“Жэтфинанс ББСБ” ХХК-ийн ТУЗ-ийн 2022 оны .....р сарын .....-ны өдрийн ..... тоот тогтоолын Хавсралт No. 5

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН БОДЛОГО

НЭГ. НИЙТЛЭГ ҮНДЭСЛЭЛ

1.1. Энэхүү бодлогын зорилго нь ББСБ, 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, Хувь хүний нууцын тухай хууль, Мэдээллийн аюулгүй байдлын ISO 27001:2013, ISO 27005:2013 стандартуудад нийцсэн байна.

1.3. Энэхүү бодлогод хэрэглэсэн нэр томьёог дор дурдсан утгаар ойлгоно. Үүнд:

1.3.1. “Мэдээллийн аюулгүй байдал” гэж мэдээлэл боловсруулах систем болон дэд бүтцийн ашиглалт, хадгалалт, хамгаалалттай холбоотой нууцлал, бүрэн бүтэн байдал, хүртээмжтэй байдал, тасралтгүй найдвартай ажиллагаа, хянан шалгах, нягтлахтай холбоотой асуудлуудыг;

1.3.2. “Нууцлал” гэж үйлчилгээ, бүрдэл хэсгүүд болон дэд бүтцийн элементүүд хууль бус нэвтрэлтээс хамгаалагдсан байх, хандах эрх олгогдоогүй аливаа этгээд мэдээллийн хөрөнгө, сүлжээ, мэдээллийн системд хандах боломжгүй байхыг;

1.3.3. “Хүртээмжтэй байдал” гэж мэдээллийн хөрөнгөд эрх бүхий этгээд хүссэн үедээ хандах, ашиглах боломжтой байхыг;

1.3.4. “Бүрэн бүтэн байдал ” гэж мэдээллийн үнэн зөв, бүрэн бүтэн байдлыг хангасан байдлыг;

1.3.5. “Мэдээллийн хөрөнгө” гэж ББСБ-д ач холбогдол, үр өгөөж, үнэ цэнэ, хэрэгцээтэй үед хялбархан хандах боломжтой цаасан, тоон, дүрс бичлэг, яриа тэдгээрийг агуулсан мэдээллийн систем, файл, гэрээ хэлцэл, сүлжээ, програм хангамж, мэдээллийн нөөцүүд, компьютер, зөөврийн тооцоолох төхөөрөмжүүд, системийн бичиг баримт, судалгааны мэдээлэл, хэрэглэгчийн гарын авлага, сургалтын материал, үйл ажиллагааны журам, заавар, бизнес төлөвлөгөө, тайлан, аудитын бичиг баримт, архивын материалыг тус тус хэлнэ.

1.4. Мэдээллийн аюулгүй байдлын бодлогыг Төлөөлөн удирдах зөвлөлийг хурлаар хэлэлцэн батална.

1.5. Мэдээллийн аюулгүй байдлын бодлогыг ББСБ-ын оролцогч талууд, ажилтнууд, хөндлөнгийн аудит, ББСБ-ыг таньж мэдэхээр шалгаж буй санхүүгийн байгууллагуудад танилцуулж болно.

1.6. ББСБ-ын мэдээллийн аюулгүй байдлын бодлогыг хэрэгжүүлэх арга зам нь мэдээллийн аюулгүй байдлыг хангах журам, стандарт байх бөгөөд тэдгээрийг боловсруулан мөрдөж ажиллана.

1.7. Мэдээллийн аюулгүй байдлын бодлого нь ББСБ-ын оролцогч талууд болон ажилтнуудад хамаарна.

ХОЁР. МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН БОДЛОГЫН ҮНДСЭН ЗАРЧИМ

2.1.Мэдээллийн аюулгүй байдлын бодлогыг хэрэгжүүлэхдээ дараах бодлого, бодлого тус бүрийн хүрээнд зорилгыг хангаж ажиллана. Үүнд:

2.1.1.Хүний нөөцийн аюулгүй байдал

2.1.1.1.Ажилд авахын өмнө. Ажилтан болон гэрээт ажилтнууд өөрсдийн үүрэг хариуцлагыг ойлгож, гүйцэтгэх ажлаа харгалзах үүрэгтээ тохирсон эсэхийг баталгаажуулах. Ажилд орох болон гэрээгээр ажиллах ажил горилогчийн намтрыг зохих хууль тогтоомж, журмын дагуу хянаж сонгон шалгаруулалт хийж, үүргийг танилцуулж хөдөлмөрийн гэрээ болон ББСБ-ын нууц мэдээллийн аюулгүй байдлыг хангах гэрээ байгуулах;

2.1.1.2.Ажиллаж байх үе. Ажилтан болон гэрээт ажилтан нь мэдээллийн аюулгүй байдлын талаар хүлээх үүргээ ухамсарлаж, биелүүлэх, гүйлгээ хийх эрхийн хүрээнд ажиллах, мэдээллийн аюулгүй байдалд нийцэхгүй үйл ажиллагааг таслан зогсоох, шууд болон гүйцэтгэх удирдлагад мэдээллэх үүрэгтэй;

2.1.1.3.Ажлаас гарах үед. Ажлын байр өөрчлөх эсвэл ажлаас гарч байгаа тохиолдолд ажилтны нэвтрэх эрхийг хязгаарлах, ажилтан нууцыг задлахгүй байх.

2.1.2.Мэдээллийн хөрөнгийн удирдлага

2.1.2.1.ББСБ-ын мэдээллийн хөрөнгийг тодорхойлох, хөрөнгийг хамгаалахад тохиромжтой үүрэг хариуцлагыг тодорхойлох;

2.1.2.2.Мэдээлэл нь ББСБ-д ач холбогдолынхоо эрэмбээр тохирох хэмжээний нууцлалтай байгаа эсэхийг хангах;

2.1.2.3.Файлаар байгаа мэдээллийг зөвшөөрөлгүйгээр мэдээллэх, өөрчлөх, устгах, гэмтээхээс урьдчилан сэргийлэх.

2.1.3.Хандалтын хяналт

2.1.3.1.Мэдээлэл, мэдээлэл боловсруулагчид хандах хандалтыг хязгаарлах;

2.1.3.2.Зөвшөөрөгдсөн хэрэглэгчийн эрхийг баталгаажуулах, систем болон үйл ажиллагаанд зөвшөөрөлгүй хандахаас урьдчилан сэргийлэх;

2.1.3.3.Хэрэглэгчид өөрийгөө баталгаажуулах нууц үг нь чухал гэдэг үүргийг таниулах;

2.1.3.4.Систем болон програмуудад зөвшөөрөлгүй хандахаас урьдчилан сэргийлэх.

2.1.4.Нууцлалын удирдлага

2.1.4.1.Мэдээллийн нууцлал, үнэн зөв, бүрэн бүтэн байдлыг хамгаалахын тулд криптографийг зүй зохистойгоор ашиглаж байгаа эсэхийг баталгаажуулах.

2.1.5.Биет болон орчны аюулгүй байдал

2.1.5.1.Байгууллагын мэдээлэл, мэдээлэл боловсруулах хэрэгсэлд зөвшөөрөлгүйгээр биет байдлаар нэвтрэх, хохирол учруулах, хөндлөнгөөс оролцохоос урьдчилан сэргийлэх;

2.1.5.2.Хөрөнгийн алдагдал, эвдрэл гэмтэл болон байгууллагын үйл ажиллагаанд саатал учруулахаас урьдчилан сэргийлэх.

2.1.6.Үйл ажиллагааны аюулгүй байдал

2.1.6.1.Мэдээлэл боловсруулах хэрэгслүүдийн зөв, найдвартай ажиллагааг хангах;

2.1.6.2.Мэдээлэл, мэдээлэл боловсруулах хэрэгслүүд нь хортой програмаас хамгаалагдсан эсэхийг баталгаажуулах;

2.1.6.3.Өгөгдөл алдагдахаас хамгаалах;

2.1.6.4.Үйл ажиллагааг бүртгэж, баримтжуулах;

2.1.6.5.Үйл ажиллагааны системийн бүрэн бүтэн байдлыг хангах;

2.1.6.6.Техникийн ашиглалтын эмзэг байдлаас урьдчилан сэргийлэх;

2.1.6.7.Үйл ажиллагааны систем дэх хяналтыг оновчтой бага түвшинд байлгах.

2.1.7.Харилцаа холбооны аюулгүй байдал

2.1.7.1.Сүлжээ дэх мэдээлэл болон түүний мэдээллийг боловсруулдаг хэрэгслүүдийг хамгаалах;

2.1.7.2.ББСБ доторх болон гадны байгууллагатай мэдээлэл солилцохдоо мэдээллийн аюулгүй байдлыг хангах.

2.1.8. Системийн худалдан авалт, хөгжүүлэлт болон хэвийн үйл ажиллагааг хангах

2.1.8.1.Мэдээллийн аюулгүй байдлыг мэдээллийн системийн үе шат бүрт болон олон нийтийн сүлжээний аюулгүй байдлын шаардлагыг хангах;

2.1.8.2.Мэдээллийн системийн бүхий л үе шатанд мэдээллийн аюулгүй байдал нь хамаарсан байхыг хангах;

2.1.8.3.Туршилтад ашиглах өгөгдлийн хамгаалалтыг хангах.

2.1.9.Мэдээллийн технологийн үйлчилгээ үзүүлэгчтэй харилцах бодлого

2.1.9.1.Үйлчилгээ үзүүлэгч хандах эрхтэй байгууллагын хөрөнгийг хамгаалах;

2.1.9.2.Үйлчилгээ үзүүлэгчтэй байгуулсан гэрээнд заасны дагуу мэдээллийн аюулгүй байдлыг хангах.

2.1.10.Мэдээллийн аюулгүй байдлын будлианы удирдлага

2.1.10.1.Аюулгүй байдлын сул тал болон үйл явдлын харилцаа хамаарлыг харуулсан мэдээллийн аюулгүй байдлын удирдлагын үр дүнтэй байдлаар хангах.

2.1.11.Бизнесийн тасралтгүй үйл ажиллагааны мэдээллийн аюулгүй байдал

2.1.11.1.Мэдээллийн аюулгүй байдал нь байгууллагын бизнесийг тасралтгүй үйл жиллагаатай нийцсэн байна.

2.1.12.Хянан нийцүүлэлт

2.1.12.1.Мэдээллийн аюулгүй байдал болон аюулгүй байдлын шаардлагуудтай холбоотой эрх зүйн, хууль тогтоомж, дүрэм журам эсвэл гэрээний үүргийг зөрчихөөс зайлсхийнэ.

ГУРАВ. ХЯНАЛТ

3.1.Мэдээллийн аюулгүй байдлын бодлогод дараах хүчин зүйлсээс шалтгаалан томоохон өөрчлөлт гарсан тохиолдолд бодлогыг үнэлэх, хянах, хөгжүүлэх ажлыг Гүйцэтгэх захирал Төлөөлөн удирдах зөвлөлд танилцуулна. Үүнд:

3.1.1. Бизнесийн стратеги;

3.1.2. Дүрэм журам, хууль тогтоомж болон гэрээнүүд;

3.1.3. Мэдээллийн аюулгүй байдлын өнөөгийн болон ирээдүйд учирч болох аюул заналын орчин.

3.2.Үнэлгээ нь технологийн орчин, хуулийн нөхцөл, бизнесийн онцлог, байгууллагын орчны өөрчлөлт болон тэдгээрийн мэдээллийн аюулгүй байдлыг удирдах арга зам, ББСБ-ын бодлогыг сайжруулах боломжийн талаарх дүгнэлт зэргийг хамруулсан байна.

3.3.Мэдээллийн аюулгүй байдлын бодлогын хяналтад удирдлагын хяналтын үр дүнг харгалзана.

3.4. Мэдээллийн аюулгүй байдлын бодлогын хэрэгжилтэд хийгдэх хяналтыг Дотоод аудитын газар хариуцна.

ДӨРӨВ. ХАРИУЦЛАГА

4.1.Мэдээлийн аюулгүй байдлын бодлого, Мэдээллийн аюулгүй байдлыг хангах журам, мэдээллийн аюулгүй байдалтай холбоотой бусад журам, зааврыг хөдөлмөрлөх үедээ өөрийн бууутай үйл ажиллагааны улмаас зөрчсөн үйлдлийг ноцтой гэж үзсэн тохиолдолд Хөдөлмөрийн дотоод журам, Монгол Улсын хууль тогтоомжийн дагуу хариуцлага хүлээнэ.

“ЖЭТФИНАНС ББСБ” ХХК