Хувьцаа эзэмшигчдийн хурлын
2023 оны 09 сарын 29-ны өдрийн 08/23 тоот
тогтоолын Нэгдүгээр хавсралт

НОМИН	НОМИН Карт ББСБ ХХК		Иш татсан заалт: ISO/IEC 27001:2022 5.2 **Нууцын зэрэг: Нийтэд нээлттэй**
МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН БОДЛОГО		Хувилбар: 1	

ЭХ ХУВЬ	ХУУЛБАР ХУВЬ	ХҮЧИНГҮЙ ХУВЬ
	Хувилалт №.....	

БАРИМТ БИЧГИЙН ТҮҮХ

Хувилбар	Товч утга	Батлагдсан огноо, тушаалын дугаар	Мөрдөж эхлэх огноо
Хувилбар 1	“Номин Карт ББСБ” ХХК-д мэдээллийн аюулгүй байдлын менежментийн тогтолцоог хэрэгжүүлэхэд чиглэсэн зорилго, зорилтуудыг тодорхойлох, тэдгээрт чиглэсэн мэдээллийн аюулгүй байдлыг хангах төлөвлөгөөг боловсруулах, батлуулах, хэрэгжүүлэх, мэдээллийн аюулгүй байдлыг хангахтай холбоотой хэмжүүр үзүүлэлтүүдийг бий болгож, ашиглагдаж буй систем, сүлжээ, программ хангамж, тоног төхөөрөмжүүдийн тасралтгүй ажиллагааг хангах, халдлагаас урьдчилан сэргийлэх, түүнийг таслан зогсоох, мэдээлэл болон хөрөнгийн нууцлагдсан байдал, бүрэн бүтэн байдал, хүртээмжтэй байдлыг хангах, шаардлагатай тохиолдолд бусдаар гүйцэтгүүлэх, сонирхогч талуудын мэдээллийн аюулгүй байдлын талаарх мэдлэгийг дээшлүүлэх зорилготой.		

ХОЛБОГДОХ БАРИМТ БИЧГҮҮД

д/д	Баримт бичгийн дугаар	Нэр
1.	COBIT 2019	Мэдээллийн аюулгүй байдлын засаглал, удирдлагын тогтолцоо
2.	ISO/IEC 27001: 2022	Мэдээллийн аюулгүй байдлын менежментийн тогтолцоо
3.	УАБ/1/06	Мэдээллийн аюулгүй байдлын бодлого
4.	ISACA	Мэдээллийн хөрөнгийн бүртгэл

5.	COBIT 2019, APO13.01.1	МТ-ийн баримт бичгийн жагсаалт
6.	ISO/IEC 27003	МАБМТ-ны гарын авлага
7.	№ 01/324	Мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээний аргачлал
8.	ISO 37301:2021	Нийцлийн менежментийн тогтолцоо
9.	MNS ISO 37301:2022,	Нийцлийн менежментийн тогтолцоо — Шаардлага ба хэрэгжүүлэх арга зүйн заавар
10.	Монгол Улсын хууль	Байгууллагын нууцын тухай хууль
11.	Монгол Улсын хууль	Хүний хувийн мэдээлэл хамгаалах тухай хууль
12.	Монгол Улсын хууль	Нийтийн мэдээллийн ил тод байдлын тухай хууль
13.	Монгол Улсын хууль	Хэрэглэгчийн эрх ашгийг хамгаалах тухай хууль
14.	Байгууллагын дотоод хэм хэмжээнүүд / хэрэгжилтэд холбогдох, хүчинтэй үйлчлэл бүхий хэм хэмжээнүүд хамаарна./	Нэгдэл компанид хүчин төгөлдөр мөрдөгдөж буй бусад бодлого, журмууд

ГАРЧИГ

Агуулга Хуудас

НЭГ. НИЙТЛЭГ ҮНДЭСЛЭЛ

1.1. Зорилго. Энэхүү бодлогын баримт бичгийн зорилго нь Мэдээллийн аюулгүй байдлын менежментийн тогтолцоо */цаашид МАБМТ гэх/* -ны хамрах хүрээг тодорхойлсон баримт бичигт заасан нэгжүүдийн мэдээллийн хөрөнгө болон бизнес процессууд, үндсэн болон дэмжих үйл ажиллагаанд мэдээллийн аюулгүй байдлын менежментийн тогтолцоог олон улсын зохих стандартын дагуу бий болгох, хэрэгжүүлэх, хэвшүүлэх, тасралтгүй сайжруулах, тэдгээрт хамаарах үйл ажиллагаанд баримтлах чиглэлийг тодорхойлоход оршино.

1.2. Хамрах хүрээ. “Номин Карт ББСБ” ХХК-ийн */цаашид “Байгууллага” гэх/* Мэдээллийн аюулгүй байдлын бодлогын хамрах хүрээ нь байгууллагын МАБМТ-ны хамрах хүрээг тодорхойлсон баримт бичигт заасны дагуу тодорхойлогдоно. Энэхүү бодлогыг байгууллагын Хувьцаа эзэмшигчид, Удирдлагын багийн гишүүд, Нийт ажилтнууд, Харилцагч зэрэг бүхий л оролцогч талууд өдөр тутамдаа мөрдлөг болгоно.

1.3. Харьяалах салбар, нэгж. Энэхүү бодлогыг хариуцах этгээд буюу хэрэгжилтийг шууд зохион байгуулах этгээд нь Мэдээллийн аюулгүй байдал хариуцсан нэгж */цаашид МАБ хариуцсан нэгж гэх/* байна.

1.4. Гүйцэтгэлийг тооцох үнэлгээ

№	Гүйцэтгэлийн хэмжүүр	Хэмжих аргачлал KPI	Өгөгдлийн эх үүсвэр	Давтамж
1.	МАБ-ын эрсдэлүүдийг тодорхойлох, тодорхойлсон эрсдэлүүдэд зохих хяналтуудыг хэрэгжүүлэх	Хэрэгжүүлж байгаа хяналтын тоо / Нийт хэрэгжүүлэх шаардлагатай хяналтын тоо * 100%	Хяналтуудын хэрэгжилтийн тайлан	Жилд нэг удаа
2.	ISO 27001 стандартын дагуу Мэдээллийн аюулгүй байдлын менежментийн тогтолцоог хэрэгжүүлэх бодлого, журмуудыг боловсруулах, сайжруулах, тэдгээрийн хэрэгжилтийг хангах	Бодлого, журмуудын KPI дундаж үзүүлэлт / Нийт журмын тоо * 100%	Бодлого, журмуудын хэрэгжилтийн үнэлгээний тайлан	Жилд нэг удаа
3.	Компанийн нийт ажилчдад МАБ-ын мэдлэг, ойлголтыг эзэмшүүлэх, соёлыг төлөвшүүлэх	Сургалтын дараах шалгалтын нийт дүн / нийт сургалтад хамрагдсан хүний тоо * 100%	Сургалтуудын үр дүнгийн нэгдсэн тайлан	Жилд нэг удаа
4.	ISO 27001 стандартын хөндлөнгийн аудит хийлгэж, гэрчилгээ авах, сунгах	ISO 27001нэвтрүүлэх төлөвлөгөөний хийгдсэн ажил / ISO 27001 нэвтрүүлэх төлөвлөгөөний нийт ажил * 100%	Гэрчилгээ	Жилд нэг удаа
5.	ISO 27001 стандартын хэрэгжилт	Стандартын хангасан шаардлага / хангах ёстой шаардлага * 100	Төлөвлөгөө	Жилд нэг удаа

ХОЁР. НЭР ТОМЬЁОНЫ ТОДОРХОЙЛОЛТ

2.1. Энэхүү бодлогын баримт бичигт хэрэглэсэн дараах нэр томьёог дор дурдсан утгаар ойлгоно. Үүнд:

2.1.1. “Мэдээллийн технологийн удирдлага, үйл ажиллагааны нэгж”- гэж мэдээллийн технологийн үйл ажиллагаа явуулж буй нэгжийг /МТС, МТГ гэх зэрэг/;

2.1.2. “МАБМТ-ын хамрах хүрээний нийцлийн баримт бичиг”-гэж ISO27001 стандартын дагуу Компанийн онцлогтой уялдуулан хяналтуудыг тодорхойлон тогтмол хөтлөх барим бичгийг;

2.1.3. “МАБ”- гэж Мэдээллийн аюулгүй байдлыг, мэдээллийн нууцлагдсан байдал, бүрэн бүтэн, хүртээмжтэй байдал баталгаатай хангагдсан байхыг;

2.1.4. “МТ”- гэж мэдээллийн технологийг;

2.1.5. "КОБИТ-2019"-гэж мэдээллийн технологийн засаглал удирдлагын стандартуудыг нэгтгэсэн зөвлөмж бүхий тогтолцоог;

2.1.6. "МАБ хариуцсан нэгж"- гэж МАБ-ын бодлогыг тодорхойлох, үйл ажиллагааг үнэлэх, зөвлөмж гаргах нэгжийг /МТ-ийн эрсдэлийн удирдлагын хэлтэс, ДСДУХ гэх зэрэг/

2.1.7. "Эрсдэлийн удирдлага хариуцсан нэгж"- гэж Эрсдэлийн удирдлагыг хэрэгжүүлж буй хэлтсийг тус тус ойлгоно.

2.2. Энэхүү бодлогын баримт бичигт хэрэглэсэн дараах товчлол болон оноосон нэрийг дор дурдсан утгаар ойлгоно. Үүнд:

2.2.1. "МАБМТ"- гэж мэдээллийн аюулгүй байдлын менежментийн тогтолцоог, байгууллагын мэдээллийн аюулгүй байдлыг хангах зорилгоор хоорондоо уялдаа, хамааралтайгаар хэрэгжүүлэх бодлого, журам, стандарт, заавар, тэдгээрт хамаарах процесс, үйл ажиллагаа, холбогдох зохион байгуулалтын бүтэц, нөөцийн нэгдмэл цогц системийн нэршлийг;

2.2.2. "ISO27003"-гэж мэдээллийн аюулгүй байдлын менежментийн тогтолцоо болон холбогдох аюулгүй байдлын зөвлөмж, хяналтыг хэрэгжүүлэх ОУ-ын стандартыг;

2.2.3. "ОУ" гэж олон улс гэх холбоо үгний товчлолыг.

ГУРАВ. ЕРӨНХИЙ ЗАРЧИМ

3.1. Байгууллагын хэмжээнд МАБМТ-г бий болгох, хэрэгжүүлэх, хэвшүүлэх, тэдгээрт холбогдох үйл ажиллагаанд дараах зарчмыг мөрдлөг болгоно. Үүнд:

3.1.1. Байгууллагын хэмжээнд МАБМТ-г олон улсын ISO 27001 стандартад заасан шаардлагуудын хүрээнд бий болгож, хэрэгжүүлэх, хэвшүүлэх;

3.1.2. Байгууллагад МАБМТ-г бий болгох, хэрэгжүүлэх, хэвшүүлэх болон холбогдох бусад үйл ажиллагаа нь байгууллагын бизнесийн стратеги, зорилго, зорилтуудтай уялдсан, тэдгээрийг дэмжихэд чиглэсэн байх;

3.1.3. Байгууллагын МАБ-ыг хангах үйл ажиллагаа нь эрсдэлийн удирдлагад суурилсан байх;

3.1.4. Байгууллагын МАБ-ыг хангах үйл ажиллагаа нь Олон Улсын болон Монгол Улсын холбогдох стандартын нөхцөл, шаардлага, Монгол Улсын холбогдох хууль тогтоомж, зохицуулагч байгууллагуудын шаардлагуудтай нийцсэн байх;

3.1.5. МАБМТ-г бий болгож, хэрэгжүүлэх, хэвшүүлэхэд дэвшилтэт техник, технологи, хэрэгсэл, программ хангамжийг ашиглах, бусдаар гүйцэтгүүлэх;

3.1.6. МАБ бодлого, түүний зорилтууд, тэдгээрийн өөрчлөлт, мэдээллийн аюулгүй байдлын эрсдэлийн талаарх зохих түвшний мэдээллийг холбогдох оролцогч талуудад давтамжит хугацаанд тогтмол танилцуулж, мэдэгдэх арга хэмжээг хэрэгжүүлэх;

3.1.7. Байгууллагын хэмжээнд МАБМТ-г бий болгох, хэрэгжүүлэх, тасралтгүй сайжруулахад нийт ажилтнуудын оролцоог хангах.

ДӨРӨВ. МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН БОДЛОГЫН ЗОРИЛТУУД

4.1. Энэхүү бодлогын зорилгод хүрэхийн тулд дараах зорилтуудыг дэвшүүлэн хэрэгжүүлнэ. Үүнд:

Нэгдүгээр зорилт:

МАБ -ын эрсдэлийг мэдээллийн хөрөнгөд суурилан тодорхойлох, тодорхойлсон эрсдэлүүдэд зохих хяналтуудыг хэрэгжүүлэх (*Эрсдэлийн удирдлагын COSO*

тогтолцооны зарим, COBIT-2019 тогтолцооны арга аргачлалыг ашиглана);

Хоёрдугаар зорилт:

ISO 27001/2022 стандартын дагуу Мэдээллийн аюулгүй байдлын менежментийн тогтолцоог хэрэгжүүлэх журмуудыг боловсруулах, сайжруулах, тэдгээрийн хэрэгжилтийг хангах;ISO 27001/2022 стандартын хэрэгжилтэд хөндлөнгийн үнэлгээ хийлгэж, гэрчилгээ авах.

Гуравдугаар зорилт:

Компанийн нийт ажилчдад МАБ-ын мэдлэг, ойлголтыг эзэмшүүлэх, соёлыг төлөвшүүлэх, хяналт мониторинг тасралтгүй сайжруулалтаар хангах.

ТАВ. МАБМТ-НЫ ЭЛЕМЕНТҮҮД, ТЭДГЭЭРТ БАРИМТЛАХ БОДЛОГО

5.1. Мэдээллийн аюулгүй байдлын бодлого

5.1.1. "Номин Карт ББСБ" ХХК нь Санхүүгийн цогц, шинэлэг үйлчилгээгээрээ зах зээлд танигдсан насан туршийн санхүүгийн хөтөч байх эрхэм зорилгын хүрээнд мэдээллийн хөрөнгийн нууцлал, хүртээмж, бүрэн бүтэн байдлыг хангаж байгууллагад МАБМТ-г бий болгох, хэрэгжүүлэх, хэвшүүлэх ба түүний хэрэгжилтийг хянаж удирдан зохион байгуулна.

5.1.2. МАБМТ-ны аливаа үйл ажиллагаа төлөвлөгөөг хэрэгжүүлэх, өөрчлөх, эхлүүлэхдээ цар хүрээнээс хамаарч бизнесийн болон мэдээллийн аюулгүй байдлын эрсдэлийг хамгийн бага байлгах үүднээс холбогдох стандарт, хууль дүрэм, зохицуулалтыг дагаж мөрдөж, холбогдох удирдлагаас зөвшөөрөл авна.

5.1.3. МАБ-ын хэрэгжилтийн хяналтын зардал нь хүлээгдэж буй үр ашгаас хэтрэхгүй байхаар төлөвлөж МАБМТ-г тасралтгүй сайжруулж ажиллана.

5.2. Мэдээллийн аюулгүй байдлын бодлогын болон бусад баримт бичиг

5.2.1. Энэхүү бодлогын баримт бичиг нь Байгууллагын МАБ-ын зорилго, зорилтууд, баримтлах чиглэлийг тодорхойлсон суурь баримт бичиг болно.

5.2.2. МАБ-ыг хангахтай холбоотой шаардлагатай бусад бодлого, журам, стандартууд, хөтөлбөр, төлөвлөгөөг энэхүү бодлогын баримт бичигтэй уялдуулан, зохих олон улсын стандартад тавигдсан шаардлагуудтай нийцүүлэн боловсруулж, хэрэгжүүлнэ;

5.3. МАБ-ын төлөвлөгөө

5.3.1. МАБМТ-г хэрэгжүүлэх зорилгоор дараах гурван МАБ-ын төлөвлөгөөг МАБ хариуцсан нэгж боловсруулж, холбогдох дээд удирдлагаар батлуулж хэрэгжилтийг хангуулна:

i. Стратегийн төлөвлөгөө - 10-15 жил;
ii. Тактикийн төлөвлөгөө 3-5 жил;
iii. Үйл ажиллагааны төлөвлөгөө - Жил бүр.

5.3.2. Дээрх төлөвлөгөөнүүдэд МАБ-ын тодорхойлсон зорилтуудад хүрэх төлөвлөгөөг багтаасан байна.

ЗУРГАА. ХЯНАЛТ, ТАЙЛАГНАЛ

6.1 МАБ-ын бодлогын баримт бичгийн хэрэгжилтийг хянах үйл ажиллагааг явуулахдаа энэхүү бодлогын хүрээнд боловсруулсан төлөвлөгөөний биелэлт, холбогдох журмуудыг ашиглана.

6.2 Энэхүү бодлогын баримт бичгийн 5.1-д заасан хяналтыг МАБ хариуцсан нэгжийн шууд удирдлага, дээд удирдлага, гүйцэтгэх захирал нь холбогдох мэдээлэл, тайланг ашиглан жилд нэг удаа зохистой байдлыг хянана.Энэхүү бодлогын баримт бичгийн хэрэгжилтэд МАБ хариуцсан нэгж хяналт тавьж нийцтэй байдлыг жилдээ нэг удаа шалгаж, бизнесийн үйл ажиллагаанд мэдэгдэхүйц өөрчлөлт гарах эсвэл аюулгүй байдалтай холбоотой эрсдэл гарах үед түүний тогтвортой байдал, хангалттай, үр дүнтэй байдлыг хангах гэх мэт шаардлагатай тохиолдолд холбогдох өөрчлөлтийг оруулж батлуулна.

ДОЛОО. ХАРИУЦЛАГА

7.1 Энэхүү бодлогын баримт бичгийг зохих ёсоор дагаж мөрдөөгүйн улмаас Байгууллагад хохирол, эрсдэл учирсан бол холбогдох буруутай удирдах албан тушаалтан,ажилтнуудыг захиргааны болон эрүүгийн хариуцлага хүлээлгэсэн эсэхээс үл хамааран Хөдөлмөрийн гэрээ, Эд хөрөнгийн бүрэн хариуцлагын гэрээ, Хөдөлмөрийн дотоод журам болон бусад холбогдох дүрэм, журамд заасны дагуу хариуцлага хүлээлгэнэ.

7.2 Ажилтан хэрэглэгчийн эрхээ хувийн ашиг сонирхолдоо нийцүүлэн зүй бусаар ашигласан, бусдад дамжуулсан, хэрэглүүлсэн, өөр ажилтны хэрэглэгчийн эрхийг ашигласан нь гэмт хэргийн болон зөрчлийн шинжтэй бол холбогдох хууль хяналтын байгууллагад мэдэгдэж шалгуулна.

---------- oOo ----------