УЛААНБААТАР ХОТЫН МУЗЕЙН ЗАХИРЛЫН ТУШААЛ

2015 оны 09 сарын 15 өдөр Дугаар А/46 Улаанбаатар хот

Мэдээллийн аюулгүй байдлыг хангах журам батлах тухай

Монгол Улсын "Засаг захиргаа нутаг дэвсгэрийн нэгж, түүний удирдлагын тухай" хуулийн 33 дугаар зүйлийн 33.5 дахь хэсэг, Нийслэлийн Засаг даргын 2013 оны 05 сарын 14 өдрийн А/477 дугаар захирамжийг үндэслэн ТУШААХ нь:

1. Музейн мэдээллийн аюулгүй байдлыг хангах журмыг хавсралтаар батлагдсугай.

2. Батлагдсан журмыг үйл ажиллагаандаа мөрдлөг болгон ажиллахыг мэдээлэл технологийн ажилтан /Д.Болд/ -д үүрэг болгосугай.

ЗАХИРАЛ С. ЦАЦРАЛТ

D: /tushaal/2015 tushaal/tushaalA/A4.doc

Улаанбаатар хотын музейн захирлын
2015 оны 09 дүгээр сарын 15-ны өдрийн
А/1[illegible] дугаар тушаалын хавсралт

УКЖ0080 909[illegible]104

УЛААНБААТАР ХОТЫН МУЗЕЙН
МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ЖУРАМ

Нэг. Зорилго

1.1. Улаанбаатар хотын музей /цаашид музей гэх/-н мэдээллийн аюулгүй байдал, дотоод 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 нэн даруй засаж, сэргээх, хариу арга хэмжээ авахад оршино.

Хоёр. Хамрах хүрээ

2.1. Музейн нийт ажилтан албан хаагчид, мэдээллийн технологийн мэргэжилтэн ажил үүргээ гүйцэтгэхдээ энэхүү журмыг мөрдлөг болгон ажиллана.

Гурав. Нэр томьёо

3.1.Мэдээлэл - гэдэг нь эзэмшиж, хадгалж байгаа төхөөрөмжөөс үл хамааран боломжит бүх л хэлбэрээр оршин байгаа, уншиж ойлгож болох бүх төрлийн баримт бичиг, мэдээ, мэдээлэл, биет зүйлсийг;

3.2.Хадгалагдах мэдээлэл – Даргын тушаал, шийдвэр, мэдээлэл судалгаа, санхүүгийн мэдээлэл, тайлан мэдээ

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

3.4.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.

3.5.Аюул занал - гэж систем болон байгууллагад хор учруулж болох мэдээллийн аюулгүй байдлыг ямар нэг байдлаар зөрчиж болох боломж, үйлдэл, үйл явдлыг;

3.6.Өмч хөрөнгө - гэж байгууллагын аливаа биет болон биет бус юмс, эд зүйл, мэдээлэл, түүнтэй холбоотой аливаа юмс, эд зүйл;

3.7.Нөөц – гэж тухайн ажилтны локал “Д” диск

3.8.Зохицуулагч - гэж байгууллагын мэдээллийн технологи хариуцсан эрх, үүрэг бүхий мэргэжилтэн

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

Дөрөв. Мэдээлэл

4.1 Мэдээллийн өмч хөрөнгийн ангилал

4.1.1. Биет мэдээллийн хөрөнгө гэдэг нь судалгааны материалууд, үйл ажиллагааны төлөвлөгөө, төсөл хөтөлбөрүүд, бүртгэлийн мэдээллүүд, сургалтын материал, тараах хуудсууд, гарын авлага, хяналт шалгалтын тайлан, хэвлэмэл зургууд зэрэг бүх төрлийн хэвлэмэл мэдээллийг;

4.1.2. Цахим мэдээллийн хөрөнгө гэдэг нь биет мэдээллийн, цахим хэлбэрүүд, өгөгдлийн сангийн өгөгдлүүд болон бусад төрлийн цахим мэдээллийг;

4.1.3. Програм хангамжийн хөрөнгө гэдэг нь зөвшөөрөлтэй хэрэглээний, мэргэжлийн болон системийн програм хангамж, өөрсдийн боловсруулсан болон тусгай захиалгаар хийлгэсэн програм хангамжууд, системүүд

4.1.4. Техник хангамжийн хөрөнгө гэдэг нь компьютер ба харилцаа холбооны төхөөрөмжүүд (процессор, дэлгэц, зөөврийн компьютер, телефон, факсын аппарат), зөөврийн төхөөрөмжүүд (зөөврийн хард диск, флаш, диск, хуурцаг), сүлжээний тоног төхөөрөмжүүд (рутер, свич, сүлжээний утас, толгой) зэрэг бүх төрлийн мэдээлэл боловсруулах, дамжуулах, хадгалах хэрэгслүүдийг;

4.2 Мэдээлэл хадгалалт

4.2.1.Хэрэглэгч нь тухайн ажлын байртай холбогдох баримт бичгийг төрөлжүүлж, өөрийн компьютерийн нөөцөд хадгална. Шаардлагатай бол зохицуулагчид өгч хадгалуулна.

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

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

4.2.4 Хадгалагдах мэдээллийг зохицуулагч жил бүр архивлана.

4.3.Мэдээллийн хамгаалалт

4.3.1.Байгууллагын мэдээлэл гаргадаг, хүлээн авдаг, боловсруулдаг, дамжуулдаг, хадгалдаг албан хаагч бүр мэдээллийг хамгаалах үүрэг хүлээнэ.

4.3.2.Байгууллагын ажилтан, албан хаагчид өөрийн, компьютер дээр шууд харьяалах албан тушаалтны зөвшөөрөлгүйгээр гадны этгээдийг ажиллуулахыг хориглоно.

4.3.3 Байгууллагын ажилтан бүр өөрийн комьютер дээрээ нэвтрэх нууц үгийг нээнэ.

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

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

4.4.Вирусээс хамгаалах

4.4.1.Байгууллагын хэрэгцээнд хэрэглэгдэж байгаа компьютер, мэдээлэл хадгалагч болон тээгч зөөврийн хэрэгслүүдэд лицензтэй, антивирусын програм хангамжийг ашиглана.

4.4.2. Антивирусын програмын шинэчлэлтийг тогтмол жил бүр хийнэ.

4.4.3. Вирус илэрсэн тохиолдолд арилгах арга хэмжээг авна.

4.4.4. Гаднаас зөөврийн хадгалах төхөөрөмж системд оруулах бол заавал вирусын эсрэг програм уншуулах

Тав. Эрх, үүрэг

5.1. Системийн зохицуулагчийн эрх

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

5.1.2. Мэдээллийн аюулгүй байдлын шаардлага зөрчиж буй хэрэглэгчийн эрхийг хаах, тэдгээрийн ажиллагааг хэсэгчлэн болон бүрэн зогсоох.

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

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

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

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

5.1.7. Байгууллагын компьютерын системд 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.

5.2.Системийн зохицуулагчийн үүрэг

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

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

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

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

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

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

5.3 Хэрэглэгчийн үүрэг, хариуцлага

5.3.1. Мэдээллийн аюулгүй байдалтай холбоотой асуудал гарсан тохиолдолд системийн зохицуулагчид тухай бүрд мэдэгдэнэ.

5.3.2. Систем болон үйлчилгээнд ажиглагдсан, байж болох сул талд анхаарлаа хандуулах, түүний тухай мэдээлэх,

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

5.3.4. Ажлын өрөө болон хонгилд ил болон далд угсрагдсан сүлжээний утсууд гэмтсэн, ороцолдсон, далд монтажаас утас ил гарсан тохиолдолд байгууллагын холбогдох нэгж, мэргэжилтэнд мэдэгдэх,

5.3.5. Мэдээллийн аюулгүй байдлыг хангах талаар өгсөн системийн зохицуулагчийн шаардлагыг биелүүлэх,

Зургаа. Хориглох зүйл

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

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

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

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

6.5. Системийн зохицуулагч нь ажил үүргийн дагуу олгосон эрхээ буруугаар ашиглах.

Долоо. Хариуцлага

7.1. Ажилтны анхаарал болгоомжгүй үйлдлээс болж мэдээллийн системийн аюулгүй байдал алдагдах, мэдээллийн аюулгүй байдлын бодлого, журам зөрчигдөж, байгууллагын үйл ажиллагаанд хохирол учруулсан нь эрүүгийн хариуцлага хүлээлгэхээргүй бол Хөдөлмөрийн хуулийн 131-р зүйлийн дагуу дор дурдсан хэлбэрийн сахилгын шийтгэлийн аль нэгийг шат дараалан харгалзахгүйгээр шийдвэр гаргаж ногдуулна.

7.1.1 Сануулах;

7.1.2 Үндсэн цалинг 3 сар хүртэл хугацаагаар 20 хүртэл хувиар бууруулах;

7.1.3 Ажлаас халах;

7.2. 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