



МЭДЭЭЛЭЛ ХОЛБООНЫ СҮЛЖЭЭ ХХК

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН БОДЛОГО

Улаанбаатар хот

2025 он

Баримт бичгийн төрөл:	Бодлого
Баримт бичгийн төлөв:	
Ангилал:	Нийтэд нээлттэй
Баталсан огноо:	2025 он
Боловсруулсан газар:	Технологийн үйлчилгээний бизнесийн газар, Технологийн шинэ үйлчилгээний хэлтэс
Баталсан:	Гүйцэтгэх захирал
Баримт бичгийн хариуцагч:	Технологийн үйлчилгээний бизнесийн газар, Технологийн шинэ үйлчилгээний хэлтэс

Баримт, бичгийн хувилбарын түүх

Хувилбар	Сүүлд шинэчлэгдсэн огноо	Тайлбар	Өөрчлөлт оруулсан ажилтан	Баталсан
1.0	2025.01.25	Анхны хувилбар	Технологийн шинэ үйлчилгээний хэлтэс	

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН БОДЛОГО

АГУУЛГА

НИЙТЛЭГ ҮНДЭСЛЭЛ.....	4
УДИРДЛАГЫН МАНЛАЙЛАЛ.....	4
ҮЙЛ АЖИЛЛАГААНД ХЭРЭГЖҮҮЛЭХ БОДЛОГО	5
АЖИЛТНУУДЫН ХҮЛЭЭХ ҮҮРЭГ.....	5
ХҮРЭХ ҮР ДҮН.....	7
ХАРИУЦЛАГА.....	7

НЭГ. НИЙТЛЭГ ҮНДЭСЛЭЛ

1.1. Энэхүү баримт бичгийн зорилго нь “Мэдээлэл холбооны сүлжээ” ХХК (цаашид “Компани” гэх)-ийн үйл ажиллагаанд ашиглагдаж буй мэдээлэл, мэдээллийн систем, дэд бүтэц, эдгээрийн ашиглалт, хадгалалт, хамгаалалт, нууцлал, бүрэн бүтэн байдал, хүртээмжтэй байдал, тасралтгүй ажиллагаа болон хяналтыг хэрэгжүүлэхэд оршино.

1.2. Компани нь мэдээллийн аюулгүй байдлын үйл ажиллагаандаа Кибер аюулгүй байдлын тухай хууль, Төрийн болон албаны нууцын тухай хууль, Харилцаа холбооны тухай хууль, Тагнуулын байгууллагын тухай хууль, Байгууллагын нууцын тухай хууль, Нийтийн мэдээллийн ил тод байдлын тухай хууль, Хүний хувийн мэдээлэл хамгаалах тухай хууль, Цахим гарын үсгийн тухай хууль тогтоомж болон холбогдох журмууд, мэдээллийн аюулгүй байдлын менежмент удирдлагын тогтолцооны ISO/IEC 27001:2023 стандартын холбогдох шаардлагуудыг мөрдлөг болгон ажиллана.

1.3. Компани нь холбогдох байгууллагаас гаргасан хууль, дүрэм, журам, заавар, зөвлөмж, гэрээний үүрэг ба нөхцөл шаардлагыг бүрэн хангаж ажиллана.

1.4. Мэдээллийн аюулгүй байдлын бодлогын хэрэгжилт нь ажилтан, хүний нөөцийн аутсорсинг, оролцогч талууд, харилцагч, түнш, хэрэглэгч, компаниудад мөн хамаарах бөгөөд бодлогын талаарх ойлголтыг өгч, хамтран ажиллана.

1.5. Энэхүү бодлогыг хэрэгжүүлэхдээ холбогдох журам, аргачлалыг боловсруулан мөрдөж ажиллана.

1.6. Мэдээллийн аюулгүй байдлын бодлого нь нийтэд нээлттэй байна.

ХОЁР. УДИРДЛАГЫН МАНЛАЙЛАЛ

2.1. Компанийн Гүйцэтгэх удирдлага, захирлын зөвлөл нь мэдээллийн аюулгүй байдлын удирдлагын тогтолцоог хэрэгжүүлэхэд бүхий л талаар дэмжиж, үр дүнтэй байдлыг хангахад дараах алхамуудыг авч хэрэгжүүлнэ. Үүнд:

2.1.1. мэдээллийн аюулгүй байдлын бодлого, зорилтуудыг компанийн бизнес төлөвлөгөө, нөхцөл байдалтай нийцүүлж боловсруулж, батлуулна;

2.1.2. мэдээллийн аюулгүй байдал, мэдээллийн аюулгүй байдлын менежментийн тогтолцоог хэрэгжүүлэхдээ компанийн бизнесийн болон бусад процесстой уялдсан байна;

2.1.3. мэдээллийн аюулгүй байдал, мэдээллийн аюулгүй байдлын менежментийн тогтолцоог нэвтрүүлэх, хэрэгжүүлэх, тогтвортой байлгах, тасралтгүй сайжруулах үйл ажиллагааг дэмжиж, шаардагдах нөөцөөр тогтмол хангана;

2.1.4. мэдээллийн аюулгүй байдлыг хангах үйл ажиллагааг оновчтой зохион байгуулж, мэдээллийн аюулгүй байдал болон мэдээллийн аюулгүй байдлын менежментийн тогтолцооны шаардлагад нийцэх ач холбогдлын талаар тодорхой ойлголттой байна;

2.1.5. мэдээллийн аюулгүй байдлын менежментийн тогтолцоог төлөвлөсөн үр дүнд нь хүргэх талаар бүхий л арга хэмжээг авч удирдлагын тогтолцоог үр дүнтэй болгоход хувь нэмрээ оруулахыг бүх ажилтнуудад уриална;

2.1.6. компанийн мэдээллийн аюулгүй байдлын бодлого, зорилт, хяналт нь

газар, хэлтсийн дарга, ажилтан бүрийн үүрэг хариуцлага, гүйцэтгэлийн үнэлгээнд туссан байна.

ГУРАВ. ҮЙЛ АЖИЛЛАГААНД ХЭРЭГЖҮҮЛЭХ БОДЛОГО

3.1. Захирлын зөвлөл нь компанийн мэдээллийн аюулгүй байдлыг хангах үйл ажиллагааг удирдан чиглүүлэх зорилгоор дараах бодлогыг үйл ажиллагаандаа тусган хэрэгжүүлнэ. Үүнд:

3.1.1 компанийн мэдээллийн технологийн үйлчилгээ болон системийн үйл ажиллагаа, өөрийн хөгжүүлсэн программ хангамж, бүтээгдэхүүн, үйлчилгээгээр харилцагч, хамтран ажиллагч байгууллагуудын мэдээллийн нууцлал, бүрэн бүтэн байдлыг ханган ажиллана;

3.1.2 мэдээллийн аюулгүй байдлын учирч болзошгүй эрсдэлийг тодорхойлж, үнэлэлт дүгнэлт өгөх, эрсдэлээс урьдчилан сэргийлэх, бууруулах зорилгоор мэдээллийн аюулгүй байдлын эрсдэлийг удирдаж, байнгын сайжруулалтыг хангаж ажиллана;

3.1.3 мэдээллийн аюулгүй байдлын тухай холбогдох хууль, тогтоомж, стандарт, зохицуулагч байгууллагын шаардлага, харилцагчдын гэрээний шаардлага, оролцогч талуудын хэрэгцээнд нийцсэн үйл ажиллагааг эрхлэнэ;

3.1.4 мэдээллийн аюулгүй байдлыг хангахын тулд мэдээллийн аюулгүй байдлын удирдлагын тогтолцоог үр дүнтэй хэрэгжүүлж, урт хугацаанд тогтмол хянаж, сайжруулна.

3.2. Захирлын зөвлөл нь мэдээллийн аюулгүй байдлын бодлого, журамд тусгасан үйл ажиллагааг жил бүр хурлаар хэлэлцэж шаардлагатай шийдвэрийг цаг алдалгүй, түргэн шуурхай, оновчтой шийдвэрлэж ажиллана.

3.3. Захирлын зөвлөл нь мэдээллийн аюулгүй байдлын зорилтыг энэ бодлогод нийцүүлэн газар, нэгж бүрээр дэвшүүлж, хэрэгжилтийг тогтмол хугацаанд хянаж, үнэлж, үнэлгээнд тулгуурлан сайжруулалтыг хийнэ.

ДӨРӨВ. АЖИЛТНУУДЫН ХҮЛЭЭХ ҮҮРЭГ

4.1. Компанийн нийт ажилтнууд нь мэдээллийн аюулгүй байдлын удирдлагын тогтолцоог нэвтрүүлэх, хэрэгжүүлэх, сайжруулах зорилго бүхий үндсэн чиг үүргийг дараах хуваарийн дагуу хариуцна. Үүнд:

№	Үүрэг	Хариуцагч
1.	Компанийн нөхцөл байдлыг тодорхойлох, стратеги, чиглэлийг тогтоох, мэдээллийн аюулгүй байдлын бодлого боловсруулах, удирдлагын дүн шинжилгээний хурал хийх	<ul style="list-style-type: none">• Гүйцэтгэх захирал• Захиргаа удирдлагын газар• ДСАГазар• ТШҮХ• Мэдээллийн аюулгүй байдлын эрсдэлийн удирдлагын баг

2.	Мэдээллийн аюулгүй байдал, мэдээллийн аюулгүй байдлын менежментийн тогтолцооны зорилго, зорилт, төлөвлөгөөг боловсруулах	<ul style="list-style-type: none"> • ЗУГазар, ТШҮХ, ДСАГазар • Мэдээллийн аюулгүй байдлын эрсдэлийн удирдлагын баг • Мэдээллийн аюулгүй байдлын мэргэжилтэн
3.	Мэдээллийн аюулгүй байдал, мэдээллийн аюулгүй байдлын менежментийн тогтолцооны баримт бичгийн удирдлага	<ul style="list-style-type: none"> • Мэдээллийн аюулгүй байдлын мэргэжилтэн • Мэдээллийн аюулгүй байдлын эрсдэлийн удирдлагын баг
4.	Нийт ажилтнуудад Мэдээллийн аюулгүй байдлын сургалт болон мэдлэг ойлголт олгох	<ul style="list-style-type: none"> • Мэдээллийн аюулгүй байдлын мэргэжилтэн • Мэдээллийн аюулгүй байдлын эрсдэлийн удирдлагын баг • Сургалтын алба
5.	Мэдээллийн аюулгүй байдал, мэдээллийн аюулгүй байдлын менежментийн тогтолцооны дотоод аудит	<ul style="list-style-type: none"> • Дотоод хяналтын мэргэжилтэн • Эрсдэлийн мэргэжилтэн • Эрсдэлийн удирдлагын баг • Мэдээллийн аюулгүй байдлын дотоод хяналт, шалгалтын баг
6.	Залруулах болон урьдчилан сэргийлэх үйл ажиллагаа	<ul style="list-style-type: none"> • Мэдээллийн аюулгүй байдлын мэргэжилтэн • Эрсдэлийн мэргэжилтэн • Дотоод хяналтын мэргэжилтэн • Нийт ажилтнууд
7.	Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээ, эрсдэл бууруулах төлөвлөгөө	<ul style="list-style-type: none"> • Эрсдэлийн мэргэжилтэн • Мэдээллийн аюулгүй байдлын мэргэжилтэн • Мэдээллийн аюулгүй байдлын эрсдэлийн удирдлагын баг
8.	<ul style="list-style-type: none"> - Мэдээллийн аюулгүй байдлын менежментийн тогтолцооны эрх зүйн баримт бичгийг бусад стандарт, хууль тогтоомжид нийцүүлэх - Хууль тогтоомж, зохицуулагч байгууллагын шаардлагад нийцэх 	<ul style="list-style-type: none"> • ЗУГазар,ТШҮХ • Хуулийн хэлтэс • Мэдээллийн аюулгүй байдлын мэргэжилтэн • Эрсдэлийн мэргэжилтэн
9.	Мэдээллийн аюулгүй байдлын менежментийн тогтолцоог хэрэгжүүлэх, хянах, сайжруулах	<ul style="list-style-type: none"> • Нийт ажилтнууд • Мэдээллийн аюулгүй байдлын мэргэжилтэн • Эрсдэлийн мэргэжилтэн • Мэдээллийн аюулгүй байдлын эрсдэлийн удирдлагын баг • Цахим үйл ажиллагааны хэлтэс

10.	Өөрчлөлтийг төлөвлөх, гүйцэтгэх үед мэдээллийн аюулгүй байдал болон мэдээллийн аюулгүй байдлын менежментийн тогтолцоонд нийцүүлэх	<ul style="list-style-type: none"> • ЗУГазар, ТШҮХ • Мэдээлэл, технологийн мэргэжилтнүүд
11.	Мэдээллийн аюулгүй байдлын менежментийн тогтолцоонд хөндлөнгийн хяналт, шалгалтыг зохион байгуулах	<ul style="list-style-type: none"> • Мэдээллийн аюулгүй байдлын дотоод хяналт, шалгалтын баг
12.	Компанийн мэдээллийн хөрөнгийг зохих ёсоор хамгаалах, мэдээллийг зохих түвшинд хүлээн авахад анхаарах	<ul style="list-style-type: none"> • Нийт ажилтнууд
13.	Хүний нөөцийн аюулгүй байдал	<ul style="list-style-type: none"> • Захиргаа удирдлагын газар
14.	Тоног төхөөрөмж, бодит орчны аюулгүй байдал	<ul style="list-style-type: none"> • Мэдээлэл, технологийн мэргэжилтнүүд
15.	<ul style="list-style-type: none"> - Харилцаа холбоо, үйл ажиллагааны удирдлага - Мэдээлэл солилцох, дамжуулах аюулгүй байдал - Сүлжээний аюулгүй байдал, хандах эрхийн удирдлага - Мэдээллийн аюулгүй байдлын удирдлага - Бизнесийн тасралтгүй байдлын төлөвлөгөө 	<ul style="list-style-type: none"> • ЗУГазар, ТШҮХ • Мэдээлэл технологийн мэргэжилтнүүд • Стратеги төлөвлөлтийн газар
16.	Программ хангамж хөгжүүлэх, хүлээлгэн өгөх, хэвийн ажиллагааг хангах	<ul style="list-style-type: none"> • Мэдээлэл технологийн мэргэжилтнүүд • ДСАГ, Программ хөгжүүлэгч
17.	Гэрээ, хэлэлцээрийн хүлээсэн шаардлагад нийцэх	<ul style="list-style-type: none"> • ЗУГазар, Хуулийн хэлтэс

ТАВ. ХҮРЭХ ҮР ДҮН

5.1. Мэдээллийн аюулгүй байдал алдагдахаас урьдчилан сэргийлэх тогтолцоог бүрдүүлж ажиллана.

5.2. Мэдээллийн аюулгүй байдлын тогтолцоог эрсдэлд суурилсан хэлбэрээр үнэлэх ажиллагаа хэвшсэн байна.

5.3. Мэдээллийн аюулгүй байдлын эрсдэл буурсан байна.

5.4. Мэдээллийн аюулгүй байдал, мэдээллийн аюулгүй байдлын менежментийн тогтолцоог тогтмол хангаж, тасралтгүй сайжруулан ажилладаг болно.

ЗУРГАА. ХАРИУЦЛАГА

6.1. Энэхүү бодлого, түүний хүрээнд боловсруулсан журмыг зөрчсөн ажилтанд

холбогдох хууль тогтоомж, хөдөлмөрийн дотоод журам, хөдөлмөрийн гэрээнд заасан хариуцлага хүлээлгэнэ.

6.2. Энэхүү бодлогын хэрэгжилтэд компанийн Хуулийн хэлтэс, Технологийн үйлчилгээний бизнесийн газрын Технологийн шинэ үйлчилгээний хэлтэс, дотоод хяналтын мэргэжилтэн нар хяналт тавьж ажиллана.

МЭДЭЭЛЭЛ ХОЛБООНЫ СҮЛЖЭЭ ХХК