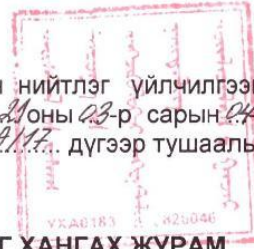


Нийслэлийн нийтлэг үйлчилгээний газрын
даргын 2011 оны 03-р сарын 04 ны өдрийн
.../117... дүгээр тушаалын хавсралт



МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ЖУРАМ

Нэг. Ерөнхий зүйл

- 1.1 Энэхүү журмын зорилго нь Нийслэлийн нийтлэг үйлчилгээний газар /цаашид байгууллага гэх/-ын мэдээллийн аюулгүй байдлын удирдлагын тогтолцоог бий болгох, мэдээллийн сүлжээ, системийн найдвартай ажиллагаа, мэдээллийн сангийн нууцлал, аюулгүй байдлыг хангах, гаднаас болон дотоодоос учирч болох аливаа халдлага эрсдэлээс урьдчилан сэргийлэхэд оршино.
- 1.2 Байгууллагын нийт ажилтан албан хаагчид энэхүү журмыг өдөр тутмын үйл ажиллагаандаа мөрдлөг болгон ажиллана.
- 1.3 Журамд хэрэглэгдэх нэр томъёог Нийслэлийн Засаг даргын 2013 оны А/477 дугаар захирамжаар баталсан "Мэдээллийн аюулгүй байдлыг хангах журам"-д зааснаар ойлгоно.

Хоёр. Мэдээллийн нууцлал, ангилал

- 2.1 Байгууллага дотор нээлттэй мэдээлэл:
 - 2.1.1 Байгууллагын ажилтан албан хаагчдад зориулагдсан нээлттэй мэдээ, мэдээллүүд багтах бөгөөд эдгээр мэдээллийг байгууллага дотроо хувилж олшруулж, тараахад хязгаарлалт тавихгүй, харин мэдээллийг гадагш задруулсан тохиолдолд хариуцлага тооцно.
 - 2.1.2 Байгууллага дотор нээлттэй мэдээлэлд ажилтан албан хаагчдад зориулагдсан мэдээ, мэдээллүүд, удирдлагаас өгсөн үүрэг даалгавар, өдөр тутмын үйл ажиллагааны мэдээллүүд хамаарна.
- 2.2 Нууц мэдээлэл:
 - 2.2.1 Байгууллагын нууцад хамаарах мэдээлэлд холбогдох хууль тогтоомж, дүрэм журмаар тодорхойлсон мэдээлэл болон энэхүү журамд заасан мэдээлэл хамаарах бөгөөд эдгээрийн жагсаалтыг газрын даргын тушаалаар баталгаажуулна.
 - 2.2.2 Нууцад хамаарах аливаа мэдээллийг ажил хэргийн хүрээнд олж мэдсэн этгээд цааш задруулахыг хориглоно.

Гурав. Мэдээллийн хадгалалт, хамгаалалт

- 3.1 Компьютер, серверийг хамгаалах:
 - 3.1.1 Байгууллага болон албан хаагч нь компьютер, серверийг орчны нөлөөлөөс хамгаалах үүрэг хүлээнэ.
 - 3.1.2 Программ болон техник хангамжийн суурилуулалт түүний шинэчлэл, тохиргоог зөвхөн мэдээллийн технологийн ажилтан хийнэ.
 - 3.1.3 Ажилтны компьютерыг форматлан үйлдлийн системийг дахин суулгах тохиолдолд хэрэгцээт файлуудыг өөр дискэнд хуулж, үйлдлийн системийг суулгаж тохируулга хийсний дараа файлын вирусийг шалгаж арилгаад, буцааж хуулна.
 - 3.1.4 Нууц зэрэглэлийн мэдээллийг шифрлэх, кодлох байдлаар хадгалж хамгаална.
 - 3.1.5 Байгууллагын сүлжээний байнгын ажиллагааг мэдээллийн технологийн ажилтан шалгаж хариуцна.

- 3.1.6 Мэдээллийн аюулгүй байдлыг хангах, мэдээлэлд зөвшөөрөлгүй нэвтрэх оролдлогыг таслан зогсоох, илрүүлэх зорилгоор байгууллагаас техникийн хяналтын систем байршуулах, программ хэрэгслийг нэвтрүүлэх ажлыг зохион байгуулж хэрэгжүүлнэ.
- 3.2 Мэдээлэл, программыг хадгалах:
 - 3.2.1 Архивын ажилтан цахим архив үүсгэж мэдээллийг хадгалах ба уг мэдээлэлд нэвтрэх эрхийг гагцхүү архивын ажилтан эзэмшинэ.
 - 3.2.2 Цахим архивт зөвхөн газрын даргын зөвшөөрлөөр нэвтэрч болох бөгөөд энэ тохиолдолд архивын ажилтан бүртгэл хөтөлнө.
 - 3.2.3 Хэрэглэгч нь цахим баримт бичиг боловсруулахдаа холбогдох стандартуудыг мөрдлөг болгоно.
 - 3.2.4 Хэрэглэгч нь тухайн ажлын байртай холбогдох бичиг баримтыг төрөлжүүлж өөрийн компьютерын нөөцөд хадгалах ба шаардлагатай бол зөвшөөрөгдсөн бусад санд хадгална.
 - 3.2.5 Хэрэглэгч нь албан хэрэгцээний файлаа нэр төрлөөр нь ангилж хавтас үүсгэн хадгална. Шаардлагатай бол дэд хавтас үүсгэн хадгалж, хэрэглэж хэвшинэ.
 - 3.2.6 Хэрэглэгч нь жил бүрийн эхний улиралд архивын ажилтанд өмнөх оны хадгалагдсан файл, хавтсаа байгууллагын мэдээллийн цахим сан хөмрөгт хадгалуулах зорилгоор хүлээлгэн өгнө.

**Дөрөв. Байгууллагын мэдээллийн систем, сүлжээ,
мэдээллийн сангийн нууцлал, хамгаалалт**

- 4.1 Биет хамгаалалт:
 - 4.1.1 Мэдээллийн системд холбогдсон компьютер, техник хэрэгслүүд нь газардуулгатай өрөөнд байрласан, тэжээлийн нөөц эх үүсвэрт холбогдсон байна.
 - 4.1.2 Байгууллагын ажилтан, албан хаагчид өөрийн компьютер дээр шууд харьяалах албан тушаалтны зөвшөөрөлгүйгээр гадны этгээдийг ажиллуулах, компьютерыг түгжилгүйгээр /screen lock, log off/ орхиж явахыг хориглоно.
 - 4.1.3 Байгууллагын ажилтан, албан хаагчид нууц үгийг дараах байдлаар боловсруулна:
 - а) Анхдагч нууц үгийг заавал солих.
 - б) Нууц үг нь үсэг, тоо, тэмдэгт ашигласан 8-аас багагүй оронтой байх.
 - в) Нууц үгийг бусдад дамжуулахгүй байх, илчлэгдсэн гэж үзвэл даруй солих.
 - д) Аюулгүй байдлын шаардлага хангасан нууц үгийг эргэн санахад хялбар байхаар логик дараалалтай үүсгэх.
 - е) Нууц үгээ ил бичиж тэмдэглэхийг хориглоно.
 - ф) Өөрийн болон гэр бүл, төрөл төрөгсөд, ойр дотны хүмүүсийн нэр, төрсөн он сар өдөр, утас, машины дугаар, зэрэг таныг таньдаг болон судалсан хүн мэдэж болох мэдээлэл, түүний урвуулсан хэлбэр, дан буюу дараалсан тоо, гарын хөдөлгөөнөөр амархан илрүүлж болох үг, өмнө нь хэрэглэж байсан нууц үг зэргийг нууц үгэнд хэрэглэхийг хориглоно.
- 4.2 Хортой кодоос хамгаалах:
 - 4.2.1 Байгууллагын хэрэгцээнд хэрэглэгдэж байгаа компьютер, мэдээлэл

- хадгалагч болон тээгч зөөврийн хэрэгслүүдэд зөвшөөрөгдсөн хортой кодын эсрэг програм хангамжийг ашиглана.
- 4.2.2 Хортой кодын эсрэг програмын шинэчлэлтийг тогтмол хийнэ.
- 4.2.3 Тодорхой хугацаанд системийн хортой кодын эсрэг програмыг уншуулж, илэрсэн тохиолдолд арилгах арга хэмжээг нэн даруй авна.
- 4.3 Мэдээллийн системд нэвтрэх эрхийг цуцлах:
- 4.3.1 Мэдээллийн сан, мэдээллийн системд хандах эрх бүхий албан хаагч ажлаас гарсан, халагдсан, өөр ажилд шилжсэн тохиолдолд нэвтрэх эрхийг цуцална.
- 4.3.2 Мэдээллийн систем, мэдээллийн санд нэвтрэх эрх бүхий ажилтан мэдээллийн аюулгүй байдлын бодлого, журмыг зөрчсөн байвал системд нэвтрэх эрхийг системийн зохицуулагчийн зүгээс түдгэлзүүлж болно.

Тав. Байгууллагын мэдээллийн аюулгүй байдал хариуцсан ажилтны эрх, үүрэг

- 5.1 Ажил үүргийн хуваарийн дагуу мэдээллийн аюулгүй байдлыг шалгах зорилгоор мэдээллийн систем, ажилтнуудын компьютерт нэвтрэх;
- 5.2 Аюулгүй байдлын шаардлагыг зөрчигчдөд хариуцлага тооцох талаар байгууллагын удирдлагад санал оруулах;
- 5.3 Байгууллагад ашиглагдах мэдээллийн систем, техник технологи худалдан авах болон шинээр нэвтрүүлэх үйл явцад хяналт тавих;
- 5.4 Мэдээллийн систем, сангийн бүрэн бүтэн байдалд хяналт тавих, мэдээллийн сангийн нөөц хувийг хувилж хадгалах нөхцөлийг хангах;
- 5.5 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;
- 5.6 Мэдээллийн системийг байгуулах, турших, ашиглах, засвар үйлчилгээ хийх, хэвийн үйл ажиллагааг хангах;
- 5.7 Мэдээллийн аюулгүй байдлыг хангахад чиглэсэн сургалт, сурталчилгааг байгууллагын албан хаагчдад зориулан зохион байгуулах;
- 5.8 Байгууллагын компьютерууд, дагалдах тоног төхөөрөмж, хэрэгслүүдийн ажиллагаа, шинэ тоног төхөөрөмжийн суурилуулалтыг хариуцах;
- 5.9 Байгууллагын үйл ажиллагааны явцад үүссэн мэдээ мэдээллийг бэлтгэдэг, дамжуулдаг, хүлээн авдаг, хадгалдаг албан хаагч бүр тухайн мэдээллийн аюулгүй байдлыг хангаж, хамгаалах үүрэг хүлээнэ.

Зургаа. Мэдээллийн системийн хэрэглэгчийн үүрэг

- 6.1 Мэдээллийн аюулгүй байдалтай холбоотой асуудал гарсан даруй системийн зохицуулагчид мэдэгдэж, шаардлагатай арга хэмжээг авч ажиллах;
- 6.2 Компьютерын нэр, сүлжээний нэрийг солихгүй байх, шаардлага гарсан тохиолдолд системийн зохицуулагчид мэдэгдэн зохих үйлчилгээг хийлгэх;
- 6.3 Ажлын өрөө болон нийтийн эзэмшлийн талбайд ил болон далд угсрагдсан сүлжээний утсууд гэмтсэн, орооцолдсон, далд монтажаас утас ил гарсан тохиолдолд байгууллагын холбогдох нэгж, мэргэжилтэнд мэдэгдэх;
- 6.4 Мэдээллийн аюулгүй байдлыг хангах талаар системийн зохицуулагчаас өгсөн заавар, шаардлагыг биелүүлэх;
- 6.5 Байгууллагын нууцад хамаарах мэдээ мэдээллийн аюулгүй байдлыг хангаж ажиллах, ажил хэргийн хүрээнд олж авсан мэдээллийг цааш задруулахгүй

- байх;
- 6.6 Энэхүү журамд заасан хориглох зүйлийг зөрчихгүй байх;
- 6.7 Өөрийн компьютерт шаардлагагүй дундын хавтас сүлжээнд нээхгүй байх, сүлжээнд нээсэн дундын хавтас дотор чухал мэдээ материал, өгөгдлийг удаан хугацаагаар хадгалахгүй байх.

Долоо. Хориглох зүйл

- 7.1 Албан хэрэгцээнээс бусад зөвшөөрөлгүй программ хангамжийг суулгаж ажиллуулах;
- 7.2 Интернетээс албан ажилтай холбогдолгүй програм, дуу, кино, зураг, тоглоом зэрэг мэдээлэл татах;
- 7.3 Байгууллагын бус компьютер, зөөврийн хэрэгслийг сүлжээнд зөвшөөрөлгүй холбох, мэдээлэл авах, солилцох;
- 7.4 Бусдад компьютер, техник хэрэгслээ хэрэглүүлэх, сүлжээнд нэвтрүүлэх, компьютер, серверийн нэвтрэх нэр, нууц үгийг дамжуулах, мэдээллэх;
- 7.5 Хариуцаж буй компьютер техник хэрэгсэлд засвар, үйлчилгээг зөвшөөрөлгүй гадны хүнээр хийлгэх;
- 7.6 Компьютерыг түгжилгүйгээр /screen lock, log off/ орхиж явах;
- 7.7 Ажлын өрөө солих, байрлалаа шилжүүлэх тохиолдолд дур мэдэн сүлжээний утсаа солих, өөрийн компьютерт тохируулсан сүлжээний тохиргоог дур мэдэн өөрчлөх;
- 7.8 Өөрийн компьютерт шаардлагагүй дундын хавтас сүлжээнд нээх, сүлжээнд нээсэн дундын хавтас дотор чухал мэдээ материал, өгөгдлийг удаан хугацаагаар хадгалахгүй байх;
- 7.9 Сүлжээнд холбогдсон бусад компьютер доторх дундын хавтас дахь материалыг устгах;
- 7.10 Нууцад хамаарах мэдээлэл хадгалагдаж буй өрөө тасалгаа, шүүгээ савыг түгжилгүй орхих, эдгээр мэдээллийг удирдлагын зөвшөөрөлгүй хадгалж буй газраас авч гарах, өөр газарт байршуулах;
- 7.11 Ажил хэргийн хүрээнд олж мэдсэн нууцад хамаарах аливаа мэдээ мэдээллийг бусдад дамжуулах, хувийн зорилгоор хуулбарлах, зураг авах, бичлэг хийх;
- 7.12 Системийн зохицуулагчаас ажил үүргийн дагуу олгосон эрхийг урвуулан ашиглах;
- 7.13 Хууль тогтоомж, дүрэм журмаар хориглосон бусад хэм хэмжээг зөрчих.

Найм. Хариуцлага

- 8.1 Ажилтан, албан хаагчдын санаатай болон санамсаргүй үйлдлээс болж мэдээллийн системийн сүлжээний аюулгүй байдал алдагдах, мэдээллийн аюулгүй байдлын бодлого, журам зөрчигдөх, нууцад хамаарах мэдээ мэдээлэл алдагдах зэргээр байгууллагын үйл ажиллагаанд хохирол учруулсан нь эрүүгийн хариуцлага хүлээхээргүй бол Хөдөлмөрийн тухай хуулийн 131 дүгээр зүйл, Хөдөлмөрийн дотоод журмын 7 дугаар зүйлд заасан сахилгын шийтгэлийн аль нэгийг шат дараалал харгалзахгүйгээр ногдуулна.
- 8.2 Нууц мэдээллийг санаатай буюу санамсаргүй байдлаар бусдад задруулснаас байгууллагад учирсан хохирлыг нөхөн төлүүлэх түүнчлэн Эрүүгийн хууль, Захиргааны хариуцлагын тухай хууль, Байгууллага, хувь

хүний нууцын тухай хуулийн зохих заалтын дагуу асуудлыг шүүхийн байгууллагаар шийдвэрлүүлнэ.