



МОНГОЛ УЛСЫН
ЭРҮҮЛ МЭНДИЙН ЯАМ

14210 Улаанбаатар хот, Сүхбаатар дүүрэг,
Олимпийн гудамж 2, Засгийн газрын VIII байр,
Утас: 26-36-95, Факс: (976-11) 32-35-41
И-мэйл: moh@moh.gov.mn, http://www.moh.gov.mn

2023.04.28 № 4/1933

танай _____ -ны № _____ -т

АЙМАГ, НИЙСЛЭЛИЙН ЭРҮҮЛ
МЭНДИЙН ГАЗАР БОЛОН ХАРЬЯА
БАЙГУУЛЛАГУУДЫН ДАРГА ЗАХИРАЛ
НАРТ

Эрүүл мэндийн сайдын “Эрүүл мэндийн цахим мэдээллийн аюулгүй байдлыг хангаж ажиллах тухай” 2023 оны 04 дүгээр сарын 28-ны өдрийн 03 дугаар Албан даалгаврыг хүргүүлж байна.

Засгийн газрын 2022 оны 207 дугаар тогтоолоор баталсан Онц чухал мэдээллийн дэд бүтэцтэй өөрийн харьяа байгууллагуудад яаралтай хүргүүлнэ үү.

Хавсралт... хуудастай.

БОДЛОГО ТӨЛӨВЛӨЛТИЙН ГАЗРЫН
ДАРГЫН АЛБАН ҮҮРГИЙГ ТҮР ОРЛОН
ГҮЙЦЭТГЭГЧ П.ОЮУНЦЭЦЭГ

1118270972 - 9037443

145224509



МОНГОЛ УЛСЫН
ЭРҮҮЛ МЭНДИЙН САЙДЫН
АЛБАН ДААЛГАВАР

2023 оны 04 сарын 28 өдөр

Дугаар 03

Улаанбаатар хот

Эрүүл мэндийн цахим мэдээллийн
аюулгүй байдлыг хангаж ажиллах тухай

Төрийн болон албаны нууцын тухай хууль, Кибер аюулгүй байдлын тухай хуулийн 10.1.5, Засгийн газрын 2022 оны 05 дугаар сарын 25-ны өдрийн 207 дугаар тогтоолыг тус тус үндэслэн “Онц чухал мэдээллийн дэд бүтэцтэй байгууллагын жагсаалт”-д багтсан эрүүл мэндийн байгууллагуудын дарга, захирал нарт даалгах нь:

1. Байгууллагын нууц хадгалах ажилтанг Тагнуулын байгууллагын аюулгүй байдлын шалгалтад хамруулж томилох.

2. Байгууллагын удирдлага өөрийн болон харьяа байгууллагын хэмжээнд төрийн болон албаны нууцыг хамгаалах тухай хууль тогтоомжийн хэрэгжилтийг зохион байгуулж ажиллах.

3. Төрийн болон албаны нууцтай танилцах эрх бүхий албан тушаалтнууд Төрийн болон албаны нууцын тухай хуулийн 13 дугаар зүйл “Жагсаалт батлах тухай” Засгийн газрын 2017 оны 247 дугаар тогтоолоор баталсан “Эрүүл мэндийн салбарын төрийн нууцад хамаарах мэдээллийн жагсаалт”, Эрүүл мэндийн сайдын 2020 оны 5 дугаар сарын 04-ний өдрийн А/279 дугаар тушаалаар баталсан “Албаны нууцын жагсаалт”-ыг нийт албан хаагчдад танилцуулж, төрийн болон албаны нууцыг хамгаалах чиглэлээр сургалт, мэдээлэл зохион байгуулж, тогтмол мэргэжил арга зүйн туслалцаа үзүүлэх.

4. Төрийн болон албаны нууцын хадгалалт, хамгаалалтыг боловсронгуй болгох, нууц хамгаалах ажлыг зохион байгуулахад шаардлагатай хөрөнгийг төсөвтөө тусгаж, шийдвэрлүүлэх ажлыг зохион байгуулах.

5. Цахим системд хандаж буй хэрэглэгчдэд нууц үгийн стандарт мөрдүүлэх.

6. Цахим системийн өгөгдлийн санд хандаж буй хэрэглэгчдээс нууцын баталгаа авах.

7. Кибер аюулгүй байдлын тухай хуулийн 19 дүгээр зүйлийн 19.2 дахь хэсэгт заасан Онц чухал мэдээллийн дэд бүтэцтэй байгууллагын үүргийг хэрэгжүүлэх, хэрэгжилтэд хяналт тавих. Үүнд:

7.1 кибер аюулгүй байдлыг хангах үйл ажиллагааны дотоод журам батлах;

7.2 кибер халдлага, зөрчлийн үед дагаж мөрдөх төлөвлөгөөг баталж хэрэгжүүлэх;

7.3 мэдээллийн аюулгүй байдлыг хангах талаар стандартыг нэвтрүүлэх;

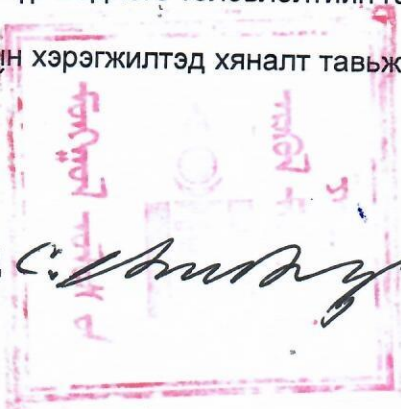
7.4 кибер аюулгүй байдлыг хангах үйл ажиллагаа хариуцсан нэгж, эсхүл албан тушаалтантай байх;

7.5 кибер аюулгүй байдлын эрсдэлтийн үнэлгээг жил тутамд, эсхүл мэдээллийн систем, мэдээллийн сүлжээний өөрчлөлт хийгдэх бүрд хэсэгчлэн, эрх бүхий байгууллагын шаардсанаар тухай бүр хийлгэж, гарсан дүгнэлт, зөвлөмж, шаардлагын дагуу холбогдох арга хэмжээг авч хэрэгжүүлэх;

- 7.6 мэдээллийн аюулгүй байдлын аудитыг хоёр жил тутамд хийлгэх;
- 7.7 мэдээллийн систем, мэдээллийн сүлжээний аюулгүй байдлыг хангахад шаардлагатай удирдлага, зохион байгуулалтын болон техникийн арга хэмжээг төлөвлөх, хэрэгжүүлэх;
- 7.8 кибер халдлага, зөрчлийг илрүүлэх, бүртгэх, таслан зогсоох мэдээллийн системтэй байх;
- 7.9 мэдээллийн систем, мэдээллийн сүлжээний үйлдлийн бүртгэлийг кибер аюулгүй байдлын нийтлэг журамд заасан хугацаанд хадгалах;
- 7.10 кибер аюулгүй байдлын эрсдэлийн үнэлгээний болон мэдээллийн аюулгүй байдлын аудитын тайланг хүлээн авснаас хойш нэг сарын дотор кибер халдлага, зөрчилтэй тэмцэх холбогдох төвд хүргүүлэх;
- 7.11 эрх бүхий байгууллагаас хүргүүлсэн зөвлөмж, шаардлагыг биелүүлэх, илэрсэн алдаа, зөрчлийг арилгах арга хэмжээг авах;
- 7.12 гадаадын иргэн, гадаадын хуулийн этгээдээр кибер аюулгүй байдлын эрсдэлийн үнэлгээг хийлгэх тохиолдолд тагнуулын байгууллагаас санал авах;
- 7.13 хариуцсан мэдээллийн систем, дэд бүтцийн хэвийн, найдвартай, тасралтгүй байдлыг хангах, гэмтэл саатлын үед сэргээн ажиллуулах төлөвлөгөөтэй байх;
- 7.14 кибер халдлага, зөрчлийн улмаас мэдээллийн систем, дэд бүтцийн хэвийн үйл ажиллагаа алдагдсан, тасралтгүй үйл ажиллагааг хангах боломжгүй болсон даруйд энэ талаар кибер халдлага, зөрчилтэй тэмцэх холбогдох төвд мэдэгдэх;
- 7.15 төлөвлөгөөт үзлэг шалгалт, өөрийн дэд бүтцээс гаднах сүлжээ, системд гарсан гэмтэл, саатал, гэнэтийн болон давагдашгүй хүчний шинжтэй нөхцөл байдлын улмаас дэд бүтцийн хэвийн, тасралтгүй үйл ажиллагааг хангах боломжгүй бол энэ талаар кибер халдлага, зөрчилтэй тэмцэх холбогдох төв, хэрэглэгчид даруй мэдэгдэх.
8. Эмнэлгийн тусламж үйлчилгээнд ашиглаж байгаа сервер тоног төхөөрөмж, компьютер, сүлжээний төхөөрөмжийг шинэчилэх тохиолдолд Тагнуулын ерөнхий газарт биет байдлаар хүлээлгэн өгч баталгаажуулсны дараа ашиглах.
9. Төрийн мэдээллийн нэгдсэн сүлжээнд холбогдсон болон Онц чухал мэдээллийн дэд бүтэцтэй төрийн өмчит хуулийн этгээд нь Тагнуулын байгууллагаас гадаад улсын зээл, тусламж, хөрөнгө оруулалтаар хэрэгжих мэдээллийн технологийн төсөл, хөтөлбөр, кибер аюулгүй байдлыг хангах асуудлаар дүгнэлт гаргуулан, санал, шаардлага, хүргүүлэхийг удирдлага болгон ажиллах.
10. Эрүүл мэндийн яам, Цахим хөгжил харилцаа холбооны яам, Тагнуулын ерөнхий газраас холбогдох зөвлөмж дүгнэлт аваагүй аливаа цахим систем, програм хангамжийг үйл ажиллагаандаа нэвтрүүлэхгүй байх;
11. Албан даалгаврыг хэрэгжүүлэх чиглэлээр авсан арга хэмжээ, гарсан үр дүнгийн тайланг улирал бүр Бодлого төлөвлөлтийн газарт албан бичгээр ирүүлэх.

Албан даалгаврын хэрэгжилтэд хяналт тавьж ажиллахыг Бодлого төлөвлөлтийн газарт даалгасугай.

САЙД



С.ЧИНЗОРИГ