ЗАСГИЙН ГАЗРЫН ТОХИРУУЛАГЧ АГЕНТЛАГ
БИЕИЙН ТАМИР, СПОРТЫН УЛСЫН ХОРООНЫ
ДАРГЫН ТУШААЛ

2023 оны 09 сарын 26 өдөр Дугаар А/232 Улаанбаатар хот

Журам батлах тухай

Засгийн газрын агентлагийн эрх зүйн байдлын тухай хуулийн 8 дугаар зүйлийн 8.3.1 дэх заалт, 8.4 дэх хэсэг, Нийтийн мэдээллийн ил тод байдлын тухай хуулийн 34 дүгээр зүйлийн 34.1.1 дэх заалтыг тус тус үндэслэн ТУШААХ нь:

1.“Биеийн тамир, спортын улсын хорооны мэдээллийн аюулгүй байдлыг хангах журам”-ыг нэгдүгээр хавсралтаар, “Серверийн өрөөнд ажиллах журам”-ыг хоёрдугаар хавсралтаар, “Дотоод хяналтын камерын системийн ашиглалтын журам”-ыг гуравдугаар хавсралтаар тус тус баталсугай.

2.Дээрх журмуудыг үйл ажиллагаандаа мөрдлөг болгон ажиллахыг байгууллага, харьяа байгууллагуудын нийт албан хаагчдад үүрэг болгосугай.

3.Дээрх журмуудын хэрэгжилтэд жил бүрийн 12 дугаар сарын 25-ны өдрийн дотор хяналт, үнэлгээг хийж ажиллахыг Хяналт-шинжилгээ, үнэлгээ, дотоод аудитын хэлтэс (О.Батсүх)-т даалгасугай.

4.Тус журмуудыг хэрэгжүүлэхэд мэргэжил арга зүйн дэмжлэг үзүүлэн, хэрэгжилтийг зохион байгуулж, тайлагнан ажиллахыг Гадаад харилцаа, мэдээллийн технологийн хэлтэс (Н.Оюунбат)-т, тушаалын хэрэгжилтийг хянаж ажиллахыг Төрийн захиргааны удирдлагын газарт тус тус үүрэг болгосугай.

ДАРГЫН ҮҮРГИЙГ ТҮР
ОРЛОН ГҮЙЦЭТГЭГЧ О.БАТТУЛГА

Биеийн тамир, спортын улсын хорооны даргын 2023 оны 09 сарын 26-ний өдрийн А/332 дугаар тушаалын Нэгдүгээр хавсралт

БИЕИЙН ТАМИР, СПОРТЫН УЛСЫН ХОРООНЫ МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ЖУРАМ

НЭГ. НИЙТЛЭГ ҮНДЭСЛЭЛ

1.1. Энэхүү журмын зорилго нь биеийн тамир, спортын салбарын төрийн захиргааны байгууллага, түүний харьяа байгууллагууд, салбарын мэдээллийн нэгдсэн цахим санд бүрдүүлэлт хийж буй спортын холбоодыг хамруулан 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 тухай бүр засаж, сэргээх, хариу арга хэмжээ авахад оршино.

1.2. Биеийн тамир, спортын улсын хороо болон түүний харьяа байгууллагууд болох нийслэл, аймгуудын биеийн тамир, спортын газар, дүүргүүдийн биеийн тамир, спортын хорооны нийт ажилтан албан хаагчид, мэдээллийн технологи, мэдээллийн сүлжээний чиг үүргийг хариуцсан албан хаагчид ажил үүргээ гүйцэтгэхдээ энэхүү журмыг мөрдлөг болгон ажиллана.

1.3. Тухайн байгууллага онцлогоосоо хамааруулан энэхүү журамтай уялдуулан нэмэлт журам боловсруулан мөрдөж болно. Нэмэлт журам нь энэ журмын салшгүй нэг хэсэг болон дагаж мөрдөгдөнө.

1.4. Байгууллагууд нь мэдээллийн системийг зохион байгуулахдаа холбогдох стандартууд /Мэдээллийн технологи - Аюулгүй байдлын аргууд - Мэдээллийн аюулгүй байдлын удирдлагын үйл ажиллагааны дүрэм - MNS 17799.2007, Мэдээллийн технологи- Аюулгүй байдлын арга техник - Мэдээллийн ба холбооны технологийн аюулгүй байдлын удирдлага 1-р хэсэг: Мэдээлэл холбооны технологийн аюулгүй байдлын үндсэн ойлголтууд болон загварууд - MNS ISO/IEC 13335-1:2009, Мэдээллийн технологи - Аюулгүй байдлын арга техник - Мэдээллийн аюулгүй байдлын эрсдэлийн удирдлага - MNS 5969 : 2009, Мэдээллийн технологи - Аюулгүй байдлын арга техник – Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоо - шаардлага - MNS ISO/IEC 27001:2009/-ыг мөрдсөн байна.

ХОЁР. НЭР ТОМЬЁО

2.1. Мэдээлэл гэж эзэмшиж хадгалж байгаа төхөөрөмжөөс үл хамааран боломжит бүх 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, байгууллагын нууцад хамаарахгүй 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 байгууллагын томилох эрх бүхий албан тушаалтны шийдвэрээр томилогдсон төрийн албан хаагчийг;

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 Хүний хувийн мэдээллийг хамгаалах тухай хуулийн 4 дүгээр зүйлийн 4.1.8. дахь заалтад тодорхойлсноор ойлгоно.

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

2.8. Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоо /МАБУТ/ гэж 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 зүйлс, мэдээлэл, түүнтэй холбоотой аливаа юмс;

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

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

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

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

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

ГУРАВ. БАЙГУУЛЛАГЫН МЭДЭЭЛЛИЙН ӨМЧ ХӨРӨНГӨ, АНГИЛАЛ

3.1. Мэдээллийн өмч хөрөнгийн ангилал.

3.1.1. Биет мэдээллийн хөрөнгө гэдэг нь судалгааны материалууд, үйл ажиллагааны төлөвлөгөө, төсөл хөтөлбөрүүд, бүртгэлийн мэдээллүүд, сургалтын материал, тараах хуудас, 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. Программ хангамжийн хөрөнгө гэдэг нь албан ёсны зөвшөөрөлтэй хэрэглээний, мэргэжлийн болон мэдээллийн системийн программ хангамж, өөрсдийн боловсруулсан болон тусгай захиалгаар хийлгэсэн программ хангамжууд, системүүдийг;

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

3.2. Мэдээллийн нууцлал, ангилал

3.2.1. Нийтэд хүртээмжтэй: Нийтэд зориулагдсан, нууцлах шаардлагагүй мэдээллүүд- хэрэглэгчдэд зориулсан гарын авлага, зөвшөөрөл авахад бүрдүүлэх материалууд, ил тод байдлыг илэрхийлсэн материалууд- байгууллагын төлөвлөгөө, тайлан, төсөв, санхүүгийн мэдээ, буруугаар ашиглан байгууллагад ямар нэгэн хохирол учруулах боломжгүй материалууд

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

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

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

а/ Байгууллага дотроо хувилж, олшруулж, тараахад хязгаарлалт тавихгүй

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

3.2.3. Нууц мэдээлэл: Хуульд 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 нууцын зэрэглэл бүхий мэдээлэл, баримт бичиг, үйл ажиллагаатай холбоотой нууц, харилцагчийн мэдээллийн нууц зэрэг мэдээллүүдийн нууцыг хадгалах хамгаалахтай холбоотой ажилтантай хийх "НУУЦЫГ ХАДГАЛАХ БАТАЛГАА"-ний загварыг **Маягт №1**-ээр батална.

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

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

Зэрэглэл I: Нээлттэй бүс

Зэрэглэл II: Нийтэд хаалттай бүс

Зэрэглэл III: Хаалттай бүс

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

ДӨРӨВ. БАЙГУУЛЛАГЫН МЭДЭЭЛЛИЙН ХАМГААЛАЛТ

4.1.Эрх зүйн орчин, зохион байгуулалтын хувьд

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

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

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

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

4.1.5. Онцгой нөхцөл үүссэн үед мэдээллийн системээ нөхөн сэргээх, нүүлгэн шилжүүлэх төлөвлөгөөтэй байна.

4.1.6. Мэдээллийн системийг шинээр байгуулахдаа мэдээллийн аюулгүй байдлын эрх зүйн акт болон бусад холбогдох баримт бичигт нийцүүлэн төлөвлөж, хамгаалалтыг зохицуулна.

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

4.2.Физик орчны хувьд

4.2.1. Сервер болон мэдээллийн сан, мэдээлэл хадгалагддаг компьютер техник хэрэгслийг орчны нөлөөнөөс хамгаалах шаардлагатай.

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

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

б/ Нийтэд хаалттай бүс – зөвхөн тухайн байгууллагын ажилтнууд орох эрхтэй хэсэг (Байгууллагын үйл ажиллагааны тасралтгүй байдалтай холбоотой цахилгааны удирдлагын цэг, сантехникийн зангилаа цэг, техникийн өрөө гэх мэт)

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

Хаалттай бүсэд нэвтрэх: Зөвхөн орох эрх бүхий зөвшөөрөлтэй албан хаагчид нэвтрэлтийг тусгай төхөөрөмж (электрон цоож, соронзон цоож гэх мэт) ашиглан нэвтэрнэ.

- Хаалттай бүсэд аливаа албан хаагч болон хөндлөнгийн хүн орох тохиолдолд "Серверийн өрөөнд ажиллах журам"-ын дагуу
- эрх бүхий албан тушаалтнаас зөвшөөрөл авч, бүртгүүлж орно.

4.2.3.Тоног төхөөрөмжийн нууцлал, хамгаалалт

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

4.2.3.2. Компьютерт программ хангамж, техник хангамжийг суурилуулах

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

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

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

4.2.3.3.Зөөврийн компьютер ашиглахад анхаарах зүйлс

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

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

в/ Зөөврийн компьютерыг албан хэрэгцээнээс бусад зориулалтаар ашиглахыг хориглох

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

д/ Зөөврийн компьютерт хулгайгаас сэргийлэх зориулалтын цоожлогч ашиглах

е/ Нууц зэрэглэлийн мэдээллийг шифрлэх, кодлох байдлаар хамгаалах шаардлагатай.

4.2.3.4.Сүлжээний кабел

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

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

4.2.3.5.Тоног төхөөрөмжийн байрлал

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

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

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

4.2.3.6.Хэвлэх, олшруулах төхөөрөмжийг ашиглах

а/ Хэвлэх төхөөрөмжийг үйл ажиллагаандаа өргөнөөр хэрэглэдэг байгууллага ашиглалтаа хяналттай байлгах

б/ Дундын хэвлэх төхөөрөмж рүү холбогдохдоо эрхээр ордог байх;

в/ Олшруулагчаар хийгдсэн ажлыг тэмдэглэж гүйцэтгэлийг дүгнэдэг байх;

4.2.3.7.Зөөврийн хадгалах төхөөрөмжийг ашиглах

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

б/ Зориулалтын сав, хайрцагт хийж зөөвөрлөдөг байх

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

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

4.3.Программ, техникийн хувьд

4.3.1. Архивын бүртгэлийн цахим мэдээллийн системтэй байна.

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

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

4.3.4.Техник программд мэдээлэл дамжуулах хэрэгсэл байгаа эсэхийг хэрэглээнд нэвтрүүлэхээс өмнө шалгах

4.3.5.Харилцаа холбооны нууцлал хамгаалалтыг хангах

4.2.6.Хамгаалалтын шаардлагатай түвшнийг хангахуйц техникийн шийдлийг боловсруулах.

ТАВ. БАЙГУУЛЛАГЫН МЭДЭЭЛЛИЙН СИСТЕМ, СҮЛЖЭЭ, МЭДЭЭЛЛИЙН САНГИЙН НУУЦЛАЛТ, ХАМГААЛАЛТ

5.1.Биет хамгаалалт

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

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

5.1.3.Байгууллагын биет хамгаалалтын үйл ажиллагааг дотоод хяналтын камерын системээр хянана.

5.1.4.Дотоод хяналтын камерын системийн үйл ажиллагааг “Дотоод хяналтын камерын системийн ашиглалтын журам”-аар зохицуулна.

5.2.Нууц үгийн бодлого

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

5.2.2.Нууц үгээ сонгох

а/ Нууц үгээ ил бичиж тэмдэглэхийг хориглоно.

б/ Анхдагч нууц үгийг заавал солих.

в/ Нууц үгийг бусдад дамжуулахгүй байх, илчлэгдсэн гэж үзвэл даруй солих.

г/ Зохицуулагчийн нууц үгийг дундаа хэрэглэхгүй байх.

5.2.3.Нууц үгийн бүрдэл

а/ Том, жижиг үсэг, тоо, тусгай тэмдэгтийг хослуулсан байх.
б/ Үүсмэл үг үүсгэх.

в/ Аюулгүй байдлын шаардлага хангасан нууц үгийг эргэн санахад хялбар байхаар логик дараалалтай үүсгэх.

г/ Нууц үгийн агуулгыг 8-аас дээш оронтой байхаар тооцон үүсгэх.

5.2.4.Нууц үг үүсгэхдээ ашиглахад хориглох зүйлс

а/ Өөрийн болон гэр бүл, төрөл төрөгсөд, ойр дотно хүмүүсийн нэр, төрсөн он сар өдөр, утас, машины дугаар, зэрэг таныг таньдаг болон судалсан хүн мэдэж болох мэдээлэл, түүний урвуулсан хэлбэрийг хэрэглэх.

б/ Хэрэглэгчийн нэрийг давтах, түлхүүр үгээ адил өгөх.
в/ Нууц үгээ дахин хэрэглэх, хуучин нууц үгээ эргүүлэн өгөх
г/ Нүдэнд ил харагдах зүйлс /ширээ, ном, компьютер гэх мэт/ таах боломжтой үгс
д/ Гарын хөдөлгөөнөөр амархан илрүүлж болох үгс, тоо /asd, aabbcc, 1234 гэх мэт/
е/ Дан буюу дараалсан тоо, үсэг /1111, 123456, ааа/
ё Тэгш хэмтэй үг, тоо

5.3.Нууц үгийн хамгаалалт

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

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

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

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

5.3.5.Байгууллагын мэдээллийн систем, программ 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 системүүдийн хэрэглэгчийн жагсаалтыг хянах үүрэг хүлээнэ.

5.4.Лог файлын бүртгэл

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

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

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

5.5.Хандалтын удирдлага

5.5.1.Системийн зохицуулагчаас албан хэрэгцээнд ашиглах мэдээллийн системд ажиллах ажилтан болон хэрэглэгчдэд хандах эрхийг олгохдоо зөвшөөрөгдсөнөөс бусад мэдээлэлд хандах боломжгүй байхаар зохион байгуулна.

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

5.5.3.Ажилтнуудын мэдээллийн санд нэвтрэх эрхийг тухайн ажилтныг томилсон шийдвэрт үндэслэн шаардлагатай эрхийг нээж өгөх, спортын холбоодын нэвтрэх эрхийг асуудал хариуцсан нэгийн саналыг үндэслэн системийн зохицуулагч нээж өгнө.

5.6.Хортой кодоос хамгаалах

5.6.1.Байгууллагын хэрэгцээнд ашиглагдаж буй компьютер, мэдээлэл хадгалагч сервер болон бусад техник хэрэгслүүдэд зөвшөөрөгдсөн буюу албан ёсны эрхтэй хортой кодын эсрэг программ хангамж ашиглана.

5.6.2.Хортой кодын эсрэг программын шинэчлэлтийг тогтмол хийнэ.

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

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

5.7.Цахим баримт бичиг боловсруулах, хадгалах.

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

5.7.2. Хэрэглэгч нь тухайн ажлын байртай холбогдох бичиг баримтыг төрөлжүүлж өөрийн компьютерын нөөц хадгалах төхөөрөмжид хадгалах. Шаардлагатай бол зөвшөөрөгдсөн нэмэлт зөөврийн хадгалах төхөөрөмж болон бусад санд хадгална.

5.7.3. Хэрэглэгч нь албан хэрэгцээний файлаа оны мэдээллийг агуулсан хавтас үүсгэн нэр төрлөөр нь ангилж дэд хавтас үүсгэн ажлын файлыг англи үсгээр галиглан давхардахгүй байдлаар хадгална. Шаардлагатай бол дэд хавтас үүсгэн хадгалж, хэрэглэж хэвшинэ.

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

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

5.7.6. Файлд нэр өгөхдөө "Монгол кирилл цагаан толгойн үсгүүдийг романчилах" MNS 5217:2003 стандартыг мөрдлөг болгоно.

ЗУРГАА. БАЙГУУЛЛАГЫН МЭДЭЭЛЛИЙН НӨӨЦЛӨЛТ, ХАДГАЛАЛТ

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

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

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

6.4. Серверт хадгалагдах өгөгдөл, мэдээллийг юникод ашиглан оруулах.

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

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

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

6.6. Мэдээллийн системээс мэдээллийг устгахдаа дахин сэргээгдэхгүй байдлаар устгана.

ДОЛОО. БАЙГУУЛЛАГЫН МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН АСУУДАЛ ХАРИУЦСАН 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 чиг үүргийг хариуцаж буй нэгжид тус чиг үүргийг хариуцсан мэргэжилтэн байх ба тус ажилтан нь системийн зохицуулагч байна.

7.2. Байгууллагын мэдээлэл, дүн шинжилгээний болон захиргаа удирдлагын нэгжүүд эсвэл ажил хариуцсан мэргэжилтнүүд чиг үүргийн дагуу мэдээллийн аюулгүй байдлыг хангахад дэмжиж ажиллана.

7.2. Мэдээллийн системийн зохицуулагчийн эрх

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

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

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

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

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

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

7.2.7. Байгууллагын компьютерын систем, серверт нэмэлт өөрчлөлт, шинэчлэлт, техникийн үйлчилгээг хийхэд гаднын байгууллага, мэргэжилтнийг зайлшгүй ажиллуулах тохиолдолд тухайн ажлыг гүйцэтгэх байгууллагыг сонгох үйл явцад оролцох бөгөөд ажил гүйцэтгэх явц, гүйцэтгэлд нь хяналт тавих.

7.3. Системийн зохицуулагчийн үүрэг.

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

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

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

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

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

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

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

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

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

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

НАЙМ. МЭДЭЭЛЛИЙН СИСТЕМ ХЭРЭГЛЭГЧИЙН ҮҮРЭГ, ХАРИУЦЛАГА

8.1. Мэдээллийн системд ажиллаж байгаа Биеийн тамир, спортын улсын хороо болон харьяа байгууллагуудын ажилтан, албан хаагчид энэхүү журмыг өдөр тутмын үйл зажилгаандаа мөрдлөг болгон ажиллана.

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

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

8.4. Ажлын өрөө болон хонгилд ил болон далд угсрагдсан сүлжээний утас гэмтсэн, ороцолдсон, 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 гаднын төхөөрөмжийг сүлжээнд нээж өгөхгүй байх. Хэрэв сүлжээнд нээж ажиллуулж байгаад салгасан бол сүлжээнээс хассан байх шаардлагатай.

ЕС. ХОРИГЛОХ ЗҮЙЛ

9.1.Албан хэрэгцээнээс бусад зөвшөөрөлгүй программ хангамжийг суулгаж ажиллуулах.

9.2.Интернэтээс албан ажилтай холбогдолгүй программ, дуу, кино, зураг, тоглоом зэрэг мэдээлэл татах.

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

9.4.Хариуцаж буй компьютер техник хэрэгсэлд засвар, үйлчилгээг зөвшөөрөлгүй гаднын хүнээр хийлгэх.

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

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

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

9.8.Сүлжээнд холбогдсон бусад компьютерт зөвшөөрөлгүй нэвтрэх, дундын хавтас доторх материалыг зөвшөөрөлгүй устгах.

9.9.Мэдээлэл тээгчийг өөр зориулалтаар ашиглахыг хориглох ба актлагдсан үед физик устгал хийж, устгасан тухай нотломж 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 алдагдах, мэдээллийн аюулгүй байдлын бодлого, журам зөрчигдөж, байгууллагын үйл ажиллагаанд хохирол учруулсан ба эмзэг байдал үүсгэсэн нь эрүүгийн хариуцлага хүлээлгэхээргүй бол Хөдөлмөрийн тухай хуулийн 131-р зүйлийн дагуу хариуцлага хүлээнэ.

10.2.Нууц мэдээллийг санаатай буюу санамсаргүй байдлаар бусдад задруулснаас учрах хохирлыг нөхөн төлүүлэх түүнчлэн Монгол улсын Эрүүгийн хууль, Зөрчлийн тухай хууль, Байгууллагын нууцын тухай хууль, Захиргааны хариуцлагын тухайн хууль, Хүний хувийн мэдээллийг хамгаалах тухай хуулийн зохих заалтын дагуу асуудлыг шүүхийн байгууллагаар шийдвэрлүүлнэ.

АРВАН НЭГ. БУСАД

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

12.2.Нууц ангиллын мэдээлэлтэй шууд харьцах, нууцад зэрэглэл хамаарахгүйгээр нэвтрэх албан тушаалтныг байгууллагын даргын тушаалаар томилох бөгөөд шаардлагатай тохиолдолд өөрчлөлт оруулж болно.

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

----- oo0oo -----