

ТАВАНТОЛГОЙ ТӨМӨР ЗАМ ХХК-ИЙН ГҮЙЦЭТГЭХ ЗАХИРЛЫН ТУШААЛ

2026 оны 06 сарын 26 өдөр

Дугаар А/64

Улаанбаатар хот

"Мэдээллийн аюулгүй байдлын журам"-ыг шинэчлэн батлах тухай

Компанийн тухай хуулийн 83 дугаар зүйлийн 83.1, Архив, албан хэрэг хөтлөлтийн тухай хуулийн 35 дугаар зүйл, Засгийн газрын 2023 оны 224 дүгээр тогтоолын хавсралтаар баталсан "Кибер аюулгүй байдлыг хангах нийтлэг журам"-ын 1.2 дахь заалт, Компанийн дүрмийн 9 дүгээр зүйлийн 9.5.5, Хөдөлмөрийн дотоод журмын 1.4 дэх заалтыг тус тус үндэслэн ТУШААХ НЬ:

1. Компанийн "Мэдээллийн аюулгүй байдлын журам"-ыг хавсралтаар шинэчлэн баталсугай.
2. Журмыг шинэчлэн баталсантай холбогдуулан холбогдох арга хэмжээг авч ажиллахыг Захиргаа, эрх зүйн газар (Э.Түмэнжаргал)-т даалгасугай.
3. Энэ тушаал гарсантай холбогдуулан 2020 оны 01 дүгээр сарын 31-ний өдрийн А/08 тушаалыг хүчингүй болсонд тооцсугай.
4. Тушаалын хэрэгжилтэд хяналт тавьж ажиллахыг Хяналт, шинжилгээ, үнэлгээ, дотоод аудитын алба (Б.Нарангарав)-нд үүрэг болгосугай.

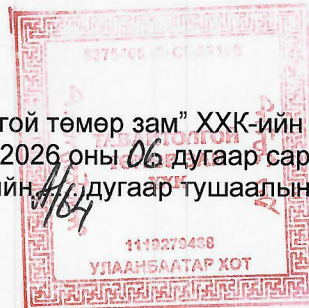
ГҮЙЦЭТГЭХ ЗАХИРЛЫН
ҮҮРЭГ ГҮЙЦЭТГЭГЧ



Х.ПҮРЭВЖАРГАЛ

0000000041

“Тавантолгой төмөр зам” ХХК-ийн Гүйцэтгэх
захирлын 2026 оны 06 дугаар сарын 26-ны
өдрийн 164 дугаар тушаалын хавсралт



МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ЖУРАМ

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДАЛ БА ХАРИЛЦААНЫ ЖУРАМ	4
1. Ерөнхий зүйл	4
1.1 Зорилго	4
1.2 Хамрах хүрээ	4
1.3 Ерөнхий зарчим	4
1.4 Мөрдөлт	4
2. Нэр томъёо ба тодорхойлолт	4
3. Мэдээллийн ангилал	5
3.1 Ангиллын зорилго	5
3.2 Мэдээллийн ангилал	5
3.3 Ангилал тогтоох	5
3.4 Ангиллын дагуу хэрэглэх шаардлага	5
3.5 Тэмдэглэгээ	5
4. Мэдээллийн эзэмшил, хариуцлага	5
4.1 Ерөнхий зохицуулалт	5
4.2 Мэдээллийн эзэмшигч	5
4.3 Хэрэглэгчийн үүрэг	5
4.4 Мэдээллийн аюулгүй байдлын хариуцлага	5
5. Мэдээллийн хадгалалт, хамгаалалт	5
5.1 Ерөнхий шаардлага	5
5.2 Мэдээллийн хадгалалт	6
5.3 Мэдээллийн хамгаалалт	6
5.4 Нөөцлөлт (Backup)	6
5.5 Мэдээлэл дамжуулах хамгаалалт	6
5.6 Устгал	6
6. Мэдээлэл ашиглалт, дамжуулалт (харилцаа)	6
6.1 Ерөнхий шаардлага	6
6.2 Дотоод харилцаа	6
6.3 Гадаад харилцаа	6
6.4 Мэдээлэл нийтлэх, зөвшөөрөл	6
6.5 Хориглолт	6
7. Мэдээллийн аюулгүй байдлын менежмент	6
7.1 Ерөнхий зохицуулалт	7
7.2 Эрсдэлийн удирдлага	7
7.3 Хяналт, хамгаалалтын арга хэмжээ	7
7.4 Зөрчлийн удирдлага	7
7.5 Сургалт, мэдлэг	7
7.6 Хяналт, сайжруулалт	7
7.7 Мэдээллийн аюулгүй байдлыг хариуцсан нэгжийн эрх, үүрэг	7
8. Мэдээллийн системийн аюулгүй байдал	7
8.1 Ерөнхий шаардлага	8
8.2 Хандалтын хяналт	8
8.3 Нэвтрэх аюулгүй байдал	8
8.4 Системийн хамгаалалт	8

8.5 Сүлжээний аюулгүй байдал.....	8
8.6 Бүртгэл, хяналт	8
8.7 Төхөөрөмжийн аюулгүй байдал.....	8
9. Мэдээллийн технологийн хамгаалалт	8
9.1 Ерөнхий шаардлага.....	8
9.2 Дэд бүтцийн хамгаалалт.....	8
9.3 Нөөцлөлт ба сэргээх	8
9.4 Физик аюулгүй байдал	8
9.5 Төхөөрөмжийн ашиглалт	9
9.6 Тоног төхөөрөмжийн нууцлал, хамгаалалт	9
9.7 Хортой кодоос хамгаалах.....	9
10. Нэвтрэх эрхийг цуцлах	10
11. Мэдээллийн аюулгүй байдлын осолд авах хариу арга хэмжээ.....	11
11.1 Ерөнхий шаардлага.....	11
11.2 Ослын илрүүлэлт ба мэдэгдэл.....	11
11.3 Анхан шатны үнэлгээ ангилал.....	11
11.4 Хязгаарлалт ба таслан зогсоох арга хэмжээ	11
11.5 Судалгаа, шинжилгээ	11
11.6 Нөхөн сэргээх	11
11.7 Мэдээлэх, тайлагнах	11
11.8 Дүгнэлт, сайжруулалт	11
11.9 Яаралтай арга хэмжээ авах.....	11
11.10 Хариуцлага	11
12. Бусад.....	12
Хавсралт 1: Мэдээллийн ангиллын жишээ.....	13
Хавсралт 2: Хандалтын эрхийн матриц	14

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ЖУРАМ

Нэг.Ерөнхий зүйл

1.1. Зорилго

1.1.1. Энэхүү журмын зорилго нь Компанийн мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмжийг хангах, мэдээллийг хамгаалах, ашиглах, дамжуулах үйл ажиллагааг зохицуулах, мэдээллийн аюулгүй байдлын эрсдэлийг бууруулахад оршино.

1.2. Хамрах хүрээ

1.2.1. Энэхүү журам нь Компанийн ажилтан, удирдлага, гэрээт болон гадаад этгээдэд хамаарах бөгөөд Компанийн бүх төрлийн мэдээлэл, мэдээллийн систем, мэдээллийн технологийн дэд бүтцийг хамарна.

1.2.2. Энэхүү журам нь Компанийн бүх төрлийн мэдээллийн (цахим, аман, дүрс, системийн өгөгдөл) аюулгүй байдал, ашиглалт, дамжуулалтыг зохицуулна.

1.3. Ерөнхий зарчим

1.3.1. Компани мэдээллийн аюулгүй байдлыг хангахдаа дараах зарчмыг баримтална:

1.3.1.1. Нууцлал

1.3.1.2. Бүрэн бүтэн байдал

1.3.1.3. Хүртээмж

1.3.1.4. Хариуцлага

1.3.1.5. Хууль, дүрмийн нийцэл

1.4. Мөрдөлт

1.4.1. Энэхүү журмыг Компанийн хэмжээнд заавал мөрдөх бөгөөд хэрэгжилтэд хяналт тавьж, шаардлагатай тохиолдолд сайжруулна.

Хоёр. Нэр томьёо ба тодорхойлолт

2.1. Энэхүү журамд хэрэглэсэн дараах нэр томьёог дор дурдсан утгаар ойлгоно:

2.1.1. **“Мэдээлэл”** – Компанийн үйл ажиллагаатай холбоотой бичгийн, цахим, дүрс, дуу, аман болон бусад хэлбэрээр илэрхийлэгдсэн өгөгдөл;

2.1.2. **“Мэдээллийн аюулгүй байдал”** – мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмжийг хангах үйл ажиллагаа;

2.1.3. **“Нууц мэдээлэл”** – зөвшөөрөлгүй этгээдэд задруулахыг хориглосон, хязгаарлагдмал хандалттай мэдээлэл;

2.1.4. **“Мэдээллийн систем”** – мэдээллийг боловсруулах, хадгалах, дамжуулах зориулалт бүхий программ, техник хэрэгсэл, сүлжээний цогц;

2.1.5. **“Хэрэглэгч”** – Компанийн мэдээлэл, мэдээллийн системд нэвтрэх эрхтэй ажилтан болон бусад этгээд;

2.1.6. **“Нийлүүлэгч”** – Компанид бүтээгдэхүүн, үйлчилгээ, эсхүл үйл явц нийлүүлдэг гадаад хувь хүн болон хуулийн этгээд;

2.1.7. **“Хандалтын эрх”** – мэдээлэл, мэдээллийн системд нэвтрэх, ашиглах зөвшөөрөгдсөн түвшин;

2.1.8. **“Тохиолдол”** – мэдээллийн аюулгүй байдалд сөргөөр нөлөөлсөн эсхүл нөлөөлөх эрсдэлтэй үйл явдал;

2.1.9. **Мэдээллийн эзэмшигч** – Компанийн тодорхой мэдээлэлд өмчлөл, хариуцлага хүлээж, тухайн мэдээллийн ангиллыг тогтоох, хамгаалалт, ашиглалт, хадгалалт болон хандалтын эрхийг тодорхойлох, зөвшөөрөх эрх бүхий албан тушаалтан эсхүл нэгж /Компанийн удирдлагын нэрийн өмнөөс тухайн мэдээлэл хариуцсан нэгжийн удирдлага жишээ: хэлтсийн дарга) томилогддог/;

2.1.10. **Хэрэглэгч** – Компанийн мэдээлэл, мэдээллийн системд нэвтрэх, ашиглах эрхтэй ажилтан болон бусад этгээд /Ажилтан, гэрээт ажилтан, нийлүүлэгч бүгд орно/;

2.1.11. **Мэдээллийн аюулгүй байдлын осол** – мэдээлэл задрах, алдагдах, зөвшөөрөлгүй өөрчлөгдөх, систем тасалдах, халдлагад өртөх тохиолдол;

2.1.12. **МАБ-ын хариуцсан ажилтан** – мэдээллийн аюулгүй байдлыг хариуцсан албан

тушаалтан.

Гурав. Мэдээллийн ангилал

3.1. Ангиллын зорилго

3.1.1. Мэдээллийн хөрөнгө нь биет, цахим, программ хангамж, техник хангамжийн хэлбэртэй байна. Компанийн мэдээллийг ач холбогдол, нууцлалын түвшнээр нь ангилан хамгаалалтын зохих арга хэмжээг хэрэгжүүлэхэд энэхүү ангиллын зорилго оршино.

3.2. Мэдээллийн ангилал

3.2.1. Компанийн мэдээллийг дараах ангилалд хуваана:

3.2.1.1. **Нээлттэй мэдээлэл** – олон нийтэд чөлөөтэй түгээж болох мэдээлэл (жишээ: вэб сайт, нийтэд зориулсан мэдээ, тайлан);

3.2.1.2. **Дотоод мэдээлэл** – зөвхөн Компанийн ажилтанд хамаарах, гадагш түгээхийг хязгаарласан мэдээлэл;

3.2.1.3. **Нууц мэдээлэл** – зөвшөөрөгдсөн хязгаарлагдмал этгээдэд хамаарах, задруулах нь Компанид сөрөг нөлөө үзүүлэх мэдээлэл;

3.2.1.4. **Маш нууц мэдээлэл** – стратегийн ач холбогдол бүхий, задруулах нь ноцтой эрсдэл үүсгэх мэдээлэл;

3.3. Ангилал тогтоох

3.3.1. Мэдээллийн ангиллыг тухайн мэдээллийг үүсгэгч болон хариуцагч этгээд тогтооно.

3.4. Ангиллын дагуу хэрэглэх шаардлага

3.4.1 Мэдээллийг ангиллын дагуу хадгалах, ашиглах, дамжуулах;

3.4.2 Нууц болон маш нууц мэдээлэлд зөвшөөрөгдсөн этгээд хандах;

3.4.3 Мэдээллийг зөвшөөрөлгүйгээр хуулбарлах, дамжуулахыг хориглоно.

3.5. Тэмдэглэгээ

3.5.1. Шаардлагатай тохиолдолд мэдээлэлд ангиллын тэмдэглэгээг (жишээ: “НУУЦ”, “ДОТООД”) тодорхой байдлаар байршуулна.

Дөрөв. Мэдээллийн эзэмшил, хариуцлага

4.1. Ерөнхий зохицуулалт

4.1.1. Компанийн бүх мэдээлэл нь тодорхой эзэмшигчтэй байх бөгөөд мэдээллийг хамгаалах, зөв ашиглах, ангилах, хандалтыг зохицуулах үүргийг хүлээнэ.

4.2. Мэдээллийн эзэмшигч

4.2.1. Мэдээллийн эзэмшигч нь дараах үүргийг хэрэгжүүлнэ:

4.2.1.1. Мэдээллийн ангиллыг тогтоох;

4.2.1.2. Хандалтын эрхийг тодорхойлох, зөвшөөрөх;

4.2.1.3. Мэдээллийн ашиглалт, хамгаалалтад хяналт тавих;

4.2.1.4. Шаардлагатай тохиолдолд мэдээллийн ангиллыг шинэчлэх.

4.3. Хэрэглэгчийн үүрэг /Мэдээлэл, мэдээллийн систем ашиглаж буй хэрэглэгч/

4.3.1 Зөвшөөрөгдсөн хүрээнд мэдээллийг ашиглах;

4.3.2 Нууц мэдээллийг задруулахгүй байх;

4.3.3 Хандалтын эрхийг бусдад дамжуулахгүй байх;

4.3.4 Аюулгүй байдлын зөрчлийг илэрсэн даруйд мэдэгдэх;

4.4. Мэдээллийн аюулгүй байдлын хариуцлага

4.4.1. Компани мэдээллийн аюулгүй байдлыг хангахтай холбоотойгоор дараах арга хэмжээг авна:

4.4.1.1. Дүрэм, журам мөрдүүлэх;

4.4.1.2. Хяналт, хамгаалалтын арга хэмжээг хэрэгжүүлэх;

4.4.1.3. Ажилтнуудад мэдээллийн аюулгүй байдлын мэдлэг олгох, сургалт зохион байгуулах.

Тав. Мэдээллийн хадгалалт, хамгаалалт

5.1. Ерөнхий шаардлага

- 5.1.1. Компанийн мэдээллийг түүний ангилалд нийцүүлэн хадгалах, хамгаалах бөгөөд мэдээллийг алдагдах, устгах, өөрчлөгдөх, зөвшөөрөлгүй нэвтрэхээс сэргийлнэ.
- 5.2. Мэдээллийн хадгалалт**
- 5.2.1. Мэдээллийг баталгаат, хамгаалалттай орчинд хадгална (сервер, систем, архив);
- 5.2.2. Цахим мэдээллийг зөвшөөрөгдсөн систем, төхөөрөмж дээр хадгална;
- 5.2.3. Мэдээллийг ангиллын дагуу хадгалах хугацааг мөрдөнө;
- 5.2.4. Тухайн шаардлагын дагуу боловсруулагдсан мэдээллийг нөөц хувь үүсгэн хадгална.
- 5.3 Мэдээллийн хамгаалалт**
- 5.3.1. Нууц болон дотоод мэдээлэлд зөвшөөрөгдсөн этгээд хандах;
- 5.3.2. Нууц мэдээллийг зөвшөөрөлгүйгээр хуулбарлах, дамжуулах, гадагш тараахыг хориглоно;
- 5.3.3. Хандалтын эрхийг албан тушаал, үүрэгтэй уялдуулан олгоно;
- 5.3.4. Ажилтан ажлаас чөлөөлөгдөх, үүрэг өөрчлөгдөх үед хандалтын эрхийг цуцална;
- 5.4 Нөөцлөлт (Backup)**
- 5.4.1. Чухал мэдээллийг дараах байдлаар тогтмол нөөцөлнө:
- 5.4.1.1. Нөөцлөлтийг тусгаарласан, аюулгүй орчинд хадгална;
- 5.4.1.2. Нөөц мэдээллийг шаардлагатай үед сэргээх боломжийг хангана;
- 5.5. Устгал**
- 5.5.1. Хэрэгцээгүй болсон мэдээллийг зохих журмын дагуу устгана;
- 5.5.2. Нууц мэдээллийг сэргээх боломжгүй байдлаар устгана (жишээ: устгах программ, бутлагч);
- 5.5.3. Мэдээлэл устгасан тухай бүртгэл хөтөлж болно.

Зургаа. Мэдээлэл ашиглалт, дамжуулалт (харилцаа)

- 6.1. Ерөнхий шаардлага**
- 6.1.1. Мэдээллийг зөвхөн албан хэрэгцээнд, тухайн мэдээллийн ангилалд нийцүүлэн ашиглах бөгөөд зөвшөөрөлгүйгээр дамжуулах, түгээхийг хориглоно.
- 6.2 Дотоод харилцаа**
- 6.2.1. Компанийн дотоод мэдээллийг зөвшөөрөгдсөн сувгаар (албан и-мэйл, дотоод систем) дамжуулна;
- 6.2.2. Нууц болон дотоод мэдээллийг олон нийтэд ил тод сувгаар дамжуулахыг хориглоно;
- 6.2.3. Ажилтнууд мэдээллийг зөвхөн өөрийн хандалтын эрхийн хүрээнд ашиглана.
- 6.3. Гадаад харилцаа**
- 6.3.1. Компанийн мэдээллийг гадаад этгээдэд дамжуулахдаа зохих зөвшөөрөл авна;
- 6.3.2. Хэвлэл мэдээлэл, олон нийтэд мэдээлэл өгөхийг зөвхөн эрх бүхий албан тушаалтан хэрэгжүүлнэ;
- 6.3.3. Нууц болон хязгаарлагдмал мэдээллийг гадагш дамжуулахыг хориглоно;
- 6.4. Мэдээлэл нийтлэх, зөвшөөрөл**
- 6.4.1. Олон нийтэд мэдээлэл нийтлэхээс өмнө холбогдох албан тушаалтнаар хянуулж, батлуулна;
- 6.4.2. Компанийн нэрийн өмнөөс мэдээлэл түгээх эрхийг тодорхой албан тушаалтанд олгоно.
- 6.5 Хориглолт**
- 6.5.1. Компанийн мэдээллийг зөвшөөрөлгүйгээр олон нийтэд түгээх;
- 6.5.2. Нууц мэдээллийг хувийн и-мэйл, төхөөрөмжөөр дамжуулах;
- 6.5.3. Компанийн мэдээллийг хувийн зорилгоор ашиглах.

Долоо. Мэдээллийн аюулгүй байдлын менежмент

- 7.1. Ерөнхий зохицуулалт**
- 7.1.1. Компани мэдээллийн аюулгүй байдлыг хангах зорилгоор бодлого, журам,

хяналтын арга хэмжээг хэрэгжүүлж, мэдээллийн аюулгүй байдлын эрсдэлийг тогтмол үнэлж, бууруулна.

7.2 Эрсдэлийн удирдлага

7.2.1. Мэдээллийн аюулгүй байдалтай холбоотой эрсдэлийг тодорхойлох, үнэлэх, бууруулах арга хэмжээ авч хэрэгжүүлнэ.

7.2.2. Эрсдэлийн үнэлгээг шаардлагатай үед болон тогтмол хугацаанд хийж, шинэчилнэ.

7.3. Хяналт, хамгаалалтын арга хэмжээ

7.3.1 Мэдээлэлд зөвшөөрөгдсөн хандалтыг хангах, хяналт тавих;

7.3.2 Мэдээллийн систем, сүлжээ, төхөөрөмжийг хамгаалах арга хэмжээ авах;

7.3.3 Хандалтын бүртгэл (лог)-ийг хөтөлж, хяналт тавих.

7.4 Зөрчлийн удирдлага

7.4.1 Мэдээллийн аюулгүй байдлын зөрчлийг илрүүлэх, бүртгэх, мэдээлэх;

7.4.2 Зөрчлийг шуурхай арга хэмжээ авч хязгаарлах, засварлах;

7.4.3 Зөрчлийн шалтгааныг тодорхойлж, давтагдахаас сэргийлэх арга хэмжээ авах.

7.5 Сургалт, мэдлэг

7.5.1. Ажилтнуудад мэдээллийн аюулгүй байдлын сургалт, зааварчилгааг тогтмол зохион байгуулах;

7.5.2. Мэдээллийн аюулгүй байдлын талаарх мэдлэг, ойлголтыг нэмэгдүүлэх;

7.6. Хяналт, сайжруулалт

7.6.1 Журмын хэрэгжилтэд дотоод хяналт тавих;

7.6.2 Илэрсэн зөрчил, сул талыг засах, сайжруулах арга хэмжээ авах;

7.6.3 Мэдээллийн аюулгүй байдлын тогтолцоог тасралтгүй сайжруулна.

7.7. Мэдээллийн аюулгүй байдлыг хариуцсан нэгжийн эрх, үүрэг

7.7.1. Мэдээллийн аюулгүй байдлыг хариуцсан нэгж (эсхүл холбогдох албан тушаалтан) нь дараах эрх, үүргийг хэрэгжүүлнэ:

7.7.1.1. Компанийн мэдээллийн аюулгүй байдлын бодлого, журам боловсруулах, хэрэгжилтэд хяналт тавих;

7.7.1.2. Мэдээллийн аюулгүй байдлын эрсдэлийг тодорхойлох, үнэлэх, бууруулах арга хэмжээ зохион байгуулах;

7.7.1.3. Мэдээллийн систем, сүлжээ, төхөөрөмжид аюулгүй байдлын хяналт шалгалт хийх;

7.7.1.4. Мэдээллийн аюулгүй байдлын зөрчлийг илрүүлэх, бүртгэх, хариу арга хэмжээ авах;

7.7.1.5. Хэрэглэгчдийн хандалтын эрхийн удирдлагад хяналт тавих;

7.7.1.6. Мэдээллийн аюулгүй байдлын сургалт, мэдлэг олгох үйл ажиллагааг зохион байгуулах;

7.7.1.7. Шаардлагатай тохиолдолд мэдээллийн системд нэвтрэх, шалгах эрх эдлэх;

7.7.1.8. Мэдээллийн аюулгүй байдлын шаардлага зөрчсөн тохиолдолд холбогдох арга хэмжээ авах талаар удирдлагад санал гаргах.

Найм. Мэдээллийн системийн аюулгүй байдал

8.1. Ерөнхий шаардлага

8.1.1. Компанийн мэдээллийн системийн аюулгүй байдлыг хангах зорилгоор систем, программ хангамж, сүлжээ, хэрэглэгчийн хандалтад зохих хамгаалалтын арга хэмжээг хэрэгжүүлнэ.

8.2. Хандалтын хяналт

8.2.1. Мэдээллийн системд нэвтрэх эрхийг албан тушаал, үүрэгтэй уялдуулан олгоно.

8.2.2 Хэрэглэгч бүр давтагдашгүй нэр, нууц үгтэй байна.

8.2.3 Нууц үгийг бусдад дамжуулахыг хориглоно.

8.2.4 Ажилтан ажлаас чөлөөлөгдөх, үүрэг өөрчлөгдөх үед хандалтын эрхийг цуцлах буюу өөрчилнө.

8.3 Нэвтрэх аюулгүй байдал

8.3.1. Мэдээллийн системд нэвтрэх нууц үгийн шаардлагыг (урт, нийлмэл байдал) тогтоож мөрдөнө.

- 8.3.2. Нууц үгийг тогтмол хугацаанд солих бөгөөд шаардлагатай тохиолдолд нэн даруй шинэчилнэ.
- 8.3.3. Нууц үгийг дахин ашиглахыг хориглоно.
- 8.3.4. Олон удаагийн буруу нэвтрэх оролдлого илэрсэн тохиолдолд нэвтрэх эрхийг түр хугацаанд хаана.
- 8.3.5. Шаардлагатай тохиолдолд нэмэлт баталгаажуулалт (жишээ: хоёр шатлалт баталгаажуулалт)-ыг хэрэглэнэ.
- 8.4 Системийн хамгаалалт**
 - 8.4.1. Программ хангамжийг зөвшөөрөгдсөн эх сурвалжаас ашиглана.
 - 8.4.2. Систем, программ хангамжийг тогтмол шинэчилж, засвар хийнэ.
 - 8.4.3. Хортой программ (вирус)-аас хамгаалах арга хэмжээ авна.
- 8.5 Сүлжээний аюулгүй байдал**
 - 8.5.1. Компанийн сүлжээг хамгаалах (жишээ: firewall, нэвтрэх хяналт) арга хэмжээг хэрэгжүүлнэ.
 - 8.5.2. Мэдээлэл технологийн мэргэжилтний зөвшөөрөөгүй төхөөрөмжийг сүлжээнд холбохыг хориглоно.
 - 8.5.3. Алсын зайнаас хандах үед хамгаалалтын арга (жишээ: VPN) хэрэглэнэ.
 - 8.5.4. Сүлжээний кабелийн үзүүрт хаяг хадан, ашиглагдаагүй гаралтуудыг тэмдэглэж, сүлжээний зохицуулагчаас өөр хүн ашиглах боломжийг хаана.
- 8.6 Бүртгэл, хяналт**
 - 8.6.1. Мэдээллийн системийн нэвтрэлт, ашиглалтын бүртгэлийг (лог) хөтөлнө.
 - 8.6.2. Сэжигтэй үйлдлийг илрүүлэх, хянах, шалгах арга хэмжээг хэрэгжүүлнэ.
 - 8.6.3. Лог мэдээллийн бүрэн бүтэн байдал, нууцлалыг хангана.
 - 8.6.4. Лог мэдээллийг тодорхой хугацаанд 1 жил хадгална.
 - 8.6.5. Лог мэдээлэлд зөвшөөрөлгүй өөрчлөлт оруулахыг хориглоно.
- 8.7 Төхөөрөмжийн аюулгүй байдал**
 - 8.7.1. Компанийн компьютер, сервер, төхөөрөмжийг хамгаалах (нууц үг, түгжээ, хамгаалалт) арга хэмжээ авна.
 - 8.7.2. Компанийн мэдээллийг хувийн төхөөрөмжид хадгалахыг хязгаарлана.

Ес. Мэдээллийн технологийн хамгаалалт

- 9.1. Ерөнхий шаардлага**
 - 9.1.1. Компанийн мэдээллийн технологийн дэд бүтэц (сервер, сүлжээ, төхөөрөмж)-ийг хамгаалах, тасралтгүй ажиллагааг хангах зорилгоор зохих техник, зохион байгуулалтын арга хэмжээг хэрэгжүүлнэ.
- 9.2. Дэд бүтцийн хамгаалалт**
 - 9.2.1. Сервер, сүлжээний төхөөрөмжийг зориулалтын орчинд байршуулж, зөвшөөрөгдсөн этгээд нэвтрэх нөхцөлийг хангана.
 - 9.2.2. Цахилгаан хангамж, тасралтгүй ажиллагааг (жишээ: UPS) хангана.
 - 9.2.3. Чийг, температур, галын аюулаас хамгаалах арга хэмжээ авна.
- 9.3 Нөөцлөлт ба сэргээх**
 - 9.3.1. Компанийн чухал мэдээлэл, системийг тогтмол нөөцөлнө.
 - 9.3.2. Нөөц мэдээллийг үндсэн системээс тусгаарласан, аюулгүй орчинд хадгална.
 - 9.3.3. Нөөцөөс сэргээх боломжийг тогтмол шалгаж баталгаажуулна.
 - 9.3.4. Онцгой нөхцөл (системийн саатал, осол, кибер халдлага зэрэг)-д мэдээлэл, системийг сэргээх төлөвлөгөө боловсруулж, хэрэгжүүлнэ.
 - 9.3.5. Сэргээх төлөвлөгөөг шаардлагатай үед туршиж, сайжруулна.
- 9.4. Физик аюулгүй байдал**
 - 9.4.1. Компанийн мэдээллийн технологийн дэд бүтэц, сервер, тоног төхөөрөмж байрлах орчны физик аюулгүй байдлыг хангах зорилгоор дараах арга хэмжээг хэрэгжүүлнэ:
 - 9.4.1.1. Сервер болон мэдээллийн сан, мэдээлэл хадгалагддаг компьютеруудыг орчны нөлөөнөөс хамгаалах шаардлагатай;
 - 9.4.1.2. Камер, хяналтын систем болон нэвтрэх хяналтын хэрэгсэл ашиглаж болно;
 - 9.4.1.3. Төхөөрөмжийг зөвшөөрөлгүй зөөвөрлөх, ашиглахыг хориглоно;

9.4.1.4. Орчны хамгаалалт: Физик хамгаалалт нь сервер болон ажлын компьютерууд, өрөөг орчны аюулаас сэргийлэх зорилготой. Физик хамгаалалтыг дараах 3 бүсэд ангилж үзнэ.

9.4.2. Компанийн байр, тоног төхөөрөмжийн орчныг мэдээллийн аюулгүй байдлын түвшнээр дараах байдлаар ангилна:

9.4.2.1. **Нээлттэй бүс** – олон нийт болон зочдод нээлттэй, мэдээллийн аюулгүй байдлын эрсдэл бага бүс;

9.4.2.2. **Хязгаарлагдмал бүс** – зөвхөн Компанийн ажилтанд нэвтрэх эрхтэй, дотоод үйл ажиллагаа явагддаг бүс;

9.4.2.3. **Хаалттай бүс** – зөвхөн эрх бүхий албан тушаалтанд нэвтрэхийг зөвшөөрсөн, серверийн өрөө болон мэдээллийн чухал дэд бүтэц байрлах өндөр хамгаалалттай бүс.

9.5. Төхөөрөмжийн ашиглалт

9.5.1. Компанийн тоног төхөөрөмжийг зөвхөн албан хэрэгцээнд ашиглана;

9.5.2. Төхөөрөмжид суурилуулсан программ, тохиргоог зөвшөөрөлгүй өөрчлөхийг хориглоно;

9.5.3. Ажилтан ажлын компьютерын дэлгэцийг бусдад шууд харагдахгүйгээр байрлуулсан байх;

9.5.4. Хэвлэгч, олшруулагч хэрэгслүүдийг удирдлагын хараа хяналттай өрөөнд байрлуулах;

9.5.5. Нууц бичиг баримт боловсруулахдаа гадаад, дотоод сүлжээнд холбогдоогүй компьютер ашиглах;

9.5.6. Зөөврийн хадгалах төхөөрөмж дээрх мэдээллийг ашиглаж дууссаны дараагаар мэдээллийг арилгах;

9.5.7. Зориулалтын сав, хайрцагт хийж зөөвөрлөдөг байх;

9.5.8. Гаднаас зөөврийн хадгалах төхөөрөмж системд оруулах бол заавал хортой кодын эсрэг програм уншуулах;

9.5.9. Хариуцаж буй компьютер техник хэрэгсэлд засвар, үйлчилгээг зөвшөөрөлгүй гадны хүнээр хийлгэх;

9.5.10. Өөрийн компьютерт шаардлагагүй дундын хавтас сүлжээнд нээхгүй байх. Сүлжээнд нээсэн дундын хавтас дотор чухал мэдээ материал, өгөгдлийг удаан хугацаагаар хадгалахгүй байх.

9.6. Тоног төхөөрөмжийн нууцлал, хамгаалалт

9.6.1. Компани нь өөрийн компьютер, техник хэрэгслийг заавал гэрчилгээжүүлсэн байна. Гэрчилгээг засвар үйлчилгээ хийсэн шинэ програм хангамж суулгасан тохиолдолд МТ-ийн мэргэжилтэн болон тухайн компьютер техник хэрэгслийг эзэмшигч хоёул гарын үсэг зурж баталгаажуулна.

9.6.2. Ажилтны компьютерыг форматлан үйлдлийн системийг дахин суулгах тохиолдолд хэрэгцээт файлуудыг өөр дискэнд хуулж, үйлдлийн системийг суулгаж тохируулга хийсний дараа файлын вирусийг шалган, арилгаад буцааж хуулна.

9.7. Хортой кодоос хамгаалах

9.7.1. Компанийн хэрэгцээнд хэрэглэгдэж байгаа компьютер, мэдээлэл хадгалагч болон тээгч зөөврийн хэрэгслүүдэд зөвшөөрөгдсөн хортой кодын эсрэг програм хангамжийг ашиглана.

9.7.2. Хортой кодын эсрэг програмын шинэчлэлтийг тогтмол хийнэ.

9.7.3. Тодорхой хугацаанд системийн хортой кодын эсрэг програмыг уншуулж, илэрсэн тохиолдолд арилгах арга хэмжээг авна.

9.7.4. Гаднаас мэдээллийг өөрийн системд оруулах бол сүлжээнд холбогдоогүй компьютерт эхэлж хортой кодын шинжилгээг заавал хийсний дараа системд нэвтрүүлнэ.

9.7.5. Мэдээллийн санд нэвтрэх эрхийн түвшин: Компаний ажилтан ажлын чиг үүргийнхээ дагуу мэдээллийн санд эрхийн өөр өөр түвшинд хандана. Үүнд:

9.7.5.1. Админ эрх - Систем шинээр суулгах, тохируулга хийх, нэмэлт, өөрчлөлт оруулах, системд хэрэглэгч нэмэх, хасах эрхтэй байна.

9.7.5.2. Бичих - Мэдээллийн санд шинэ бичлэг нэмэх, өөрчлөх, хадгалах эрхтэй.

9.7.5.3. Зөвхөн харах эрх - Зөвхөн харах, унших эрхтэй байна.

Арав. Нэвтрэх эрхийг цуцлах

- 10.1. Мэдээллийн сан, мэдээллийн системд хандах эрх бүхий ажилтан ажлаас гарсан, халагдсан, өөр ажилд шилжсэн тохиолдолд нэвтрэх эрхийг цуцална. Компанийн хүний нөөцийн нэгж, ажилтан тухайн ажилтанг ажлаас чөлөөлсөн тухай системийн зохицуулагчид мэдэгдсэн байна.
- 10.2. Ажилтан өөрийн эрхийн түвшнээс өөр гадна ажлын шаардлагаар мэдээллийн системд нэвтрэх шаардлага гарсан үед холбогдох хариуцагч ажилтнаас заавал зөвшөөрөл авсан байна.

Арван нэг. Мэдээллийн аюулгүй байдлын осолд авах хариу арга хэмжээ

11.1. Ерөнхий шаардлага

- 11.1.1 Байгууллагын мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмж алдагдах ослын үед авах арга хэмжээг зохицуулна.
- 11.1.2 Журам нь бүх ажилтан, гэрээт ажилтан, мэдээллийн систем ашиглагчдад хамаарна.

11.2. Ослын илрүүлэлт ба мэдэгдэл

- 11.2.1. Ослын шинж тэмдэг илэрсэн даруйд тухайн ажилтан 1 цагийн дотор МАБ-ын хариуцсан ажилтанд мэдэгдэнэ.
- 11.2.2. Мэдэгдэлд дараах мэдээллийг багтаана:
 - 11.2.2.1. Илэрсэн огноо, цаг
 - 11.2.2.2. Холбогдох систем, өгөгдөл
 - 11.2.2.3. Илрүүлсэн этгээдийн нэр

11.3. Анхан шатны үнэлгээ, ангилал

- 11.3.1. МАБ-ын хариуцсан ажилтан ослыг дараах байдлаар ангилна:
 - 11.3.1.1. Бага – үйл ажиллагаанд бага нөлөөтэй
 - 11.3.1.2. Дунд – тодорхой систем, хэрэглэгчид нөлөөлсөн
 - 11.3.1.3. Өндөр (онц ноцтой) – чухал мэдээлэл, үндсэн системд нөлөөлсөн
- 11.3.2. Осол бүрт үнэлгээний протокол хөтөлнө.

11.4. Хязгаарлалт ба таслан зогсоох арга хэмжээ

- 11.4.1. Сэжигтэй системийг сүлжээнээс тусгаарлах
- 11.4.2. Хэрэглэгчийн эрхийг түр түдгэлзүүлэх
- 11.4.3. Холбогдох IP, данс, процессийг хаах

11.5. Судалгаа, шинжилгээ

- 11.5.1. Шалтгааныг тодорхойлох зорилгоор дараах арга хэмжээг авна:
 - 11.5.1.1. Лог файл, системийн бүртгэл шалгана.
 - 11.5.1.2. Ямар өгөгдөл өртсөнийг тогтооно.
 - 11.5.1.3. Судалгааны үр дүнг бичгээр баримтжуулна.

11.6. Нөхөн сэргээх

- 11.6.1 Системийг аюулгүй байдлыг хангасан нөхцөлд дараах аргаар сэргээнэ:
 - 11.6.1.1. Нөөц хуулбараас сэргээх;
 - 11.6.1.2. Нууц үг, түлхүүр солих;
 - 11.6.1.3. Аюулгүй байдлын цоорхой арилгах;
 - 11.6.1.4. Эмзэг байдал (vulnerability) засах;
 - 11.6.1.5. Сэргээгдсэн системд тест хийж баталгаажуулах.

11.7. Мэдээлэх, тайлагнах

- 11.7.1. Ослыг удирдлагад тайлагнана.
- 11.7.2. Хуулиар шаардлагатай тохиолдолд холбогдох байгууллага, харилцагчид мэдэгдэнэ.
- 11.7.3. Тайланд дараах мэдээлэл орно:
 - 11.7.3.1. Ослын товч тайлбар;
 - 11.7.3.2. Авсан арга хэмжээ.

11.8. Дүгнэлт, сайжруулалт

- 11.8.1 Ослын дараа дүгнэсэн уулзалт зохион байгуулна.

11.8.2 Журам, техник, сургалтыг сайжруулна.

11.9 Яаралтай арга хэмжээ авах

11.9.1 Ажилтан – ослыг нэн даруй мэдээлэх

11.9.2 IT алба – техникийн арга хэмжээ авах

11.9.3 МАБ-ын ажилтан – удирдлага, зохицуулалт

11.9.4 Удирдлага – шийдвэр гаргах, хариуцлага тооцох

11.10. Хариуцлага

11.10.1. Энэхүү журмыг зөрчсөн этгээдэд холбогдох хууль тогтоомж, Компанийн дотоод дүрэм, журамд заасны дагуу хариуцлага хүлээлгэнэ.

Арван хоёр.Бусад

12.1. Энэхүү журамд тусгагдаагүй асуудлыг холбогдох хууль тогтоомж, Компанийн бусад дүрэм, журамд нийцүүлэн шийдвэрлэнэ.

12.2. Журмын хэрэгжилтэд хяналт тавих, хэрэгжилтийг үнэлэх, шаардлагатай тохиолдолд нэмэлт, өөрчлөлт оруулах ажлыг холбогдох нэгж хариуцан хэрэгжүүлнэ.

12.3. Энэхүү журам батлагдсан өдрөөс эхлэн хүчин төгөлдөр мөрдөгдөнө.

-О-

Мэдээллийн аюулгүй байдлын журмын
Хавсралт №1: Мэдээллийн ангиллын жишээ

№	Мэдээллийн төрөл	Ангилал	Жишээ	Хандалтын түвшин	Хамгаалалтын шаардлага
1	Олон нийтэд мэдээлэл	Нээлттэй	Вэб сайт, хэвлэлийн мэдээ	Бүх хүн	Хязгаарлалтгүй
2	Дотоод үйл ажиллагааны мэдээлэл	Дотоод	Дотоод тайлан, журам	Ажилтнууд	Гадагш түгээхийг хориглоно
3	Санхүү, гэрээний мэдээлэл	Нууц	Гэрээ, санхүүгийн тайлан	Зөвшөөрөгдсөн ажилтан	Нууцлал, хандалтын хяналт
4	Стратегийн мэдээлэл	Маш нууц	Тендер, төлөвлөгөө	Удирдлага	Хатуу хяналт, шифрлэл
5	Хүний нөөцийн мэдээлэл	Нууц	Ажилтны хувийн мэдээлэл	HR, удирдлага	Хувийн мэдээллийн хамгаалалт
6	IT системийн мэдээлэл	Нууц / Маш нууц	Нэвтрэх эрх, серверийн тохиргоо	IT нэгж	Хандалтын хязгаарлалт

-О-

Мэдээллийн аюулгүй байдлын журмын
Хавсралт №2: Хандалтын эрхийн матриц

№	Мэдээллийн төрөл	Удирдлага	Хэлтсийн дарга	Ажилтан	IT админ	Гуравдагч этгээд
1	Нээлттэй мэдээлэл	✓	✓	✓	✓	✓
2	Дотоод мэдээлэл	✓	✓	✓	✓	✗
3	Нууц мэдээлэл	✓	✓	Хязгаарлагдмал	✓	Зөвшөөрөлтэй
4	Маш нууц мэдээлэл	✓	Хязгаарлагдмал	✗	✓	✗
5	IT системийн мэдээлэл	✓	✗	✗	✓	✗
6	Хүний нөөцийн мэдээлэл	✓	✗	✗	✓ (техник)	✗

-0-