боловсруулах талаар;
5.13.5 халдлага зөрчлийн үед ажил гүйцэтгэгч, эсхүл үйлдвэрлэгчээс техникийн туслалцаа үзүүлэх талаар;
5.13.6 ажил гүйцэтгэгч нь үйлчилгээтэй холбоотой туслан гүйцэтгэх гэрээ байгуулахад байгууллагын кибер аюулгүй байдлын шаардлагыг хангуулах талаар;
5.13.7 кибер халдлага, зөрчлийн дараа нөхөн сэргээхэд техникийн туслалцаа үзүүлэх талаар;
5.13.8 үйлчилгээг зогсоох үед ажил гүйцэтгэгчийн зүгээс зохих хугацаанд үйлчилгээний хүртээмжтэй байдлыг баталгаажуулах талаар;
5.13.9 нөөц өгөгдөл, тохиргооны файл, эх код, байгууллагын эзэмшлийн өгөгдлийг шаардлагатай үед гаргаж өгөх талаар.

5.14 Үйлчилгээтэй холбоотой дараах өөрчлөлтийн үед ажил гүйцэтгэгч нь төвд урьдчилан мэдэгдэл хүргэнэ. Үүнд:
5.14.1 үйлчилгээний тасралтгүй ажиллагаа, аюулгүй байдалд нөлөөлөл үзүүлэх хэмжээний техникийн өөрчлөлт орсон;
5.14.2 мэдээллийг хадгалах, боловсруулах газар зүйн байршил өөрчлөгдсөн;
5.14.3 гэрээ байгуулсан туслан гүйцэтгэгчийн үйлчилгээнд өөрчлөлт орсон.

Зургаа. Төвийн мэдээллийн нөөцлөлт, хадгалалт

6.1 Компьютер, принтер, техник хэрэгсэл болон програм хангамжийн хувьд дараах байдлаар зохицуулна. Үүнд:
6.1.1 өөрийн хэрэглэж буй компьютер дээрх мэдээллийн нөөцлөлт, хадгалалт, бүрэн бүтэн байдлыг тухайн хэрэглэгч өөрөө хариуцна;

6.2 Сүлжээ болон сүлжээний тоног төхөөрөмжүүдийн хувьд дараах байдлаар зохицуулна. Үүнд:
6.2.1 сүлжээ болон сүлжээнд холбогдох дагалдах тоног төхөөрөмжүүдийн топологи зургийг сүлжээний бүтэц, зохион байгуулалт өөрчлөгдөх бүрт шинэчлэн хадгална;
6.2.2 сүлжээний тоног төхөөрөмжид хандах нэр, нууц үгийг мэдээлэл технологи хариуцсан ажилтан, систем хариуцсан инженерүүд нууцлан хадгална;
6.2.3 сүлжээний тоног төхөөрөмжүүдийн тохиргооны болон лог файлыг техник үйлчилгээ хийх, тохиргоог өөрчлөх бүрт нөөцлөн хадгална;
6.3.1 www.mail.gov.mn домэйн бүхий цахим шуудангийн сервер нь захидал, мэдээллийг удаан хугацаагаар хадгалах боломжгүй тул цахим шуудан хэрэглэгч нь өөрийн нэн шаардлагатай шуудангаа серверээс татан авч хэвлэмэл эсвэл файл байдлаар хадгална;
6.3.2 системийн ачааллаас шалтгаалан цахим мэдээллийн санд хадгалагдаж байгаа хэрэглэгчдийн хуучин цахим шуудангууд тогтмол устгагдана;

6.3 Цахим хуудасыг дараах байдлаар зохицуулна. Үүнд::

6.3.1 цахим хуудасны эх код, өгөгдлийн санг тогтмол техник ашиглалтын зааврын

хуваарийн дагуу хуулбарлан авч хадгалах ажлыг мэдээллийн технологи хариуцсан ажилтан зохион байгуулна;

6.4 Сервер, дагалдах тоног төхөөрөмжийн хувьд дараах байдлаар зохицуулна. Үүнд:

6 4.1 төвийн үйл ажиллагаанд ашиглагдаж байгаа серверүүдийн өгөгдлийн санг техник ажиллагааны зааврын хуваарийн дагуу хуулбарлан авч хадгалах ажлыг ТХНҮА-ны мэдээллийн технологи хариуцсан албан хаагчид зохион байгуулна;

ДОЛОО. Төвийн мэдээлэл технологи хариуцсан нэгж, ажилтны эрх, үүрэг

7.1 Мэдээллийн технологи хариуцсан ажилтны эрх, үүрэг:

7.1.1 төвийн мэдээллийн аюулгүй байдлын бодлогыг тодорхойлох, мэдээллийн аюулгүй байдлын тогтолцоог бүрдүүлэх, холбогдох дүрэм, журмыг боловсруулж батлуулах, тэдгээрт нэмэлт өөрчлөлт оруулах санал боловсруулах;

7.1.2 мэдээллийн аюулгүй байдлыг хангахад чиглэсэн арга хэмжээг төлөвлөх, хэрэгжүүлэх, тайлагнах, шаардагдах зардлыг төсөвт суулгах санал боловсруулах;

7.1.3 мэдээллийн технологийн асуудал хариуцсан нэгж нь мэдээллийн системд заналхийлж буй халдлагыг бүртгэх, илрүүлэх, таслан зогсоох болон эмзэг байдлыг тогтоох, түүнийг бууруулах, аюулгүй байдлын бодлого боловсруулах зорилгоор мэдээллийн аюулгүй байдлыг хангах мэргэжилтнийг /системийн зохицуулагч/ ажиллуулна. Энэ арга хэмжээг захиргаа болон алба нэгжүүд чиг үүргийн дагуу мэдээллийн аюулгүй байдлыг хангахад дэмжиж ажиллана.

7.1.4 мэдээллийн аюулгүй байдлын учрал, онц нөхцөл байдал тохиолдоход мэдээллийн системүүдийг сэргээх, хэвийн ажиллагааг хангах арга, гүйцэтгэх дараалал, хариуцах албан хаагчийг тодорхойлсон төлөвлөгөөг боловсруулж, мөрдүүлж ажиллах;

7.1.5 нэгжийн мэдээллийн аюулгүй байдлыг хариуцсан мэргэжилтний, мэргэжил, ур чадварыг дээшлүүлэх сургалтад байнга хамруулах.

7.1.6 албан хаагчдыг мэдээллийн аюулгүй байдлыг хангаж ажиллах талаар жил бүр тогтмол сургалт хийх.

7.1.7 мэдээллийн аюулгүй байдлыг хангах мэргэшүүлэх

7.1.8 мэдээллийн аюулгүй байдлыг хангахад шаардлагатай үйл ажиллагаа, нөөцийг төлөвлөх;

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 үйл ажиллагаанд оролцох, санал оруулах, нэвтрүүлэх үйл явцад хяналт тавих;

7.2.5 эрсдэлийн үнэлгээг жил тутам хийж мэдээллийн аюулгүй байдлын эмзэг байдлыг тодорхойлох, хамгаалалтын төвшинг тогтоох, хөндлөнгийн хяналтыг хэрэгжүүлэх;

7.2.6 мэдээллийн систем, мэдээллийн сангийн бүрэн бүтэн байдалд хяналт тавих, мэдээллийн сангийн нөөцлөлт, нөөцийг хадгалах нөхцөлийг хангах;