БЭРС ФИНАНС

Гүйцэтгэх захирлын 20.25 оны
02 дугаар сарын 08-ны өдрийн
25/17а/74 тоот тушаалын хавсралт

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН БОДЛОГО

2025 он

БЭРС ФИНАНС

БАТАЛГААЖУУЛАЛТЫН ХҮСНЭГТ

Баримт бичгийн нэр	Мэдээллийн аюулгүй байдлын бодлого		
Баримт бичгийн дугаар			
Баримт бичгийн нууцлалын зэрэг	Дотоод хэрэгцээнд		
Хамрах хүрээ	Нийт ажилтнууд		
Хариуцах нэгж	Мэдээлэл технологийн газар		
Хувийг хадгалах	Үйл ажиллагааны газар		
Хүчинтэй хугацаа	хугацаагүй		
Шинэчлэх хугацаа			
Боловсруулсан	Албан тушаал	Гарын үсэг	Огноо
Б.Баясгалан	Системийн инженер		2025.08.08
О.Болортуяа	Аудитор		2025.08.08
Хянаж санал өгсөн	Албан тушаал	Гарын үсэг	Огноо
Танилцсан	ЗГ-н захирал Ө.Ган-Өлзий		2025.08.09
санал өгсөн	ХЗГ захирал Л.Дуламхүү		2025.08.14
Танилцсан	ДАГ-ын [illegible]		2025.08.14
Танилцсан	МТГ-ын Г.Энхтайвхан		2025.08.14
Баталсан	Албан тушаал	Гарын үсэг	Огноо
Г.Гомсурэн	Гүйцэтгэх захирал		2025.08.14
Баримт бичгийн батлагдсан огноо			
Хувилбар	V-1.0		

ӨӨРЧЛӨЛТИЙН БҮРТГЭЛ

Хувилбарын дугаар	Өөрчлөлтийн агуулга	Шинэчилсэн албан тушаалтан	Огноо
01	Анхлан боловсруулсан	МТГ системийн инженер Б.Баясгалан ДАГ аудитор О.Болортуяа	2025.08.08
02			
03			

АГУУЛГА

НЭГ. ЗОРИЛГО

1.1 "Бэрс финанс ББСБ" ХХК-д ISO/IEC 27001:2022 Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоо (*цаашид МАБУТ гэх*)-г нэвтрүүлэх зорилго нь гадаад, дотоод бүх аюул заналаас сэргийлж, байгууллагын мэдээллийн биет болон биет бус хөрөнгүүдийн нууцлал, бүрэн бүтэн, хүртээмжтэй байдлыг хангахад оршино.

ХОЁР. ХАМРАХ ХҮРЭЭ

2.1 Энэхүү бодлогын хүрээнд "Бэрс финанс ББСБ" ХХК-ийн бүхий л үйл ажиллагаанд ашиглагдаж буй мэдээллийн хөрөнгүүд, түүнийг хадгалах, боловсруулах, дамжуулахтай холбоотой үйл ажиллагаа, байгууллагын нийт үндсэн ажилтнууд, туршилтын ажилтнууд, гэрээт ажилтнууд, зөвлөх болон гадны байгууллагаас ирж ажиллаж буй бусад ажилтнууд хамаарна.

ГУРАВ. ҮҮРЭГ ХАРИУЦЛАГА

3.1. Энэхүү бодлоыг батлах, эзэмших бүрэн эрх нь Гүйцэтгэх захиралд байна.

3.2. Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоог хэрэгжүүлэх баг нь байгууллагын хэмжээнд энэхүү бодлогыг бүрэн хэрэгжүүлнэ.

ДӨРӨВ. БОДЛОГО

4.1. "Бэрс финанс ББСБ" ХХК нь санхүүгийн цогц шийдлийг хүн бүрт мэргэжлийн, ёс зүйтэй, хариуцлагатай мэргэшсэн хүчирхэг хамт олноор хүргэхээр зорьж байна.

4.2. Бид үүний тулд байгууллагынхаа бүхий л түвшинд мэдээллийн аюулгүй байдлын соёлыг төлөвшүүлж, мэдээлэл болон мэдээллийн хөрөнгийн нууцлал, бүрэн бүтэн, хүртээмжтэй байдлыг ханган ажиллахдаа мэдээллийн аюулгүй байдлын удирдлагын тогтолцооны ISO/IEC 27001:2022 стандартын холбогдох шаардлагууд болон Монгол Улсын хууль, тогтоомж, дүрэм, журмыг мөрдлөг болгон ажиллана. Тус тогтолцооны хүрээнд дараах зорилтуудыг хэрэгжүүлнэ.

Үүнд:

- Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоог ISO/IEC 27001:2022 стандартын дагуу баталгаажуулж, тогтмол шинэчилж, сайжруулна.
- Мэдээллийн аюулгүй байдлын эрсдэлийн удирдлагын тогтолцоог бүрдүүлнэ.
- Мэдээллийн аюулгүй байдлын эрсдэлийг жил бүр тогтмол хугацаанд үнэлж, бууруулна.
- Мэдээллийн аюулгүй байдлын хяналтуудын хэрэгжилтийг тогтмол хугацаанд үнэлнэ.
- Байгууллагын дотоод болон гадаад оролцогч талуудад чиглэсэн мэдээллийн аюулгүй байдлын сургалт хөтөлбөрүүдийг хэрэгжүүлнэ.
- Санхүүгийн цогц шийдлийг хүртээмжтэй, найдвартай бүтээгдэхүүн, үйлчилгээгээр харилцагчид хүргэнэ.

ТАВ. МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН БҮТЭЦ, ЗОХИОН БАЙГУУЛАЛТ

5.1 Мэдээллийн аюулгүй байдлын үүрэг, хариуцлага

5.1.1 Төлөөлөн Удирдах Зөвлөл

5.1.1.1 Мэдээллийн аюулгүй байдлын бодлого болон аюулгүй байдлын томоохон төсөл, хөтөлбөрүүдийг жил бүр хянаж, батлах;

5.1.1.2 Мэдээллийн аюулгүй байдлын тогтолцоонд шаардлагатай нөөцийг хуваарилж, нөөцөөр хангах;

5.1.1.3 Мэдээллийн аюулгүй байдлын томоохон эрсдэл болон зөрчилд тайлагналаар дамжуулан хяналт тавих;

5.1.1.4 Жил бүрийн мэдээллийн аюулгүй байдлын тогтолцооны хэрэгжилтийн үр дүнтэй байдлыг хэмжих хэмжүүр болон үнэлгээг хянах;

5.1.1.5 Мэдээллийн аюулгүй байдалтай холбоотой эрсдэлийн хүлээн зөвшөөрөх болон тэсвэрлэх түвшинг батлах;

5.1.2 Гүйцэтгэх удирдлага ***/С түвшний удирдлагууд/***

5.1.2.1 Байгууллагын хэмжээнд МАБУТ-ны хүчирхэг соёлыг бий болгож, хадгалах;

5.1.2.2 Мэдээллийн аюулгүй байдлын стратеги, бодлого, томоохон санаачлагуудыг батлах;

5.1.2.3 Байгууллагын үйл ажиллагааны процессуудад мэдээллийн аюулгүй байдлын шаардлагуудыг нэгтгэж, аюулгүй байдлыг хангах;

5.1.2.4 Мэдээллийн аюулгүй байдлын хяналтуудыг үр ашигтай хэрэгжүүлэхэд шаардлагатай санхүү, хүний нөөц болон техникийн шаардлагатай нөөцийг хуваарилах;

5.1.2.5 Мэдээллийн аюулгүй байдлын гүйцэтгэлийн үзүүлэлтүүд болон эрсдэлийн үзүүлэлтүүдийг улирал тутам хянах;

5.1.2.6 Бизнес төлөвлөлт болон шийдвэр гаргалтад аюулгүй байдлын асуудлуудыг анхаарч, тусгах;

5.1.3 Эрсдэлийн хороо

5.1.3.1 МАБ–ын удирдлагын бодлого, журмыг хэрэгжүүлэхэд дүн шинжилгээ хийж, зөвлөгөө өгөх;

5.1.3.2 МАБ-ын бодлого, журмын хэрэгжилтийг мөрдүүлэх;

5.1.3.3 ISO/IEC 27001:2022 стандартын дагуу МАБУТ-г тасралтгүй удирдан, сайжруулахад дэмжин ажиллах;

5.1.3.4 МАБУТ-ны үр ашигт дүн шинжилгээ хийх, Гүйцэтгэх удирдлага болон Төлөөлөн удирдах зөвлөлд тайлагнах;

5.1.3.5 Мэдээллийн аюулгүй байдлын тодорхойлсон эрсдэлүүдийн бууруулах төлөвлөгөөг хянаж, батлах;

5.1.3.6 Эрсдэлийг бууруулах төлөвлөгөөний хэрэгжилтийг хянах;

5.1.3.7 МТ-н системүүдийн аюулгүй байдлын суурь стандартуудыг хянах, санал болгох;

5.1.3.8 Тус хорооны хурлын шийдвэрийн хэрэгжилтэнд хяналт тавих;

5.1.4 Мэдээллийн аюулгүй байдлын зөвлөх

5.1.4.1 ISO/IEC 27001:2022 стандартын шаардлагын дагуу сонирхогч талуудад өгөх зааварчилгааг бэлдэх, боловсруулах болон МАБУТ-г нэвтрүүлэх, хадгалах, баримтжуулах;

5.1.4.2 Аюулгүй байдлын үнэлгээ, гуравдагч талуудаар үнэлүүлсэн тайланд дүн шинжилгээ хийж, байгууллагын аюулгүй байдлын төлөв байдлын тайланг мэдээллийн аюулгүй байдал хариуцсан удирдлагаар чиглүүлж, Гүйцэтгэх удирдлагад тайлагнах;

5.1.4.3 Гүйцэтгэх удирдлагууд, мэдээллийн аюулгүй байдал хариуцсан удирдлага болон МАБ хариуцсан ажилтанд хамгийн багадаа жилд 1 удаа МАБ-н талаар сургалт зохион байгуулах;

5.1.4.4 Мэдээллийн аюулгүй байдлын бодлого, журам, үйл явцын хяналтад оролцох;

5.1.4.5 Мэдээллийн аюулгүй байдлын ажилтанд болон МАБ-ын аудит хийхэд дэмжлэг үзүүлж ажиллах;

5.1.4.6 Мэдээллийн аюулгүй байдлын багт МАБ-н аудит хийх болон будлианы удирдлагад дэмжлэг үзүүлж ажиллах;

5.1.5 Мэдээллийн аюулгүй байдал хариуцсан удирдлага

5.1.5.1 Байгууллагын мэдээллийн аюулгүй байдлын стратеги, бодлогыг боловсруулж, хэрэгжүүлж, тасралтгүй сайжруулах;

5.1.5.2 Байгууллагын хэмжээнд аюулгүй байдлын хяналтуудын хэрэгжилт, үйл ажиллагааг удирдан зохион байгуулах;

5.1.5.3 Мэдээллийн аюулгүй байдлын нөхцөл байдал, эрсдэл, тэдгээртэй холбоотой чухал асуудлуудыг мэдээллийн аюулгүй байдлын хороо болон гүйцэтгэх удирдлагад тайлагнах;

5.1.5.4 Мэдээллийн аюулгүй байдал хариуцсан ажилтны ажил үүрэг болон аюулгүй байдлын үйл ажиллагааг удирдах;

5.1.5.5 МАБУТ-ны шаардлага, стандартад нийцүүлж аюулгүй байдлыг хангах;

5.1.5.6 Мэдээллийн аюулгүй байдлын зөрчилд хариу арга хэмжээ авах үйл ажиллагааг зохицуулах;

5.1.5.7 Гуравдагч болон гадаад сонирхогч талуудтай үүсгэх харилцаа холбоонд аюулгүй байдлыг хангах;

5.1.5.8 Мэдээллийн аюулгүй байдлын мэдлэг олгох, сургалт хөтөлбөрүүдийг удирдах;

5.1.5.9 Бизнесийн нэгжүүдэд мэдээллийн аюулгүй байдлын зөвлөгөө, зааварчилгаа өгөх;

5.1.5.10 Аюулгүй байдлын архитектур, загваруудыг хянаж, батлах;

5.1.6 Мэдээллийн технологийн газар

5.1.6.1 ISO/IEC 27001:2022 стандартын дагуу МАБУТ-г үр дүнтэйгээр хэрэгжүүлэхэд дэмжлэг үзүүлж ажиллах;

5.1.6.2 Батлагдсан бодлого, журмын дагуу мэдээллийн аюулгүй байдлын хяналтуудыг хэрэгжүүлэх;

5.1.6.3 Мэдээллийн аюулгүй байдлын үйл явдал (event)-уудыг хянаж, зөрчилд хариу арга хэмжээ авах;

5.1.6.4 Мэдээллийн аюулгүй байдлын үнэлгээ, аудит, тест хийх;

5.1.6.5 Бизнесийн нэгжүүд болон төслүүдэд мэдээллийн аюулгүй байдлын зөвлөгөө өгөх;

5.1.6.6 Мэдээллийн аюулгүй байдлын түүл хэрэгсэл, технологиудыг удирдах;

5.1.6.7 Мэдээллийн аюулгүй байдлын журам, зааварчилгаа боловсруулах;

5.1.6.8 Мэдээллийн аюулгүй байдлын мэдлэг олгох сургалтууд зохион байгуулах;

5.1.6.9 Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээ хийх;

5.1.6.10 Бодлого, журмын нийцлийн үйл ажиллагаа болон аудитад дэмжлэг үзүүлэх;

5.1.6.11 Мэдээллийн аюулгүй байдлын зөрчил, алдаа дутагдалд дүн шинжилгээ хийх;

5.1.7 Дотоод аудитын газар

5.1.7.1 МАБ-ын аудит, хөндлөнгийн аудит, баталгаажуулалтын аудит болон нийцлийн аудитын төлөвлөгөө, хөтөлбөрийг боловсруулж, хэрэгжүүлэх;

5.1.7.2 МАБ-ын аудитын журмын дагуу тогтмол хугацаанд МАБ-ын аудит болон нийцлийн аудитыг хийж, удирдлагад аудитын үеэр илэрсэн асуудлуудыг тайлагнах;

5.1.7.3 Бизнесийн газар, нэгжүүдэд аудитын үеэр илэрсэн асуудлуудыг засаж залруулах, шийдвэрлэхэд дэмжлэг үзүүлэх;

5.1.7.4 Бизнесийн газар, нэгжүүдэд тогтмол хугацаанд нийцлийн шалгалтыг хийх;

5.1.7.5 МАБ-н үйл ажиллагааны хэрэгжилт болон үр дүнтэй байдлыг бататгахын тулд гэнэтийн МАБ-ын аудит хийх;

5.1.7.6 ISO/IEC 27001 стандартыг баталгаажуулалт хийдэг гуравдагч талуудтай хамтран баталгаажуулалтын аудитыг зохион байгуулах;

5.1.8 Төвийн газар, нэгжийн ажилтнууд

5.1.8.1 Хариуцсан ажлын хүрээнд мэдээллийн аюулгүй байдлын хяналтуудыг хэрэгжүүлэх;

5.1.8.2 Хариуцаж буй ажилтнуудад мэдээллийн аюулгүй байдлын бодлого, журмыг дагаж мөрдүүлэх;

5.1.8.3 Бизнесийн үйл ажиллагаанд шаардлагатай мэдээллийн аюулгүй байдлын хэрэгцээ шаардлагыг тодорхойлж, мэдээллийн аюулгүй байдал хариуцсан багт мэдээлэх;

5.1.8.4 Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээ, аудитад дэмжлэг үзүүлэх;

5.1.8.5 Мэдээллийн аюулгүй байдлын зөрчлийг мэдээллийн аюулгүй байдал хариуцсан ажилтанд шуурхай мэдээлэх;

5.1.8.6 Бизнесийн газар, нэгжийн мэдээллийн хөрөнгийн бүртгэлийг хөтлөж, хадгалах;

5.1.8.7 Ажилтнуудын хандах эрхүүдийг тогтмол хянах;

5.1.8.8 Төслийн төлөвлөлтөд мэдээллийн аюулгүй байдлын шаардлагыг тусгаж байх;

5.1.8.9 Хариуцаж буй газар, нэгж, багийн хэмжээнд мэдээллийн аюулгүй байдлын мэдлэгт дэмжлэг үзүүлэх;

5.1.8.10 Гуравдагч талуудтай байгуулсан гэрээ, хамтын ажиллагаанд мэдээллийн аюулгүй байдлыг шаардлагуудыг анхаарч үзэж байх;

5.1.9 Систем болон өгөгдөл эзэмшигч

5.1.9.1 Хариуцсан мэдээллийн хөрөнгийн ангиллын түвшинг тодорхойлох;

5.1.9.2 Хариуцсан систем болон өгөгдөлд хандах эрхийг зөвшөөрөх;

5.1.9.3 Систем болон өгөгдөлд хандах эрхийг тогтмол хянах;

5.1.9.4 Зохих аюулгүй байдлын хяналтуудыг хэрэгжүүлэх;

5.1.9.5 Эрсдэлийн үнэлгээ болон мэдээллийн аюулгүй байдлын шалгалтуудад оролцох;

5.1.9.6 Нөөцлөлт болон сэргээх шаардлагыг тодорхойлох;

5.1.9.7 Мэдээллийн аюулгүй байдалд нөлөөлөх системийн өөрчлөлтүүдийг батлах;

5.1.9.8 Мэдээллийн аюулгүй байдлын зөрчлүүдэд дүн шинжилгээ хийхэд дэмжлэг үзүүлэх;

5.1.9.9 Системийн аюулгүй байдлын шаардлагын баримт бичгийг хадгалах;

5.1.9.10 Хариуцсан мэдээллийн хөрөнгөд холбогдох мэдээллийн аюулгүй байдлын бодлого, журмыг дагаж мөрдөх;

5.1.10 Үндсэн болон гэрээт ажилтнууд, гуравдагч талууд

5.1.10.1 Байгууллагын хэмжээнд хэрэгжүүлж буй бүх мэдээллийн аюулгүй байдлын бодлого, журмыг дагаж мөрдөх;

5.1.10.2 Мэдээллийн аюулгүй байдлын мэдлэг олгох сургалтад тогтмол хамрагдах;

5.1.10.3 Хариуцсан мэдээллийн хөрөнгийн мэдээллийн аюулгүй байдлыг тогтмол хангаж, аюул заналаас хамгаалах;

5.1.10.4 Мэдээллийн аюулгүй байдлын зөрчил, алдаа дутагдлыг мэдээллийн аюулгүй байдал хариуцсан ажилтанд шуурхай мэдээлэх;

5.1.10.5 Мэдээллийн хөрөнгийг зөвхөн зөвшөөрөгдсөн зорилгоор ашиглах;

5.1.10.6 Эмзэг, нууцлалтай мэдээллийн нууцлалыг хадгалах;

5.1.10.7 Аюулгүй ажиллагааны арга хэмжээ, практикыг дагаж мөрдөх;

5.1.10.8 Танилт, нэвтрэлтийн мэдээллээ бусдад задруулахгүй, хамгаалах;

5.1.10.9 Биет орчны аюулгүй байдлыг хангаж ажиллах;

5.1.10.10 Мэдээллийн аюулгүй байдлын үнэлгээ, аудитад шаардлагатай үед дэмжлэг үзүүлэх;

5.2 Ажил үүргийг ангилах, тусгаарлах

5.2.1 Байгууллагын бүх үйл ажиллагааны процессыг хамгийн боломжит хэмжээнд хүртэл ажил үүргийг ангилан тусгаарлана.

5.2.2 Өдөр тутмын ердийн гүйцэтгэх үүрэг хариуцлагыг ажилтнуудад хуваарьлахдаа нэг хүнээс хамаарах хамаарлаас аль болох зайлсхийх бөгөөд шууд удирдлага нь орлох ажилтныг томилно.

5.2.3 Ажил үүргийг ангилан тусгаарлах боломжгүй бол хийж буй үйл ажиллагааны хувьд аудит болон удирдлагын хяналт заавал байх ёстой.

5.3 Мэдээллийн аюулгүй байдлын ажилтан нь дараах холбоо барих мэдээллийн жагсаалтыг хөтөлнө.

5.3.1 Байгууллагын аюулгүй байдалтай холбоотойгоор онцгой тохиолдолд холбоо барих хүмүүсийн жагсаалтыг хөтөлж, мэдээллийн самбарт эсвэл нүдэнд ил харагдахуйц газар байршуулна.

5.3.2 Ашиг сонирхлын бүлгүүдтэй харилцах үүднээс холбогдох аюулгүй байдлын чиглэлийн форумууд, мэргэжлийн байгууллагуудтай холбоо барих мэдээллийн жагсаалтыг хөтөлнө.

5.3.3 Холбогдох мэдээлэл технологи болон мэдээллийн аюулгүй байдлын чиглэлийн мэргэжлийн байгууллагуудтай холбоо барих мэдээллийн жагсаалтыг хөтөлнө.

5.4 Төслийн удирдлага дахь мэдээллийн аюулгүй байдал

5.4.1 Төслийн хүрээнд мэдээллийн аюулгүй байдлын эрсдэлүүдийг тодорхойлон шийдвэрлэх явдлыг хангахын тулд байгууллагын төслийн удирдлагын аргачлалд аюулгүй байдлын заалтуудыг тусгана.

5.4.2 Дээрх аюулгүй байдлын заалтууд нь бүх төрлийн төслүүдэд хамааралтай байна. Тухайлбал, бизнесийн үндсэн үйл ажиллагаа, мэдээлэл технологи болон бусад дэмжих үйл явцуудтай хамааралтай төслүүд гэх мэт.

5.4.3 Мэдээллийн хөрөнгө хариуцагч нь өөрийн төслүүдэд мэдээллийн аюулгүй байдлын заалтуудыг тусгаж өгч эрсдэлийн үнэлгээг тодорхойлох үүрэгтэй.

ЗУРГАА. БАРИМТ БИЧГИЙН ХЯНАЛТ

6.1 Энэхүү бодлогыг Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоо хариуцсан ажилтан жилд хамгийн багададаа нэг удаа, шаардлагатай тохиолдолд тухай бүр хянан өөрчлөлтийг хийж, Гүйцэтгэх захирлаар батлуулна.