Мэдээллийн аюулгүй байдлыг хангах үйл ажиллагааны дотоод журам 2023

БҮСИЙН ОНОШИЛГОО ЭМЧИЛГЭЭНИЙ ТӨВИЙН КИБЕР БОЛОН МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ХАНГАХ ҮЙЛ АЖИЛЛАГААНЫ ДОТООД ЖУРАМ

Хувилбарын дугаар:1
Хүчин төгөлдөр болсон огноо: 2023-10-25
Баримт бичгийн дугаар:01

Баримт бичгийг хариуцах нэгж	Нийт тасаг, нэгжүүд		
Баримт бичгийн нууцлалын зэрэглэл	Дотоод	Баримт бичгийн түвшин	3
	Овог нэр	Албан тушаал	Гарын үсэг
Боловсруулсан.	Ц.Лувсандамдин Б.Эрдэнэзул	ЭМТҮЧАБАлбаны дарга Хөдөлмөрийн аюулгүй байдал, орчны эрсдэлийн менежер	
Санал өгсөн	Д.Баянмөнх	Үйл ажиллагаа эрхэлсэн дэд захирал	
Хянаж баталсан	Г.Дашжанцан	БОЭТөвийн захирал	

Баримт бичгийн өөрчлөлтийн бүртгэл

Хувилбарын дугаар	**Хүчин төгөлдөр болсон огноо**	**Өөрчлөлтийг батласан албан тушаалтан**	**Өөрчлөлтийн утга** (баримт бичигт ямар өөрчлөлт орсоныг товч тайлбарлана)
1			
2			
3			
4			
5			
6			

АГУУЛГА

КИБЕР БОЛОН МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ҮЙЛ АЖИЛЛАГААНЫ ДОТООД ЖУРАМ

Нэг. Нийтлэг үндэслэл.

1.1 Өвөрхангай аймаг дахь Бүсийн оношилгоо эмчилгээний төвийн кибер болон мэдээллийн аюулгүй байдлын удирдлагын тогтолцоог бий болгох, мэдээ, мэдээлэл, сүлжээ, системийн тасралтгүй, найдвартай ажиллагаа, мэдээллийн сангийн нууцлал, аюулгүй байдлыг хангах, гаднаас болон дотоодоос учирч болох халдлага, аюул заналаас урьдчилан сэргийлэх, хор хохирол, эрсдэл учирсан тохиолдолд нэн даруй шаардлагатай арга хэмжээг авахтай холбогдсон харилцааг энэхүү журмаар зохицуулна.

1.2 Энэхүү журмын зорилго нь Мэдээллийн аюулгүй байдлын тогтолцоог бий болгохдоо “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: мэдээллийн холбооны технологийн аюулгүй байдлын үндсэн ойлголтууд болог загварууд- MNS ISO/IEC 13335-1:2009, Мэдээллийн технологи-Аюулгүй байдлын арга техник-мэдээллийн аюулгүй байдлын эрсдлийн удирдлага-MNS 5969:2009, Мэдээллийн технологи-Аюулгүй байдлын арга техник-мэдээллийн аюулгүй байдлын удирдлагын тогтолцооны шаардлага –MNS ISO/IEC27001:2009 стандартуудыг мөрдөж, бүсийн оношилгоо эмчилгээний төвийн мэдээллийн аюулгүй байдлыг хангах, эрсдлээс урьдчилан сэргийлэхэд оршино.

1.3 Бүсийн оношилгоо эмчилгээний төвийн мэдээллийн системд ажиллаж байгаа бүх эмч, эмнэлгийн мэргэжилтэн, бусад албан хаагчид, гэрээт албан хаагчид энэхүү журмыг өдөр тутмын үйл ажиллагаандаа мөрдөж ажиллана.

1.4 Энэхүү журамд хэрэглэсэн дараах нэр томъёог дор дурдсан утгаар ойлгоно.

1.4.1 "кибер аюулгүй байдал" гэж кибер орчинд мэдээллийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй байдал хангагдсан байхыг;

1.4.2 "кибер орон зай" гэж интернэт болон бусад мэдээлэл, харилцаа холбооны сүлжээ, тэдгээрийн ажиллагааг хангах мэдээллийн дэд бүтцийн харилцан хамааралтай цогцоос бүрдсэн биет болон биет бус талбар;

1.4.3 "кибер орчин" гэж мэдээлэлд хандах, нэвтрэх, цуглуулах, түүнийг боловсруулах, хадгалах, ашиглах боломж олгож байгаа мэдээллийн систем, мэдээллийн сүлжээний орчныг;

1.4.4 "бүрэн бүтэн байдал" гэж мэдээллийг зөвшөөрөлгүй устгах, өөрчлөхөөс хамгаалсан байхыг;

1.4.5 "нууцлагдсан байдал" гэж мэдээлэлд зөвшөөрөлгүй хандах, нэвтрэх боломжгүй байхыг;

1.4.6 "хүртээмжтэй байдал" гэж зөвшөөрөгдсөн хүрээнд мэдээлэлд хандах, нэвтрэх, цуглуулах, ашиглах боломжтой байхыг;

1.4.7 "мэдээллийн систем" гэж Нийтийн мэдээллийн ил тод байдлын тухай хуулийн 4.1.1-д заасныг;

1.4.8 "мэдээллийн сүлжээ" гэж Нийтийн мэдээллийн ил тод байдлын тухай хуулийн 4.1.2-т заасныг;

1.4.9 "кибер аюулгүй байдлын эрсдэлийн үнэлгээ" гэж цахим мэдээлэл, мэдээллийн систем, мэдээллийн сүлжээний кибер аюулгүй байдал алдагдах, аюул занал тохиолдох магадлал, эмзэг байдлын түвшин, түүнээс үүсэх үр дагавар, эрсдэлийг бууруулах, урьдчилан сэргийлэх арга хэмжээг тодорхойлох мэргэшсэн үйл ажиллагааг;

1.4.10 "мэдээллийн аюулгүй байдлын аудит" гэж кибер аюулгүй байдлын хууль тогтоомж, холбогдох журам, стандартад нийцсэн эсэхэд дүгнэлт гаргах, зөвлөмж өгөх хараат бус хөндлөнгийн мэргэжлийн үйл ажиллагааг;

1.4.11 "мэдээллийн системийн үйлдлийн бүртгэл" гэж тухайн мэдээллийн системд хандсан, нэвтэрсэн, боловсруулсан, цуглуулсан, ашигласан үйлдэл, цаг хугацааг тодорхойлох бүртгэлийг;

1.4.12 "онц чухал мэдээллийн дэд бүтэцтэй байгууллага" гэж кибер аюулгүй байдал алдагдсанаар хэвийн үйл ажиллагаа нь доголдож Монгол Улсын үндэсний аюулгүй байдал, нийгэм, эдийн засагт хохирол учруулж болох мэдээллийн систем, мэдээллийн сүлжээ бүхий байгууллагыг;

1.4.13 "кибер аюулгүй байдлын зөрчил" гэж мэдээллийн системийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй байдалд заналхийлж байгаа аливаа үйлдэл, эс үйлдлийг;

1.4.14 "кибер халдлага" гэж мэдээллийн систем, мэдээллийн сүлжээний кибер аюулгүй байдлыг алдагдуулах зорилго бүхий үйлдлийг;

1.4.15 "үндэсний хэмжээний кибер халдлага" гэж онц чухал мэдээллийн дэд бүтэцтэй байгууллагын мэдээллийн систем, мэдээллийн сүлжээнд халдсаны улмаас тухайн байгууллагын хэвийн үйл ажиллагааг алдагдуулж, Монгол Улсын үндэсний аюулгүй байдал, нийгэм, эдийн засагт хохирол учруулахуйц кибер халдлагыг;

1.4.16 "кибер халдлага, зөрчилтэй тэмцэх төв" гэж кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, илрүүлэх, таслан зогсоох, хариу арга хэмжээ авах, мэдээллийн системийг нөхөн сэргээх үйл ажиллагааг зохицуулж, мэргэжлийн удирдлагаар хангах үндсэн чиг үүрэг бүхий этгээдийг;

1.4.17 "төрийн мэдээллийн нэгдсэн сүлжээ" гэж төрийн байгууллага хоорондын мэдээлэл солилцох, кибер аюулгүй байдлыг хангахад чиглэсэн нэгдсэн дэд бүтэц бүхий төрийн интернэт хэрэглээ, албан болон тусгай хэрэглээний сүлжээний цогцыг;

1.4.18 "төрийн өмчит хуулийн этгээд" гэж Төрийн болон орон нутгийн өмчийн тухай хуулийн 13 дугаар зүйлд заасныг.

1.4.19 “байгууллагын мэдээлэл” гэж ямар хэлбэрээр оршин байгаагаас үл хамааран уншиж ойлгож болох бүх төрлийн баримт бичиг, өгөгдлийг хэлнэ.

1.4.20 “Эд хөрөнгө” гэж байгуллага өөрөө мэдэж захиран зарцуулах эрхтэй, байгууллагад үнэ цэнэтэй биеь болон биет бус эд зүйлийг хэлнэ.

1.4.21 “мэдээлэл эзэмшигч” гэж албан ажлаа гүйцэтгэх явцдаа аливаа мэдээллийг олж мэдсэн, танилцсан, тухайн мэдээллийг эзэмшиж байгаа албан хаагчийг хэлнэ.

1.4.22 “мэдээлэл хариуцагч” гэж мэдээллийг эзэмшиж байгаа ажилтан болон дээд албан тушаалтныг хэлнэ.

1.4.23 “кибер болон мэдээллийн аюулгүй байдал хариуцсан мэргэжилтэн” гэж байгууллагын мэдээллийн аюулгүй байдал, мэдээллийн технологийн үйл ажиллагааны хэвийн нөхцлийг хангах чиг үүрэгтэй албан хаагчийг хэлнэ.

1.4.24 “хэрэглэгч” гэж байгууллагын мэдээлэл, мэдээллийн системд хандах эрх бүхий албан хаагчийг хэлнэ.

1.4.25 “зохицуулагч” гэж байгууллагын мэдээллийн технологи хариуцсан эрх, үүрэг бүхий мэргэжилтэн админ, IT инженерийг хэлнэ.

1.4.26 “Мэдээллийн аюулгүй байдал” гэж мэдээллийн нууцлал, бүрэн бүтэн, хүртээмжтэй байдлыг хадгалах зорилгоор мэдээллийн бодит байдал, эх хувь, хариуцлагатай, тасралтгүй найдвартай байдал зэрэг бусад шинжүүдийг хэлнэ.

1.4.27 “мэдээллийн аюулгүй байдлын тогтолцоо” гэж мэдээллийн аюулгүй байдлыг хангах, хэрэгжүүлэх хянах, дэмжих, сайжруулахын тулд систем, программ

хангамж, тоног төхөөрөмж, тэдгээртэй ажиллах дүрэм, журам, ажилтнуудын харилцан үйл ажиллагааны үр дүнд бий болсон цогц үйл ажиллагааг хэлнэ.

1.4.28 “аюул занал” гэж байгууллагын үйл ажиллагааг алдагдуулах, мэдээллийн аюулгүй байдалд заналхийлэх бодит боломжтой, гэнэтийн эсвэл дэс дараалсан аюулыг хэлнэ.

Хоёр. Байгууллагын мэдээллийн аюулгүй байдлын тогтолцоонд хамаарах мэдээлэл

2.1 Байгууллагын мэдээллийг биет болон биет бус гэж 2 ангилна.

2.2. Биет мэдээлэл гэдэгт дараах төрлийн мэдээллийг хамааруулна.

2.2.1 Эрх зүйн баримт бичиг, үндсэн болон нэмэлт үйл ажиллагааны хүрээнд боловсруулсан болон цуглуулсан мэдээлэл, тайлан, төлөвлөгөө, төсөл хөтөлбөр, бүртгэлийн мэдээлэл, сургалтын материал, тараах хуудас, гарын авлага, хэвлэмэл зураг зэрэг бүх төрлийн цаасан суурьт мэдээллүүд

2.2.2 Биет байдлаар оршин буй бусад төрлийн мэдээллүүд

2.3 Биет бус мэдээлэл гэдэгт дараах төрлийн мэдээллийг хамааруулна.

2.3.1 Биет мэдээллийн цахим хэлбэр, өгөгдлийн сан, файлын сан, цахим шуудан, дүрс бичлэг, дуу бичлэг зэрэг мэдээллүүд

2.3.2 Бусад төрлийн цахим мэдээллүүд

2.4 Байгууллагын мэдээллийн аюулгүй байдлын тогтолцоонд хамаарах эд хөрөнгө гэдэгт дараах эд хөрөнгийг хамааруулна.

2.4.1 Хэрэглээний болон тусгай зориулалтын программ хангамж, системүүд

2.4.2 Өөрсдийн хөгжүүлсэн болон тусгай захиалгаар өөр этгээдээр хөгжүүлэлт хийлгэсэн программ хангамж, системүүд

2.4.3 Серверийн болон оффисын хэрэглээний компьютер, тоног төхөөрөмжүүд (сервер, процессор, дэлгэц, хэвлэгч, хувилагч, скайнер, зөөврийн компьютер, телефон, факсын аппарат, зөөврийн хард диск, флаш, CD)

2.4.4 Сүлжээний тоног төхөөрөмжүүд (файрвол, рутер, свич, салаалагч, сүлжээний утас)

2.4.5 Серверийн үйл ажиллагааг дэмжих тоног төхөөрөмжүүд (хөргүүр, тог баригч, нөөц тэжээлийн үүсгүүр)

Гурав. Мэдээллийн ангилал

3.1 Байгууллагын мэдээллийг хэрэглээний зориулалт, нууцлалаас хамаарч дараах байдлаар ангилна.

3.1.1 Нийтэд хүртээмжтэй мэдээлэл: Хувилах, хадгалах, дамжуулахад ямар нэгэн шаардлага тавихгүй нийтэд зориулагдсан, нууцлах шаардлагагүй, “Мэдээллийн ил тод байдал ба мэдээлэл авах эрхийн тухай” хуульд зааснаар иргэн, аж ахуйн нэгжид саадгүй олгох мэдээллүүд

3.1.2 Байгууллага дотор нээлттэй мэдээлэл: Байгууллагын бүх эмч, эмнэлгийн мэргэжилтэн, албан хаагчдад зориулагдсан, байгууллагын үндсэн болон нэмэлт үйл ажиллагаатай холбоотой, байгууллага дотор нээлттэй, гадагш задруулахгүй байх мэдээллүүд

3.1.3 Байгууллага дотор хаалттай мэдээлэл: Байгууллагын эмч, эмнэлгийн мэргэжилтэн, албан хаагчид тодорхой эрхийн хүрээнд хязгаарлалттайгаар ашиглах боломжтой, байгууллагын үндсэн болон нэмэлт үйл ажиллагаатай холбоотой, гадагш задруулахгүй, “Хувь хүний нууцын тухай”, “Төрийн болон албаны нууцын тухай” болон “Байгууллагын нууцын тухай” хуулиар хамгаалагдсан мэдээллүүд

3.1.4 Албаны нууц мэдээлэл: Байгууллагын албаны нууц мэдээллийг хадгалах, хамгаалах, аюулгүй байдлыг хангах асуудлыг энэ журмаар зохицуулна.

3.1.5 Цахим хэлбэрээр оршин буй албаны нууц мэдээллийг хариуцагч, эзэмшигч, хэрэглэгчтэй нууц хадгалах баталгааг **“Нууц хадгалах баталгаа”** Маягт №1-н дагуу, байгууллагын нууц мэдээллийг хариуцагч, эзэзмшигч, хэрэглэгчийн жагсаалтыг Маягт №2-оор баталгаажуулна.

3.1.6 Албаны нууц мэдээллийг хадгалж буй өрөө тасалгаанд нэвтрэх эрхийг тухайн нууц мэдээллийг хариуцагч олгох бөгөөд Маягт №2-оор баталгаажуулна.

Дөрөв. Байгууллагын мэдээллийн хамгаалалт

4.1 Байгууллагын мэдээллийг бүрдүүлдэг, дамжуулдаг, хадгалдаг албан хаагч бүр мэдээллийг хамгаалах үүрэг хүлээнэ.

4.2 Байгууллага нь мэдээллийн аюулгүй байдлыг хангах чиглэлийн ажлыг тогтмол зохион байгуулж, зардлыг төлөвлөн жил бүрийн төсөвт суулгаж батлуулах

4.3 Байгууллагын нийтэд хүртээмжтэй мэдээллийг эзэмшигч, хариуцагч нь тухайн мэдээллийг авахыг хүссэн иргэн, аж ахуйн нэгжид саадгүй гаргаж өгөх ба байгууллагын мэдээллийн самбар, цахим хуудас бусад мэдээллийн сувгуудад ил тод байршуулна.

4.4 Байгууллага дотор нээлттэй мэдээллийг эзэмшигч, хариуцагч нь мэдээллийн хадгалалт, хамгаалалт аюулгүй байдлыг бүрэн хариуцаж, мэдээллийг зөвхөн байгууллагын ажилтан, албан хаагчдад саадгүй гаргаж өгөх ба байгууллагын үйл ажиллагаанд харшлахгүй бол иргэд, аж ахуйн нэгж, бусад төрийн байгууллагад харьяалах нэгжийн даргын зөвшөөрснөөр гаргаж өгнө.

4.5 Байгууллага дотор хаалттай мэдээллийг эзэмшигч, хариуцагч нь мэдээллийн хадгалалт, хамгаалалт аюулгүй байдлыг бүрэн хариуцаж, мэдээллийг байгууллагын эмч, эмнэлгийн мэргэжилтэн, албан хаагчдад харъяалах нэгжийн даргын зөвшөөрснөөр гаргаж өгнө. Байгууллага дотор хаалттай мэдээллийг дээд удирдлагын зөвшөөрснөөр бусад төрийн байгууллага, аж ахуйн нэгжид гаргаж өгнө.

4.6 Албаны нууц мэдээллийг хадгалах, хамгаалах асуудлыг “Байгууллагын нууц хамгаалах тухай” хуулиар болон энэхүү журмаар зохицуулна.

4.7 Байгууллага дотор хаалттай болон албаны нууц ангиллын мэдээллийн хадгалалт, хамгаалалт, дамжуулах үйл ажиллагаанд мэдээлэл хариуцагч, эзэзмшигч болон системийн зохицуулагч хяналт тавьж ажиллах бөгөөд энэхүү журмыг зөрчсөн, алдаа дутагдал илэрсэн тохиолдолд заавар зөвлөмж өгөх, засаж сайжруулах талаар арга хэмжээ авч байгууллагын удирдлагад мэдэгдэж ажиллана.

4.8 Физик орчинд мэдээллийг дараах байдлаар хамгаална.

4.8.1 Физик хамгаалалтыг 3 бүсэд ангилж үзнэ.

А) Нээлттэй бүс-Нийтэд мэдээллээр үйлчлэх хэсэг (лавлагаа, мэдээлэл, зөвшөөрөл өгөх өрөө, цахим үйлчилгээ, уулзалтын өрөө зэрэг орно)

Б) Нийтэд хаалттай бүс-Зөвхөн тухайн байгууллагын эмч, эмнэлгийн мэргэжилтэн, албан хаагчид орох эрхтэй хэсэг (ажлын өрөө, эмчийн өрөө, цахилгааны өрөө гэх мэт)

В) Хаалттай бүс-Зөвхөн эрх бүхий эмч, эмнэлгийн мэргэжилтэн, албан хаагчид нэвтрэх эрхтэй хэсэг (серверийн өрөө, нууцын өрөө, архивын өрөө гэх мэт)

4.8.2 Нээлттэй, нийтэд хаалттай, хаалттай бүсэд байршуулсан мэдээ, мэдээлэл, тоног төхөөрөмж бусад зүйлсийн аюулгүй байдлыг тухайн бүсийг хариуцах үүрэг бүхий эмч, эмнэлгийн мэргэжилтэн, албан хаагч энэ журмын дагуу хангаж ажиллана.

4.8.3 Нээлттэй бүсэд зөвхөн нийтэд хүртээмжтэй мэдээллийг ил байршуулна.

4.8.4 Нийтэд хаалттай бүсэд байгууллага дотор нээлттэй болон нууцлалтай мэдээллийг хадгална. Аюул занал, учирч болох эрсдлээс 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 албан хаагчийн зөвшөөрлөөр түүний хяналт дор гадны этгээдийг нэвтрүүлнэ.

4.8.5 Хаалттай бүсэд албаны нууц мэдээллийг хадгалах бөгөөд зөвхөн тухайн мэдээллийг хариуцагч, эзэмшигч буюу нэвтрэх эрх бүхий албан тушаалтан нэвтэрнэ. Аюул занал, учирч болох эрсдлээс 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.

4.8.6 Серверийн өрөөнд нэвтрэх эмч, эмнэлгийн мэргэжилтэн, албан хаагчдын жагсаалтыг Маягт №2-н дагуу гаргаж, IT инженер, нэгжийн дарга батална.

4.8.7 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 хариуцан хийнэ. Засвар үйлчилгээг тогтмол хийх төлөвлөгөөг баталж мөрдөж ажиллана.

Тав. Тоног төхөөрөмж, сүлжээний нууцлал, хамгаалалт

1.1 Байгууллагын тоног төхөөрөмж, мэдээллийн сан, сүлжээг эзэмшигч, хариуцагч, IT инженерүүд нь тэдгээрийг аюул заналаас хамгаалах, эрсдлээс урьдчилан сэргийлэх зорилгоор энэ журамд заасан болон бусад бүхий л шаардлагатай арга хэмжээг авч ажиллах үүрэгтэй.

1.2 Байгууллага нь албаны хэрэгцээнд ашиглагдаж байгаа компьютер, техник хэрэгслийг заавал гэрчилгээжүүлсэн байна. Гэрчилгээг байгууллагын IT инженер хөтлөх бөгөөд шинэчлэл, өөрчлөлт, засвар, үйлчилгээ хийсэн, шинэ программ хангамж суулгасан тохиолдолд тухайн ажлыг гүйцэтгэсэн албан хаагч болон компьютер, техник хэрэгсэлийг эзэмшигч нар гарын үсэг зурж баталгаажуулна.

1.3 Программ хангамж, техник хангамжийг суурилуулах

1.3.1 Программ болон техник хангамжийн суурилуулалт түүний шинэчлэл, тохиргоог зөвхөн IT инженер хийж гүйцэтгэнэ.

1.3.2 Компьютер тоног төхөөрөмж эзэмшигч нь IT инженерийн зөвшөөрөлгүйгээр дур мэдэн программ хангамж шинээр суулгах, программ хангамжид өөрчлөлт, шинэчлэлт хийх, техник хангамжид өөрчлөлт, засвар, үйлчилгээ хийхийг хориглоно.

1.3.3 IT инженер аливаа компьютерыг форматлан үйлдлийн системийг дахин суулгах тохиолдолд хэрэгцээт файлуудыг өөр хард дискэнд хуулж, үйлдлийн системийг суулгаж тохируулга хийсний дараа файлын вирусыг шалган, устгаж буцааж хуулна.

1.3.4 IT инженер нь систем, техник хангамж суурилуулах, шинэчлэх, өөрчлөх, засвар үйлчилгээ хийхдээ тухайн систем, техник хангамжийн үндсэн үүрэг, үйл ажиллагааг алдагдуулахгүй байхаар чанартай гүйцэтгэнэ.

1.3.5 Программ хангамж, техник хангамжийг суурилуулах, шинэчлэх, өөрчлөлт оруулах, засвар, үйлчилгээ хийх бүрд энэ журмын 6.2-т зааснаар гэрчилгээнд тэмдэглэл хийж баталгаажуулна.

1.4 Компьютер тоног төхөөрөмж ашиглах

1.4.1 Байгууллагын эмч, эмнэлгийн мэргэжилтэн, албан хаагчид өөрийн эзэмшиж буй компьютер, хэвлэгч, хувилагч болон бусад тоног төхөөрөмжийг зөвхөн зориулалтын дагуу албан ажлын хэрэгцээнд ашиглана. Гадны этгээдэд зөвшөөрөлгүйгээр компьютер, тоног төхөөрөмжийг ашиглуулахыг хориглоно.

1.4.2 Суурин болон зөөврийн компьютер нь энэ журмын 5.9-д заасны дагуу заавал нэвтрэх нууц үгтэй байна.

1.4.3 Суурин болон зөөврийн компьютерт зөвхөн албан ажлын хэрэгцээний мэдээллийг хадгалах бөгөөд хувийн мэдээллүүд (кино, зураг, дүрс бичлэг, дуу бусад файл гэх мэт)-ийг хадгалахыг хориглоно. Албан ажлын хэрэгцээнд чухал шаардлагатай мэдээллийг устгах эрсдлээс сэргийлж заавал хуулбарыг үүсгэн зөөврийн болон дундын хадгалах төхөөрөмжид байршуулна.

1.4.4 Эмч, эмнэлгийн мэргэжилтэн, албан хаагчдын албаны компьютерт мэдээллийн аюулгүй байдлын аюул эрсдэл учирч болзошгүй эсвэл учирсан гэж үзвэл IT инженерт мэдэгдэнэ.

1.4.5 Түр хугацаагаар гарах бол компьютерыг заавал түгжих буюу нууц үгээр хамгаалагдсан дэлгэцийн хамгаалалтыг ажиллуулна. Ажлын цаг дуусаж, албан хаагч явахдаа компьютер, тоног төхөөржмүүдийг унтрааж, цахилгааны хүчдэлээс салгана.

1.4.6 Албан өрөөнд дундаа ашигладаг хэвлэх, хувилах төхөөрөмжийг хяналттай байлгаж, тэдгээрийг ашиглахад тодорхой эрхийн хязгаарлалт хийж өгнө.

1.4.7 Байгууллагын мэдээллийн сан, системүүд ажиллаж буй сервер компьютерыг зориулалтын хөргүүр, чийгшүүлэгч, хяналтын камер, нэмэлт цахилгааны үүсгүүр бүхий серверийн тусгай зориулалтаар тохижуулсан өрөөнд хаалттай бүсэд байрлуулна.

1.4.8 Сервер компьютер нь энэ журмын 5.9-д заасны дагуу заавар нэвтрэх нууц үгтэй байна. Нэвтрэх нууц үгийг ажил үүргийн хуваарийн дагуу мэдээллийн сан, мэдээллийн системийн чиглэлийн IT инженер өөртөө хадгалах бөгөөд нууцлалыг өндөр түвшинд хамгаалж, Маягт №1-н дагуу баталгаа гаргаж өгнө.

1.5 Сүлжээ ашиглах

1.5.1 IT инженерийн 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.

1.5.2 Эмч, эмнэлгийн мэргэжилтэн, албан хаагчид өөрийн ашиглаж буй сүлжээнд мэдээллийн аюулгүй байдлын эрсдэл учирч болзошгүй эсвэл учирсан гэж үзвэл IT инженерт нэн даруй мэдэгдэнэ.

1.5.3 Байгууллагын сүлжээний зохион байгуулалт, байнгын ажиллагаа, сүлжээний тоног төхөөрөмжийн тохиргоо, тэдгээрийн хяналтыг IT инженер гүйцэтгэнэ.

1.5.4 Байгууллагын сүлжээг зохион байгуулахдаа сүлжээний порт, сүлжээний кабелын 2 талын үзүүрт тэмдэглэгээ бүхий хаяг заавал хадна.

1.5.5 Сүлжээний зохион байгулалтын 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 IT инженер өөртөө хадгалах бөгөөд нууцлалыг өндөр түвшинд хамгаалж, Маягт №1-н дагуу баталгаа гаргаж өгнө.

1.5.6 Сүлжээ ашиглан байгууллага хооронд нууцлалын зэрэглэл бүхий мэдээлэл дамжуулах, солилцох бол заавал нууцлал бүхий сүлжээ (VPN, төрийн сүлжээ) ашиглан дамжуулна.

1.6 Зөөврийн хадгалах төхөөрөмж ашиглах

1.6.1 Зөөврийн хадгалах төхөөрөмж дээрх мэдээллийг ашиглаж дууссаны дараа шаардлагагүй бол мэдээллийг төхөөрөмжөөс тухай бүр арилгах үйлдэл хийнэ.

1.6.2 Гаднаас зөөврийн хадгалах төхөөрөмж системд оруулах бол заавал вирусын эсрэг программ уншуулж, вирус илэрсэн тохиолдолд түүнийг устгасны дараа мэдээлэл авах, хадгалах, үйлдлийг хийнэ.

1.6.3 Зөөврийн хадгалах төхөөрөмжийг албан бусаар ашиглах бусдад дамжуулахыг хориглоно.

1.7 Албаны цахим шуудан ашиглах

1.7.1 Байгууллагын албаны цахим шуудан (дотоод сүлжээ) хэрэглэгчдийн бүртгэл хөтлөх, шинээр хэрэглэгч нэмэх, өөрчлөх, хасах, хэрэглэгчдийн бүртгэлийн нууцлал аюулгүй байдлыг хангах асуудлыг IT инженерүүд хариуцна.

1.7.2 Эмч, эмнэлгийн мэргэжилтэн, албан хаагчид албаны цахим шууданг зөвхөн албан ажлын хэрэгцээнд ашиглаж, өөрийн цахим шуудангийн нууцлал аюулгүй байдлыг хариуцна.

1.7.3 Албаны цахим шуудангийн нэвтрэх нууц үгийг энэ журмын 6.9-д заасны дагуу зохион байгуулна.

1.8 Байгууллагын кибер аюулгүй байдлыг хангах, мэдээллийн сангийн нууцлал, хамгаалалтыг хангах, аюул заналаас урьдчилан сэргийлэх ажлын хүрээнд IT инженерүүд дараах арга хэмжээг авна.

1.8.1 Цахим мэдээллийн архив бүртгэлийн автоматжуулсан системтэй байна.

1.8.2 Сүлжээний хамгаалалтыг зохион байгуулах, мэдээллийн системийг хууль бус гадны халдлагаас хамгаалах

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

1.8.4 Техник программд мэдээ дамжуулах хэрэгсэл байгаа эсэхийг хэрэглээнд нэвтрүүлэхээс өмнө шалгах харилцаа холбооны, кибер аюулгүй байдлын нууцлал хамгаалалтыг хангах

1.8.5 Харилцаа холбоо, кибер аюулгүй байдлын нууцлал хамгаалалтыг хангах, хамгаалалтын шаардлагатай түвшинг хангахуйц техникийн шийдлийг боловсруулах

1.9 Нууц үгийн бодлого

1.9.1 Нууц үгийн том, жижиг үсэг, тоо, тусгай тэмдэгт агуулсан байдлаар 8-12 оронтойгоор үүсгэнэ. Нууц үгээ ил бичиж тэмдэглэх, бусдад дамжуулахыг хориглоно.

1.9.2 Эхний нууц үгийг 3 сар тутамд шинэчилж байх, ингэхдээ хуучин нууц үгийг ахин хэрэглэхгүй, тэмдэгтүүдийг заавал солино.

1.9.3 Байгууллагын мэдээллийн систем, өгөгдлийн сан, программ хангамжийн нууц үгийн сонголт, бүртгэл, ашиглах хугацааг IT инженер, системийн зохицуулагч, мэдээллийн (Кибер) аюулгүй байдал хариуцсан мэргэжилтэн нар хариуцан ажиллаж хяналт тавина. Шинээр үүсгэх, өөрчлөх, устгах тохиолдолд Маягт №3-аар баталгаажуулах ба улирал тутам системийн хэрэглэгчдийн жагсаалтыг хянана.

1.10 “Logfile”-н бүртгэл

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

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

1.10.3 Лог мэдээллийг сар бүр нөөцөлж, 3 жил тутам нягтлан шинжилсний дараа системийн зохицуулагч устгана.

1.11 Хортой кодоос хамгаалах

1.11.1 Байгууллагын хэрэгцээнд хэрэглэгдэж байгаа компьютер, мэдээлэл хадгалагч болон тээгч зөөврийн хэрэгслүүдэд зөвшөөрөгдсөн хортой кодын (вирус) эсрэг программ хангамжийг ашиглана.

1.11.2 Хортой кодын болон кибер халдлагын эсрэг программын шинэчлэлтийг тогтмол хийнэ.

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

1.11.4 Системд гаднаас мэдээлэл оруулах бол сүлжээнд холбогдоогүй компьютерт эхэлж хортой кодын шинжилгээг заавал хийсний дараа системд нэвтрүүлнэ.

Зургаа. Мэдээллийн систем, мэдээллийн сангийн нууцлал, хамгаалалт, хандалтын удирдлага

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

6.2 Эмч, эмнэлгийн мэргэжилтэн, албан хаагчдын системд нэвтрэх эрхийг IT инженерүүд, нэгжийн удирдлагын зөвшөөрлийг үндэслэн системийн зохицуулагч нээнэ.

6.3 Байгууллагын эмч, эмнэлгийн мэргэжилтэн, албан хаагчид ажлын чиг үүргийн дагуу мэдээллийн сан, мэдээллийн системд эрхийн өөр өөр түвшинд хандана.

6.3.1 Админ эрх (Admin)-Систем шинээр суулгах, тохируулга хийх, нэмэлт өөрчлөлт оруулах, системд хэрэглэгч нэмэх, хасах эрхтэй

6.3.2 Бичих эрх (Modirator, writing)- шинэ бичлэг нэмэх, өөрчлөх, хадгалах эрх

6.3.3 Зөвхөн харах эрх (read only)-Зөвхөн харах, унших эрх

6.4 Нэвтрэх эрхийг цуцлах

6.4.1 Мэдээллийн сан, мэдээллийн системд хандах эрх бүхий албан хаагч ажлаас гарсан, халагдсан, өөр ажилд шилжсэн тохиолдолд байгууллагын хүний нөөцийн менежер тухайн эмч, эмнэлгийн мэргэжилтэн, албан хаагдыг ажлаас чөлөөлөх тухай системийн зохицуулагчид тухай бүр мэдэгдсэнээр нэвтрэх эрхийг цуцална. Тухайн эмч, эмнэлгийн мэргэжилтэн, албан хаагчийн цахим баримт бичиг болон цахим шуудангийн мэдээллийг устгахгүй, цахим архивт шилжүүлнэ.

6.4.2 Мэдээллийн систем, мэдээллийн санд нэвтрэх эрх бүхий ажилтан энэ журмыг зөрчсөн нь тогтоогдвол системд нэвтрэх эрхийг системийн зохицуулагчийн зүгээс түдгэлзүүлж болно.

6.5 Байгууллагын мэдээллийн санг тогтмол хугацаанд серверт байрлуулна. Мэдээллийн санд хандах эрхийг энэ журмын 6.1, 6.3-т зааснаар системийн зохицуулагч олгоно.

6.6 Серверт хадгалагдах мэдээллийн сангийн хандах эрхийн нууцлал хамгаалалтыг мэдээллийн сангийн зохицуулагч бүрэн хариуцаж, энэ журмын Маягт №1-т зааснаар баталгаа гаргаж өгнө.

6.7 Серверт хадгалагдах мэдээллийн санг байнга болон түр хадгалах гэж 2 ангилж үзнэ.

6.7.1 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.

6.7.2 Байнга хадгалах өгөгдлийн сан, мэдээллийг хадгалах хугацаа дууссан тохиолдолд цахим архивт шилжүүлнэ.

6.7.3 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.

6.8 Байгууллага нь мэдээллийн систем, өгөгдөл, мэдээллийг өөрийн серверийн өрөөнд байршуулахаас гадна газарзүйн байршлын хувьд өөр газарт нөөц дата төвд хуулбарыг заавал байршуулна.

6.9 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 IT инженер зохион байгуулна.

Долоо. Байгууллагын цахим баримт бичиг, мэдээллийн сангийн нөөцлөлт, хадгалалт

7.1 Байгууллага нь мэдээллийн цахим сан хөмрөгийг бүрдүүлэх зорилгоор байгууллагын цахим архивын сантай байна.

7.1.1 Цахим архивын сангийн компьютер, тоног төхөөрөмжийг серверийн өрөөнд байрлуулж, цахим архивын бүрдүүлэлт, хадгалалт, нууцлалыг архивын асуудал хариуцсан албан хаагч IT инженерүүдтэй хамтран зохион байгуулна.

7.1.2 Байгууллагын эмч, эмнэлгийн мэргэжилтэн, албан хаагчид цахим баримт бичиг боловсруулахдаа, Төрийн албан хэрэг хөтлөлтийн заавар болон бусад холбогдох стандартуудыг мөрдлөг болгоно.

7.1.3 Хэрэглэгч тухайн ажлын байртай холбогдох бичиг баримтыг төрөлжүүлж өөрийн компьютерт хадгалах ба шаардлагатай бол хуулбарыг нөөц мэдээллийн санд хадгална.

7.1.4 Хэрэглэгч нь албан хэрэгцээний файлаа нэр төрлөөр нь ангилж хавтас үүсгэн хадгална. Шаардлагатай бод дэд хавтас үүсгэн хадгалж, жил тутмын эхний улиралд архивын ажилтанд өмнөх оны файл, хавтсаа байгууллагын мэдээллийн цахим сан хөмрөгт хадгалуулах зорилгоор хүлээлгэн өгнө.

7.1.5 Архивын ажилтан цахим мэдээллийг хүлээн авч байгууллагын мэдээллийн цахим архивт хадгална. Ингэхдээ холбогдох тэмдэглэлийг заавал хөтөлнө. Файлд нэр өгөхдөө “Монгол кирилл цагаан толгойн үсгүүдийг романчилах” MNS5217:2003 стандартыг мөрдлөг болгоно.

7.2 Байгууллагын үйл ажиллагаанд хэрэглэгддэг худалдаж авсан, захиалгаар хөгжүүлсэн, өөрсдийн хөгжүүлсэн, тусгай зориулалтын программ хангамжийн эх хувийг болон хувилбаруудыг байнгын хэрэгцээнд зориулан серверт байрлуулна.

Найм. Байгууллагын IT инженерийн эрх үүрэг

8.1 Байгууллагын IT инженерийн эрх үүрэг

8.1.1 Байгууллагын мэдээллийн аюулгүй байдлын бодлогыг тодорхойлох, мэдээллийн аюулгүй байдлын тогтолцоог бүрдүүлэх, холбогдох дүрэм, журмыг боловсруулж батлуулах, тэдгээрт нэмэлт өөрчлөлт оруулах санал боловсруулах

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

8.1.3 Байгууллагын IT инженерүүд мэдээллийн системд заналхийлж буй халдлагыг бүртгэх, илрүүлэх, таслан зогсоох болон эмзэг байдлыг тогтоох, түүнийг бууруулах, аюулгүй байдлын бодлого боловсруулах зорилгоор кибер аюулгүй байдал хариуцсан мэргэжилтэн (системийн зохицуулагч) ажиллуулна. Байгууллагын бусад албад мэдээллийн аюулгүй байдлыг хангахад дэмжиж ажиллана.

8.1.4 Мэдээллийн аюулгүй байдлын эрсдэл, онц нөхцөл байдал үүссэн тохиолдолд байгууллагын мэдээллийн системийг сэргээх, хэвийн үйл ажиллагааг хангах арга, гүйцэтгэх дараалал, хариуцах албан тушаалтныг тодорхойлсон төлөвлөгөөг боловсруулж, мөрдүүлж ажиллах

8.1.5 Байгууллагын эмч, эмнэлгийн мэргэжилтэн, албан хаагчид мэдээллийн аюулгүй байдлыг хангаж ажиллах талаар жил бүр тогтмол сургалтанд хамрагдана. Сургалтын талаарх мэдээллийг тухай бүрд нь Сургалт хариуцсан ерөнхий менежер дотоод сүлжээ, цахим орчноор мэдээ мэдээллийг хүргэж ажиллана.

8.1.6 Байгууллагын удирдлага мэдээллийн аюулгүй байдал хариуцсан мэргэжилтний, мэргэжил ур чадварыг дээшлүүлэх сургалтанд байнга хамруулах, төсвийг шийдвэрлэж ажиллана.

8.2 Системийн зохицуулагчийн эрх

8.2.1 Ажил үүргийн хуваарийн дагуу мэдээллийн аюулгүй байдлыг шалгах, эмзэг байдлыг бууруулах зорилгоор мэдээллийн систем, эмч, эмнэлгийн мэргэжилтэн, албан хаагчдын компьютерт нэвтрэх

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

8.2.3 Аюулгүй байдлын шаардлагыг зөрчигчдөд хариуцлага тооцох талаар байгууллагын удирдлагад санал оруулах

8.2.4 Байгууллагад ашиглагдах мэдээллийн систем, техник технологи худалдан авах үйл ажиллагаанд оролцох, санал оруулах, нэвтрүүлэх үйл явцад хяналт тавих

8.2.5 Кибер аюулгүй байдлын эрсдлийн үнэлгээг жил тутам хийж мэдээллийн аюулгүй байдлын эмзэг байдлыг тодорхойлох, хамгаалалтын түвшинг тогтоох, хөндлөнгийн хяналтыг хэрэгжүүлэх

8.2.6 Мэдээллийн систем, мэдээллийн сангийн бүрэн бүтэн байдалд хяналт тавих, мэдээллийн сангийн нөөцлөлт, нөөцийг хадгалах нөхцөлийг хангах

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

8.3 Системийн зохицуулагчийн үүрэг

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

8.3.2 Мэдээллийн сан, программ хангамж, компьютерыг хортой кодоос хамгаалах

8.3.3 Мэдээллийн аюулгүй байдлыг хангахад чиглэсэн сургалт, сурталчилгааг байгууллагад зохион байгуулах

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

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

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

8.3.7 Байгууллагын компьютерүүд, дагалдах тоног төхөөрөмж, хэрэгслүүдийн ажиллагаа, битүүмжлэл, шинэ тоног төхөөрөмжийн суурилуулалтыг хариуцан гүйцэтгэх

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

8.3.9 Системийн зохицуулагч нь ажил үүргийн дагуу олгосон эрхээ буруугаар ашиглахгүй байх

Ес. Мэдээллийн системийн хэрэглэгчийн үүрэг

9.1 Мэдээллийн аюулгүй байдлын эрсдэл (кибер халдлага) тохиолдсон, тохиолдож болзошгүй нөхцөл байдлыг илрүүлсэн бол системийн зохицуулагчид нэн даруй мэдэгдэх үүрэгтэй.

9.2 Компьютерын нэр, сүлжээний нэрийг солихгүй байх, шаардлага гарсан тохиолдолд системийн зохицуулагчид мэдэгдэн зохих үйлчилгээг хийлгэх

9.3 Ажлын өрөө болон хонгилд ил болон далд угсрагдсан сүлжээний утсууд, гэмтсэн, ороцолдсон, далд монтажаас утас ил гарсан тохиолдолд сүлжээ хариуцсан зохицуулагчид мэдэгдэх

9.4 Мэдээллийн аюулгүй байдлыг хангах талаар системийн зохицуулагчийн тавьсан шаардлагыг биелүүлэх

Арав. Хариуцлага

10.1 Эмч, эмнэлгийн мэргэжилтэн, албан хаагчидын анхаарал болгоомжгүй үйлдлээс болж байгууллагын мэдээллийн систем, сүлжээ, мэдээллийн сангийн аюулгүй байдал, алдагдах, мэдээллийн болон кибер аюулгүй байдлын бодлого, журам зөрчигдөж, байгууллагын үйл ажиллагаанд хохирол учруулсан ба хохирч болзошгүй байдал үүсгэсэн нь эрүүгийн хариуцлага хүлээлгэхээргүй бол Зөрчлийн

тухай хууль, Хөдөлмөрийн тухай хууль, Байгууллагын хөдөлмөрийн дотоод журамд заасны дагуу сахилгын арга хэмжээ авна.

10.2 Нууц мэдээллийг санаатай буюу санамсаргүй байдлаар бусдад задруулснаас үүсэх хохирлыг нөхөн төлүүлэх, буруутай этгээдэд хариуцлага оногдуулах асуудлыг Эрүүгийн хууль, Захиргааны ерөнхий хууль, Төрийн болон албаны нууцын тухай хууль, Байгууллагын нууцын тухай хууль, Хувь хүний нууцын тухай хуулийн холбогдох заалтыг баримтлан шүүхээр шийдвэрлүүлнэ.

Маягт №1

НУУЦЫН БАТАЛГАА

Байгууллагын нэр: ӨВ БОЭТөв

Эмч, эмнэлгийн мэргэжилтэн, албан хаагчийн харъяалагдах алба, тасаг нэгжийн нэр.....
Овог .....
Нэр.....

Би өөрийн албан үүргээ гүйцэтгэх явцад олж мэдсэн, хадгалж байсан (байгаа), үйл ажиллагаандаа ашиглаж байсан Өвөрхангай аймаг дахь Бүсийн оношилгоо эмчилгээний төвийн нууцад хамаарах зүйлсийг цааш задруулахгүй байх үүргийг зөвшөөрч байна.

Байгууллагын нууцыг задруулсан тохиолдолд Монгол Улсын холбогдох хууль болон Байгууллагын “Кибер болон мэдээллийн аюулгүй байдлыг хангах үйл ажиллагааны дотоод журам”-ын дагуу хариуцлага хүлээхэд бэлэн байна гэдгээ энэхүү баталгаагаар хүлээн зөвшөөрч байна.

БАТАЛГАА ГАРГАСАН

(эмч, эмнэлгийн мэргэжилтэн, албан хаагчийн овог нэр, гарын үсэг)

Маягт №1

НУУЦЫН БАТАЛГАА

Байгууллагын нэр: ӨВ БОЭТөв
Эмч, эмнэлгийн мэргэжилтэн, албан хаагчийн харъяалагдах алба, тасаг нэгжийн нэр.....
Овог .....
Нэр.....

Би өөрийн албан үүргээ гүйцэтгэх явцад олж мэдсэн, хадгалж байсан (байгаа), үйл ажиллагаандаа ашиглаж байсан Өвөрхангай аймаг дахь Бүсийн оношилгоо эмчилгээний төвийн нууцад хамаарах зүйлсийг цааш задруулахгүй байх үүргийг зөвшөөрч байна.

Байгууллагын нууцыг задруулсан тохиолдолд Монгол Улсын холбогдох хууль болон Байгууллагын “Кибер болон мэдээллийн аюулгүй байдлыг хангах үйл ажиллагааны дотоод журам”-ын дагуу хариуцлага хүлээхэд бэлэн байна гэдгээ энэхүү баталгаагаар хүлээн зөвшөөрч байна.

БАТАЛГАА ГАРГАСАН

(эмч, эмнэлгийн мэргэжилтэн, албан хаагчийн овог нэр, гарын үсэг)

Маягт №2

НУУЦ АНГИЛЛЫН МЭДЭЭЛЭЛ, ТЭДГЭЭРИЙГ ХАРИУЦАГЧ, ЭЗЭМШИГЧ БОЛОН ХЭРЭГЛЭГЧИЙН ЖАГСААЛТ

№	Мэдээллийн нэр	Тайлбар	Нууцын зэрэглэл	Хариуцагч	Эзэмшигч	Хэрэглэгч

МЭДЭЭЛЛИЙН СИСТЕМИЙН БАЙР, ӨРӨӨ ТАСАЛГААНЫ ХАМГААЛАЛТЫН ЗЭРЭГЛЭЛИЙН ЖАГСААЛТ

№	Өрөөний нэр	Тайлбар	Зэрэглэл	Хэрэглэгч

Маягт №3

Хүсэлтийн дугаар №

Хүсэлтийн төрөл

Шинэ хэрэглэгч үүсгэх ☐

Хандах эрхийг өөрчлөх ☐

Хэрэглэгчийг устгах ☐

Эрх хүсэж буй эмч, эмнэлгийн мэргэжилтэн, албан хаагчийн мэдээлэл

Хэрэглэгчийн нэр.....

Алба/хэлтэс/ нэгж/ албан тушаал.....

.....

Холбогдох хаяг:

Байгууллагын мэдээлэлд хандах эрх нэмэх			
№	Хандах эрхийн нууцлалын түвшин, төрөл, хэлбэр	Хандах эрх үүсвэр	Хандах эрх нэмэх шалтгаан, тайлбар
1			
Хандах эрх өөрчлөх			
№	Хандах эрхийн нууцлалын түвшин, төрөл, хэлбэр	Хандах эрх үүсвэр	Хандах эрх өөрчлөх шалтгаан, тайлбар
1			
Хандах эрх устгах			
№	Хандах эрхийн нууцлалын түвшин, төрөл, хэлбэр	Хандах эрх үүсвэр	Хандах эрх устгах шалтгаан, тайлбар
1			
Нэмэлт тайлбар мэдээлэл:			

Хүсэлт гаргасан эмч, эмнэлгийн мэргэжилтэн, албан хаагч	Хүсэлтийг зөвшөөрсөн алба/нэгж, тасаг хариуцсан албан тушаалтан
Гарын үсэг ( ) 20.....он.....сар.....өдөр	Гарын үсэг ( ) 20.....он.....сар.....өдөр