

Монголын хөрөнгийн бирж "ХК-ийн Гүйцэтгэх захирлын
2023 оны 11 дүгээр сарын 22-ны өдрийн
А/288 дугаар тушаалын хавсралт



МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН БОДЛОГО

Улаанбаатар хот
2023 он

Хувилбар № 1.0

Хэрэглэгч: Нийт ажилтнууд

Мэдээллийн аюулгүй байдлын бодлого

Баримт бичгийн төрөл:	Бодлого
Баримт бичгийн төлөв:	
Ангилал:	Нийтэд нээлттэй
Баталсан огноо:	2023.11.22
Боловсруулсан ажилтан:	Захиргаа, санхүүгийн газрын захиргааны албаны ахлах мэри эжилтэн
Баталсан:	Гүйцэтгэх захирал
Баримт бичгийн хариуцагч:	Үйл ажиллагааны газар, Мэдээлэл технологийн алба, Мэдээллийн аюулгүй байдлын мэргэжилтэн

Баримт, бичгийн хувилбарын түүх

Хувилбар	Сүүлд шинэчлэгдсэн огноо	Тайлбар	Өөрчлөлт оруулсан ажилтан	Баталсан
1.0	2023.11.22	Анхны хувилбар	ЗСГ-ын ЗА-ны ахлах мэргэжилтэн	A/288

Мэдээллийн аюулгүй байдлын бодлого

АГУУЛГА

НИЙТЛЭГ ҮНДЭСЛЭЛ.....	4
УДИРДЛАГЫН МАНЛАЙЛАЛ.....	4
ҮЙЛ АЖИЛЛАГААНД ХЭРЭГЖҮҮЛЭХ БОДЛОГО.....	4
АЖИЛТНУУДЫН ХҮЛЭЭХ ҮҮРЭГ.....	5
ХҮРЭХ ҮР ДҮН.....	6
ХАРИУЦЛАГА.....	7

НЭГ. НИЙТЛЭГ ҮНДЭСЛЭЛ

1.1. “Монголын хөрөнгийн бирж” ХК (цаашид “Компани” гэх)-ийн үйл ажиллагаанд ашиглагдаж буй мэдээлэл, мэдээллийн систем, дэд бүтэц, тэдгээрийн ашиглалт, хадгалалт, хамгаалалт, нууцлал, бүрэн бүтэн байдал, хүртээмжтэй байдал, тасралтгүй ажиллагаа, хяналтыг хэрэгжүүлэхэд энэ бодлогын зорилго оршино.

1.2. Компани нь мэдээллийн аюулгүй байдлын үйл ажиллагаандаа Олон улсын мэдээллийн аюулгүй байдлын удирдлагын тогтолцооны ISO 27001:2022 стандартын холбогдох шаардлагууд болон Монгол Улсын хууль, тогтоомж, дүрэм, журмыг мөрдлөг болгон ажиллана.

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

1.4. Мэдээллийн аюулгүй байдлын бодлогын хэрэгжилт нь ажилтан, аутсорсингийн нөөц, оролцогч талууд, харилцагч, түнш, арилжааны систем хэрэглэгч, гишүүн 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 байдлын менежментийн тогтолцоо (цаашид “МАБМТ-гэх)-г хэрэгжүүлэхдээ компанийн бизнесийн болон бусад процесстой уялдсан байна.

2.1.3. МАБМТ-г 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, МАБМТ-ны шаардлагад нийцэх ач холбогдлын талаар тодорхой ойлголттой байна.

2.1.5. МАБМТ-г 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 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 арилжааны систем, өөрийн хөгжүүлсэн программ хангамж, бүтээгдэхүүн, үйлчилгээгээр харилцагч, гишүүн, хамтран ажиллагч байгууллагуудын мэдээллийн нууцлал, хүртээмжтэй болон 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.

Мэдээллийн аюулгүй байдлын бодлого

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 МАБМТ-г нэвтрүүлэх, хэрэгжүүлэх, сайжруулах зорилго бүхий үндсэн чиг үүргийг дараах хуваарийн дагуу хариуцна. Үүнд:

Үүрэг	Гол хариуцагч
Компанийн нөхцөл байдлыг тодорхойлох, стратеги, чиглэлийг тогтоох, мэдээллийн аюулгүй байдлын бодлого боловсруулах, удирдлагын дүн шинжилгээний хурал хийх.	<ul style="list-style-type: none">Гүйцэтгэх захиралЗахирлын зөвлөлМэдээллийн аюулгүй байдлын эрсдэлийн удирдлагын баг
МАБМТ-ны зорилго, зорилт, төлөвлөгөөг боловсруулах	<ul style="list-style-type: none">Мэдээллийн аюулгүй байдлын эрсдэлийн удирдлагын багМэдээллийн аюулгүй байдлын мэргэжилтэн
МАБМТ-ны баримт бичгийн удирдлага	<ul style="list-style-type: none">Мэдээллийн аюулгүй байдлын мэргэжилтэнМэдээллийн аюулгүй байдлын эрсдэлийн удирдлагын баг
Нийт ажилтнуудад МАБ-ын сургалт болон мэдлэг ойлголт олгох.	<ul style="list-style-type: none">Мэдээллийн аюулгүй байдлын мэргэжилтэнМэдээллийн аюулгүй байдлын эрсдэлийн удирдлагын баг
МАБМТ-ны дотоод аудит	<ul style="list-style-type: none">Дотоод хяналтын мэргэжилтэнЭрсдэлийн мэргэжилтэнЭрсдэлийн удирдлагын багМэдээллийн аюулгүй байдлын дотоод хяналт, шалгалтын баг
Залруулах болон урьдчилан сэргийлэх үйл ажиллагаа	<ul style="list-style-type: none">Мэдээллийн аюулгүй байдлын мэргэжилтэнЭрсдэлийн мэргэжилтэнДотоод хяналтын мэргэжилтэнНийт ажилтнууд
МАБ-ын эрсдэлийн үнэлгээ, эрсдэл бууруулах төлөвлөгөө	<ul style="list-style-type: none">Эрсдэлийн мэргэжилтэнМэдээллийн аюулгүй байдлын мэргэжилтэнМэдээллийн аюулгүй байдлын эрсдэлийн удирдлагын баг

Мэдээллийн аюулгүй байдлын бодлого

<ul style="list-style-type: none"> • МАБМТ-г бусад стандарт, хууль тогтоомжид нийцүүлэх • Хууль тогтоомж, зохицуулагч байгууллагын шаардлагад нийцэх 	<ul style="list-style-type: none"> • Мэдээлэл технологийн алба • Хуулийн алба • Мэдээллийн аюулгүй байдлын мэргэжилтэн • Эрсдэлийн мэргэжилтэн
МАБМТ-г хэрэгжүүлэх, хянах, сайжруулах	<ul style="list-style-type: none"> • Нийт ажилтнууд • Мэдээллийн аюулгүй байдлын мэргэжилтэн • Эрсдэлийн мэргэжилтэн • Мэдээллийн аюулгүй байдлын эрсдэлийн удирдлагын баг • Мэдээлэл, технологийн алба
Өөрчлөлтийг төлөвлөх, гүйцэтгэх үед МАБМТ-г нийцүүлэх	<ul style="list-style-type: none"> • Мэдээлэл, технологийн алба
МАБМТ-нд хөндлөнгийн хяналт, шалгалтыг зохион байгуулах	<ul style="list-style-type: none"> • Мэдээллийн аюулгүй байдлын дотоод хяналт, шалгалтын баг
Компанийн мэдээллийн хөрөнгийг зохих ёсоор хамгаалах, мэдээллийг зохих түвшинд хүлээн авахад анхаарах	<ul style="list-style-type: none"> • Нийт ажилтнууд
Хүний нөөцийн аюулгүй байдал	<ul style="list-style-type: none"> • Захиргаа, санхүүгийн газар
Тоног төхөөрөмж, бодит орчны аюулгүй байдал	<ul style="list-style-type: none"> • Мэдээлэл, технологийн алба
<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"> • Үйл ажиллагааны газар • Мэдээлэл технологийн алба • Бизнес хөгжлийн газар
Программ хангамж хөгжүүлэх, хүлээлгэн өгөх, хэвийн ажиллагааг хангах	<ul style="list-style-type: none"> • Мэдээлэл технологийн алба • Программ хөгжүүлэгч
<ul style="list-style-type: none"> • Гэрээ, хэлэлцээр хүлээсэн шаардлагад нийцэх 	<ul style="list-style-type: none"> • Хуулийн алба

ТАВ. ХҮРЭХ ҮР ДҮН

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

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

5.3. Мэдээллийн аюулгүй байдлын эрсдэл буурсан байна.

5.4. МАБМТ-г 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 журмын хэрэгжилтэд компанийн Мэдээлэл технологийн алба, дотоод хяналтын мэргэжилтэн хяналт тавьж ажиллана.