БАТЛАВ.
МОНГОЛ УЛСЫН ЕРӨНХИЙ АУДИТОРЫН
ОРЛОГЧ З.ЦЭДЭНЖАВ

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН АУДИТ ХИЙХ АЖЛЫН ДААЛГАВАР

2025 оны 06 дугаар сарын 10-ны өдөр Дугаар ..... Улаанбаатар хот

Зорилго: Төрийн аудитын байгууллагын мэдээллийн технологийн үйл ажиллагаанд Кибер аюулгүй байдлын хууль тогтоомж, холбогдох журам, олон улсын стандартад нийцсэн эсэхэд дүгнэлт гаргах, зөвлөмж өгөх хараат бус хөндлөнгийн мэдээлэл технологийн аудитыг хэрэгжүүлэх ажлын даалгавар болно.

Эхлэх хугацаа: 2025 оны 06 дугаар сарын 16,
Дуусах хугацаа: 2025 оны 08 дугаар сарын 15

Аудитын үйл ажиллагаанд баримтлах зарчим

- хараат бус, мэргэжлийн байх;
- мэдээллийн нууцыг чандлан хадгалах;
- дотоод итгэлээр нотолгоонд суурилан үнэлэх.

НЭГ. ЕРӨНХИЙ ШААРДЛАГА

1.1. Кибер аюулгүй байдлын тухай хууль тогтоомж, түүнд нийцүүлэн гаргасан дүрэм, журам, Олон улсын стандартад Төрийн аудитын байгууллагын мэдээлэл технологийн үйл ажиллагаа нь нийцсэн эсэхэд дүгнэлт гаргах, зөвлөмж өгөх үйлчилгээг үзүүлнэ.

1.2. Зөвшөөрлийн тухай хуулийн 8.1-т заасан Мэдээллийн аюулгүй байдлын аудит хийх зөвшөөрөлтэй бөгөөд Цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллагад бүртгүүлсэн хуулийн этгээд байна.

ХОЁР. ГҮЙЦЭТГЭХ АЖЛЫН ШААРДЛАГА

2.1. Төрийн аудитын байгууллага буюу 21 аймаг дахь Төрийн аудитын газар, Нийслэл дэх Төрийн аудитын газар, Үндэсний аудитын газрын Мэдээллийн аюулгүй байдлын засаглал, зохион байгуулалт, дүрэм, журам, олон улсын стандартын түвшинд үнэлгээ, дүгнэлт, зөвлөмж өгнө.

2.2. Мэдээллийн аюулгүй байдлын аудитын тайлан иж бүрэн Монгол хэлээр боловсруулж, хугацаандаа хүлээлгэн өгнө.

2.3. Мэдээлэл технологийн хөрөнгийн удирдлагын хэрэгжилтэд үнэлгээ, дүгнэлт, сайжруулах ажил, хэрэгжүүлэх сайн туршлага, анхаарах, тулгамдаж буй асуудлыг шийдвэрлэх талаар зөвлөмжийг гүйцэтгэнэ.

2.4. Мэдээллийн системийн дараах кибер орчинд аудитыг гүйцэтгэнэ.

2.4.1. мэдээллийн систем;

2.4.2. мэдээллийн сан, түүний нөөц сан;
2.4.3. өгөгдөл солилцоо, сервис;
2.4.4. тохируулсан физик болон виртуал, клауд сервер, төхөөрөмж.

2.5. Мэдээлэл технологийн тодорхойлсон дараах кибер орон зайд аудитыг гүйцэтгэнэ.
2.5.1. сүлжээний зохион байгуулалтын архитектур;
2.5.2. сүлжээний хаяглалт;
2.5.3. виртуал сүлжээ;
2.5.4. галт хана, түүний нэмэлт хамгаалалтын хэрэгслүүд;
2.5.5. сүлжээний удирдлагын систем;
2.5.6. төгсгөлийн төхөөрөмжийн хамгаалалтын программ;
2.5.7. техник хангамжийн аюулгүй байдал;
2.5.8. программ хангамжийн аюулгүй байдал;
2.5.9. зориулалтын серверийн өрөө;
2.5.10. танилт, нэвтрэлтийн системийн аюулгүй байдал;
2.5.11. цахим захидал, харилцааны аюулгүй байдал;
2.5.12. үйлдлийн бүртгэл /auditm log/-ийн хяналт, удирдлага;

2.6. Нэвтрэлт хандалтын аюулгүй байдлын тест (Penetration test)-ийг алхам бүрээр туршилт хийж гүйцэтгэн, тайлан, үнэлгээ, дүгнэлт, зөвлөмж өгнө.

2.7. Аудитын үйл ажиллааны тасралтгүй байдал ба гамшиг, гэмтэл саатлын нөхөн сэргээлтийн төлөвлөгөө, зохион байгуулалтад үнэлгээ, дүгнэлт, зөвлөмж өгнө.

2.8. Өөрчлөлтийн удирдлага, зохион байгуулалт, хэрэгжилтэд үнэлгээ, дүгнэлт, зөвлөмж өгнө.

2.9. Мэдээллийн технологийн үйл явцын бүртгэл, тайлан, хяналтын удирдлагын байдалд үнэлгээ, дүгнэлт, зөвлөмж өгнө.

2.10. Сургалтын чанар, сургалтын материалд үнэлгээ, дүгнэлт, зөвлөмж өгнө.

2.11. Эрсдэлийн үнэлгээг хийж, бууруулах төлөвлөгөө, дүгнэлт, зөвлөмж өгнө.

2.12. Мэдээллийн аюулгүй байдлын гарын авлага боловсруулж, зөвлөмж, дүгнэлт өгнө.

ГУРАВ. ХҮНИЙ НӨӨЦИЙН ШААРДЛАГА

3.1. Олон улсын мэргэжлийн холбоо, стандартын байгууллага, эсхүл түүнтэй дүйцэхүйц байгууллагаас олгосон Мэдээллийн аюулгүй байдал, кибер аюулгүй байдал, сүлжээний аюулгүй байдлын чиглэлээрх аудит хийх хүчин төгөлдөр гэрчилгээ бүхий орон тооны 3-аас дээш ажилтантай байх ба дараах хүний нөөцийн бүрэлдэхүүнтэй байна.

Мэргэжлийн чиглэл	Тавигдах шаардлага
Мэдээллийн аюулгүй байдлын шинжээч/инженер	• Мэдээллийн аюулгүй байдлын чиглэлээр Олон улсын албан ёсны гэрчилгээтэй байна. • Мэдээллийн ауюлгүй байдлын олон улсын стандартыг нэвтрүүлсэн, хэрэгжүүлсэн, сургалт, зөвлөх үйлчилгээ, аудит хийсэн 5-аас дээш жилийн туршлагатай байна.

Кибер аюулгүй байдлын шинжээч/инженер	• Кибер аюулгүй байдлын чиглэлээр Олон улсын албан ёсны гэрчилгээтэй байна. • Нэвтрэх үеийн аюулгүй байдлын тест (Penetration test) сул, эмзэг байдлын скан (Vulnerability scan), гэмтэл саатал, ослын үеийн төлөвлөлт, хариу арга хэмжээ авах, бууруулах зэрэг кибер аюулгүй байдлын тогтолцооны түвшинд аудит хийсэн 1-ээс дээш жилийн тушлагатай байна.
Сүлжээний аюулгүй байдлын шинжээч/инженер	• Сүлжээний архитектур, аюулгүй байдлын чиглэлээр олон улсын түвшний гэрчилгээтэй байна. • Мэргэжлээрээ 2-оос дээш жил ажилласан байна.
Програм хангамжийн шинжээч/инженер	Мэдээллийн системийн хөгжүүлэлтийн аюулгүй байдал, эх кодын түвшинд аудит, хийх чадвартай
Өгөгдлийн сангийн администратор	Өгөгдлийн сангийн зохион байгуулалт, архитектор, аюулгүй байдлын чиглэлээр 2-оос дээш жил ажилласан туршлагатай байна.
Хуульч	• Хуульчийн гэрчилгээтэй хуульчтай бол давуу тал болно. • Мэдээллийн технологийн чиглэлийн хуулийн зөвөлгөө өгөх болон дүрэм журам боловсруулсан туршлагатай бол давуу тал болно.

ДӨРӨВ. АУДИТЫГ ХЭРЭГЖҮҮЛЭХ ЗОХИОН БАЙГУУЛАЛТЫН ШААРДЛАГА

4.1. Аудит эхлэхээс өмнө арга зүй, аргачлал, ашиглах төхөөрөмж, программ хангамж, хэрэгсэл болон ажиллах төлөвлөгөөг Үндэсний аудитын газрын холбогдох нэгжид танилцуулж, мэдээлнэ. Шаардлагатай бол өөрчлөлтийг тохирч оруулж болно.

4.2. Аудитын баг нь ажиллахдаа дараах үүргийг мөрдөж ажиллана.

4.2.1. Аудит хийх явцад хүлээн авсан мэдээлэл, баримт бичгийн бүрэн бүтэн, нууцлагдсан байдлыг хангана.

4.2.2. Гаргасан аудитын дүгнэлт, зөвлөмжийн үнэн зөв байдлыг бүрэн хариуцна.

4.2.3. Аудит хийх үйл ажиллагааг эхлүүлэхээс өмнө аудитын үйл ажиллагаанд оролцох ажилтны хараат бус, ашиг сонирхлын зөрчилгүй эсэхийг баталгаажуулна.

4.2.4. Аудитын үр дүнд олж авсан, үйлчлүүлэгчээс эсхүл хуулиар олон нийтэд нээлттэй байхаар тогтоосон мэдээллээс бусад мэдээллийн нууцлалыг хадгалах, гуравдагч этгээдэд задруулах, хувийн зорилгоор ашиглахгүй байх баталгааг ажилтнаас гаргуулна.

4.2.5. Аудит хийх үйл ажиллагааг өөрийн нэрийн өмнөөс бусдаар гүйцэтгүүлэхгүй байна.

4.2.6. Аудит хийхэд шаардлагатай бүх хяналт, туршилтын тоног төхөөрөмж, программ хангамж, арга аргачлалаар ажил гүйцэтгэх баг бүрэн хангагдсан байна.

4.2.7. Аудитын явцад байгууллагын хэвийн үйл ажиллагаанд саад учруулахгүй байна.

ТАВ. ХҮЛЭЭГДЭЖ БУЙ ҮР ДҮН

5.1. Мэдээллийн аюулгүй байдлын аудитын чиглээрх дүрэм журам, Олон улсын стандартад нийцсэн иж бүрэн аудитын тайлан, зөвлөмжтэй байхаас гадна дараах үр дүн гарсан байна. Үүнд:

5.1.1. Мэдээллийн аюулгүй байдлын сул, эмзэг байдал тодорхойлогдож, хэрэгжүүлэх зөвлөмж, төлөвлөгөөтэй болсон байна.
5.1.2. Эрсдэл бууруулах талаар зөвлөмж, төлөвлөгөөтэй болсон байна.
5.1.3. Аюулгүй байдлын мэдлэг, чадварыг нэмэгдүүлэх сургалтын гарын авлага, онолын түвшний материалтай болсон байна.
5.1.4. Төрийн аудитын байгууллагын хэмжээнд Мэдээллийн аюулгүй байдлын иж бүрэн тайлан, зөвлөмж, дүгнэлттэй болсон байна.

ХЯНАСАН:

МЭДЭЭЛЭЛ, ТЕХНОЛОГИЙН НЭГДСЭН
ТӨВИЙН ЗАХИРАЛ, ТЭРГҮҮЛЭХ АУДИТОР Б.СЭР-ОД

АТА9693 9026109
9023030583

БОЛОВСРУУЛСАН:

МЭДЭЭЛЛИЙН ТЕХНОЛОГИЙН МЕНЕЖЕР Б.ОЮУНТУЯА