ДОТООДОД

BID BUSINESS INVEST DEVELOPMENT

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН БОДЛОГО

Улаанбаатар
2023 он

Хамрах хүрээ: БИД ББСБ	Хариуцах эзэн: МАБХороо
Хүчинтэй хугацаа: 2023.12.06-ий өдрөөс эхэлнэ.	Хуудасны тоо: 6
Журмын дугаар:12/06/01	Хувилбар: Хувилбар 2- Эх хувь
Хянасан: Үйл ажиллагаа эрхэлсэн захирал А.Баясгалан	Баталсан: Гүйцэтгэх захирал Ц.Бат-Эрдэнэ

№	Хувилбар	Өөрчлөлт хийгдсэн огноо	Өөрчлөлтийн агуулга	Өөрчлөлт
1	Хувилбар 1	2023/05/01	Анхны хувилбар	
2	Хувилбар 2	2023/12/06	Агуулгын өөрчлөлт оруулсан	А. Баясгалан О. Оюусондор
3				

Агуулга

1. ЗОРИЛГО

1.1 Энэхүү бодлогын зорилго нь БИД ББСБ-ын стратегийн зорилго зорилттой нийцсэн, тэдгээрийн харилцагчийн мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмжтэй байдал, бизнесийн үйл ажиллагааны тасралтгүй байдлыг хангах, мэдээллийн аюулгүй байдалд учирч болох эрсдэлээс урьдчилан сэргийлэх хяналтын тогтолцоог бий болгох арга замаар мэдээллийн аюулгүй байдлыг удирдахад оршино.

1.2 Мэдээллийн аюулгүй байдлын бодлого нь Монгол улсын үндэсний аюулгүй байдлын үзэл баримтлал, Байгууллага нууцын тухай хууль, Кибер аюулгүй байдлын тухай хууль, Нийтийн мэдээллийн ил тод байдлын тухай хууль, Хувь хүний нууцын тухай хууль, Хүний хувийн мэдээлэл хамгаалах тухай хууль, Цахим гарын үсгийн тухай хууль, Мэдээллийн аюулгүй байдлын ISO 27001:2022 стандартад нийцсэн байна.

1.3 Биет болон биет бус мэдээллүүд эдгээртэй ажиллаж байгаа бүх ажилтан, харилцагч байгууллагууд энэхүү бодлогын баримт бичгийг дагаж мөрдөнө.

2. НЭР ТОМЬЁОНЫ ТАЙЛБАР

БИД	Бизнес Инвест Девелопмент
ББСБ	Банк бус санхүүгийн байгууллага
МАБМТ	Мэдээллийн аюулгүй байдлын менежментийн тогтолцоо
МАБ	Мэдээллийн аюулгүй байдал
ISO 27001:2022	Мэдээллийн аюулгүй байдлын олон улсын стандарт /2022 оны/
ТУЗ	Төлөөлөн удирдах зөвлөл
МАБМТ	Мэдээллийн аюулгүй байдлын менежментийн тогтолцоо

3. ХАМААРАЛТАЙ БИЧИГ БАРИМТУУД

3.1 Компьютер, техник хэрэгсэлтэй ажиллах журам
3.2 Цахим аюулгүй ажиллагааны журам
3.3 Хамрах хүрээний бичиг баримт
3.4 Хэрэглэх тухай мэдэгдэл

5.2 ХАРИЛЦАА

5.2.1 Энэхүү бодлого нь МАБМТ-ны хамрах хүрээний бүхий л оролцогч талуудтай хэзээ хэрхэн холбогдохыг тодорхойлсон байна.

5.2.2 Мэдээлэл, мэдээллийн систем, дэд бүтэц, программ хангамж, мэдээллийн сүлжээ, түүнчлэн мэдээлэл боловсруулах аппликэйшн, хадгалах өгөгдлийн сан зэрэгт нууцлал, бүрэн бүтэн болон хүртээмжтэй байдалд учирч болзошгүй эрсдэлийг тодорхойлох зорилгоор эрсдэлийн үнэлгээг тогтмол хугацаанд хийнэ.

5.2.3 Мэдээллийн аюулгүй байдлын зөрчил гарах /мэдээлэл задруулах, халдлагад өртөх, луйвар гарах, гэнэтийн осол, давагдашгүй хүчин зүйлс тохиолдох/ үед үр дүнтэй арга хэмжээ авч ажиллах богоод тайлагналын механизмыг хэрэгжүүлж, ирээдүйд дахин давтагдахаас сэргийлж үндсэн шалтгаанд суурилсан дүн шинжилгээ хийдэг байна.

5.2.4 Ханган нийлүүлэгчид болон бусад сонирхогч талуудад шаардлагатай үед МАБМТ-ны баримт бичгийг хүртээмжтэй байлгана.

5.2.5 Энэхүү бодлогын бичиг баримтад Эрсдэлийн хорооны саналд үндэслэн Гүйцэтгэх зөвлөлөөр хэлэлцэж, ТУЗ батална.

6. МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ЗАСАГЛАЛЫН ПРОЦЕСС

6.1 Мэдээллийн аюулгүй байдлын засаглалын үндсэн дөрвөн процесс болон удирдлагын багийн үүрэг хариуцлагыг тодорхойлсон.

Процесс 1: Үнэлэх процесс нь одоогоор хэрэгжүүлж буй үйл ажиллагаа, төлөвлөгдсөн өөрчлөлтүүд дээр үндэслэн одоогийн болон хүрэхийг зорьж буй зорилтуудад ямар зохицуулалт хийх шаардлагатайг тодорхойлдог засаглалын процесс юм.

Процесс 2: Чиглүүлэх процесс нь байгууллагын стратеги зорилтуудын тухай чиглэлийг өгдөг засаглалын процесс юм. Тухайн чиглүүлэгт байгууллагын нөөцүүдийн хуваарилалт, үйл ажиллагааны тэргүүлэх чиглэл, эрсдэлийн хүлээн зөвшөөрөгдөх түвшин, эрсдэлийн удирдлагын төлөвлөгөө багтана.

Процесс 3: Байнгын хяналт процесс нь байгууллагын стратегийн зорилтуудаа хүрэхийг үнэлэх боломжийг олгодог засаглалын процесс юм.

Процесс 4: Харилцаа процесс нь удирдах байгууллага болон сонирхогч талууд өөрсдийн хэрэгцээнд тохирсон мэдээлэл солилцдог хоёр талын засаглалын үйл явц юм.

7. НИЙЦЭЛ

7.1 ХЭМЖИЛТ

7.1.1 Байгууллага нь дотоод, гадаад аудитаар, бизнесийн бусад тайлан үзүүлэлтээр удирдлагын багт өгч буй санал хүсэлт гэх мэт олон төрлийн арга замаар энэхүү бодлогод нийцэж буйг шалгана.

7.1.2 Байгууллагын үйл ажиллагаа нь мэдээллийн технологийн систем, дэд бүтцийн нууцлал, мэдээллийн аюулгүй байдлын эрсдэлийг олж илрүүлэх, үнэлэх, эрсдэлээс хамгаалах, эрсдэлийг буруулах ажиллагааг энэхүү бодлогын хүрээнд нийцүүлж ажиллаж байгаа эсэхэд дотоод аудит хяналт тавин шалгана.

7.1.3 7.1.2 заалтад дурдсан хяналт шалгалтыг тохирол, үл тохирол, сайжруулах гэсэн аргачлалаар дүгнэнэ.

7.1.4 Байгууллагын мэдээллийн аюулгүй байдлын бүхий л үйл ажиллагаа нь Монгол улсын үндэсний аюулгүй байдлын үзэл баримтлал, Байгууллага нууцын тухай хууль, Кибер аюулгүй байдлын тухай хууль, Нийтийн мэдээллийн ил тод байдлын тухай хууль, Хувь хүний нууцын тухай хууль, Хүний хувийн мэдээлэл хамгаалах тухай хууль, Цахим гарын үсгийн тухай хууль, Мэдээллийн аюулгүй байдлын ISO 27001:2022 стандартад нийцсэн хүрээнд зохицуулагдана.

7.1.5 Байгууллагын мэдээллийн аюулгүй байдлын бүхий л үйл ажиллагаа нь зохицуулагч байгууллагын шаардлагад нийцүүлэн ажиллах ба байгууллагын бусад бодлоготой уялдсан байна.

7.2 ХАСАХ ТОХИОЛДОЛ

7.2.1 Оролцогч талтай зайлшгүй хамтын ажиллагааг өрнүүлэх тохиолдолд Мэдээллийн аюулгүй байдлын хорооноос зөвшөөрөл авч хамтын ажиллагааг эхлүүлж болно.

7.3 ЗӨРЧИЛ

7.3.1 Энэхүү бодлогын 7.2-т зааснаас бусдаар бодлого зөрчсөн, сонирхогч талуудад эсрэг хуурамч мэдээлэл өгөх, эрх мэдлээ хэтрүүлэх, мэдээллийн нууцыг санаатай болон санаандгүй задруулсан, хувийн ашиг сонирхлоор асуудалд хандсан зэргээр ББСБ-д шууд болон шууд бус хохирол учруулсан ажилтныг ажлаас халах хүртэл арга хэмжээ авах ба шаардлагатай гэж үзвэл хууль хяналтын байгууллагад асуудлыг тавьж шийдвэрлүүлнэ.

7.3.2 Энэхүү бодлогыг зөрчсөн нь тогтоогдвол байгууллагын ажилтнуудад сахилгын шийтгэл ноогдуулж, ажлаас нь халах хүртэл арга хэмжээ авах үндэслэл болно.