



Ж-09-37-01

ДАРХАН-УУЛ АЙМАГ
“ДАРХАНЫ ДУЛААНЫ СҮЛЖЭЭ” ТӨХК-НИЙН
ЗАХИРЛЫН ТУШААЛ

2018 оны 02 сарын 24 өдөр

Дугаар А/47

Дархан

Мэдээлэл, мэдээллийн системийн
аюулгүй байдлыг хангах журам батлах тухай

Монгол Улсын Засгийн газрын 2010 оны 141 дүгээр тогтоолоор батлагдсан “Мэдээллийн аюулгүй байдлыг хангах” үндэсний хөтөлбөрийг үндэслэн ТУШААХ нь:

1. “Дарханы дулааны сүлжээ” ТӨХК-ийн “Мэдээлэл, мэдээллийн системийн аюулгүй байдлыг хангах журам”-ыг хавсралт №1-ээр, “Компанийн мэдээлэл, дотоод сүлжээ болон интернет сүлжээ ашиглах журам”-ыг хавсралт №2-оор тус тус баталсугай.

2. Дээрх журмыг хэрэгжүүлэхэд компанийн нийт ажилтан, албан хаагчдад мэргэжил арга зүйн дэмжлэг үзүүлж, хяналт тавьж, хамтарч ажиллахыг компьютер, мэдээлэл сурталчилгааны мэргэжилтэн /Э.Ууганбаяр/-т, тушаалын биелэлтэд хяналт тавьж, үр дүнг тооцож ажиллахыг Захиргаа, удирдлагын алба /Ц.Алтанцэцэг/-нд тус тус даалгасугай.

ГҮЙЦЭТГЭХ ЗАХИРАЛ



Д.ГАНТУУЛ

КОМПАНИЙН МЭДЭЭЛЭЛ ДОТООД СҮЛЖЭЭ БОЛОН ИНТЕРНЭТ СҮЛЖЭЭ АШИГЛАХ ЖУРАМ

НЭГ. ЕРӨНХИЙ ЗҮЙЛ

1. Энэхүү журмын зорилго нь байгууллагын дотоод болон интернет сүлжээний хэвийн ажиллагааг хангах, зохистой хэрэглээг бий болгох, мэдээллийн аюулгүй байдлыг хангах, ажилтнуудын ажлын цаг ашиглалтыг сайжруулахад оршино.
2. Энхүү журмыг байгууллагын бүх ажилтан. албан хаагчид /цаашид ажилтнууд гэх/ мөрдөж ажиллах ба журмын хэрэгжилтийг Захиргаа удирдлагын хэлтэс хариуцаж, хяналт тавина.

ХОЁР. ДОТООД СҮЛЖЭЭ

2.1. Үндсэн ойлголт

- 2.1.1 Энэ журамд заасан "Дотоод сүлжээ" гэдэг нь байгууллагын бүх компьютерууд, тэдгээрийг холбосон кабель болон утасгүй сүлжээг хэлнэ.

2.2. Зохион байгуулалт, ашиглалт

- 2.2.1 Дотоод сүлжээнд зөвхөн байгууллагын бүртгэлтэй компьютерууд холбогдох бөгөөд шаардлагатай гэж үзвэл ажилтнуудын хувийн зөөврийн компьютерыг компьютерийн мэргэжилтэнгээр холбуулж болно.
- 2.2.2 Компьютер, зөөврийн компьютер, хэвлэгч төхөөрөмжийг утасгүй сүлжээгээр дотоод сүлжээнд холбохдоо тухайн утасгүй сүлжээний төхөөрөмжид бүртгүүлсэн байх ёстой.
- 2.2.3 Ажилтан байгууллагын дотоод сүлжээг ашиглахдаа тусгай зориулалтын сүлжээний орчинд ажилладаг хатуу дискээр файл хавтсаа дамжуулах бөгөөд хатуу дискний тохиргоог компьютер бүрт `serverId` гэж нэрлэн нэмэлтээр тохируулсан байна.
- 2.2.4 `serverId` хавтас нь аливаа мэдээллийг зөвхөн түр зуур хадгалах, дамжуулан ашиглахад зориулагдсан болно. Ажилтан тухайн хавтас руу хуулсан файл, хавтсыг ашиглаж дууссан даруйд устгаж байх ёстой.
- 2.2.5 Ажилтнууд шууд өөрсдийн компьютертээ үүсгэсэн Share хавтсаар дамжуулан файл дамжуулан ашиглаж болно.
- 2.2.6 Дотоод сүлжээнд холбогдсон хэвлэгч төхөөрөмжийн тохиргоог компьютерийн мэргэжилтэнгээр хийлгэнэ.
- 2.2.7 `serverId` хадгалах төхөөрөмжөөр дамжуулсан хэрэгцээгүй болсон файлууд, ашиглах хугацаа нь өнгөрсөн, шаардлагагүй болсон файл, хавтсыг тухай бүрт нь оруулсан ажилтан зөвхөн өөрөө цэвэрлэж, устгаж байх шаардлагатай.

2.3. Санамж

- 2.3.1 `serverId` хавтсанд хуулагдсан, үүсгэгдсэн бүх файл, хавтсуудыг бүх ажилтнууд унших, засах, устгах боломжтойг анхаарна уу.

- 3.1.2 Ажилтан өөрт чухал файл, хавтсыг дээрх төхөөрөмжид хуулж архивлах, бусдад нээлттэй орхихгүй байх ба үүнээс үүдэн гарсан хохирлыг ажилтан өөрөө хариуцна.
- 3.1.3 Байгууллагын нууц болон хувийн нууцтай холбоотой мэдээлэл, дуу, кино, тоглоом зэргийг serverId хадгалах төхөөрөмжөөр дамжуулах, хадгалахыг хориглоно.
- 3.1.4 Дотоод сүлжээний хуваарилах төхөөрөмжид ажилтан дур мэдэн гадны төхөөрөмж холбох, өргөтгөхийг хориглох бөгөөд шаардлагатай тохиолдолд хариуцсан мэргэжилтэнд мэдэгдэж холболтыг хийлгүүлнэ.
- 3.1.5 Гадны байгууллага, хувь хүмүүсийн төхөөрөмжүүдийг компанийн дотоод сүлжээнд дур мэдэн холбохыг хориглоно.
- 3.1.6 Ажилтнууд компьютер, зөөврийн компьютер, хэвлэгчдийн тохиргоог дур мэдэн өөрчлөхийг хориглоно.

4. Хариуцлага

- 4.1 Ажилтан компанийн интернэт сүлжээ ашиглах журмыг зөрчсөний улмаас байгууллагын үйл ажиллагаанд хохирол учруулсан тохиолдолд харьяа алба, хэлтсийн даргын саналыг үндэслэн "Компанийн дотоод журам"-д заасны дагуу сахилгын хариуцлага хүлээлгэнэ.

ГУРАВ. ИНТЕРНЭТ СҮЛЖЭЭ

1. Үндсэн ойлголт

- 1.1 "Интернет сүлжээ" гэдэг нь хангагч байгууллагаас ирж байгаа гадаад сүлжээний урсгалыг хэлэх бөгөөд уг урсгалыг хүлээн авч дамжуулах төхөөрөмж (Router) дээр дотоод сүлжээний компьютеруудад хуваарилах тохиргоог хийсэн байна.

2. Зохион байгуулалт, ашиглалт

- 2.1 Компанийн интернэт сүлжээг кабелиар болон утасгүй сүлжээгээр зохион байгуулах ажлыг Захиргаа удирдлагын хэлтэс хариуцна.
- 2.2 Интернэт сүлжээний зохион байгуулалт, нууцлалт, аюулгүй байдлыг хангах ажиллагаа, ашиглалтын хяналтыг Захиргаа удирдлагын хэлтсийн сүлжээний мэргэжилтэн хариуцаж ажиллана.
- 2.3 Ажилтнууд компанийн интернэт сүлжээг зөвхөн албан үүргээ гүйцэтгэх зорилгоор мэдээлэл судлах, цуглуулах, дамжуулахад ашиглана.

3. Интернэт сүлжээний хамгаалалт

- 3.3.1 Сүлжээний мэргэжилтэн байгууллагын интернэт хэрэглэгчдийн бүртгэлийг интернэтийн хүлээн авах төхөөрөмж дээр бүртгэж интернэтэд холбогдох эрхийг тодорхойлсон байна.
- 3.3.2 Шаардлагагүй вэб сайт, блог, торрент бүхий эрсдэлтэй програмуудыг хааж, орох эрхийг хязгаарлаж тогтооно.
- 3.3.3 Олон нийтийн сошиал вэб сайтуудыг (www.facebook.com, www.twitter.com, www.instagram.com, www.youtube.com, www.hi5.com гэх мэт) ажлын цагаар хязгаарлаж тохируулсан байна.

- 3.4.1 Байгууллагын бүртгэлтэй компьютер болон тоног төхөөрөмжөөс бусад гадны төхөөрөмж (ажилтнуудын хувийн гар утас, таблет, notebook зэрэг)-ийг утасгүй сүлжээнд холбохыг хориглоно.
- 3.4.5 Ажлын шаардлагаар гадны байгууллагын ажилтны төхөөрөмжүүдийн интернэтийн сүлжээнд холбох шаардлага гарвал Захиргаа удирдлагын хэлтсийн даргаас зөвшөөрөл авч холбогдох мэргэжилтнээр холбуулна.
- 3.4.6 Ажлын шаардлагаар гадны байгууллагын ажилтны төхөөрөмжийг дотоод сүлжээ болон интернет сүлжээнд холбосон, тухайн хэрэглэгч сүлжээг ашиглаж дууссан бол холболт хийсэн инженер тухайн гадны төхөөрөмжийн бүртгэлийг сүлжээний хуваарилах төхөөрөмжөөс нэн даруй хасах үүрэгтэй.

4 Хариуцлага

- 4.1 Ажилтан компанийн интернэт сүлжээ ашиглах журмыг зөрчсөний улмаас байгууллагын үйл ажиллагаанд хохирол учруулсан тохиолдолд харьяа алба, хэлтсийн даргын саналыг үндэслэн "Компанийн дотоод журам"-д заасны дагуу хариуцлага хүлээлгэнэ.

“ДДС”ТӨХК-ийн гүйцэтгэх захирлын 2018.02.27-ны
өдрийн А/47 тоот тушаалын хавсралт №1

“ДАРХАНЫ ДУЛААНЫ СҮЛЖЭЭ” ТӨХК-ИЙН МЭДЭЭЛЛИЙН СИСТЕМИЙН АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ЖУРАМ

Нэг. Ерөнхий зүйл

Энэхүү журмын зорилго нь “ДДС” ТӨХК-ийн мэдээлэл, мэдээллийн систем, мэдээлэл дамжуулах сүлжээ, мэдээллийн сангийн нууцлал, аюулгүй байдлыг хангах, хангас болон дотроос учирч болох аюул, хор хөнөөлөөс урьдчилан сэргийлэх, хор хөнөөлийг багасгах, таслан зогсоох, гэмтэл саатал учирсан тохиолдолд нэн даруй аргаарлан сэргээх, хариу арга хэмжээ авахад оршино.
“ДДС” ТӨХК-ийн нийт ажилтнууд ажил үүргээ гүйцэтгэхдээ энэхүү журмыг мэддэг болгоно.

Хоёр. Нэр томьёо

“Мэдээлэл” гэж компьютер, компьютерын программ болон ижил төрлийн бусад хэрэгслийг ашиглан үүсгэх, илгээх, хүлээн авах, хадгалах боломжтой мэдээллийг хэлнэ.
“Мэдээллийн систем” гэж байгууллагын үйл ажиллагаанд ашиглагдаж буй мэдээллийн технологийн техник хангамж, програм хангамж, дотоод болон гадаад сүлжээ тэдгээрийн холболтыг бий болгон ажиллаж буй бүрдлийг хэлнэ.
“Хэрэглэгч” гэж мэдээллийн системд хандах эрх авсан ажилтныг хэлнэ.
“Системийн удирдагч” гэж байгууллагын мэдээллийн технологи хариуцсан эрх, үүрэг бүхий ажилтан /мэдээлэл сурталчилгааны мэргэжилтэн/-г хэлнэ;
“Халдлага” гэж мэдээллийн систем болон байгууллагын компьютеруудад хор хөнөөл үүсгэж болох код, мэдээллийн нууцлал, аюулгүй байдлыг ямар нэг байдлаар үершиж болох боломж, үйлдэл, үйл явдлыг хэлнэ.
“Мэдээллийн нууцлал” гэж мэдээлэл, мэдээллийн системд зөвшөөрөлгүй хандахаас хамгаалсан байхыг хэлнэ.

Гурав. Мэдээллийн хадгалалт, хамгаалалт

1 Мэдээллийн хадгалалт

3.1.1. Ажилтан нь тухайн ажлын байртай холбогдох бичиг баримтыг зөвхөн өөрөөрөө өөрийн компьютерын нөөцөд хадгална. Шаардлагатай бол системийн удирдагчид өгч хадгалуулна.

3.1.2. Ажилтан нь албан хэрэгцээний файлаа нэр төрлөөр нь ангилж хавтас үүсгэн хадгална. Шаардлагатай бол дэд хавтас үүсгэн хадгалж, хэрэглэж хэвшинэ.

3.1.3. Мэдээллийн системийн мэдээллийг системийн удирдагч жилд 1 удаа архивлана.

2 Мэдээллийн хамгаалалт

3.2.1. Байгууллагын мэдээлэл гаргадаг, хүлээн авдаг, боловсруулдаг, дамжуулдаг, хадгалдаг ажилтан бүр мэдээллийг хамгаалах үүрэг хүлээнэ.

3.2.2. Байгууллагын ажилтан өөрийн компьютер дээр шууд харьяалах албан тушаалтны зөвшөөрөлгүйгээр гадны этгээдийг ажиллуулахыг хориглоно.

3.2.3. Байгууллагын ажилтан бүр өөрийн компьютер дээрээ нэвтрэх нууц үгийг нэгэнэ.

3.2.4. Хэрэглэгч нь мэдээллийн системийн нууц үгээ хамгаалах үүрэгтэй бусдад дамжуулахыг хориглоно.

3.2.5. Нууц үгийг тодорхой хугацаанд буюу жилд нэг удаа заавал сольдог

3.2.6. Нууц үг илэрсэн гэж үзвэл даруй солих бөгөөд хуучин нууц үгийг дахин ашиглахээс зайлсхийж, хуучин тэмдэгтүүдийг солино.

Дөрөв. Халдлагаас хамгаалах

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

4.2. Гаднаас зөөврийн хадгалах төхөөрөмж системд оруулах бол заавал хортой кодын эсрэг программ уншуулна.

4.3. Хортой кодын эсрэг программын шинэчлэлтийг жилд 1 удаа хийнэ.

4.4. Тодорхой хугацаанд системийн хортой кодын эсрэг программыг уншуулж, системийн тохиолдолд устгах арга хэмжээг авна.

Тав. Системийн удирдагчийн эрх, үүрэг

5.1. Системийн удирдагч дараах эрх эдэлнэ:

5.1.1. Ажил үүргийн хуваарийн дагуу мэдээллийн нууцлал, аюулгүй байдлыг хангах, эмзэг байдлыг бууруулах зорилгоор мэдээллийн систем, ажилтнуудын компьютерт нэвтрэх;

5.1.2. Мэдээллийн нууцлал, аюулгүй байдлын шаардлага зөрчиж буй хэрэглэгчийн мэдээллийн системд нэвтрэх эрхийг удирдах, тэдгээрийн ажиллагааг зогсоолон болон бүрэн зогсоох;

5.1.3. Мэдээллийн нууцлал, аюулгүй байдлын шаардлагыг зөрчигчдөд шаардлага тооцох талаар байгууллагын удирдлагад санал оруулах;

5.1.4. Мэдээллийн систем, техник технологи худалдан авах болон шинээр оруулах үйл явцад хяналт тавих;

5.1.5. Мэдээллийн системийн бүрэн бүтэн байдалд хяналт тавих, мэдээллийн системийн нөөц хувийг хувилж хадгалах нөхцлийг хангах;

5.1.6. Мэдээллийн системийн болон сервер компьютерт нэмэлт өөрчлөлт, шинэчлэлт, техникийн үйлчилгээг хийхэд гадны байгууллага, мэргэжилтнийг аюулгүй ажиллуулах тохиолдолд тухайн ажлыг гүйцэтгэх байгууллагыг сонгон зарцуулах үйл явцад оролцох бөгөөд ажил гүйцэтгэх явц, гүйцэтгэлд нь хяналт тавих.

5.2. Системийн удирдагч дараах үүрэг хүлээнэ:

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

5.2.2. Мэдээллийн систем, программ хангамж, компьютерыг хортой кодоос хамгаалах, мэдээллийн нууцлалыг хангах;

5.2.3. Мэдээллийн нууцлал, аюулгүй байдлыг хангахад чиглэсэн сургалт, үйлчилгээг зохион байгуулах;

5.2.4. Байгууллагын сүлжээ, мэдээллийн системд нэвтэрсэн халдлагыг нэн даруй таслан зогсоож хариу үйлдэл хийх, хурдан хугацаанд системийг сэргээх арга хэмжээ авах;

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

5.2.6. Байгууллагын компьютерууд, дагалдах тоног төхөөрөмж, хэрэгслүүдийн ажиллагаа, шинэ тоног төхөөрөмжийн суурилуулалтыг хариуцах;

5.2.7. Компьютер, техник хэрэгслүүдийн битүүмжлэлийг хариуцаж, хяналт ажиллах;

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

5.2.9. Мэдээллийн нууцлал, аюулгүй байдлыг хангахад шаардагдах мэргэжилтнүүдэд сургалтад байнга хамрагдаж байх;

5.3. Хэрэглэгчийн үүрэг, хариуцлага:

5.3.1. Мэдээллийн нууцлал, аюулгүй байдалтай холбоотой зөрчил гарсан тохиолдолд системийн удирдагчид тухай бүрд нь мэдэгдэнэ;

5.3.2. Компьютерын нэр, сүлжээний нэрийг солихгүй байх. Шаардлага гарсан тохиолдолд системийн зохицуулагчид мэдэгдэн зохих үйлчилгээг хийлгэнэ;

5.3.3. Ажлын өрөө болон хонгилд ил, далд угсрагдсан сүлжээний утсууд өгсөн, орооцолдсон, далд монтажаас утас ил гарсан тохиолдолд байгууллагын холбогдох нэгж, мэргэжилтэнд мэдэгдэнэ;

5.3.4. Мэдээллийн нууцлал, аюулгүй байдлыг хангах талаар өгсөн системийн удирдагчийн шаардлагыг биелүүлнэ;

5.3.5. Өөрийн компьютерт түр холбосон гадны төхөөрөмжийг сүлжээнд нээж ашиглахгүй байх;

Зургаа. Хориглох зүйл

6.1. Хариуцаж буй компьютер техник хэрэгсэлд засвар, үйлчилгээг зөвшөөрөлгүй ажилны хүнээр хийлгэх;

6.2. Ажлын өрөө солих, байрлалаа шилжүүлэх тохиолдолд дур мэдэн сүлжээний талаар солих. Өөрийн компьютерт тохируулсан сүлжээний тохиргоог дур мэдэн өөрчлөх;

6.3. Мэдээлэл хадгалсан, мэдээлэл хадгалах хэрэгслийг буруу хадгалах, гэмтээх, өөрчлөх үрэгдүүлэх;

6.4. Сүлжээнд холбогдсон бусад компьютер доторх дундын хавтас дахь материалыг устгах;

6.5. Системийн удирдагч нь ажил үүргийн дагуу олгосон эрхээ буруугаар ашиглах;

6.6. Хувийн цахим хаягаар ажлын файл илгээхийг хориглоно.

Долоо. Хариуцлага

7.1. Ажилтны мэдээллийн аюулгүй байдлын журам зөрчсөний улмаас байгууллагын үйл ажиллагаанд хохирол учруулсан, эмзэг байдал үүсгэсэн нь эрүүгийн хариуцлага үүлээлгэхээргүй бол сахилгын шийтгэл ногдуулна.

7.2. Нууц мэдээллийг санаатай, санамсаргүй байдлаар бусдад задруулснаас үлгирсэн хохирлыг нөхөн төлүүлэх асуудлыг хууль, шүүхийн байгууллагаар шийдвэрлүүлнэ.