МОНГОЛ УЛСЫН
ҮНДЭСНИЙ СТАТИСТИКИЙН ХОРООНЫ
ДАРГЫН ТУШААЛ

2019 оны 07 сарын 10 өдөр Дугаар А/106 Улаанбаатар хот

Мэдээллийн аюулгүй байдлын журмыг
шинэчлэн батлах тухай

Монгол Улсын Статистикийн тухай хуулийн 15 дугаар зүйлийн 1 дүгээр хэсгийн 1 дэх заалт, Төрийн болон албаны нууцын тухай тухай хуулийн 30 дугаар зүйлийн 30.5 дахь заалтыг тус тус үндэслэн ТУШААХ нь:

1.Үндэсний статистикийн хорооны “Мэдээллийн аюулгүй байдлын журам”-ыг хавсралтаар шинэчлэн баталсугай.

2.Энэхүү тушаалын хэрэгжилтэд хяналт тавьж ажиллахыг Тамгын газрын дарга Ч.Цэвэгдоржид үүрэг болгосугай.

3.Мэдээллийн аюулгүй байдлын журмыг шинэчилэн баталсантай холбогдуулан Үндэсний статистикийн хорооны даргын 2008 оны 1/29 тоот тушаалыг хүчингүй болсонд тооцсугай.

ДАРГА А.АРИУНЗАЯА

000258

Үндэсний статистикийн хорооны даргын
2019 оны 07 сарын 10 өдрийн А/106 дугаар
тушаалын хавсралт

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ЖУРАМ

Нэг. Нийтлэг үндэслэл

1.1 Энэхүү журмын зорилго нь Үндэсний статистикийн хороо (цаашид ҮСХ гэх) болон нийслэл, аймаг, орон нутгийн статистикийн газар хэлтсийн үйл ажиллагаанд 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, хамгаалахад оршино.

1.2 Энэхүү журмыг Монгол Улсын “Төрийн болон албаны нууцын тухай” хууль, “Байгууллагын нууцын тухай” хууль, “Хувь хүний нууцын тухай” хууль, “Статистикийн тухай” хууль, “Харилцаа холбооны тухай” хууль, “Үндэсний статистикийн хорооны нууцын журам”, “Үндэсний статистикийн хорооны хөдөлмөрийн дотоод журам”-тай нийцүүлэн мөрдөнө.

1.3 ҮСХ болон нийслэл, аймаг орон нутгийн статистикийн хэлтэс, тэдгээрийн нийт албан хаагч ажил үүргээ гүйцэтгэхдээ энэхүү журмыг мөрдлөг болгон ажиллана.

1.4 Мэдээллийн технологийн арга техник өөрчлөгдсөн тохиолдолд энэхүү журмыг нягтлан зохих өөрчлөлт, сайжруулалтыг хийнэ.

1.5 Энэхүү журамд нэмэлт өөрчлөлт оруулах асуудлыг ҮСХ-ны даргын зөвлөлийн хурлаар (цаашид ДЗХ гэх) хэлэлцэж, ҮСХ-ны даргын тушаалаар шийдвэрлэнэ.

Хоёр. Нэр томьёоны тодорхойлолт

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 зүйлс.

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 мэдээлэл.

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 мэдээлэл.

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

2.5 Мэдээлэл хариуцагч – гэж мэдээллийг эзэмшиж байгаа ажилтны удирдах дээд албан тушаалтан.

2.6 Мэдээллийн систем - гэж байгууллагын үйл ажиллагаанд ашиглаж байгаа бүх төрлийн программ хангамж болон техник хангамж дээр суурилсан цогц үйл ажиллагаа.

2.7 Мэдээллийн аюулгүй байдал – гэж мэдээлэл, мэдээлэл боловсруулах хэрэгсэл, холбогдох дэд бүтцийн нууцлал, бүрэн бүтэн байдал, хүртээмжтэй

байдал, тасралтгүй, найдвартай ажиллагааг тодорхойлох, бий болгохтой холбоотой бүх асуудал.

2.8 Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоо (цаашид МАБУТ гэх) - гэж мэдээллийн аюулгүй байдлыг хангах, хэрэгжүүлэх, ажиллуулах, хянах, нягтлан шалгах, дэмжих, сайжруулах зорилготой байгууллагын үйл ажиллагааны тогтолцоо.

2.9 Аюул занал – гэж систем болон байгууллагад хор, хохирол учруулж болох мэдээллийн аюулгүй байдлыг ямар нэг байдлаар зөрчиж болох боломж, үйлдэл, үйл явдал.

2.10 Мэдээллийн аюулгүй байдлын зөрчил – гэж мэдээллийн аюулгүй байдлын зөрчил гарсан, аюулгүй байдалтай холбоотой ямар нэг нөхцөл байдал үүссэн гэдгийг илтгэж буй систем, үйлчилгээ, сүлжээний хэвийн байдалд нөлөөлөх аливаа тохиолдол, үйл явдал.

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

2.12 Зохицуулагч – гэж байгууллагын мэдээллийн технологи хариуцсан эрх, бүхий мэргэжилтэн, администратор.

2.13 Хэрэглэгч – гэж байгууллагын мэдээллийн системтэй харьцдаг бүх шатны албан хаагч.

2.14 Программ хангамжийн хөрөнгө – гэж зөвшөөрөлтэй хэрэглээний, мэргэжлийн болон системийн программ хангамж, өөрсдийн боловсруулсан болон тусгай захиалгаар хийлгэсэн программ хангамж, систем.

2.15 Техник хангамжийн хөрөнгө – гэж сервер компьютер, зөөврийн төхөөрөмж, сүлжээний тоног төхөөрөмж зэрэг бүх төрлийн мэдээлэл боловсруулах дамжуулах, хадгалах хэрэгсэл.

Гурав. Мэдээллийн нууцлал, ангилал

3.1 Мэдээллийг хэрэглээний зориулалтаар нь дараах байдлаар ангилна.

а/Нийтэд хүртээмжтэй: Нийтэд зориулагдсан, нууцлах шаардлагагүй мэдээлэл.

б/Байгууллага дотор нээлттэй: Байгууллагын албан хаагчдын зориулагдсан мэдээ мэдээлэл.

в/Нууц мэдээлэл: хуульд заагдсан болон тухайн байгууллагын нууцын тухай журамд тусгагдсан мэдээлэл.

3.2 Байгууллагын албан хаагчид нууц ангиллын мэдээллийг энэхүү журамд заасан арга хэлбэрээр эзэмших, ашиглах, хадгалах, хамгаалах, дамжуулах үүрэг хүлээнэ.

3.3 Хадгалагдах мэдээллийн зэрэглэлээс хамаарч өрөө тасалгаа дараах байдлаар зэрэглэн ангилна.

а/ Нээлттэй бүс
б/ Нийтэд хаалттай бүс
в/ Хаалттай бүс

Дөрөв. Мэдээллийн хамгаалалт

4.1 Мэдээллийн аюулгүй байдал нь хууль эрхзүй, дүрэм журмын хүрээнд, хамгаалалтын техник, технологийн хүрээнд, программ хангамжийн хүрээнд тус бүрдээ заавал зохицуулагдах ёстой

4.2 Мэдээлэл гаргадаг, хүлээн авдаг, боловсруулдаг, дамжуулдаг, хадгалдаг албан хаагч бүр мэдээллийг хамгаалах үүрэг хүлээнэ.

4.3 Байгууллагын үйл ажиллагааны онцлог, байрлал, өмч хөрөнгө, технологийн онцлогийн дагуу МАБУТ-ын хүрээ, хил хязгаарыг тогтоосон байна.

4.4 Мэдээллийн системийг шинээр байгуулахдаа мэдээллийн аюулгүй байдлын журамд нийцүүлэн төлөвлөж хамгаалалтыг зохицуулна.

4.5 Мэдээллийн аюулгүй байдлын чиглэлээр хэрэгжүүлэх ажлын төлөвлөгөө, гүйцэтгэлийн тайлан гаргаж ажиллана.

Тав. Биет орчны хамгаалалт

5.1 Байгууллага нь үйл ажиллагаа явуулдаг ажлын байр, бусад орчныг гадаад, дотоод эрсдэлээс хамгаалсан байх ёстой.

5.2 Серверийн өрөөг тусгай стандартын дагуу хамгаалах ёстой.

5.3 Байгууллагын гадаад, дотоод сүлжээг тусгайлан хамгаалах ёстой.

5.4 Биет орчны хамгаалалт нь сервер, ажлын компьютер бусад тоног төхөөрөмж байрлаж буй өрөө, тасалгааг аюулаас сэргийлэх зорилготой. Физик хамгаалалтыг дараах гурван бүсэд ангилж үзнэ.

а/ Нээлттэй бүс: Нийтэд мэдээллээр үйлчлэх хэсэг

б/ Нийтэд хаалттай бүс: ҮСХ болон нийслэл, аймаг орон нутгийн статистикийн хэлтэс албан хаагчид орох эрхтэй хэсэг

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

5.5 Хаалттай бүсэд нэвтрэх

а/ Зөвхөн орох эрх бүхий албан хаагч нэвтэрнэ.

б/ Орох эрхгүй этгээд нэвтрэх тохиолдолд эрх бүхий албан тушаалтнаас зөвшөөрөл авч, бүртгүүлж орно.

Зургаа. Тоног төхөөрөмжийн нууцлал, хамгаалалт

6.1 Мэдээллийн аюулгүй байдлыг хангах тусгай техник, тоног төхөөрөмжийг сүлжээ, сервер, ажлын компьютер, бусад тоног төхөөрөмжийг ашиглах үйл ажиллагаанд нэвтрүүлсэн байна.

6.2 Мэдээллийн систем болон мэдээллийн сан байршсан сервер компьютер, техник хэрэгслүүдийг газардуулгатай, хөргөлтийн системтэй, тэжээлийн нөөц эх үүсвэртэй, стандартын дагуу тохижуулсан өрөөнд байрлуулсан байна.

6.3 Компьютер, техник, тоног төхөөрөмжийг заавал гэрчилгээжүүлж байгууллагын мэдээллийн технологийн ажилтан (цаашид МТА гэх) хөтөлнө. Шинэ программ хангамж суулгах, засвар үйлчилгээ хийсэн тохиолдолд МТА болон эзэмшигч албан хаагч хоёул гарын үсэг зурж баталгаажуулна.

6.4 Компьютерт программ хангамж, техник хангамжийг суурилуулах

а/ Программ болон техник хангамжийн суурилуулалт түүний шинэчлэл, тохиргоог зөвхөн МТА хийнэ.

б/ Компьютерыг форматлан, үйлдлийн системийг дахин суулгах тохиолдолд хэрэгцээт файлуудыг өөр дискэнд хуулж, үйлдлийн системийг суулган, тохируулж, файлын хортой кодыг шалган, устгаж, буцааж хуулна.

в/ Хувийн компьютер, бусад техник хэрэгслийг албаны сүлжээ болон компьютер, техник хэрэгсэлд холбохыг хориглоно

6.5 Зөөврийн төхөөрөмж ашиглахад анхаарах зүйлс.

а/ Хулгайд алдах, эвдэрч гэмтсэний улмаас мэдээлэл алдагдахаас урьдчилан сэргийлж мэдээллийг нөөцөлнө.

б/ Зөөврийн төхөөрөмжийг албан хэрэгцээнээс бусад зориулалтаар ашиглахыг хориглоно.

в/ Зөөврийн төхөөрөмжийг албан томилолтоор авч явахдаа зориулалтын цоожлогч ашиглах, мэдээллийг кодлох хамгаалах шаардлагатай.

6.6 Байгууллагын сүлжээний байнгын ажиллагааг МТА шалгаж хариуцна. Сүлжээний кабелийн үзүүрт хаяг хийж, ашиглагдаагүй кабелийг тэмдэглэж, өөр хүн ашиглах боломжийг хаана.

6.7 Хэвлэх төхөөрөмжийн үйл ажиллагаандаа ашиглалтын хяналттай байна. Дундын хэвлэх төхөөрөмж рүү хэвлэхдээ хэрэглэгчийн эрхээр ордог байна.

6.8 Зөөврийн хадгалах төхөөрөмж дээрх мэдээллийг ашиглаж дууссаны дараа мэдээллийг устгана. Гаднаас зөөврийн хадгалах төхөөрөмж системд оруулах бол заавал хортой кодын эсрэг программ уншуулна. Зөөврийн хадгалах төхөөрөмжийг албан бусаар ашиглах бусдад дамжуулахыг хориглоно.

Долоо. Программ хангамжийн хамгаалалт

7.1 Цахим мэдээллийн нөөцлөлтийн автоматжуулсан системтэй байна.

7.2 Программ хангамжийг хууль бус гаднын халдлагаас хамгаална.

7.3 Мэдээллийн аюулгүй байдлыг хангах, аюул заналыг таслан зогсоох, илрүүлэх, хариу үйлдэл үзүүлэх зориулалтаар хамгаалалт, хяналтын техник, тоног төхөөрөмж, программ хангамжийн цогц системийг нэвтрүүлсэн байна.

7.4 Программд хортой код байгаа эсэхийг хэрэглээнд нэвтрүүлэхээс өмнө шалгана.

Найм. Мэдээллийн систем, сүлжээ, мэдээллийн сангийн хамгаалалт

8.1 Мэдээллийн систем, сүлжээ, мэдээллийн сан ашиглаж буй бүх албан хаагч аюулгүй байдлыг хангаж ажиллана.

8.2 Байгууллагын албан хаагчид өөрийн компьютер болон бусад тоног төхөөрөмж дээр эрх бүхий албан тушаалтны зөвшөөрөлгүйгээр гаднын этгээдийг ажиллуулахыг хориглоно.

8.3 Компьютерыг түгжилгүйгээр /screen lock, log off / орхиж явахыг хориглоно.

8.4 Байгууллагын албан хаагчид мэдээллийн системд нууц үгээр хандана. Нууц үгээр хандахдаа дараах дүрмийг мөрдөнө.

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 хэрэглэхгүй байх.

8.5 Нууц үг үүсгэх

а/ Том, жижиг үсэг, тоо, тусгай тэмдэгтийг хослуулан зургаа болон түүнээс дээш тэмдэгттэй байх.

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

в/ Нууц үгийг тодорхой хугацаанд буюу улиралд заавал сольдог байх.

г/ Өөрийн болон гэр бүл, төрөл төрөгсөд, ойр дотнын хүмүүсийн нэр, төрсөн он, сар, өдөр, утас, машины дугаар, зэрэг таньдаг болон судалсан хүн мэдэж болох мэдээллийг ашиглахгүй байх.

д/ Хэрэглэгчийн нэрийг давтах, түлхүүр үгээ ижил өгөх, нууц үгээ дахин хэрэглэх, хуучин нууц үгээ эргүүлэн өгөх, нүдэнд ил харагдах зүйлс/ширээ, ном, үзэг гэх мэт/ таах боломжтой үгсийг ашиглахгүй байх

е/ Гарын хөдөлгөөнөөр амархан илрүүлж болох үгс, дан буюу дараалсан тоо, үсэг /qwerty, 123456, aaasssddd гэх мэт/ тэмдэгтийг ашиглахгүй байх.

8.6 Байгууллагын мэдээллийн систем, программ хангамжийн нууц үгийн сонголт, бүртгэл, ашиглах хугацааг МТА, системийн зохицуулагч, мэдээллийн аюулгүй байдлын ажилтан нар хариуцан ажиллаж, хяналт тавина.

Ес. Лог файлын бүртгэл

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

9.2 Лог файлын бүртгэл, үнэн зөв, бүрэн байдлыг системийн зохицуулагч хариуцна. Лог мэдээллийг 6 сар тутам нөөцөлж, 2 жилийн дараа нягтлан шинжилсний дараа системийн зохицуулагч устгана.

Арав. Хандалтын удирдлага

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

10.2 Албан хаагчид мэдээллийн санд нэвтрэх эрхийг эрх бүхий албан тушаалтны ирүүлсэн зөвшөөрлийг үндэслэн системийн зохицуулагч нээж өгнө.

10.3 Албан хаагчийн ажлын чиг үүргээс хамаарч мэдээллийн санд хандах эрхийн түвшин ялгаатай байна.

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

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

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

10.4 Нэвтрэх эрхийг цуцлах

а/ Байгууллагын хүний нөөцийн нэгж мэдээллийн системд хандах эрх бүхий албан хаагчийг ажлаас чөлөөлөх буюу өөрчлөгдсөн тухай системийн зохицуулагчид мэдэгдсэний дагуу нэвтрэх эрхийг цуцална.

б/ Мэдээллийн системд нэвтрэх эрх бүхий албан хаагч мэдээллийн аюулгүй байдлын бодлого, журмыг зөрчсөн тохиолдолд системд нэвтрэх эрхийг системийн зохицуулагчийн зүгээс түдгэлзүүлж болно.

10.5 Байгууллагад гаднаас урт, богино хугацаагаар ажиллах бүх төрлийн зочин, дадлагажигч, түр ажилтныг интернэтийн сүлжээгээр хангахаас бусад төрлийн систем, дотоод сүлжээ, нууц мэдээллийн санд хандуулахыг хориглоно.

Арван нэг. Цахим баримт бичиг боловсруулах, хадгалах

11.1 Албан хаагч нь цахим баримт бичиг боловсруулахдаа **цахим хэлбэрээр албан хэрэг хөтлөх нийтлэг журмыг** мөрдлөг болгоно.

11.2 Албан хаагч нь тухайн ажлын байртай холбогдох бичиг баримтыг төрөлжүүлж, өөрийн компьютерт нөөцлөн шаардлагатай бол зөвшөөрөгдсөн бусад санд хадгална.

11.3 Албан хаагч нь албан хэрэгцээний файлаа нэр төрлөөр нь ангилж, хавтас үүсгэн хадгална. Шаардлагатай бол дэд хавтас үүсгэн хадгалж, хэрэглэж хэвшинэ.

11.4 Албан хаагч жил тутмын эхний улиралд нууцын эрхлэгч, архивын ажилтанд өмнөх оны хадгалагдсан файл, хавтсаа байгууллагын мэдээллийн цахим санд хадгалуулах зорилгоор хүлээлгэн өгнө.

11.5 Нууцын эрхлэгч, архивын Албан хаагч нь хүлээн авснаас долоо хоногийн дотор байгууллагын мэдээллийн цахим санд хадгална. Ингэхдээ тэмдэглэлийг заавал хөтөлнө.

Арван хоёр. Хортой кодоос хамгаалах

12.1 Байгууллагын хэрэгцээнд хэрэглэгдэж байгаа компьютер, мэдээлэл хадгалагч зөөврийн хэрэгслүүдэд зөвшөөрөгдсөн хортой кодын эсрэг программ хангамжийг ашиглана.

12.2 Хортой кодын эсрэг программын шинэчлэлтийг тогтмол хийнэ. Тодорхой хугацаанд системийн хортой кодын эсрэг программыг уншуулж, илэрсэн тохиолдолд арилгах арга хэмжээг авна.

12.3 Гаднын төхөөрөмж мэдээллийн системд оруулах бол сүлжээнд холбохоос өмнө хортой кодын шинжилгээг заавал хийсний дараа системд нэвтрүүлнэ.

Арван гурав. Мэдээллийн нөөцлөлт, хадгалалт

13.1 Мэдээллийн аюулгүй байдлын үүднээс мэдээллийн систем, мэдээллийн санг хадгалах, нөөцлөх, архивлах, устгах арга хэмжээ тогтмол хийнэ.

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

13.3 Байнгын өөрчлөгддөг мэдээллийн сангийн өөрчлөлтийг тогтоосон хугацаанд серверт байрлуулна.

13.4 Серверт хадгалагдах өгөгдлийн нэрийг латин үсгээр галиглан бичсэн байна.

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

а/ Байнга хадгалах: Байнгын хэрэгцээнд зориулагдсан мэдээллийн сан, мэдээллийг серверт тусгай хавтаст хадгална. Мөн заавал нөөц хувь үүсгэн хадгална.

б/ Түр хадгалах: Түр хадгалагдах мэдээллийг хадгалах хугацаа дууссан тохиолдолд эрх бүхий албан тушаалтны зөвшөөрлөөр устгаж тэмдэглэл хөтөлнө.

13.6 Мэдээллийн системээс мэдээллийг устгахдаа дахин сэргээгдэхгүй байдлаар устгана.

Арван дөрөв. Мэдээллийн аюулгүй байдлын албан хаагч

14.1 Мэдээллийн аюулгүй байдлын ажилтны эрх, үүрэг

а/ Ажил үүргийн хуваарийн дагуу мэдээллийн аюулгүй байдлыг шалгах, эмзэг байдлыг бууруулах зорилгоор мэдээллийн системд нэвтрэх эрхтэй.

б/ Мэдээллийн аюулгүй байдлыг хангах, шаардлагад нийцүүлэн мэдээллийг хамгаалах системийг бий болгох, түүний ажлын горимыг боловсруулах. Мэдээллийн аюулгүй байдлыг хангахад шаардагдах мэргэжил дээшлүүлэх сургалтад байнга хамрагдах эрхтэй.

в/ Байгууллагын мэдээллийн системд заналхийлж буй халдлагыг бүртгэх, илрүүлэх, таслан зогсоох болон эмзэг байдлыг тогтоох, бууруулах, аюулгүй байдлын бодлого боловсруулах зорилгоор мэдээллийн аюулгүй байдлыг хангах үүрэгтэй.

г/ Эрсдэлийн үнэлгээг жил тутам хийж мэдээллийн аюулгүй байдлын эмзэг байдлыг тодорхойлох, хамгаалалтын төвшнийг тогтоох, хөндлөнгийн хяналтыг хэрэгжүүлэх үүрэгтэй.

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

е/ Систем болон үйлчилгээнд ажиглагдсан байж болох сул талд анхаарлаа хандуулах, түүний тухай мэдээлэх, компьютерын нэр, сүлжээний нэрийг солихгүй байх. Шаардлага гарсан тохиолдолд системийн зохицуулагчид мэдэгдэн зохих үйлчилгээг хийлгэх үүрэгтэй.

14.2 Системийн зохицуулагчийн эрх, үүрэг

а/ Ажил үүргийн хуваарийн дагуу зөвхөн мэдээллийн аюулгүй байдлыг шалгах, эмзэг байдлыг бууруулах зорилгоор мэдээллийн систем, ажилтнуудын компьютерт нэвтрэх эрхтэй.

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

в/ Аюулгүй байдлын журмын зөрчсөн албан хаагчид байгууллагын дотоод журмын дагуу хариуцлага тооцно.

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

д/ Байгууллагын компьютер, 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 эрхтэй.

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

ё/ Мэдээллийн системийг байгуулах, турших, ашиглах, засвар үйлчилгээг хийх, хэвийн үйл ажиллагааг хангах үүрэгтэй.

ж/ Мэдээллийн сан, программ хангамж, компьютерыг хортой кодоос хамгаалах, мэдээллийн аюулгүй байдлыг хангахад чиглэсэн сургалт, сурталчилгааг байгууллагад зохион байгуулах үүрэгтэй.

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

и/ Байгууллагын сервер, дагалдах тоног төхөөрөмж, хэрэгслүүдийн ажиллагаа, шинэ тоног төхөөрөмжийн суурилуулалтыг хариуцах үүрэгтэй.

л/ Системийн зохицуулагч нь ажил үүргийн дагуу олгосон эрхээ буруугаар ашиглахгүй байх үүрэгтэй.

Арван тав. Нийт албан хаагчдын эрх, үүрэг, хориглох зүйлс

15.1 Мэдээллийн аюулгүй байдалтай холбоотой эрсдэл гарсан тохиолдолд системийн зохицуулагчид тухай бүр мэдэгдэх үүрэгтэй.

15.2 Аюулгүй байдлын горимыг мөрдөж ажиллахыг шаардах, зөрчигдсөн үед зөрчлийг арилгуулах санал өгөх эрхтэй.

15.2 Мэдээллийн аюулгүй байдлыг хангах зорилгоор хийж буй системийн зохицуулагчийн шаардлагыг биелүүлэх.

15.3 Зөвшөөрөлгүй программ хангамж суулгаж, ажиллуулахыг хориглоно.

15.4 Байгууллагын бус компьютер, зөөврийн хэрэгслийг сүлжээнд зөвшөөрөлгүй холбохыг хориглоно.

15.5 Ажлын өрөө солих, байрлалаа шилжүүлэх тохиолдолд дур мэдэн өөрийн компьютерт тохируулсан сүлжээний тохиргоог өөрчлөхийг хориглоно.

15.6 Ккомпьютер, түүний дагалдах төхөөрөмжийг албан бус хэрэгцээнд (тоглоом тоглох, нийгмийн сүлжээ, интернэтээр ажилд холбоогүй мэдээ мэдээлэл үзэх гэх мэт) ашиглахыг хориглоно.

15.7 Өөрийн компьютерт ажлын шаардлагагүй дундын хавтас сүлжээнд нээхийг хориглоно.

15.8 Мэдээлэл хадгалж буй төхөөрөмжийг өөр зориулалтаар ашиглахыг хориглох ба актлагдсан үед физик устгал хийж, устгасан тухай акт үйлдэх үүрэгтэй.

15.9 Албаны цахим шуудан хаягийг нийтийн сүлжээ, цахим худалдааны сайт зэрэгт бүртгүүлэхгүй байх ба зөвхөн албан хэрэгцээнд ашиглах үүрэгтэй.

15.10 Нийт албан хаагч, эрх бүхий албан тушаалтан чиг үүргийнхээ дагуу мэдээллийн аюулгүй байдлыг хангахад дэмжиж ажиллана.

Арван зургаа. Хариуцлага

16.1 Албан хаагчийн анхаарал болгоомжгүй үйлдлээс болж гадаад, дотоод сүлжээ, мэдээллийн сан, системийн аюулгүй байдал алдагдах, мэдээллийн аюулгүй байдлын бодлого, журам зөрчиж, байгууллагын үйл ажиллагаанд хохирол учруулсан ба эмзэг байдал үүсгэсэн нь эрүүгийн хариуцлага хүлээлгэхээргүй бол байгууллагын дотоод журамд заасны дагуу хариуцлага тооцно.

16.2 Нууц мэдээллийг санаатай буюу санамсаргүй байдлаар бусдад задруулснаас учрах хохирлыг нөхөн төлүүлэх түүнчлэн Монгол улсын Эрүүгийн хууль, Захиргааны хариуцлагын тухайн хууль, Байгууллага, хувь хүний нууцын тухай хуулийн зохих заалтын дагуу асуудлыг шүүхийн байгууллагаар шийдвэрлүүлнэ.

16.3 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 байгууллагын дотоод журамд заасны дагуу арга хэмжээ авна.

---oOo--