



КИБЕР АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ЖУРАМ



БОЛОВСРУУЛАХ ГАРЫН АВЛАГА

КАБ-ыг хангах үйл ажиллагааны дотоод журамд тусгах зарим шаардлагууд

Дотоод журам батлах:
[X¹: 19.2.1]

1 ЗОХИОН БАЙГУУЛАХ



- Байгууллагын стратеги төлөвлөгөөтэй уялдсан.
- МАБ-ын аудит, КАБ-ын эрсдэлийн үнэлгээг зохих стандарт, хуулийн дагуу хийлгэж, холбогдох газарт хүргүүлэх заалттай.
- Холбогдох албан хаагчдад тухай бүрт танилцуулдаг.

КАБ-ын эрсдэлийн үнэлгээг жил бүр, эсхүл систем, сүлжээний өөрчлөлт хийх бүрд хэсэгчлэн, эрх бүхий байгууллага шаардсан бол тухай бүр хийлгэх. [X¹: 19.2.5]

МАБ-ын аудитыг 2 жил тутам хийх. [X¹: 19.2.6]

2 ХҮНИЙ НӨӨЦ



- Байгууллагын КАБ хариуцсан орон тоо (хавсран гүйцэтгэх)-ын ажилтан томилсон.
- Кибер орчин, систем, сүлжээнд ханддаг, мэдээлэлтэй ажилладаг албан хаагчидтай КАБ-ыг хангах үүрэг, хариуцлага, нууц хадгалах гэрээ үйлдсэн.

КАБ хангах үйл ажиллагаа хариуцсан нэгж, эсхүл албан тушаалтай байх. [X¹: 19.2.4]

3 БАРИМТ БИЧИГ



- Хамгаалбал зохих мэдээлэл, систем, сүлжээний нууцын зэрэглэл, хариуцагчийг тодорхойлсон жагсаалттай, жагсаалтыг тогтмол шинэчлэдэг.
- Жагсаалтад хамрагдсан зүйлсийн хуваарийн дагуу тогтмол нөөцөлж, баталгажуулдаг.
- Кибер халдлага, зөрчлийн үед хариу үзүүлэх төлөвлөгөөтэй.
- Эрсдэлийг бууруулах арга хэмжээний төлөвлөгөөтэй.

Систем, сүлжээний аюулгүй байдлыг хангахад шаардлагатай удирдлага, зохион байгуулалтын болон техникийн арга хэмжээг төлөвлөж хэрэгжүүлэх. [X¹: 19.2.7]

Кибер халдлага, зөрчлийн үед даган мөрдөх төлөвлөгөөг баталж хэрэгжүүлэх. [X¹: 19.2.2]

Систем, сүлжээний хэвийн, найдвартай байдлыг хангах, шаардлагатай үед сэргээн ажиллуулах төлөвлөгөөтэй байх. [X¹: 19.2.13]

4 АРГА ХЭМЖЭЭ



- Хамгаалах:** Байгууллагын систем, сүлжээнд зөвшөөрөлгүй хандах, дамжуулах, өөрчлөх, устгахаас хамгаалсан шийдэлтэй.
- Хадгалах:** 1. ID нэвтрэх эрхийн, 2. ID нууц үгийн, 3. ID мэдээллийн харах-үүсгэх-өөрчлөх-устгах үйлдлийн бүртгэлүүдийг хөтөлж, 1 жилээс дээш хугацаанд хадгалдаг.
- Илрүүлэх:** Байгууллагын хэрэгцээнд тохирсон КАБ-ыг хангах программ хангамж, тоног төхөөрөмжтэй.
- Хэвийн бус үйлдлийг илрүүлэх, аюулыг тогтмол хянах 24/7 арга барилтай.
- Хариу үзүүлэх:** Жилд 1-ээс доошгүй удаа төлөвлөгөөний дагуу дадлага, туршилт хийж, хариу арга хэмжээ авах төлөвлөгөөг тогтмол сайжруулдаг.

Кибер халдлага, зөрчлийг илрүүлэх, бүртгэх, таслан зогсоох мэдээллийн системтэй байх. [X¹: 19.2.8]

Систем, сүлжээний үйлдлийн бүртгэл (LOG)-ийг хуульд заасан хугацаанд хадгалах. [X¹: 19.2.9]

Кибер аюулгүй байдлын дотоод журам боловсруулах жишиг бичиг баримт



5 БУСАД



- Сургалт:** КАБ-ын мэдлэг олгох сургалтад нийт албан хаагчид, холбогдох хүмүүсийг хамруулдаг. [Ж¹: 2.2.2]
- Зарчим:** Зохиогчийн эрхгүй программ хангамж, тоног төхөөрөмж ашиглахаас татгалздаг. [Ж¹: 4.13]
- Хариуцлага:** Төрийн албаны тухай, Хөдөлмөрийн тухай, Зөрчлийн тухай, гэмт хэргийн шинжтэй бол Эрүүгийн хуулийн холбогдох заалт бүхий хариуцлагын тогтолцоотой. [X¹: 24.1-3, Ж¹: 8.4]

6 МЭДЭГДЭХ



- КАБ-ын эрсдэлийн үнэлгээ, МАБ-ын аудитын тайланг 1 сарын дотор холбогдох төвд хүргүүлдэг. [X¹: 19.2.10]
- Кибер халдлага, зөрчлийн улмаас байгууллагын кибер орчны хэвийн үйл ажиллагааг хангах боломжгүй болсон даруйд холбогдох төвд мэдэгддэг. [X¹: 19.2.14]
- Кибер халдлага, зөрчилтэй тэмцэх төвөөс хүргүүлсэн зөвлөмж, шаардлагыг тогтоосон хугацаанд, эсхүл 10 өдрийн дотор хэрэгжүүлж хариу мэдэгддэг. [X¹: 21.6]

Таних тэмдэг: [X¹] - Кибер аюулгүй байдлын тухай хууль, заалт
[Ж¹] - Засгийн газрын 2023 оны 224-р тогтоол, КАБ-ыг хангах нийтлэг журмын зүйл, заалт

Товчилсон үгс: КАБ - Кибер аюулгүй байдал
МАБ - Мэдээллийн аюулгүй байдал
ОЧМДББ - Онц чухал мэдээллийн дэд бүтэцтэй байгууллага

ОЧМДББ: КАБ алдагдсанаар хэвийн үйл ажиллагаа нь доголдож Монгол Улсын Үндэсний аюулгүй байдал, нийгэм, эдийн засагт хохирол учруулж болох мэдээллийн систем, мэдээллийн сүлжээ бүхий байгууллага юм.

7000-1113
7588-0113

113.mn
pubcert.mn

Баянгол дүүрэг, 17-р хороо, Амарсанаагийн гудамж, Радио телевизийн үндэсний сүлжээний байр, 2 давхарт, Ulaanbaatar, Mongolia, 15160