



ДИПЛОМАТ БАЙГУУЛЛАГЫН
ҮЙЛЧИЛГЭЭГ ЭРХЛЭХ ГАЗРЫН
ЗАХИРЛЫН ТУШААЛ

2019 оны 08 сарын 27 өдөр

Дугаар А/102

Улаанбаатар хот

“Дипломат байгууллагын үйлчилгээг эрхлэх газрын мэдээллийн аюулгүй байдлыг хангах журам”-ыг батлах тухай

Төрийн болон орон нутгийн өмчийн тухай хуулийн 20.1.10, “Дипломат байгууллагын үйлчилгээг эрхлэх газар” ТӨҮГ-ын дүрмийн 5.5.8 дахь хэсгийг тус тус үндэслэн ТУШААХ нь:

1. “Дипломат байгууллагын үйлчилгээг эрхлэх газрын мэдээллийн аюулгүй байдлыг хангах журам”-ыг хавсралтаар баталсугай.
2. Тушаалын хэрэгжилтийг хангаж ажиллахыг нийт албан хаагчдад, тушаалын хэрэгжилтэд хяналт тавьж ажиллахыг Захиргааны хэлтэст тус тус даалгасугай.

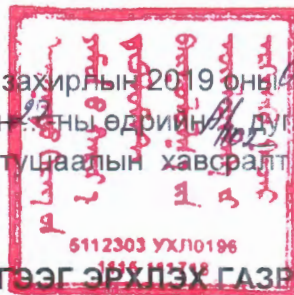
ЗАХИРАЛ



Ё.НЯМЖАВ

201900696

ДБҮЭГ-ын захирлын 2019 оны 48 дугаар
сарын 2-ны өдрийн 1 дугаар
тушаалын хавсралт



ДИПЛОМАТ БАЙГУУЛЛАГЫН ҮЙЛЧИЛГЭЭГ ЭРХЛЭХ ГАЗРЫН МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ЖУРАМ

НЭГ.ЗОРИЛГО

1.1. Энэхүү журмын зорилго нь “Дипломат байгууллагын үйлчилгээг эрхлэх газар” ТӨҮГ-ын мэдээллийн сүлжээ, системийн найдвартай ажиллагаа, мэдээллийн сангийн нууцлал, аюулгүй байдлыг хангах, учирч болох аюул заналаас урьдчилан сэргийлэхэд оршино.

ХОЁР. ХАМРАХ ХҮРЭЭ

2.1. Байгууллагын нийт албан хаагчид, мэдээллийн технологийн мэргэжилтэн ажил үүргээ гүйцэтгэхдээ энэ журмыг мөрдлөг болгон ажиллана.

ГУРАВ. БАЙГУУЛЛАГЫН МЭДЭЭЛЛИЙН ХАМГААЛАЛТ

3.1. Мэдээллийн хамгаалалт.

3.1.1. Байгууллагын мэдээлэл гаргадаг, хүлээн авдаг, боловсруулдаг, дамжуулдаг, хадгалдаг албан хаагч бүр мэдээллийг хамгаалах үүрэгтэй.

3.1.2. Ажилтнууд өөрийн компьютер дээр гаднын этгээдийг ажиллуулахыг хориглоно.

3.1.3. Ажилтан бүр өөрийн компьютер дээр нэвтрэх нууц үгийг нээх ба нууц үг нь том, жижиг үсэг, тоо холилдсон, 10 тэмдэгтээс доошгүй байна. Нууц үгийг 6 сар тутамд шинэчилнэ.

3.1.4. Ажилтан бүр өөрийн компьютерт нэвтрэх нууц үгийг хамгаалах үүрэгтэй ба бусдад дамжуулахгүй. Нууц үгийг бусдад харагдахуйц байдлаар бичиж, тэмдэглэхийг хориглоно.

3.1.5 Байгууллагын серверийн өрөөнд зөвшөөрөлгүй нэвтрэхийг хориглоно.

3.2. Хортой кодоос хамгаалах

3.2.1. Байгууллагын хэрэгцээнд ашиглаж байгаа компьютер, мэдээлэл хадгалагч болон зөөврийн хадгалагч хэрэгслүүдэд олон улсын болон Монгол улсын стандартад нийцсэн хууль ёсны лицензтэй /вирус/ программ хангамжийг ашиглана.

3.2.2. Хортой кодын эсрэг программын шинэчлэлтийг жил бүрийн *1 дүгээр улиралд тогтмол хийнэ.

3.2.3. Ажилтан нь компьютерт хортой кодын эсрэг программыг 14 хоног тутамд тогтмол уншуулж, вирус илэрсэн тохиолдолд арилгах арга хэмжээг авна.

3.3. Тоног төхөөрөмжийн нууцлал, хамгаалалт,

3.3.1. Байгууллагын компьютер, техник хэрэгслийг гэрчилгээжүүлсэн байна. Гэрчилгээг мэдээллийн технологийн мэргэжилтэн хөтлөх бөгөөд засвар үйлчилгээ хийсэн, шинэ программ хангамж суулгах, үйлдлийн системийг дахин суулгах тохиолдолд тэмдэглэл үйлдэж, компьютер, тоног төхөөрөмжийг эзэмшигчээр гарын үсэг зуруулж баталгаажуулж байна.

3.3.2. Байгууллагын компьютер, техник хэрэгсэлд серверийн тоног төхөөрөмж, компьютер, хэвлэх, хувилах төхөөрөмж, сүлжээний кабел, зөөврийн хадгалах төхөөрөмж, камер, камерын тоног төхөөрөмж хамаарна.

3.3.3. Программ болон техник хангамжийн суурилуулалт түүний шинэчлэл, тохиргоог зөвхөн мэдээллийн технологийн ажилтан хийнэ.

3.3.4. Ажилтны компьютерыг форматлан үйлдлийн системийг дахин суулгах тохиолдолд хэрэгцээт файлуудыг өөр дискэнд хуулж, үйлдлийн системийг суулгаж, тохируулга хийсний дараа файлын вирусыг шалган, арилгаад буцаан хуулна.

3.3.5. Систем суулгах, өөрчлөлт оруулах бүрд гэрчилгээнд тэмдэглэл хийн ажилтан, мэдээллийн технологийн мэргэжилтэн гарын үсэг зурна.

3.3.6. Байгууллагын сүлжээний байнгын хэвийн ажиллагааг мэдээллийн технологийн ажилтан хариуцна.

3.3.7. Сүлжээний кабелийн үзүүрт хаяг хадан, ашиглагдаагүй гаралтуудыг тэмдэглэж наана.

ДӨРӨВ. АЛБАН ХААГЧДЫН ХҮЛЭЭХ ҮҮРЭГ

4.1. Мэдээллийн аюулгүй байдлыг хангах чиглэлээр албан хаагчид дараах үүргийг хэрэгжүүлнэ.

4.1.1. Албан ажлын хэрэгцээнд хариуцуулж өгсөн компьютер, тоног төхөөрөмжийн аюулгүй байдал, бүрэн бүтэн байдлыг хариуцаж, зөвхөн албан хэрэгцээнд ашиглах.

4.1.2. Компьютер, тоног төхөөрөмжийг гаднын этгээдэд ашиглуулахгүй, зөвшөөрөлгүйгээр гадны этгээдээр засварлуулахгүй байх.

4.1.3. Ажлын байртай холбогдох баримт бичгийг төрөлжүүлж, өөрийн компьютерт хадгална. Албан хэрэгцээний файлыг нэр, төрлөөр нь ангилж, хавтас үүсгэн хадгалах.

4.1.4. Мэдээллийн аюулгүй байдлын холбоотой тохиолдлыг мэдээллийн технологийн ажилтанд яаралтай мэдэгдэх.

4.1.5. Албан хаагчид нь өөрийн ажлын байрны компьютер дэх албаны программ, мэдээллийг бусдад хуулбарлан өгөх шилжүүлэхийг хориглоно.

4.1.6. Ашиглаж буй компьютерт хортой кодын эсрэг программыг жил бүр шинэчлэн суулгуулах.

4.1.7. Дотоод сүлжээгээр зөвхөн баримт бичгийн төсөл, албан хэрэглээний мэдээллүүдийг солилцох.

4.1.8. Хувийн болон албаны бус компьютер, зөөврийн санах төхөөрөмж, санах байгууламж бүхий хэвлэх олшруулах техник хэрэгслийг ажлын байранд авч ирэх, албан хэрэгцээнд ашиглахыг хатуу хориглоно.

ТАВ. МЭДЭЭЛЛИЙН ТЕХНОЛОГИЙН АЖИЛТНЫ ЭРХ, ҮҮРЭГ

5.1. Мэдээллийн технологийн ажилтан мэдээллийн аюулгүй байдлыг хангах хүрээнд дараах эрх, үүрэгтэй байна.

5.1.1. Ажил үүргийн хуваарийн дагуу мэдээллийн аюулгүй байдлыг шалгаж, хяналт тавих.

5.1.2. Байгууллагад ашиглагдаж байгаа компьютер, тоног төхөөрөмжийн бүртгэлийг хөтөлж, гэрчилгээжүүлэх, тоног төхөөрөмжийг шинэчлэх, засварлах, шинэ технологи нэвтрүүлэх талаар саналаа боловсруулж, шийдвэрлүүлэх.

5.1.3. Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээг жил бүр хийж, удирдлагад танилцуулж байх.

5.1.4. Мэдээллийн системийг байгуулах, турших, ашиглах, засвар үйлчилгээг хийх.

5.1.5. Мэдээллийн сан, программ хангамж, компьютерыг хортой кодос хамгаалах арга хэмжээг авах.

5.1.6. Ажилтнуудын компьютер техник хэрэгсэлд үзлэг хийн, бүртгэлжүүлэх холбогдох засвар үйлчилгээг хийх, мэргэжлийн байгууллагад хандан тоног төхөөрөмжийн хэвийн ажиллагааг хангах.

5.1.7. Захирлын тушаал шийдвэр, газрын төлөвлөгөө, тайлан, захирлын зөвлөлийн болон шуурхай хурлын тэмдэглэл, уулзалт ярианы тэмдэглэл, ойн арга хэмжээний баримтууд зэрэг байгууллагын байнга хадгалах баримт бичгийг дараа оны 1-р улиралд багтаан цахим хэлбэрээр архивлах ажлыг мэдээлэл технологийн мэргэжилтэн, архив, бичиг хэргийн мэргэжилтэн хамтран гүйцэтгэх.

5.1.8. Мэдээллийн системийн талаарх сургалт семинарт хамрагдан өөрийн мэдлэг, мэргэжлийг дээшлүүлэх, мэдээлэл технологийн аюулгүй байдлыг хангах, хамгаалах чиглэлээр ажилтнуудыг мэдээ, мэдээллээр хангах, сургалт хийх.

5.1.9. Хамгаалагдсан мэдээлэлд зөвшөөрөлгүй хандах оролдлогыг илрүүлж, таслан зогсоох зорилготой аюулгүй байдлын хяналтыг тасралтгүй хийх.

5.1.10. Байгууллагын мэдээлэл технологитой холбоотой бүх програм хангамж, техник хангамж, мэдээллийн системийн сүлжээ, мэдээллийг хадгалах зөөвөрлөх, сүлжээгээр дамжуулах арга хэмжээг хариуцан ажиллах.

5.1.11. Ажилтнуудын ажлын файлын эмх цэгц, компьютерын нууц үгийн хамгаалалт, зөвшөөрөгдөөгүй програм суулгасан эсэх зэргийг улиралд 1 удаа, дотоод хяналт шалгалтын мэргэжилтний хамт шалгаж, холбогдох арга хэмжээг авах.

5.1.12. Байгууллагын хяналтын камерын хэвийн ажиллагааг хариуцан ажиллах ба хяналтын камерын бичлэгийг 10-30 хүртэл хоногоор хадгалах горимоор тогтооно. Камерын бичлэгийг нөхөж үзэх тохиолдолд Захиргааны хэлтсийн даргаас зөвшөөрөл авна.

ЗУРГАА. ХАРИУЦЛАГА

6.1. Энэхүү журмыг зөрчсөн буруутай ажилтанд хөдөлмөрийн дотоод журам болон холбогдох хууль тогтоомжид заасан хариуцлага хүлээлгэнэ.