Микро Кредит ББСБ ХХК-ийн Хувьцаа эзэмшигчдийн

хурлын 2023 оны 05 сарын 19-ны өдрийн

23/16 тоот тогтоолын Хавсралт №4 -р батлав.

“МИКРО КРЕДИТ ББСБ” ХХК-ИЙН МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ЖУРАМ

Улаанбаатар хот
2023 он

микро кредит Банк бус Санхүүгийн Байгууллага	**Мэдээллийн аюулгүй байдлын журам** **Нууцын зэрэг** **Дотоод**	**Боловсруулсан:** ..... **Хянасан:** .....

БАРИМТ БИЧГИЙН ӨӨРЧЛӨЛТИЙН БҮРТГЭЛ

№	БАТАЛСАН ОГНОО	ӨӨРЧЛӨЛТ ОРСОН ЗААЛТУУД	ТОГТООЛЫН ДУГААР
1	2023-05-19	v.1 шинэ хувилбар	23/16

АГУУЛГА

НЭГ. ЗОРИЛГО, ХАМРАХ ХҮРЭЭ, ХЭРЭГЛЭГЧИД

1. Энэхүү баримт бичгийн зорилго нь мэдээллийн аюулгүй байдлын бодлогын хүрээнд мэдээллийн аюулгүй байдалтай холбогдон үүсэх хяналт, харилцаа, ажилтан байгууллагын систем, сүлжээнд хандах зэрэг үйл ажиллагааг зохицуулахад оршино.

Энэхүү бодлогын баримт бичиг нь байгууллагын бүх төрлийн үйл ажиллагаа, түүний мэдээлэл, мэдээллийн системийг ашиглаж байгаа нийт ажилтнуудад хамааралтай.

ХОЁР. ХОЛБОГДОХ БАРИМТ БИЧИГ

2. Үүнд:

- Баримт бичиг боловсруулах заавар
- Мэдээллийн аюулгүй байдлын бодлого
- Хөдөлмөрийн дотоод журам
- Дотоод аудит журам
- Зээлийн үйл ажиллагааны журам
- Бусад холбогдох бодлого, дүрэм, журам

ГУРАВ. МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН МЕНЕЖМЕНТИЙН ТОГТОЛЦООНИЙ ХЭРЭГЖИЛТТЭЙ ХОЛБОГДОН ҮҮСЭХ УДИРДЛАГЫН ХЯНАЛТ

3. Гүйцэтгэх захирал нь тогтмол хугацаанд Мэдээллийн аюулгүй байдлын менежментийн тогтолцоо нь компанийн стратегийн чиглэлтэй нийцэж байгаа байдал, сайжруулах боломж, өөрчлөлт хийх хэрэгцээ, шаардлагыг тогтоох зорилгоор “Удирдлагын дүн шинжилгээ”-ний хурлыг удирдлагын багаар жил бүр хийж, тэмдэглэл, гарсан шийдвэрийг баримтжуулан хадгална. Хурлаас гарсан зүйлсийг ТУЗ-ын хуралд танилцуулан ажиллана.

3.1. Удирдлагын дүн шинжилгээний хурлаар дараах асуудлуудыг хэлэлцэж шийдвэрлэнэ:

3.1.1 Өмнөх хурлаас өгөгдсөн үүрэг, даалгаврын биелэлт;
3.1.2 Гадаад, дотоод хүчин зүйлсийн өөрчлөлт;
3.1.3 Сонирхогч талуудын хэрэгцээ, шаардлагын өөрчлөлт;
3.1.4 Эрсдэлийн үнэлгээний тайлан, бууруулах төлөвлөгөө;
3.1.5 Үл тохирлууд, залруулах ажиллагааны талаар;
3.1.6 Хэмжилт, мониторингийн үр дүнгүүд;
3.1.7 Дотоод, гадаад аудитын үр дүн, тайлан;
3.1.8 МАБМэдээллийн аюулгүй байдлын зорилтуудын биелэлт;

3.1.9 Мэдээллийн аюулгүй байдлын менежментийн тогтолцоог -г сайжруулах боломжууд;

3.2 Компани нь удирдлагын дүн шинжилгээний үр дүнг үндэслэж өөрийн Мэдээллийн аюулгүй байдлын менежментийн тогтолцоо ны зохистой, хүрэлцээтэй, үр нөлөөтэй байдлыг тасралтгүй дээшлүүлэхийг зорин ажиллана. Компанийн албан тушаалтнууд нь мэдээллийн аюулгүй байдлын удирдлагын тогтолцоог бий болгох, хэрэгжүүлэх, сайжруулах зорилго бүхий үндсэн чиг үүргүүдийг дараах хуваарийн дагуу хариуцна.

Үүрэг хариуцлага	**Гол хариуцагч**	**Хяналт**
Компанийн нөхцөл байдлыг тодорхойлох, стратеги, чиглэлийг тогтоох, мэдээллийн аюулгүй байдлын бодлого боловсруулах, удирдлагын дүн шинжилгээ хийх.	Гүйцэтгэх захирал	Хувьцаа эзэмшигч
- Мэдээллийн аюулгүй байдлын менежментийн тогтолцооны зорилго, зорилт, төлөвлөгөөг боловсруулах	Гүйцэтгэх захирал Мэдээллийн аюулгүй байдал хариуцсан ажилтан /МАБ/	Гүйцэтгэх захирал
Мэдээллийн аюулгүй байдлын менежментийн тогтолцооны - баримт бичгийн удирдлага	МАБ хариуцсан ажилтан	Гүйцэтгэх захирал
Мэдээллийн аюулгүй байдлын менежментийн тогтолцооны - бүртгэлийн удирдлага	МАБ хариуцсан ажилтан	Гүйцэтгэх захирал
Нийт ажилтнууд болон мэргэжилтнүүдийн Мэдээлэл аюулгүй байдлын сургалт, мэдлэг ойлголт.	МАБ хариуцсан ажилтан	Гүйцэтгэх захирал

Мэдээллийн аюулгүй байдлын менежментийн тогтолцооны дотоод аудит	МАБМТ дотоод аудитор	Гүйцэтгэх захирал
Залруулах болон урьдчилан сэргийлэх ажиллагаа	МАБ хариуцсан ажилтан	Гүйцэтгэх захирал
Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээ, эрсдэл бууруулах төлөвлөгөө	МАБ хариуцсан ажилтан Эрсдэлийн эзэн	Гүйцэтгэх захирал
Мэдээллийн аюулгүй байдлын менежментийн тогтолцоог бусад стандарт, хууль тогтоомжид нийцүүлэх	МАБ хариуцсан ажилтан	Гүйцэтгэх захирал
Мэдээллийн аюулгүй байдлын менежментийн тогтолцоог хэрэгжүүлэх, хянах, сайжруулах	МАБ хариуцсан ажилтан	Гүйцэтгэх захирал
Өөрчлөлтийг төлөвлөх, гүйцэтгэх үед Мэдээллийн аюулгүй байдлын менежментийн тогтолцоог -г нийцүүлэх	МАБ хариуцсан ажилтан	Гүйцэтгэх захирал
Мэдээллийн аюулгүй байдлын менежментийн тогтолцоо -нд хөндлөнгийн хяналт, шалгалтыг зохион байгуулах	МАБ хариуцсан ажилтан МАБМТ дотоод аудитор	Гүйцэтгэх захирал
Компанийн мэдээллийн өмч хөрөнгийг зохих ёсоор хамгаалах, мэдээллийг зохих түвшинд хүлээн авахад анхаарах	МАБ хариуцсан ажилтан	Гүйцэтгэх захирал
Хүний нөөцийн аюулгүй байдал	Хүний нөөцийн ажилтан	Гүйцэтгэх захирал

Тоног төхөөрөмж, бодит орчны аюулгүй байдал	МАБ хариуцсан ажилтан	Гүйцэтгэх захирал
Харилцаа холбоо, үйл ажиллагааны удирдлага Мэдээлэл солилцох, дамжуулах аюулгүй байдал Сүлжээний аюулгүй байдал, хандах эрхийн удирдлага Мэдээллийн аюулгүй байдлын будилааны удирдлага Бизнесийн тасралтгүй байдлын төлөвлөгөө	МАБ хариуцсан ажилтан	Гүйцэтгэх захирал
Программ хангамж, систем захиалах, хөгжүүлэх, хүлээж авч, хэвийн ажиллагааг хангах	Мэдээллийн технологийн ажилтан эсвэл Мэдээллийн аюулгүй байдлын ажилтан	Гүйцэтгэх захирал
Хууль тогтоомж, зохицуулагч байгууллагын шаардлагад нийцэх Гэрээ, хэлцлээр хүлээсэн шаардлагад нийцэх	Гүйцэтгэх захирал	Гүйцэтгэх захирал

3.3 Компанийн бусад дээд болон дунд шатын албан тушаалтан, зээлийн ажилтан, Мэдээлэл аюулгүй байдлын бодлого, дүрэм журмыг үйл ажиллагаандаа мөрдөх, ажилтнууддаа таниулж, мэдээлэх үүрэгтэй

ДӨРӨВ. ӨӨРЧЛӨЛТИЙН УДИРДЛАГА

4.1 Компани нь өөрийн Мэдээллийн аюулгүй байдлын менежментийн тогтолцоо - нд нөлөөлж болох аливаа өөрчлөлтийг төлөвлөж гүйцэтгэх ба төлөвлөөгүй, гэнэтийн өөрчлөлтийн үр дагавар, нөлөөллийг үнэлж баримтжуулна.

4.2 Компанийн хэмжээний дараах өөрчлөлтүүдийг үүсэж болох үр дагаврыг төлөвлөж, зохих хяналтыг тавих үүднээс удирдана. Үүнд:
- 4.2.1 Компанийн удирдлага, бүтэц, зохион байгуулалт,
- 4.2.2 Үүрэг хариуцлага, эрх мэдэл,
- 4.2.3 Нэгээс илүү бүтцийн нэгж дамнасан үйл ажиллагаа (процессууд)
- 4.2.4 Үйл ажиллагааны үндсэн зарчим, хяналтын бүтэц,
- 4.2.5 Ажлын байрны орчин, нөхцөл, байрлал ба хүрээлэн буй орчин,
- 4.2.6 Дэд бүтэц, тоног төхөөрөмж, систем, програм хангамж,
- 4.2.7 Ажиллах хүчин буюу хүний нөөц ихээр өөрчлөгдөх,
- 4.2.8 Хууль тогтоомжийн шаардлага ба сонирхогч талуудын шаардлага, технологийн гэх мэт гадаад орчны өөрчлөлтөөс үүдэн бий болох өөрчлөлт,
- 4.2.9 Бүтээгдэхүүн, үйлчилгээний чиглэл өөрчлөгдөх,
- 4.2.10 Шинэ бүтээгдэхүүн үйлчилгээ нэмэгдэх,
- 4.2.11 Мэдээлэл аюулгүй байдлын бодлого өөрчлөгдөх, шинэчлэгдэх,
- 4.2.12 Бусад,

4.3 Өөрчлөлт хийх, оруулах саналыг компанийн ажилтан болон ажил үйлчилгээ үзүүлэгч, хамтран ажиллагч талын эрх бүхий этгээд гаргаж болно (цаашид Хүсэлт гаргагч гэнэ).

4.4 Хүсэлт гаргагч нь Өөрчлөлтийн хүсэлтийг шийдвэрлэх этгээдэд бичгээр эсвэл цахимаар хүргэнэ.

4.5 Өөрчлөлтийн хүсэлт нь дараах мэдээллийг агуулсан байна.
- 4.5.1 Өөрчлөлтийн товч мэдээлэл
- 4.5.2 Өөрчлөлт хийж эхлэх болон дуусах хугацаа
- 4.5.3 Хамрагдах үйл ажиллагаа, систем, хэрэглэгчийн тухай
- 4.5.4 Хүсэлт гаргагч, түүний удирдлагын зөвшөөрөл
- 4.5.5 Бусад шаардлагатай хавсралтууд

4.6 Хүсэлтийг шийдвэрлэх этгээд нь дээрх мэдээлэл дээр тулгуурлан зохих мэргэжилтнүүдтэй зөвлөлдөж өөрчлөлтийг хийх эсэхийг шийдвэрлэнэ.

4.7 Шийдвэр гаргасан тухай тэмдэглэлийг тухай бүр хөтөлж, баримтжуулан хадгална.

4.8 Системийн гэмтэл саатал болон бусад яаралтай шалтгаанаар удирдлагын зөвшөөрөлгүйгээр хийгдсэн өөрчлөлтийг дараагийн ажлын өдөрт багтаан мэдэгдэж, үр дагаврыг хэлэлцэнэ.

4.9 Өөрчлөлтийг хийж дууссаны дараа Хүсэлт гаргагч нь дараах мэдээлэл бүхий тайланг бэлтгэж удирдлага болон хүсэлтийг шийдвэрлэсэн этгээдэд танилцуулна. Үүнд:
- 4.9.1 Өөрчлөлтийн зорилгын биелэлтийн хувь;
- 4.9.2 Өөрчлөлт төлөвлөлтийн дагуу хийгдсэн эсэх;
- 4.9.3 Өөрчлөлтийн үр дүнд бий болсон эерэг, сөрөг нөлөө;
- 4.9.4 Цаашид анхаарах сургамжууд;
- 4.9.5 Бусад шаардлагатай мэдээлэл.

4.10 Мэдээллийн аюулгүй байдлын менежментийн тогтолцооны хүрээнд өөрчлөлтийн бүртгэлийг Мэдээллийн аюулгүй байдал хариуцсан ажилтан бүртгэн хадгална.

ТАВ. ХАНДАЛТ, НЭВТРЭЛТ ЗОХИЦУУЛАЛТ

5.1 Хандах эрх зохицуулах үед дараах зарчмуудыг баримтална. Үүнд:

5.1.1 Ажилтны ажлын чиг үүргийн хүрээнд хандах шаардлагатайгаас бусад буюу зөвшөөрөгдөөгүй мэдээлэл, мэдээллийн системд хандах эрх олгохгүй байх;

5.1.2 Ажилтны ажлын чиг үүргийн хүрээнд хандах шаардлагатайгаас давуу эрх олгохгүй байх /зайлшгүй шаардлагаас бусад тохиолдолд/;

5.1.3 Хандах эрх хүсэгч, баталгаажуулагч, зөвшөөрөгч, олгогч ажилтнуудын ажил үүрэг тусдаа байх;

5.1.4 Хандах эрх зохицуулах, хэрэглэх үйл явц нь "Зөвшөөрөгдсөнөөс бусад хэрэглээ, нэвтрэлт, хандалт хориотой" байх;

5.2 Компанийн мэдээлэл, мэдээллийн системүүдэд хандах нэвтрэлт, хандалтыг зохицуулах үйл ажиллагаа нь уг мэдээллийн өмч хөрөнгийн эзэмшигч, хариуцагч, хандах эрхтэй хэрэглэгч гэсэн талуудын гурван талт харилцаан дээр тулгуурлан явагдана.

5.3 Хэрэглэгч нь дараах үүргийг хүлээнэ. Үүнд:

5.3.1 Хэрэглэгч нь ажлын шаардлагаар аливаа мэдээлэл, мэдээллийн системийг ашиглах хүсэлтээ мэдээлэл эзэмшигчид албан и-мэйлээр илгээнэ. Үүнд дараах мэдээллийг дурдана:

a. Мэдээлэл, мэдээллийн системийн нэр, хамрах модуль
b. Шаардлага
c. Хандах хугацаа

5.3.2 Хэрэглэгч нь хандах эрхийн мэдээллээ удирдахдаа энэхүү баримт бичгийн 6-р бүлэгт заасны дагуу аюулгүй байдлыг ханган ажиллана.

5.3.3 Хэрэглэгч нь өөрт олгогдсон хандах эрхээ зөвхөн энэхүү журмын 5.3.1-д дурдсан хүсэлтэд тодорхойлсон зориулалтын дагуу ашиглана.

5.3.4 Хууль, хяналт, аудитын байгууллага гэх мэт аливаа этгээдийн зүгээс ирүүлсэн хандах эрхийн мэдээлэл задруулах шаардлагыг өөрийн шууд удирдлагад мэдэгдэнэ. Энэ тохиолдолд удирдлага нь 5.3.6 заалтыг баримтлан шийдвэр гаргана.

5.3.5 Ажлын зайлшгүй шаардлагаар аливаа албан тушаалтныг орлон ажиллах үед түүний хандах эрхийн мэдээллийг шууд удирдлагын зөвшөөрлөөр орлон ажиллаж байгаа ажилтанд ашиглуулж болно. Энэ тохиолдолд нууц үгийг шинэчлэн ашиглах үүрэгтэй.

5.3.6 5.3.5-д зааснаас бусад тохиолдолд хандах эрхийн мэдээллийг бусдад задруулахыг хатуу хориглоно.

5.3.7 Хэрэглэгч нь алдагдсан байж болзошгүй хандах эрхийн мэдээллээ нэн даруй өөрчлөх үүрэгтэй.

5.3.8 Нууц мэдээллийг анх файл болон цаасан хуулбар хэлбэрээр авсан хэрэглэгч хэрэглэх хүсэлтийн хугацаа дуусмагц мэдээллийг өөрийн төхөөрөмж дээрээс болон цаас хувь устган үр дүнг шууд удирдлагад тайлагнана.

5.4 Хэрэглэгчийн хандах эрхийн хүсэлтийг дараах байдлаар шийдвэрлэнэ.

5.4.1 Хэрэглэгч нь хандах эрхийн хүсэлтээ энэхүү журмын 5.3.1-д заасны дагуу мэдээлэл эзэмшигчид илгээнэ.

5.4.2 Мэдээлэл, мэдээллийн систем эзэмшигч нь тухайн хүсэлт гаргасан хэрэглэгчийн гүйцэтгэж буй ажил үүрэгтэй хамааралтай болоод хандах эрхийн хүсэлтэд бичигдсэн мэдээллүүд үнэн зөв, бүрэн болохыг хянасны дараа энэхүү журмын 5.1-д дурдагдсан зарчмууд дээр үндэслэн хүсэлтийг сайтар судалж мэдээлэл, мэдээллийн системд хандах эрхийг зөвшөөрөх эсэх шийдвэр гаргана. Зөвшөөрсөн, эс зөвшөөрсөн эсэх шийдвэрийг хариуцагчид илгээнэ.

5.4.3 Хариуцагчид зөвшөөрөгдсөн хүсэлтийг илгээхдээ зарим нэг хэсэг, талбарыг нуух гэх мэтээр шаардлагагүй мэдээллийг аль болох багасгаж өгөх зааварчилгаа хамт илгээж болно.

5.4.4 Хариуцагч нь зөвшөөрөгдсөн хүсэлтийн мэдээлэл, мэдээллийн системд хандах эрхийг хүсэлтэд заасан нээх хугацаанд олгоно.

5.5 Хариуцагч нь хандах эрхийн хүсэлтэд заасан дуусах хугацаанд хандах эрхийг цуцлах үйлдлийг гүйцэтгэнэ.

5.6 Хандах эрх хүсэгч нь байгууллагатай хамтран ажиллагч байгууллагын ажилтан байх тохиолдолд хандах эрхийн хүсэлтийг хамтран ажиллаж байгаа ажилтан гаргана.

5.7 Шинэ ажилтанд байгууллагуудын и-мэйл хаягийг олгохдоо Гүйцэтгэх захиралын тушаалаар олгоно.

5.8 Шинэ ажилтанд байгууллагын нийтлэг системд хандах эрх олгохдоо холбогдох удирдлага нь хандах эрх олгох хүсэлтийг и-мэйлээр хариуцагчид шууд илгээнэ.

5.9 Давуу эрхтэй хэрэглэгчийн эрхийг олгохдоо ажлын чиг үүрэгт үндэслэн аль болох цөөн тооны ажилтанд, аль болох богино хугацаагаар олгоно.

5.10 Мэдээллийн системийн хяналтаас давсан давуу эрхт програм ашиглах тохиолдолд МАБ хариуцсан ажилтнаас зөвшөөрөл авсан байна.

5.11 Хандах эрх0 хүсэгч нь байгууллагын нууц мэдээлэл, мэдээллийн системд хандах тохиолдолд “Нууц хадгалах гэрээ”-г хугацаагүйгээр байгуулсан байна.

5.12 Ажил үүрэг өөрчлөгдсөн ажилтны мэдээлэл, мэдээллийн системд хандах эрхийг өөрчлөхдөө өмнө байсан эрхийг бүрэн устган, шинээр эрх олгох зарчмыг баримтална.

5.13 Хандах эрхийн хугацаа дууссан даруйд хариуцагч хэрэглэгчийн хандах эрхийг цуцална.

5.14 Хандах эрх цуцлах хугацаанаас өмнө хэрэглэгчдийн хөдөлмөрийн гэрээ, ажлын хэлцэл дууссан тохиолдолд хэрэглэгчийн шууд удирдлага ажил үүргийн шинэчлэлт, шаардлагаас хамааран хандах эрх цуцлах хүсэлтийг хариуцагчид илгээнэ.

5.15 Мэдээлэл, мэдээллийн системийн аливаа хандах эрхийн хүсэлтийг олгосон эзэмшигч нь өөрийн хүлээн авсан хүсэлтүүдийн бүртгэлийг Хагас жилд нэг удаа тухайн ажилтны ажил үүргийн бодит шаардлагатай нь тулган шүүж шаардлагагүй хандалтуудыг цуцлах буюу устгуулах хүсэлтийг хариуцагчид илгээнэ.

5.16 Хариуцагч нь өөрийн хариуцаж буй мэдээлэл, мэдээллийн системд хандах эрхийн зөвшөөрөл олгосон хүсэлт болон хандах эрх олгосон, цуцалсан бүртгэлийг улирал тутамд тухайн систем дээрх хандах эрхүүдтэй тулган хяналт тавьж, хандах эрхэд зохих өөрчлөлтийг оруулна.

5.17 Давуу эрхтэй хэрэглэгчийн хандах эрхүүдийн хувьд 5.14, 5.15-д заасан үйлдлийг харьцангуй ойрхон давтамжтай хийх нь зүйтэй.

5.18 Хандах эрхийн мэдээллийн аюулгүй байдал:

5.18.1 Ажилтан бүр байгууллагын мэдээллийн системд хандах давхардахгүй хэрэглэгчийн нэр эсвэл кодтой байна. Тухайн ажилтан шинээр ажилд орохоор тушаал гармагц тухайн системийн хариуцагч бүртгэн, хэрэглэгчийн нэр, бусад мэдээллийг үүсгэнэ.

5.18.2 Үйл ажиллагаанд ашиглаж буй бүх систем нууц үгийн шаардлагыг хангадаг байна.

5.18.3 Байгууллагын мэдээллийн системд хандах нууц үг, нэвтрэх мэдээлэл нь хэрэглэгчийг адилтгах, шалгах үндсэн хэрэгсэл болдог бөгөөд шивж оруулах, боловсруулалт хийх, хадгалах, дамжуулах явцад нууцлал нь бүрэн хамгаалагддаг байх шаардлагатай.

5.18.4 Хэрэглэгч өөрийн нэвтрэх мэдээллийн аюулгүй байдлыг хангахад дараах зарчмыг баримтална.

a. Бусадтай хуваалцахгүй байх /аман болоод бичгэн бүхий л хэлбэрээр/;
b. Аливаа систем, веб сервер болон цаасан дээр бичиж, тэмдэглэх, сануулах зэргээр хадгалахгүй байх /Жишээ нь: Веб браузер болон аппликешн-д сануулах, autofill тохиргоог идэвхжүүлэхгүй байх, цаасан дээр бичиж тэмдэглэхгүй байх/;
c. Password manage tool ашиглах тохиолдолд мастер түлхүүр/нууц үгийг ямар нэг байдлаар бичиж, хадгалахгүй байх;
d. Нууц үгээр түгжигдсэн файлын нууц үгийг эх файлыг дамжуулснаас бусад сувгаар дамжуулах;

5.18.5 Нууц үгэнд дараах нийтлэг шаардлага тавигдана. Үүнд:

a. Таахад хялбар нууц үгийг ашиглахгүй байх /Жишээ нь: Нэвтрэх нэр, өөрийн овог нэр, утас, төрсөн газар, зэрэг хувийн мэдээлэл агуулсан мөн толь бичигт байх энгийн үг хэллэг г.м/;
b. 10-аас доошгүй тэмдэгтэй, том, жижиг үсэг, тоо, тусгай тэмдэгт заавал орсон байх;
c. 180 хоног тутамд нууц үгийг шинэчилдэг байх;

5.18.6 Хандах эрхийн мэдээллийн аюулгүй байдалд дараах шаардлага тавигдана.

d. Аливаа мэдээллийн системд нэвтрэх үйлдэлд нууц үгийг ил харуулахгүй байх;
e. Системээс шинээр үүсгэгдсэн/ресет хийгдсэн/, систем эзэмшигч шинэчлэн оруулсан болон хэрэглэгчийн системд нэвтрэх анхны нууц үгийг эхний нэвтрэлтийн дараа солих тохиргоотойгоор тохируулах;
f. Нууц үгийг 5 удаа буруу оруулсан оролдлогын дараа дахин хандах эрхийг хязгаарладаг байх;
g. Тухайн системд идэвхтэй хэрэглээ хийхгүй 15 минут болоход холболтыг автоматаар салгадаг байх;
h. Давуу эрхтэй хэрэглэгч өөрийн хандах эрхийн мэдээллийг солих тухай бүр хэвлэн, дугтуйд хийж битүүмжлэн тухайн системийн эзэмшигчид өгч цоожтой шүүгээ, сейфэнд хадгалуулдаг байх. Систем эзэмшигч нь тухайн битүүмжилсэн мэдээллийг зөвхөн онцгой тохиолдолд ашиглаж болно;
i. Аливаа системийн хувьд хэрэглэгчийн сүүлийн 5 нууц үг дахин ашиглагдах боломжгүй байх;
j. Хэрэглэгчийн мэдээллийн системд хандаж орсон болон гарсан огноо, хугацаа, хийсэн үйлдлийн бүртгэлийг лог файлд бүртгэдэг байх;
k. Давуу эрхтэй хэрэглэгчийн бүртгэлийн логийг шууд удирдлага нь улирал бүр хянадаг байх;

5.18.7 Дээр дурдсан шаардлагуудыг аливаа мэдээллийн систем хөгжүүлэх болон худалдан авах үед дагаж мөрддөг байна

5.19 Зайнаас ажиллах үеийн мэдээллийн аюулгүй байдал

5.19.1 Компанийн дотоод сүлжээ, системд зайнаас хандахдаа шууд удирдлагын зөвшөөрлөөр, хандах эрх хүсэж, Мэдээллийн аюулгүй байдал хариуцсан ажилтанд бүртгэгдсэн зөөврийн тооцоолох төхөөрөмж болон IP холболтыг ашиглана .
5.19.2 Зайнаас хандахад ашиглах төхөөрөмжийн аюулгүй байдлын хяналтын програм болон сүлжээний галт ханыг идэвхжүүлсэн байна.
5.19.3 Компанийн дотоод сүлжээнд зайнаас хандах эрхээ бусдад ашиглуулахыг хориглоно.
5.19.4 Зайнаас хандахдаа өөрийн удирддаг буюу найдвартай, нууцлалыг хангасан сүлжээг хэрэглэнэ. Жишээ нь: Гэрийн сүлжээ, хамтран ажилладаг Компанийн сүлжээ г.м.

5.20 Үйлдлийн лог бүртгэл, хяналт

5.20.1 Компанийн бүхий л мэдээллийн системүүд нь дараах мэдээллийг агуулсан үйлдлийн бүртгэлийг бүртгэж, хадгалдаг байна.

a. Хэрэглэгчийн ID
b. Систем дээр хийгдсэн үйлдлүүд
c. Үйлдлийн огноо, цаг, минут, секунд
d. Үйл ажиллагааны үр дүн /амжилттай, амжилтгүй зэрэг/
e. Системийн тохиргоонд оруулсан өөрчлөлт
f. Давуу эрхийн нэвтрэлт, ашиглалт
g. Ашигласан файл, программ бусад хэрэгсэл
h. Хандсан файл болон хандалтын төрөл

5.20.2 Нийлүүлэгч талаас үйлдлийн бүртгэлийг хянах зохион байгуулалтын үед гэрээнд дээрх агуулгыг тусгадаг, хэрэгжилтийг хянадаг байна.

5.21 Шифрлэлтийн хяналтууд

5.21.1 Нууц мэдээллийг шифрлэж хадгална. Ингэхдээ дараах аргуудын аль нэгийг ашиглана.

Дискийг бүрэн шифрлэх

Файлыг шифрлэх

Програмыг шифрлэх

Өгөгдлийн санг шифрлэх

5.21.2 Шифрлэлтэд тавих шаардлага:

a. Тоон гарын үсэг ашиглахдаа итгэмжлэгдсэн гэрчилгээжүүлэх байгууллагаас /Монпасс г.м/ олгосон гарын үсгийг ашиглана.
b. Сүлжээний аюулгүй байдлыг хангахдаа TLS 1.2, 1.3 зэрэг хамгийн сүүлийн үеийн аюулгүй байдлын шалгалтаар баталгаажсан хувилбарыг ашиглана.

5.21.3 И-мэйлийн шаардлага:

a. Нууц мэдээлэл агуулсан хавсралт файлыг .zip эсвэл .zipx форматтайгаар шахах, ингэхдээ найдвартай нууц үгээр түгжин илгээнэ.
b. Нууц үгийг и-мэйлээс бусад сувгаар дамжуулна.

5.21.4 Шифрлэлтийн түлхүүр ашиглалт:

a. Түлхүүрүүдийг тэдний хамгаалж буй мэдээлэлтэй ижил буюу илүү түвшний нууцлалын аргыг ашиглан хамгаалсан байна.
b. Хамгаалагдаж буй мэдээлэл, өгөгдлийн сангийн эзэмшигч нь түлхүүрт хандах хандалтыг хянаж, хязгаарлана.
c. Түлхүүрийг шифрлэгдсэн өгөгдөлтэй ижил төхөөрөмж, хадгалах хэрэгсэлд хадгалахыг хориглоно.
d. Хамгаалагдаж буй мэдээлэл, өгөгдлийн сангийн эзэмшигч нь түлхүүрийг 1-2 тутамд шинэчилж байна.

5.21.5 Эдгээр шифрлэлтүүдийн хэрэгжилтийг хангахдаа холбогдох стандарт, дүрэм журамд нийцүүлэн хэрэглэдэг байна.

6 Будилааны үед авах арга хэмжээ

6.1 Компанийн ажилтан нь аливаа мэдээллийн системд үүссэн учрал тохиолдлыг Мэдээллийн аюулгүй байдал хариуцсан ажилтанд мэдэгдэнэ.

6.2 Үүссэн учрал тохиолыг Мэдээллийн аюулгүй байдал хариуцсан ажилтан нь шинжлэн будилаан мөн эсэхийг баталгаажуулж, будилаан биш тохиолдолд дотооддоо шийдвэрлэдэг байна.

6.3 Будилаан илэрсэн системийг шаардлагатай тохиолдолд систем эзэмшигчийн зөвшөөрөлтэйгөөр Компанийн сүлжээнээс тусгаарлах болон холболтыг хязгаарлах арга хэмжээг авна.

6.4 Мэдээллийн аюулгүй байдал хариуцсан ажилтан нь үүссэн будилаанд холбогдох нотлох баримтыг цуглуулж, шалтгааныг тогтоон, системийг цэвэрлэнэ. Нотлох баримт цуглуулахдаа дараах зарчмыг баримтлана.

6.4.1 Мэдээллийн аюулгүй байдал хариуцсан ажилтан нь аливаа зөрчил будилаан илэрсэн гэж тодорхойлсон үеэс эхлэн нотлох баримт цуглуулах, хадгалах, хамгаалах үйл ажиллагааг хэрэгжүүлнэ.

6.4.2 Нотлох баримтын аюулгүй байдлыг хангах зорилгоор шинжилгээний үр дүн гарах хүртэл будилаантай холбоотой хөрөнгийг тусгаарлах болон хандалтыг хянах арга хэмжээнүүдийг авч хэрэгжүүлнэ.

6.4.3 Удирдлагын зөвшөөрлөөр бусдад мэдээлэх шаардлага гарах хүртэл будилаантай холбоотой аливаа мэдээллийг нууцална.

6.4.4 Компанийн хэмжээнд сахилгын хариуцлага тооцох зорилгоор нотлох баримтыг цуглуулж, гаргаж өгөхдөө гүйцэтгэх захирлын шаардлагад үндэслэн холбогдох мэдээллийг хавсаргана.

6.4.5 Мэдээллийн аюулгүй байдлын будилааны дараа ямар нэг хүн, Компанийн эсрэг хууль зүйн нэхэмжлэл, гомдол (иргэний болон эрүүгийн) гаргах шаардлагатай бол зохих хууль тогтоомжийн дагуу цуглуулж хадгалсан нотлох баримтыг Компанийн хуульчийн зөвшөөрлөөр хавсаргаж өгч болно.

6.4.6 Хууль зүйн аливаа үйл ажиллагааг нотлох материалуудын хуулбар дээр тулгуурлан явуулна. Ингэхдээ бүх нотлох материалын бүрэн бүтэн, өөрчлөгдөөгүй байдлыг хамгаалсан байна.

6.5 Системийн хариуцагч нь Мэдээллийн аюулгүй байдал хариуцсан ажилтны зааварчилгааны дагуу системийг хэвийн ажиллагаанд оруулна.

6.6 Мэдээллийн аюулгүй байдал хариуцсан ажилтан нь үүссэн будилааны бүртгэлийг боловсруулан хадгална.

6.7 Тухайн будилаантай холбоотой үйл ажиллагааны сайжруулалтын санал хүсэлтийг удирдлагад тогтмол танилцуулж, шийдвэрлүүлдэг байна.

ЗУРГАА. БИЕТ БОЛОН ОРЧНЫ АЮУЛГҮЙ БАЙДАЛ

6.8 Компанийн эмзэг мэдээлэл, мэдээллийн өмч хөрөнгө байрлаж буй орон зайг хамгаалах зорилгоор Нууцын зэрэглэлтэй мэдээллийн, мэдээллийн

өмчийг боловсруулж, дамжуулж, хадгалж буй өрөө, тасалгааг зөвхөн эрх бүхий болон зөвшөөрөлтэй этгээд нэвтрэх боломжтой байхаар хамгаалсан байна.

6.9 Үйлчилгээ авах, үзүүлэх буюу зөвшөөрөлгүй этгээд нэвтрэх боломжтой байршлуудыг тодорхойлж, хяналтыг тогтоож, бусад өрөө тасалгаанаас тусгаарладаг байна.

6.10 7.1-д дурдсан өрөө тасалгааны биет хамгаалалт нь олон улсын болон үндэсний хууль, дүрэм журам, стандартад нийцсэн байх, аливаа гэмтэл саатлын үед саадгүй ажиллах функцээр хангагдсан байна.

6.11 7.1-д дурдсан өрөө тасалгаанд зөвшөөрөлгүй этгээд нэвтрэх тохиолдолд зочдын зорилго болон зөвшөөрлийг шалган баталгаажуулж, баримтжуулан нэвтрүүлдэг байна. Зочдын бүртгэлийг баримтжуулахдаа дараах мэдээллийг бүртгэж, хөтөлнө.

№	Огноо	Овог нэр	Утас	Уулзалт хийх ажилтан	Орсон цаг	Гарсан цаг

6.12 Шаардлагатай тохиолдолд гаднын үйлчилгээ үзүүлэгч Компанийн ажилтан нууцын зэрэглэлтэй өрөө тасалгаанд нэвтэрч болно. Ингэхдээ дээрх бүртгэлд мэдээллээ өгч, Компанийн зөвшөөрөл бүхий ажилтны хамт нэвтэрч тухайн ажилтны хяналт дор үйл ажиллагааг явуулна.

6.13 7.3 7.1-д дурдсан өрөө тасалгааны биет хамгаалалт нь олон улсын болон үндэсний хууль, дүрэм журам, стандартад нийцсэн байх, аливаа гэмтэл саатлын үед саадгүй ажиллах функцээр хангагдсан байна.

6.13.1 Эрүүл ахуй, аюулгүй ажиллагааны зохих стандарт, дүрмүүдийг Компанийн хэмжээнд хэрэгжүүлсэн байна;

6.13.2 Тэжээлийн үүсгүүр, рак зэрэг хэрэгслүүдийг ил зай талбайд байршуулахгүй байх, гаднын хүн ойртох боломжгүй газарт байрлуулна;

6.13.3 Аюултай буюу түргэн шатах материал бүхий эд зүйлсийг нууцын зэрэглэлтэй өрөө тасалгаанд хадгалахгүй байх.

6.14 Харуул хамгаалалтын үйл ажиллагааг 24 цагийн турш идэвхтэй байхаар зохион байгуулна.

6.15 Аюулгүй байдлын аливаа эрсдэлээс хамгаалан хяналтын камерыг нууцын зэрэглэлтэй өрөө, тасалгаа бүрд суурилуулсан байна. Шаардлагатай тохиолдолд хэд хэдийг буюу харагдах өнцөг тус бүрд тусгайлан байрлуулна.

ДОЛОО. ХУУЛЬ, ЭРХ ЗҮЙН ЗОХИЦУУЛАЛТ, НИЙЦЭЛ

7.1 Эзэмшигч нь мэдээллийн өмч хөрөнгө тус бүрээр холбогдох хууль эрх зүй, зохицуулалт, гэрээний үүрэг болон Компанийн бодлого, журмын шаардлагуудыг дэлгэрэнгүй тодорхойлж, баримтжуулан, шинэчилдэг байна.

7.2 Оюуны өмчийн эрхтэй болон бусдын өмчлөлийн программ хангамжийг хэрэглэхтэй холбоотой хууль эрх зүй, зохицуулалт, гэрээний үүргийн хэрэгжилтийг хангахад чиглэсэн хэрэглээг зохицуулан, бүртгэж, хянадаг байна.

7.3 Холбогдох хууль эрх зүй, зохицуулалтын шаардлагын дагуу хувь хүний мэдээллийн нууцлал, хамгаалалтыг Нууцын гэрээ болон, зээлдэгчийн үйлчилгээний нөхцөлийн дагуу зөвшөөрлийн хүрээнд хэрэгжүүлдэг байна.

7.4 Шифрлэлтийн зарчмыг бусад холбогдох гэрээний үүрэг, хууль эрх зүй, зохицуулалтын дагуу хэрэгжүүлдэг байна.

НАЙМ. ОНЦГОЙ ТОХИОЛДОЛ

8.1 Энэхүү баримт бичгийн заалтыг хэрэгжүүлэхэд аливаа хүндрэл гарсан тохиолдолд гүйцэтгэх удирдлагад мэдэгдэж шийдвэрлүүлэх хүсэлт гаргана.

8.2 Энэхүү баримт бичиг болон бусад журмуудаар зохицуулагдаагүй, МАБ-д эрсдэлтэй байж болох нөхцөл байдал үүсвэл өөрийн шууд удирдлага эсвэл гүйцэтгэх удирдлагад мэдэгдэж шийдвэрлүүлнэ.

ЕС. ХАРИУЦЛАГА

9.1 Энэхүү журмын зүйл заалт зөрчигдсөн тохиолдлыг мэдсэн ажилтан энэ тухай өөрийн шууд удирдлагад даруй мэдэгдэнэ.

9.2 Энэхүү журмыг зөрчсөн үйлдэл, эс үйлдэл гаргасан ажилтанд Хөдөлмөрийн тухай хууль, Хөдөлмөрийн дотоод журам, гэрээнд заасан сахилгын шийтгэл ногдуулахаас гадна холбогдох бусад хууль тогтоомж /Эрүүгийн хууль, Зөрчлийн тухай хууль, Байгууллагын нууцын тухай хууль, Хувь хүний нууцын тухай хууль, ... гэх мэт/-д заасны дагуу хариуцлага хүлээлгэхээр бол хууль, шүүхийн байгууллагад хандан шийдвэрлүүлнэ.

9.3 Сахилгын шийтгэл болон ял шийтгэл оногдуулсан эсэхээс үл хамааран энэхүү журмын зүйл заалтыг зөрчсөнөөс үүдэн гарсан аливаа хохирлыг ажилтнаар нөхөн төлүүлэх бөгөөд нөхөн төлөх үүргээс чөлөөлөхгүй.

АРАВ. ЭНЭХҮҮ БАРИМТ БИЧГЭЭС ГАРСАН БҮРТГЭЛИЙН ХӨТЛӨЛТ

Бүртгэлийн нэр	Хадгалах байршил	Хариуцах эзэн	Хяналт тавих эзэн	Хадгалах хугацаа
УДШ-ны хурлын тэмдэглэл, шийдвэр			Гүйцэтгэх захирал	3 жил
Өөрчлөлтийн бүртгэл			Гүйцэтгэх захирал	5 жил
Зочдын бүртгэл			Гүйцэтгэх захирал	1 жил
Зөрчлийн бүртгэл				
Хууль эрх зүй, оюуны өмчийн зохицуулалтын бүртгэл			Гүйцэтгэх захирал	5 жил

АРВАН НЭГ. БАРИМТ БИЧГИЙН ХҮЧИН ТӨГӨЛДӨР БАЙДАЛ

Энэхүү баримт бичгийн хүчин төгөлдөр болсон огноо – 2023.05.19

Гүйцэтгэх захирал нь энэхүү баримт бичгийн эзэмшигч байна. Микрокредит ББСБ нь энэхүү баримт бичгийн өмчлөгч байна. Энэхүү баримт бичгийн хариуцагч нь мэдээллийн аюулгүй байдал хариуцсан ажилтан байна. Хариуцагч нь энэхүү баримт бичгийг жилд нэг удаа эсвэл шаардлага гарсан тухай бүрд шинэчлэн сайжруулна.