КИБЕР ХАЛДЛАГА, ЗӨРЧИЛТЭЙ ТЭМЦЭХ НИЙТИЙН ТӨВ

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН АУДИТ, КИБЕР АЮУЛГҮЙ БАЙДЛЫН ЭРСДЭЛИЙН ҮНЭЛГЭЭНИЙ ЦАХИМ ТАЙЛАН

СИСТЕМ АШИГЛАХ ЗААВАР

НИЙТЛЭГ ҮНДЭСЛЭЛ

- Онц чухал мэдээллийн дэд бүтэцтэй хувийн хэвшлийн байгууллага (цаашид "тайлагнагч байгууллага" гэх) нь мэдээллийн аюулгүй байдлын аудит, кибер аюулгүй байдлын эрсдэлийн үнэлгээний цахим тайлангийн системд нэвтрэх, “Кибер халдлага, зөрчилтэй тэмцэх нийтийн төв” УТҮГ (цаашид "Нийтийн төв" гэх) тайланг хүлээн авах, хянах, мэдээллийн сан бүрдүүлэх түүний аюулгүй байдлыг хангахад энэ зааврыг мөрдөнө.
- Тайлагнагч байгууллагын мэдээллийн аюулгүй байдлын аудитын болон кибер аюулгүй байдлын эрсдэлийн үнэлгээний тайланг (цаашид "тайлан" гэх) цахим хэлбэрээр хүлээн авах, хянах, нэгтгэх үйл ажиллагаанд Нийтийн төвийн цахим системийг (цаашид "цахим систем" гэх) ашиглана.

1 СИСТЕМД НЭВТРЭХ

WWW.AUDIT.PUBCERT.MN

Цахим системийн хэвийн үйл ажиллагаа, аюулгүй байдлыг Нийтийн төв хангаж ажиллана.

70001113

Системд нэвтрэх бүртгэл үүсгэхдээ 70001113 дугаарын 3 эсвэл 5 дотоод шугамаар холбогдож, эрх нээлгэнэ.

2 ТАЙЛАНД ТАВИГДАХ ШААРДЛАГА

- Тайланг бүртгэлтэй хуулийн этгээдээр холбогдох журам, аргачлалын дагуу хийлгэсэн байх;
- КАБ тухай хуулийн 19.2.10-д заасан хугацаанд цахим системээр ирүүлэх;
- Мэдээллийн үнэн зөв байдлыг байгууллага хариуцах;
- Монгол хэл дээр бичигдсэн байх;
- Дижитал, сканнердаагүй PDF хэлбэртэй байх.

2 ТАЙЛАН ИЛГЭЭХ

- Тайлагнагч байгууллагын админ мэдээлэл хариуцагчийн системд бүртгэл хийлгэн, нэвтрэх;
- “Кибер аюулгүй байдлын эрсдэлийн үнэлгээ” эсвэл “Мэдээллийн аюулгүй байдлын аудит” гэсэн цэсээс сонгох;
- Холбогдох PDF тайланг хавсаргах;
- Илгээх товчийг дарна.

2 ТАЙЛАНГИЙН ТӨЛӨВ

- **Илгээсэн:** Нийтийн төвд тайлан илгээгдсэн.
- **Хүлээн авсан:** Тайланг хянаж, шаардлага хангасан үед хүлээн авна.
- **Буцаагдсан:** Алдаатай, дутуу бүрдэлтэй тайланг буцааж, энэ тухай цахим шуудан эсвэл утсаар мэдэгдэх бөгөөд тайлагнагч байгууллага тайлбар хэсгийн тэмдэглэлийн дагуу засварлан ажлын 5 өдрийн дотор дахин илгээнэ.

ЦАХИМ МЭДЭЭЛЛИЙН САНГИЙН АЮУЛГҮЙ БАЙДАЛ

Нийтийн төвийн системийн агуулга, бүтэц, хөгжүүлэлт нь мэдээллийн аюулгүй байдлын батлагдсан бодлого журам, шаардлагуудыг хангасан байна.

- Системд тайлагнагч байгууллагаас хандсан хандалт болон үйлдэл бүр нь хүсэлтийн түүх хэсэгт харагдах бөгөөд он тус бүрээр архивлагдана.
- Системийн эмзэг байдлын тестийг жил бүр эсвэл мэдээллийн систем шинэчлэгдэх бүр хийнэ.
- Системийн эмзэг байдалд хийсэн тестийн үр дүнд учирсан эсвэл учирч болох кибер аюулгүй байдлын эрсдэлийг тодорхойлж, эрсдэлийн үнэлгээг хийн, эрсдэлийг бууруулах арга хэмжээг авна.
- Ирүүлсэн тайланг он тус бүрээр мэдээллийн санд хадгална.

НУУЦЛАЛ

- Кибер аюулгүй байдлын тухай хуулийн 8.1-д заасан хуулийн этгээд болон кибер аюулгүй байдлын эрсдэлийн үнэлгээний тайланг хүлээн авсан холбогдох байгууллага, албан тушаалтан нууцлалыг чандлан хадгалж, задруулахгүй байх үүрэг хүлээнэ.

ҮҮРЭГ, ХАРИУЦЛАГА

- Кибер аюулгүй байдлын тухай хуулийн 19.2.10-д заасан хугацаанд тайланг Нийтийн төвийн системд хүргүүлээгүй тайлагнагч байгууллагад Зөрчлийн тухай хуулийн дагуу хариуцлага хүлээлгэн, тайланг хүлээн авна.

113 Кибер халдлагын үед **113.mn**

Эрсдэлийн үнэлгээ ба аудит **audit.pubcert.mn**