МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ЖУРАМ

I БҮЛЭГ. НИЙТЛЭГ ҮНДЭСЛЭЛ

1.1. Зорилго

Энэхүү журам нь Боловсролын зээлийн сангийн мэдээллийн аюулгүй байдлын удирдлагын тогтолцоог ISO/IEC 27001:2022 стандартын шаардлагад нийцүүлэн байгууллагын мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмжийг хангах, мэдээллийн аюулгүй байдлын эрсдэлийг бууруулах, зөрчил гарсан үед хариу арга хэмжээ авах, мэдээллийн эд хөрөнгийг хамгаалах үйл ажиллагааны зохицуулалт, шаардлагыг тогтооно.

1.2. Хамрах хүрээ

Энэхүү журам нь Боловсролын зээлийн сангийн мэдээллийн систем, сүлжээ, сервер, өгөгдлийн сан, тохиргоо, техник хэрэгсэл, программ хангамж, мэдээлэл боловсруулагч албан хаагч, эрх бүхий хэрэглэгч, гэрээт албан хаагч болон мэдээллийн аюулгүй байдалд нөлөөлөх бүх үйл ажиллагаанд хамаарна.

1.3. Эрх зүйн үндэслэл

Энэхүү журмыг Монгол Улсын Кибер аюулгүй байдлын тухай хууль, ISO/IEC 27001:2022, ISO/IEC 27002:2022 стандартуудын холбогдох заалтыг үндэслэн боловсруулав.

II БҮЛЭГ. МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ЕРӨНХИЙ ЗАРЧМУУД

2.1. Мэдээллийн аюулгүй байдлын үндсэн зарчим

Байгууллага мэдээллийн аюулгүй байдлыг хангахдаа олон улсын стандартад нийцсэн дараах үндсэн зарчмыг баримтална. Үүнд:

2.1.1. **Нууцлал** – Мэдээлэлд хандах, ашиглах эрхийг зөвхөн эрх бүхий этгээдэд олгож, мэдээллийн зөвшөөрөлгүй нэвтрэлт, ашиглалт, дамжуулалт, алдагдал, задруулахаас урьдчилан сэргийлнэ.

2.1.2. **Бүрэн бүтэн байдал** – Мэдээлэл нь үнэн зөв, гэмтэлгүй, өөрчлөгдөөгүй байх нөхцөлийг хангаж, мэдээллийг санаатай болон санаандгүй өөрчлөх, устгах, эвдэх аливаа эрсдэлээс урьдчилан сэргийлнэ.

2.1.3. **Хүртээмж** – Байгууллагын мэдээллийн систем, өгөгдөл нь шаардлагатай үед хэвийн, тасралтгүй, найдвартай ажиллах боломжтой байх бөгөөд системийн саатал, доголдол, техникийн тасалдлын үед нөхөн сэргээх зохицуулалттай байна.

2.2. Мэдээллийн ангилал

Боловсролын зээлийн сангийн мэдээллийг дараах түвшнээр ангилж, хамгаална:

1. **Нийтэд нээлттэй мэдээлэл**
2. **Дотоод хэрэглээний мэдээлэл**
3. **Хязгаарлагдмал мэдээлэл**
4. **Нууц мэдээлэл**

Тухайн ангиллын түвшинд тохирсон хамгаалалтын арга хэмжээг программ, техник, хүний нөөцийн түвшинд хэрэгжүүлнэ.

III БҮЛЭГ. ХҮНИЙ НӨӨЦИЙН АЮУЛГҮЙ БАЙДАЛ

3.1. Албан хаагч томилогдох үеийн мэдээллийн аюулгүй байдлын шаардлага

Байгууллагад шинээр албан хаагч томилогдох бүрт дараах мэдээллийн аюулгүй байдлын арга хэмжээг заавал авч хэрэгжүүлнэ:

3.1.1. **Нууцлалын гэрээ байгуулах** – Албан хаагч нь албан тушаалын үүрэг гүйцэтгэхийн өмнө мэдээллийн аюулгүй байдлын болон нууцлалын гэрээнд гарын үсэг зурж, байгууллагын нууцлалын бодлого, шаардлагыг дагаж мөрдөх үүрэг хүлээнэ.

3.1.2. **Мэдээллийн аюулгүй байдлын сургалтад хамруулах** – Шинэ албан хаагч томилогдсон даруйд мэдээллийн аюулгүй байдлын үндсэн ойлголт, байгууллагын бодлого, журам, хориглох үйлдлүүдийн талаар сургалтад хамруулна.

3.1.3. **Хандалтын эрх олгох** – Ажилтны албан үүрэгт шаардлагатай систем, сүлжээ, программ хангамжид хамгийн бага эрхийн зарчмын дагуу олгож, эрхийн бүртгэл үүсгэнэ.

3.1.4. **Төхөөрөмж олголт** – Ажил үүргээ гүйцэтгэхэд шаардлагатай компьютер, дагалдах хэрэгсэл, цахим гарын үсэг, программ хангамж, имэйл хаяг зэргийг хүлээлгэн өгч, хүлээн авалтын акт үйлдэнэ.

3.2. Албан хаагч ажлаас чөлөөлөгдөх, шилжих үеийн мэдээллийн аюулгүй байдлын шаардлага

Албан хаагч ажлаас чөлөөлөгдөх, албан тушаал өөрчлөгдөх, нэгж хооронд шилжих тохиолдолд дараах арга хэмжээг заавал авч хэрэгжүүлнэ:

3.2.1. **Хандалтын эрхийг нэн даруй хаах** – Бүх төрлийн системийн нэвтрэх эрх (имэйл, сервер, өгөгдлийн сан, программ хангамж, VPN, дотоод сүлжээ зэрэг)-ийг ажлаас чөлөөлсөн өдөрт нь хаана.

3.2.2. **Байгууллагын эд зүйлсийг бүрэн хураан авах** – Албан хаагчдад олгогдсон бүх төхөөрөмж, дагалдах хэрэгсэл, баримт бичиг, нэвтрэх эрхийн карт, USB, хатуу диск зэрэг хөрөнгийг бүрэн хүлээлгэн авна.

3.2.3. **Өгөгдлийн шилжилт, архивжуулалт хийх** – Албан хаагч хариуцсан файлууд, баримт бичиг, өгөгдлийн сангийн өгөгдлийг холбогдох нэгжид шилжүүлж, шаардлагатай тохиолдолд архивжуулна.

3.2.4. **Нууцлалын үүрэг үргэлжлэхийг сануулах** – Ажлаас гарсан албан хаагч нь байгууллагын мэдээллийг задруулахгүй байх хуулийн үүрэг хэвээр үргэлжлэхийг албан ёсоор мэдэгдэнэ.

3.2.5. **Шалтгаант тайлан гаргах (шаардлагатай бол)** – Хүний нөөцийн нэгж ба мэдээллийн аюулгүй байдлын алба хамтран мэдээллийн аюулгүй байдалтай холбоотой эрсдэл, зөрчлийн магадлалтай эсэхийг шалгаж нэгтгэнэ.

IV БҮЛЭГ. ЭД ХӨРӨНГИЙН УДИРДЛАГА

4.1. Эд хөрөнгийн бүртгэл, ангилал

Байгууллагын эзэмшил, ашиглалтад байгаа мэдээллийн болон техник хэрэгслийн бүх эд хөрөнгийг бүртгэн, ангилж, эзэнтэй болгох замаар мэдээллийн аюулгүй байдлыг хангана. Үүнд:

4.1.1. **Эд хөрөнгийн бүртгэл үүсгэх** – Компьютер, сервер, сүлжээний төхөөрөмж, программ хангамж, өгөгдлийн сан, баримт бичиг зэрэг бүх төрлийн эд хөрөнгийг стандартын дагуу нэгдсэн бүртгэлд хөтөлнө.

4.1.2. **Эд хөрөнгийг ангилах** – Эд хөрөнгийг дараах үндсэн ангиллаар тодорхойлох бөгөөд шаардлагатай тохиолдолд дэд ангилал үүсгэнэ:

- Техник төхөөрөмж (компьютер, сервер, хэвлэгч, сүлжээний төхөөрөмж);
- Программ хангамж, лиценз;
- Өгөгдлийн сан, өгөгдлийн багц;
- Баримт бичиг (цаасан болон цахим хэлбэрээр);
- Дагалдах хэрэгсэл.

4.1.3. **Эд хөрөнгийн эзэн томилох** – Эд хөрөнгө бүрт хариуцсан эзэн томилж, ашиглалт, хамгаалалт, бүрэн бүтэн байдлыг хангах үүргийг хүлээлгэнэ.

4.2. Эд хөрөнгийн олголт, ашиглалт

Эд хөрөнгийг албан хаагчид олгох, ашиглуулах үйл ажиллагааг дараах зарчмаар хэрэгжүүлнэ:

4.2.1. **Эд хөрөнгийг хүлээлгэн өгөх үйл ажиллагаа** – Албан хаагчид эд хөрөнгө олгох үед акт үйлдэж, тухайн эд хөрөнгийн дугаар, үзүүлэлт, ашиглалтын нөхцөл, хариуцлагын хүрээг тодорхой заана.

4.2.2. **Ашиглалтын заавар мөрдөх** – Эд хөрөнгийг зөвхөн албан хэрэгцээнд ашиглах бөгөөд байгууллагын дотоод журам, техникийн заавар, мэдээллийн аюулгүй байдлын шаардлагыг албан хаагч бүр мөрдөнө.

4.2.3. **Программ хангамжийн ашиглалт** – Ажилтны ашиглах программ хангамжийг мэдээллийн технологийн мэргэжилтэн суулгаж, лицензийн хүчинтэй байдал, аюулгүй байдлын тохиргоог баталгаажуулна.

4.3. Эд хөрөнгийн хамгаалалт, бүрэн бүтэн байдлыг хангах

Байгууллагын эд хөрөнгийн алдагдал, эвдрэл, буруу ашиглалт, хөндлөнгийн нэвтрэлтээс хамгаалах зорилгоор дараах хамгаалалтын арга хэмжээг авна:

4.3.1. **Физик хамгаалалт** – Төхөөрөмжийг аюулгүй, хяналттай орчинд байршуулж, зөвшөөрөлгүй этгээд нэвтрэх боломжийг хаана.

4.3.2. **Техникийн хамгаалалт** – Галтхана, антивирус, шифрлэлтийн технологи, хандалтын хяналт ашиглан эд хөрөнгөд агуулагдах мэдээллийг хамгаална.

4.3.3. **Бүрэн бүтэн байдлын хяналт** – Эд хөрөнгийн үзлэгийг тогтмол хийж, эвдрэл, доголдлыг бүртгэн засвар үйлчилгээний бүртгэл хөтөлнө.

4.3.4. **Зөөврийн төхөөрөмжийн удирдлага** – USB, хатуу диск, зөөврийн компьютер зэрэг зөөврийн төхөөрөмжийг зөвшөөрөгдсөн албан хаагч ашиглах бөгөөд төхөөрөмж бүрт вирусийн шалгалт хийнэ.

4.4. Эд хөрөнгийн буцаалт, шилжилт болон устгал

Албан хаагч ажлаас чөлөөлөгдөх, нэгж солих, эд хөрөнгийг шинэчлэх, ашиглалтаас гаргах тохиолдолд дараах журмыг мөрдөнө:

4.4.1. **Буцаалт хийх** – Албан хаагч хүлээн авсан эд хөрөнгийг бүрэн бүтэн байдлыг шалгуулж, хүлээлгэн өгөх актаар байгууллагад буцаана.

4.4.2. **Шилжилт хийх** – Эд хөрөнгийг нэгж хооронд шилжүүлэх тохиолдолд бүртгэлийг шинэчилж, эзэн шинэчлэн томилно.

4.4.3. **Мэдээлэл устгал** – Ашиглалтаас гарсан төхөөрөмжийн дотоод санах ойд хадгалагдсан мэдээллийг бүрэн устгаж, шаардлагатай бол олон улсын стандартад нийцсэн аргаар физик устгал хийнэ.

4.4.4. **Актлах, тайлагнах** – Эд хөрөнгийн элэгдэл, эд анги гэмтэл, гацалт, ашиглалтаас гарах зэрэг тохиолдолд акт үйлдэж, холбогдох өмч хамгаалах зөвлөлд хүргүүлнэ.

V БҮЛЭГ. ХАНДАЛТЫН УДИРДЛАГА

5.1. Хандалтын эрхийн зохицуулалт

Байгууллагын мэдээллийн систем, сүлжээ, программ хангамж болон техник тоног төхөөрөмжид хандах эрхийг аюулгүй байдлын бодлого, хэрэглэгчийн үүрэг, ажлын байрны шаардлагад нийцүүлэн дараах зарчмын дагуу олгоно.

5.1.1. **Хамгийн бага эрхийн зарчим** – Албан хаагч бүрд зөвхөн өөрийн албан үүрэг гүйцэтгэхэд шаардагдах түвшний хандалтын эрх олгоно. Илүүдэл, давхардсан, шаардлагагүй эрх олгогдохыг хориглоно.

5.1.2. **Эрхийн хүсэлт, баталгаажуулалт** – Хандалтын эрх нээх, өөрчлөх, хаах боломжийг зөвхөн удирдах ажилтны баталгаажуулсан хүсэлтийн дагуу мэдээллийн технологийн мэргэжилтэн гүйцэтгэнэ.

5.1.3. **Эрхийн бүртгэл хөтлөх** – Хэрэглэгчийн эрх олголт, өөрчлөлт, хаалтын бүртгэлийг системтэй хөтөлж, хяналтын зорилгоор хадгална.

5.1.4. **Эрхийн тогтмол хяналт** – Бүх ажилтны хандалтын эрхийг улирал тутамд шалгаж, шаардлагагүй эсвэл давхардсан эрхийг нэн даруй цуцална.

5.1.5. **Гадаад этгээдийн хандалт** – Гэрээт албан хаагч, үйлчилгээ үзүүлэгчид зөвшөөрөгдсөн хугацаа, хүрээний хувьд хязгаарлалттай хандалтын эрх олгож, ажил дуусмагц даруй хаана.

5.2. Нууц үгийн удирдлага

Хэрэглэгчийн таних мэдээлэл, нэвтрэх эрхийн аюулгүй байдлыг хангах зорилгоор дараах шаардлагыг мөрдөнө:

5.2.1. **Нууц үгийн бүтэц, бат бөх байдал** – Нууц үг нь 12 ба түүнээс дээш тэмдэгттэй, том үсэг, жижиг үсэг, тоо болон тусгай тэмдэгт агуулсан байна.

5.2.2. **Нууц үгийн хэрэглээ** – Нууц үгийг давхар ашиглахгүй, бусдад дамжуулахгүй, ил харагдах газар хадгалахгүй.

5.2.3. **Нууц үгийг шинэчлэх** – Хэрэглэгч нууц үгээ улирал бүр шинэчилж, хуучин нууц үгийг дахин ашиглахаас зайлсхийх үүрэгтэй.

5.2.4. **Нууц үгийг хадгалахгүй байх** – Интернэт хөтөч, имэйл клиент болон бусад программд автомат хадгалах функцийг ашиглахыг хориглоно.

5.2.5. **Нууц үг алдагдсан тохиолдол** – Нууц үг алдагдсан, бусдад мэдэгдсэн гэж сэжиглэгдсэн даруйд мэдээллийн технологийн албанд мэдэгдэж, шинэчлэх арга хэмжээг авна.

5.2.6. **Хоёр үе шаттай баталгаажуулалт** – Мэдээллийн системд нэвтрэхэд нэмэлт хамгаалалтын арга хэмжээ болох хоёр үе шаттай баталгаажуулалтыг ашиглана.

VI БҮЛЭГ. ТЕХНИКИЙН АЮУЛГҮЙ БАЙДАЛ

6.1. Сүлжээний аюулгүй байдал

Байгууллагын дотоод болон гадаад сүлжээний найдвартай ажиллагаа, хамгаалалтын түвшинг хангах зорилгоор дараах техникийн зохицуулалтыг хэрэгжүүлнэ:

6.1.1. **Сүлжээний төхөөрөмжийн бүртгэл** – Сүлжээнд холбогдох боломжтой бүх төхөөрөмжийг бүртгэж, сүлжээний хаяг болон төхөөрөмжийн хаягийн түвшинд хяналт тавина.

6.1.2. **Сүлжээний сегментчлэл** – Ажилтнуудын үүрэг, мэдээллийн ангилал, аюулгүй байдлын шаардлагаас хамааран сүлжээг дэд сүлжээ болон бусад техникийн шийдлээр сегментчилж, нэвтрэлтийн эрсдэлийг бууруулна.

6.1.3. **Гарцын хамгаалалт** – Сүлжээний ирж буй болон гарах хөдөлгөөнийг хянах зорилгоор Галтхана ашиглаж, дүрэм, шүүлтүүр, хандалтын бодлогыг тогтмол шинэчилнэ.

6.1.4. **Траффик хяналт ба бүртгэл** – Сүлжээний урсгалын лог бүртгэлийг хадгалж, сэжигтэй үйлдэл илэрсэн тохиолдолд мэдээллийн технологийн нэгжид мэдээлнэ.

6.1.5. **Вирус, хортой кодоос хамгаалах** – Байгууллагын төхөөрөмж, сүлжээг вирус, хортой кодын халдлагаас хамгаалах зорилгоор хамгаалалтын программ хангамж болон сүлжээний хамгаалалтын системүүдийг шинэчлэлтэй, идэвхтэй горимд байлгаж, илрүүлэлтийг тасралтгүй хэрэгжүүлнэ.

6.2. Серверийн өрөөний аюулгүй байдал

Сервер болон дэд бүтцийн төхөөрөмжүүдийг физик, техникийн аюулгүй байдал бүрэн хангагдсан орчинд байрлуулна.

6.2.1. **Физик хамгаалалт** – Серверийн өрөөнд зөвхөн зөвшөөрөгдсөн албан хаагч нэвтрэх бөгөөд цахилгаан түгээлт, хаалганы түгжээ, хяналтын камерын системээр хамгаална.

6.2.2. **Орчны тохиргоо** – Температур 18–24°C, чийгшил 40–60%-ийн хооронд байх бөгөөд галын дохиолол, утаа мэдрэгч, чийгшүүлэгч, хөргөлтийн төхөөрөмжийг стандартын дагуу ажиллуулна.

6.2.3. **Хяналтын камерын бичлэг** – Серверийн өрөөний хяналтын камер бичлэгийг 90 хоногоос доошгүй хугацаанд хадгална.

6.2.4. **Тоног төхөөрөмжийн байрлал, дугаарлалт** – Сервер, маршрутизатор, свич, кабель, цахилгаан хуваарилагч зэрэг тоног төхөөрөмжийг зориулалтын тавиурт байрлуулж, дугаарлаж тэмдэглэнэ.

6.2.5. **Тоосжилт, цахилгаан соронзон орчны хяналт** – Төхөөрөмжийг сар бүр цэвэрлэж, цахилгаан соронзон нөлөөлөл үүсгэх төхөөрөмжийг хол байрлуулна.

6.3. Программ хангамжийн ашиглалтын аюулгүй байдал

6.3.1. **Лицензтэй программ ашиглах** – Байгууллагын компьютер, серверт зөвшөөрөгдсөн, лицензтэй программ хангамжийг ашиглана.

6.3.2. **Программ суулгах эрх** – Шаардлагатай програмыг зөвхөн мэдээллийн технологийн мэргэжилтэн суулгана.

6.3.3. **Шинэчлэлт хийх** – Үйлдлийн систем болон программ хангамжийн хамгаалалтын шинэчлэлтийг тогтмол хийж, аюулгүй байдлын эрсдэлээс сэргийлнэ.

6.3.4. **Хортой программ илрүүлэх** – Вирус илрэх, сэжигтэй файлын үйлдэл илэрсэн тохиолдолд даруй тусгаарлаж шалгана.

6.4. Техникийн гэмтэл, саатлын үед авах арга хэмжээ

6.4.1. **Саатлын бүртгэл** – Сүлжээ, сервер, төхөөрөмжийн гэмтэл, тасалдлын бүртгэлийг хөтөлж, шалтгааныг тодорхойлно.

6.4.2. **Нөхөн сэргээх** – Системийн алдаа гарсан тохиолдолд урьдчилан тогтоосон үйл ажиллагааны зааврын дагуу нөхөн сэргээх гүйцэтгэнэ.

6.4.3. **Түр зуурын шийдэл хэрэгжүүлэх** – Ашиглалт тасалдахаас сэргийлж түр шийдэл хэрэгжүүлж, үндсэн засварыг зохион байгуулна.

6.4.4. **Мэдээлэх** – Техникийн доголдлын талаар холбогдох нэгж, удирдлагад нэн даруй мэдэгдэнэ.

VII БҮЛЭГ. ҮЙЛ АЖИЛЛАГААНЫ АЮУЛГҮЙ БАЙДАЛ

7.1. Программ хангамжийн удирдлага

Байгууллагын ашиглаж буй программ хангамжийн аюулгүй ажиллагааг хангах зорилгоор дараах шаардлагыг мөрдөнө:

7.1.1. **Лицензтэй программ ашиглах** – Байгууллагын хэмжээнд зөвхөн лицензтэй, эрх бүхий эх сурвалжаас татаж суулгасан программ хангамжийг ашиглана.

7.1.2. **Программ суулгах** – Программ хангамжийг ажилтны компьютер, серверт суулгах, устгах, өөрчлөх үйлдлийг зөвхөн мэдээллийн технологийн мэргэжилтэн гүйцэтгэнэ.

7.1.3. **Шинэчлэлт хийх** – Үйлдлийн систем болон программ хангамжийн хамгаалалтын шинэчлэлтийг тогтмол хийж, кибер халдлага, эмзэг байдлаас урьдчилан сэргийлнэ.

7.1.4. **Хортой программ илрүүлэх** – Хортой код, вирус, сэжигтэй файлын үйлдлийг илрүүлэх тохиргоог идэвхтэй байлгаж, илэрсэн тохиолдолд даруй тусгаарлан шалгана.

7.2. Нөөцлөлт ба нөхөн сэргээх

Байгууллагын үйл ажиллагааны тасралтгүй байдлыг хангах зорилгоор мэдээллийг тогтмол нөөцөлж, шаардлагатай үед сэргээн ашиглах арга хэмжээг хэрэгжүүлнэ.

7.2.1. **Нөөцлөх давтамж** – Чухал мэдээлэл, системийн тохиргоо, өгөгдлийн санг өдөр бүр; бусад төрлийн үйл ажиллагааны мэдээллийг долоо хоног бүр нөөцөлнө.

7.2.2. **Нөөцийн хадгалалт** – Нөөцлөлтийн файлуудыг шифрлэн хадгалж, үндсэн систем байрлаж буй орчноос тусгаарлагдсан аюулгүй байршилд байршуулна.

7.2.3. **Нөхөн сэргээх туршилт** – Нөөцийн хүчинтэй байдлыг шалгах зорилгоор улирал тутам нөхөн сэргээх туршилт хийнэ.

7.2.4. **Саатал, эвдрэлд хариу үйлдэл** – Системийн алдаа, ажиллагааны доголдлын үед урьдчилан боловсруулсан нөхөн сэргээх зааврыг мөрдөж, үйл ажиллагааг тасалдуулахгүй байх арга хэмжээ авч хэрэгжүүлнэ.

7.2.5. **Нөөцлөлтийн бүртгэл** – Нөөцлөлт, нөхөн сэргээх үйл явцын бүртгэлийг тогтмол хөтлөн хадгална.

VIII БҮЛЭГ. МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ЗӨРЧЛИЙН УДИРДЛАГА

8.1. Зөрчлийг илрүүлэх, хяналт тавих

Байгууллагын мэдээллийн систем, сүлжээ, төхөөрөмж болон хэрэглэгчийн үйлдэлтэй холбоотой мэдээллийн аюулгүй байдлын зөрчил үүсэхээс урьдчилан сэргийлэх, илрүүлэх, хяналт тавих зорилгоор дараах арга хэмжээг хэрэгжүүлнэ:

8.1.1. **Зөрчил илрүүлэх систем ажиллуулах** – Хортой код, сэжигтэй үйлдэл, зөвшөөрөлгүй нэвтрэх оролдлогыг илрүүлэх програм, техник хэрэгслийг ашиглана.

8.1.2. **Лог бүртгэл хадгалах** – Сервер, сүлжээ, хэрэглэгчийн үйлдлийг автоматжуулсан бүртгэлийн системээр тасралтгүй бүртгэж, баталгаатай хадгална.

8.1.3. **Сэжигтэй үйлдэл хянах** – Системийн хэвийн бус ажиллагаа, сэжигтэй файлын үйлдэл, аюулгүй байдлын зөрчил, сэжигтэй тохиолол илэрсэн үед мэдээллийн технологийн мэргэжилтэн хяналт тавина.

8.2. Зөрчил мэдээлэх, бүртгэх

Зөрчил илэрсэн тохиолдолд байгууллагын албан хаагч бүр нэн даруй мэдээлэх үүрэгтэй.

8.2.1. **Зөрчил мэдээлэх** – Ажлын байрны компьютер, сервер, сүлжээний доголдол, сэжигтэй имэйл, нууц үгийн алдагдал зэрэг аюулгүй байдлын шинжтэй аливаа үйл явдлыг мэдээллийн технологийн мэргэжилтэнд шууд мэдэгдэнэ.

8.2.2. **Зөрчил бүртгэл үүсгэх** – Илэрсэн зөрчил бүрд огноо, цаг, шалтгаан, нөлөөлөл, холбогдох хэрэглэгчийн мэдээллийг багтаасан бүртгэл үүсгэнэ.

8.2.3. **Яаралтай мэдэгдэл** – Ноцтой зөрчлүүд (өгөгдөл алдагдах, систем доголдох, гадаад халдлагын оролдлого) тохиолдолд удирдлагад нэн даруй мэдэгдэнэ.

8.3. Зөрчилд хариу арга хэмжээ авах

Мэдээллийн аюулгүй байдлын зөрчлийн нөлөөллийг багасгах, саармагжуулах, системийг хэвийн байдалд оруулах зорилгоор дараах арга хэмжээг авна:

8.3.1. **Саармагжуулах арга хэмжээ** – Зөрчлийг үүсгэж буй эх үүсвэрийг таслан зогсоож, сүлжээний нэвтрэлтийг түр хаах, хортой файлыг тусгаарлах зэрэг шуурхай арга хэмжээ авна.

8.3.2. **Нөхөн сэргээх** – Системийн тохиргоо, өгөгдлийг нөөцөөс сэргээн босгож, хэвийн ажиллагаанд оруулна.

8.3.3. **Хэрэглэгчид мэдээлэх** – Хэрэглэгчдэд зөрчлийн талаар шаардлагатай мэдээллийг өгөх бөгөөд дахин давтагдахаас урьдчилан сэргийлэх зааварчилгаа хүргэнэ.

8.4. Зөрчилд дүн шинжилгээ хийх, тайлагнах

Зөрчлөөс үүдсэн эрсдэл, давтагдах боломжийг бууруулах зорилгоор дараах үйл ажиллагааг явуулна:

8.4.1. **Шалтгааныг тодорхойлох** – Зөрчил үүссэн үндсэн болон хавсарсан шалтгааныг тодруулж, системийн лог болон бүртгэлийн мэдээлэлд дүн шинжилгээ хийнэ.

8.4.2. **Сайжруулалтын арга хэмжээ боловсруулах** – Цаашид ижил төрлийн зөрчил гарахаас урьдчилан сэргийлэх зорилгоор бодлогын болон техникийн сайжруулалтын санал гарган хэрэгжүүлнэ.

8.4.3. **Тайлан гаргах** – Илэрсэн зөрчлийн талаар тайлан боловсруулж, удирдлагад хүргүүлнэ.

IX БҮЛЭГ. ҮҮРЭГ ХАРИУЦЛАГА

9.1. Байгууллагын удирдах албан тушаалтны хариуцлага

Байгууллагын удирдах албан тушаалтан мэдээллийн аюулгүй байдлыг хангах чиглэлээр дараах үүрэгтэй:

9.1.1. Байгууллагын мэдээллийн аюулгүй байдлыг хангах үйл ажиллагааг нэгдсэн удирдлагаар хангаж, уялдуулан зохион байгуулах, байгууллагыг төлөөлөн ажиллах.

9.1.2. Мэдээллийн аюулгүй байдлыг хангах бодлого, дүрэм, журам батлах, хэрэгжилтийг хянах.

9.1.3. Мэдээллийн аюулгүй байдлыг хангах төлөвлөгөөг батлан хэрэгжүүлэхэд шаардагдах нөөцийг байгууллагын жилийн төсөв, төлөвлөгөөнд тусгах.

9.2. Мэдээллийн аюулгүй байдал хариуцсан ажилтны үүрэг

Байгууллагын мэдээллийн аюулгүй байдал хариуцсан ажилтан дараах үүрэгтэй:

9.2.1. Байгууллагын мэдээллийн аюулгүй байдлыг хангах өдөр тутмын үйл ажиллагааг хариуцан гүйцэтгэх.

9.2.2. Холбогдох бодлого, дүрэм, журмыг боловсруулах, шинэчлэх санал боловсруулах.

9.2.3. Аюулгүй байдлыг хангахад шаардлагатай үйл ажиллагаа, нөөцийг төлөвлөх, хэрэгжилтийг зохион байгуулах.

9.2.4. Мэдээллийн аюулгүй байдлын чиглэлээр мэргэшүүлэх сургалтад тогтмол хамрагдах.

9.3. Байгууллагын нийт албан хаагчийн үүрэг

Байгууллагын нийт албан хаагч мэдээллийн аюулгүй байдлыг хангах чиглэлээр дараах үүрэгтэй:

9.3.1. Энэхүү журам болон мэдээллийн аюулгүй байдлын холбогдох дүрэм, журам, шаардлагыг мөрдөх.

9.3.2. Илэрсэн халдлага, зөрчил, доголдол, сэжигтэй тохиолдол бүрийг мэдээллийн аюулгүй байдал хариуцсан ажилтанд нэн даруй мэдэгдэх.

9.3.3. Байгууллагын мэдээлэл, мэдээллийн систем, сүлжээг зөвхөн албан хэрэгцээнд, батлагдсан журам, зааврын дагуу ашиглах.

9.3.4. Байгууллагаас зохион байгуулж буй мэдээллийн аюулгүй байдлын сургалтад тогтмол хамрагдах.

9.4. Хариуцлага

Энэхүү журмыг зөрчсөн албан тушаалтан, албан хаагчид холбогдох хууль тогтоомжид заасны дагуу хариуцлага хүлээлгэнэ.