“БАГАНУУР” ХУВЬЦААТ КОМПАНИЙН ГҮЙЦЭТГЭХ ЗАХИРЛЫН ТУШААЛ

2016 оны 03 сарын 16 өдөр Дугаар А/109 Багануур дүүрэг

Бодлогын баримт бичиг батлах
тухай

Кибер аюулгүй байдлын тухай хуулийн 19 дүгээр зүйлийн 19.2.1, Компанийн тухай хуулийн 83 дугаар зүйлийн 83.1, “Багануур” ХК-ийн дүрмийн 3 дугаар зүйлийн 3.4.2.3 дахь заалтыг тус тус үндэслэл болгон ТУШААХ нь:

1.Компанийн хэмжээнд Мэдээллийн аюулгүй байдлын менежментийн тогтолцоог нэвтрүүлж, хэрэгжүүлэх зорилгоор “Мэдээллийн аюулгүй бодлого”-ыг хавсралтаар баталсугай.

2.МАБ-ын талаар баримтлах бодлогыг хэрэгжүүлэх арга хэмжээний төлөвлөгөөний зорилтын хэрэгжилтийг хангаж, үндсэн чиглэлд тусган хэрэгжүүлж ажиллахыг нэгжийн удирдлагуудад даалгасугай.

3.Бодлогын хэрэгжилтийг нийт ажилтнуудад танилцуулан, хэрэгжилтийг хангаж ажиллахыг мэдээллийн технологийн алба (Т.Эрдэнэ-Очир)-д, бодлогын хэрэгжилтэд хяналт тавьж ажиллахыг Дотоод хяналт, эрсдэлийн удирдлагын алба (Б.Хажидмаа)-д тус тус үүрэг болгосугай.

ГҮЙЦЭТГЭХ ЗАХИРЛЫН
ҮҮРЭГ ГҮЙЦЭТГЭГЧ Т.ОТГОНБОЛД

“БАГАНУУР” ХК

Баримт бичгийн нэр:

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН БОДЛОГО

Баримт бичгийн хариуцагч:	Мэдээллийн технологийн алба
Баримт бичгийн дугаар:	Б26-МТА-01-01
Баталсан огноо:	2026-03-16
Тушаалын дугаар:	А/109
Мөрдөж эхлэх огноо:	2026.03.16.
Боловсруулсан:	МТА-ны системийн зохион байгуулагч О.Содбилэг
Баталсан.	Гүйцэтгэх захирлын үүрэг гүйцэтгэгч Т.Отгонболд

Өөрчлөлтийн талаарх мэдээлэл:

Өөрчлөлт оруулсан ажилтан	Өөрчлөлт оруулсан огноо	Хувилбар	Өөрчлөлтийн утга

Жич: Энэхүү бичиг баримтыг зөвхөн “Багануур” ХК-ийн дотоод хэрэгцээнд ашиглана.

АГУУЛГА

Гүйцэтгэх захирлын ..... оны
..... тоот тушаалын хавсралт

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН БОДЛОГО

НЭГ. НИЙТЛЭГ ҮНДЭСЛЭЛ

1.1. Энэхүү Мэдээллийн Аюулгүй Байдал (МАБ)-ын Бодлого (цаашид "Бодлого" гэх)-ын зорилго нь "Багануур" ХК (цаашид "Компани" гэх)-ийн дунд болон урт хугацааны стратегийн зорилтуудтай уялдуулан, МАБ-ын нууцлал, бүрэн бүтэн байдал, хүртээмжтэй байдал (CIA: Confidentiality, Integrity, Availability)-ын зарчимд нийцүүлэн хангах замаар компанийн үйлдвэрлэлийн үйл ажиллагааны тасралтгүй байдлыг баталгаажуулахад оршино.

1.2. Энэхүү бодлого нь компанийн хэмжээнд Мэдээллийн аюулгүй байдлын менежментийн тогтолцоо (МАБМТ)-г нэвтрүүлж, хэрэгжүүлэхэд дээд удирдлагын манлайллын баталгаа болох бөгөөд тогтолцооны үр нөлөөг тасралтгүй сайжруулах, ажилтан бүрийн оролцоог хангах хөшүүрэг болно.

1.3. Энэхүү бодлого нь Монгол Улсын Кибер аюулгүй байдлын тухай хууль, Хүний хувийн мэдээлэл хамгаалах тухай, Нийтийн мэдээллийн ил тод байдлын тухай хууль, Засгийн газрын 2022 оны 207 дугаар тогтоолоор батлсан "Онц чухал мэдээллийн дэд бүтэцтэй байгууллагын жагсаалт", Засгийн газрын 2023 оны 244 дүгээр тогтоолоор батлсан "Кибер аюулгүй байдлыг хангах нийтлэг журам", олон улсын МАБМТ-ны ISO/IEC 27001:2022 стандартын шаардлага, "Кибер аюулгүй байдлын үндэсний стратеги"-ийг хэрэгжүүлэх арга хэмжээний төлөвлөгөө, "Эрдэнэс Монгол" нэгдлийн “Мэдээллийн аюулгүй байдлын бодлого” зэрэг эрх зүйн баримт бичгүүдэд үндэслэн компанийн засаглалын бүх түвшинд үр дүнтэй хэрэгжүүлэх, соёлыг хэвшүүлэх, эрсдэлд суурилсан хяналтын механизмыг тасралтгүй сайжруулах үндсэн чиглэлийг тодорхойлно.

1.4. Энэхүү бодлогын баримт бичгийг МАБ-ыг хангах үйл ажиллагаатай холбоотой дүрэм, журам, заавар боловсруулахад баримтлах бөгөөд компанийн үйл ажиллагаанд томоохон өөрчлөлт гарсан эсвэл шаардлагатай тохиолдолд компанийн стратеги төлөвлөгөөтэй уялдуулан шинэчлэн сайжруулна.

1.5. Энэхүү бодлого нь мэдээллийн аюулгүй байдлын менежментийн тогтолцооны Төлөвлөх-Хэрэгжүүлэх-Шалгах-Сайжруулах (PDCA - Plan-Do-Check-Act) мөчлөгт суурилна.

ХОЁР. НЭР ТОМЬЁО, ТОВЧИЛСОН ҮГИЙН ТАЙЛБАР

Аудит	(Аудит) Мэдээллийн аюулгүй байдлын бодлогын хэрэгжилт, журмын мөрдөлтийг хянах, үнэлэх, баримтжуулсан үйл явцыг хараат бусаар дотоод болон гадаад аудит хийх үйл ажиллагаа
Мэдээлэл	(Information) Компанийн хэмжээнд бүх төрлийн үйл ажиллагааны хүрээнд бий болсон, боловсруулагдсан, дамжуулагдсан, хадгалагдсан, хүлээж авсан болон ашиглагдсан өгөгдөл, баримт бичиг, мэдээллийн багц.
Мэдээллийн аюулгүй байдал	(Information Security) МАБ гэдэг нь мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмжтэй байдлыг хангах үйл явц, удирдлага, арга хэмжээ.
Нууцлаг байдал	(Confidentiality) Мэдээлэлд зөвхөн эрх бүхий хэрэглэгчид хандах боломжийг олгож, зөвшөөрөлгүй этгээдээс хамгаалах зарчим.
Бүрэн бүтэн байдал	(Integrity) Мэдээллийг зөвшөөрөлгүй өөрчлөлт, устгал, алдагдал, хөндлөнгийн оролцооноос хамгаалж, үнэн зөв, найдвартай байдлыг хадгалах.
Хүртээмжтэй байдал	(Availability) Мэдээлэл, системүүд нь зөвшөөрөгдсөн хэрэглэгчдэд шаардлагатай үедээ ашиглах боломжтой байх нөхцөл.
Мэдээллийн аюулгүй байдлын эрсдэл	(Risk) Компанийн мэдээлэл, мэдээллийн хөрөнгө (өгөгдөл, систем, сүлжээ, тоног төхөөрөмж)-ийн *нууцлал, бүрэн бүтэн* болон *хүртээмжтэй байдал* алдагдсанаас болж бизнесийн үйл ажиллагаа, санхүү, нэр хүнд, эсвэл хууль эрх зүйн хувьд учирч болзошгүй аливаа аюул, сул тал, эмзэг байдал, түүний нөлөөллөөс үүдэн гарах эрсдэлүүд.
Мэдээллийн хөрөнгө	(Information Assets) Компанийн өмчлөлийн болон хяналтад байгаа бүх төрлийн мэдээлэл, өгөгдөл, систем, дэд бүтэц, программ хангамж, сүлжээ, төхөөрөмжүүд.
Мэдээллийн аюулгүй байдлын менежментийн тогтолцоо	(ISMS - Information Security Management System) МАБМТ гэдэг нь компанийн менежментийн тогтолцооны мэдээллийн аюулгүй байдлыг хангах, хэрэгжүүлэх, хянах, нягтлан шалгах, дэмжих, сайжруулахын тулд хэрэгжүүлсэн үйл явцуудын цогцыг (эрсдэлийн удирдлагын хандлага дээр суурилсан)
Мэдээллийн аюулгүй байдлын зөрчил	(Security Incident) Мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмжийг зөрчих, системийн алдаа, халдлага, өгөгдөл алдагдах, хакерын үйл ажиллагаа, зөвшөөрөлгүй нэвтрэлт зэрэг аливаа аюул, эрсдэл.
Харилцагч	(Customer) Компанитай гэрээт харилцаатай боловч компанийн дотоод ажилтан биш, мэдээлэл, системд тодорхой хэмжээгээр хандах эрх бүхий түнш байгууллага, үйлчилгээ үзүүлэгч, зөвлөх.
Зөрчлийн хариу арга хэмжээ	(Incident Response) Мэдээллийн аюулгүй байдлын зөрчлийг илрүүлэх, хариу арга хэмжээ авах, сэргээн засварлах үйл явц
Эрсдэлийн удирдлага	(Risk Management) Мэдээллийн аюулгүй байдлын эрсдэлийг тодорхойлох, үнэлэх, хянах, бууруулах, урьдчилан сэргийлэх үйл явц.
Мэдээллийн аюулгүй байдлын дадал	Мэдээллийн аюулгүй байдлын дадал гэдэг нь хувь хүн эсвэл байгууллагын ажилтнуудын мэдээлэлтэй харьцах аюулгүй, хариуцлагатай, тогтсон зан үйл бөгөөд мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмжийг хангахад чиглэсэн өдөр тутмын хандлага, үйлдлүүдийг хэлдэг.
Мэдээллийн технологи	(IT - Information Technology) Байгууллагын тасралтгүй болон удирдлагын үйл ажиллагааг дэмжих зорилгоор мэдээлэл цуглуулах, боловсруулах, хадгалах, дамжуулахад ашиглагдаж буй техник хангамж, программ хангамж, сүлжээний дэд бүтэц, өгөгдлийн сан болон холбогдох үйлчилгээний цогцыг хэлнэ.
Үйлдвэрлэлийн технологи	(OT - Operational Technology) Байгууллагын физик үйлдвэрлэлийн процессыг шууд хянах, удирдах, хэмжих болон автоматжуулах зорилгоор ашиглагдаж буй тусгай зориулалтын техник хангамж, программ хангамж, хяналтын систем (үйлдвэрийн хяналтын системүүд) болон холбогдох сүлжээний нэгдлийг хэлнэ.

Сонирхогч тал	(Interested party / Stakeholder) Шийдвэр, үйл ажиллагаанд нөлөө үзүүлдэг, эсхүл түүнд нөлөөлж болохуйц хувь хүн, байгууллага.
Удирдлага	(Top management) Байгууллагыг хамгийн дээд түвшинд удирдан чиглүүлж, хянадаг хүн эсвэл хэсэг бүлэг хүмүүс. Дээд удирдлага нь байгууллагын хүрээнд эрх мэдлийг төлөөлүүлэн шилжүүлэх, нөөцөөр хангах эрхтэй
Бодлого	(Policy) Дээд удирдлагаас албан ёсоор илэрхийлсэн байгууллагын хүсэл эрмэлзэл, чиглэл.
Зорилт	(Objective) Хүрэхээр тэмүүлж буй үр дүн. Зорилт нь стратегийн эсвэл үйл ажиллагааны түвшнийх байж болно.

ГУРАВ. СОНИРХОГЧ ТАЛУУД, ТЭДНИЙ ШААРДЛАГА

3.1. Компани нь гадаад, дотоод сонирхогч талуудын МАБМТ-нд хамааралтай шаардлагыг авч үзэн, хангаж ажиллана.

Сонирхогч талуудын бүлэг	**Сонирхогч талууд**	**МАБ-ын менежментийн тогтолцоонд хамааралтай шаардлага**
Дотоод сонирхогч тал		
Ажилтан ба дотоод бүлэг	Нийт ажилтан Үйлдвэрчний эвлэл Гэрээт ажилтан Дадлагын оюутан	• Нийт ажилтанд МАБ-ын сургалт явуулах, зөрчлөөс сэргийлэх. • Ажилтны хувийн мэдээлэл хамгаалах. • Хуулийн нийцлийг хангах. • Дотоод зөрчил (авлига, хөдөлмөрийн маргаан)-с үүдэлтэй өгөгдөл алдагдах эрсдэлийг үнэлэх. • МАБ-ын зөрчил, аюул заналыг мэдээлэх. • МАБ-ын зохистой хэрэглээг хангах, хариуцах.
Удирдах ажилтан	Төлөөлөн удирдах зөвлөл (ТУЗ) Компанийн удирдлага (гүйцэтгэх захирал, нэгжийн удирдлагууд)	• МАБМТ-ны манлайллыг хангаж, амлалтаа хэрэгжүүлэх. • МАБ-ын эрсдэлийг удирдах
Гадаад сонирхогч тал		
Төрийн/ Зохицуулагч байгууллагууд	Засгийн газар “Эрдэнэс Монгол” ХХК Тагнуулын ерөнхий газар Бүх яамдууд, газар, агентлагууд (ЭХЯ, УУЭБЯ) Үндэсний аудитын газар (гэрээт аудитын газрууд) Баганаар дүүргийн ЗДТГ	• Төрийн нууц, кибер аюулгүй байдал, авлига, байгаль орчны мэдээллийг хамгаалах – Кибер аюулгүй байдлын тухай хууль, Газрын тухай хууль, Авлигын эсрэг хууль, Радио долгионы хууль, Компанийн тухай хууль зэрэгт нийцүүлэх. • Төрийн шаардлагатай мэдээлэл (тайлан, аудит) алдагдах эрсдэлийг үнэлэх, хяналт (аудит, тайлан) хийх. • Тайланг тодорхой хугацаанд, шифрлэгдсэн байдлаар илгээх

	Багануур дүүргийн Нийгмийн даатгалын газар, Дүүргийн Татварын хэлтэс, Татварын ерөнхий газар, "Багануур-Ус" ААТҮГ	• Аудит, шүүхийн шаардлагад өгөх мэдээллийг хяналттай өгөх. • Кибер халдлага, зөрчил илэрвэл холбогдох байгууллагад мэдэгдэх.
	УБТЗ ХНН	
	Бүх шатны шүүх, цагдаагийн газар, эмнэлэг	
	Кибер халдлага, зөрчилтэй тэмцэх үндэсний төв - National CSIRT байгууллага	
Харилцагч, худалдан авагчид	Амгалан ДС, ДЦС-4,3,2, Дархан ДЦС, Эрдэнэт ДЦС, “Төв чандмань ДЭХГ” ОНӨААТҮГ, Багануур ДС, Налайх ДС, “Сэлэнгэ энерго” ОНӨААТҮГ	• Гэрээнд МАБ-ын шаардлага оруулах. • Хууль тогтоомжид нийцүүлэх.
Бизнесийн түншүүд/ ханган нийлүүлэгчид	ISP байгууллагууд (Мобиком, Юнител, “УБТЗ” МОХНН , МХС ХХК)	• Интернэт үйлчилгээ, гэрээт системд хандахдаа МАБ-ын шаардлага хангах. • Үйлчилгээний түвшний гэрээний бэлэн байдлыг хангах. • Гэрээнд МАБ-ын шаардлага оруулах, нийлүүлэгчийн эрсдэлийг үнэлэх, хяналт тавих. • Компанийн нууц мэдээлэл алдагдахаас сэргийлэх.
	Гэрээт туслан гүйцэтгэгч байгууллагууд	
	Худалдан авалт, хангамжтай холбоотой оролцогч байгууллагууд	
	Бизнесийн түнш байгууллага	
	Даатгалын компаниуд	
Боловсрол, сургалтын байгууллагууд	Их дээд сургуулиуд	• Дадлагын оюутан, сургалтад оролцогчдод МАБ-ын сургалт явуулах, Нууцын баталгааг хангуулах. • Сургалт, Дадлагын үед мэдээлэлд хандахыг хязгаарлах. • Сургалтын мэдээлэл алдагдах эрсдэлийг үнэлэх.
	МСҮТ Коллеж	
	Сургалтын байгууллагууд	
	Уул уурхайн салбарын мэргэжлийн холбоод	
Олон нийт, хэвлэл мэдээлэл	Багануур дүүргийн иргэд	• Иргэд, хэвлэлд өгөх мэдээллийг нууцлалгүй хүртээмжтэй хүргэх. • Олон нийтэд нууц мэдээлэл алдагдахаас хамгаалах. • Хэвлэл мэдээллийн эрх чөлөөний тухай хуульд нийцүүлэх. • Хүний хувийн мэдээлэл алдагдахаас сэргийлэх.
	Хэвлэл мэдээллийн байгууллагууд	
	Хувьцаа эзэмшигчид	
	Ажил горилогч	

ДӨРӨВ. МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН МЕНЕЖМЕНТИЙН ТОГТОЛЦООНЫ ХАМРАХ ХҮРЭЭ

4.1. Компанийн хууль эрх зүйн, зохицуулалт, гэрээний шаардлага, сонирхогч талуудын шаардлага, бусад хүчин зүйлсийг харгалзан МАБМТ-ны хамрах хүрээг дараах байдлаар тодорхойлов:

4.1.1 Үйл ажиллагаа: Компанийн үндсэн үйл ажиллагаа болох ил уурхайн нүүрс олборлолт, боловсруулалт, ачилт, тээвэрлэлт, борлуулалтын мэдээ болон эдгээрийг удирдах, дэмжих мэдээллийн системд хадгалагдсан, боловсруулсан, дамжуулсан бүх мэдээллийг хамарна;

4.1.2 Зохион байгуулалтын нэгжүүд: МАБМТ нь компанийн гүйцэтгэх удирдлага болон нэгж (хэлтэс, алба, хэсэг)-ийн нийт ажилтан хамарна;

4.1.3 Физик байршил: Компанийн мэдээлэл боловсруулах үйл ажиллагаа явагдаж буй дараах биет байршлыг хамарна.

- Улаанбаатар хот, Багануур дүүрэг 3-р хороо, (Үйлдвэрийн хэсэг), Зип код: 12150

4.1.4 Дэд бүтэц ба мэдээллийн хөрөнгө: МАБМТ-ны хамрах хүрээнд компанийн хөрөнгийн бүртгэлд жагсаасан бүх төрлийн мэдээллийн хөрөнгө, техник хангамж, программ хангамж, өгөгдлийн сан, сүлжээний дэд бүтэц (Дата төвийн сүлжээний хадгалах төхөөрөмж, серверийн өрөө, АТС-ын өрөө болон сүлжээний зангилаа цэгүүдийн компьютерийн дотоод ба гадаад сүлжээ, шилэн кабель) болон мэдээллийн технологи, үйлдвэрлэлийн технологийн системүүд хамаарна;

ТАВ. УДИРДЛАГЫН МАНЛАЙЛАЛ БА ҮҮРЭГ АМЛАЛТ

5.1. Компанийн удирдлага нь мэдээллийн аюулгүй байдлын менежментийн тогтолцоог хэрэгжүүлэхэд бүхий л талаар дэмжин, үр дүнтэй байдлыг хангах талаар дараах байдлаар удирдан манлайлна. Үүнд:

5.1.1. МАБ-ын энэхүү бодлого, зорилтуудыг компанийн стратеги төлөвлөгөө, нөхцөл байдалтай уялдуулан боловсруулж, батална.

5.1.2. МАБМТ-ны шаардлагыг компанийн үйл явцтай нэгтгэн хэрэгжүүлэхийг баталгаажуулна.

5.1.3. МАБМТ-нд шаардлагатай нөөцийг (хүний нөөц, санхүү, технологи, мэдлэг) хангаж, хуваарилна.

5.1.4. МАБМТ-г дагаж мөрдөх, үр дүнтэй менежментийн ач холбогдлыг нийт ажилтанд мэдээлж, хариуцлагыг ухамсарлуулна.

5.1.5. МАБМТ-г төлөвлөсөн үр дүнд хүрч байгааг баталгаажуулна.

5.1.6. МАБМТ-г үр дүнтэй болгоход хувь нэмрээ оруулахыг нийт ажилтанд уриалж, дэмжлэг үзүүлэн оролцуулна.

5.1.7. МАБМТ-г төлөвлөсөн үр дүнд хүргэх талаар бүхий л арга хэмжээг авч, тасралтгүй сайжруулалтыг байнга дэмжинэ.

5.1.8. Компанийн удирдлага нь мэдээллийн аюулгүй байдлыг компанийн соёлын салшгүй хэсэг болгон төлөвшүүлж, нэгжийн удирдлагуудыг (хэлтэс, алба, хэсгийн дарга нар) өөрийн хариуцсан чиг үүргийн хүрээнд манлайлал үзүүлэх, нөөцөөр ханган дэмжиж, МАБМТ-ны үр дүнтэй байдлыг хамтын хариуцлагын зарчмаар баталгаажуулна.

5.2. Компанийн Мэдээллийн аюулгүй байдлын менежментийг хэрэгжүүлэх үүрэг хариуцлагыг дараах байдлаар хуваарилна. Үүнд:

Хариуцагч	Үүрэг
Төлөөлөн удирдах зөвлөл	МАБ-ын стратеги чиглэл өгөх, нөөц хангах, шийдвэр гаргах
Гүйцэтгэх захирал	Бодлого, журам батлах, нөөцийг хуваарилах, дүн шинжилгээ хийх
Мэдээллийн технологийн алба	ISO/IEC 27001:2022 стандартын нийцлийг хангах, МАБ-ын хяналтууд хийх, тасралтгүй сайжруулалтыг удирдах, удирдлагад тайлагнах
Захиргаа хүний нөөцийн хэлтэс	МАБ-ын хууль эрх зүйн шаардлагын нийцлийг хянах; МАБ-ын сургалт, МАБ-ын соёлыг төлөвшүүлэх, хүний нөөцийн аюулгүй байдлыг удирдах
ДХЭУ-ын алба, Мэдээллийн технологийн алба	МАБМТ-ны гүйцэтгэл, нийцлийн хяналт, дотоод аудит хийх, удирдлагад тайлагнах
Нэгжийн удирдлагууд	Өөрийн нэгжид МАБ-ын бодлого, журмыг мөрдүүлэх, Нууцын гэрээний үүргийг хангуулах
Нийт ажилтан	МАБ-ын хууль тогтоомж, бодлого, дүрэм журам, заавар мөрдөх, МАБ-ын зөрчлийг мэдээлэх

ЗУРГАА. МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН БОДЛОГО

6.1. “Багануур” ХК-ийн Мэдээллийн аюулгүй байдлын бодлого :

“Багануур” ХК нь Монгол Улсын эрчим хүчний системийн тогтвортой байдлыг хангах стратегийн үүргээ биелүүлэх, нүүрс олборлолтын үйл ажиллагааг тасралтгүй явуулахын тулд компанийн Мэдээллийн технологи болон Үйлдвэрлэлийн технологийн системийн Нууцлаг байдал, Бүрэн бүтэн байдал, Хүртээмжтэй байдлыг хангах замаар компанийн үнэ цэнэ, нэр хүнд, засаглалын тогтвортой байдлыг хамгаална.

6.2. Компанийн удирдлага нь мэдээллийн аюулгүй байдлын зорилтууд болон хууль тогтоомжийн нийцлийг хангах, мэдээллийн аюулгүй байдлын менежментийн тогтолцоог тасралтгүй сайжруулах замаар компанийн мэдээллийн хөрөнгийг хамгаалах бүх талын нөхцөл боломжийг бүрдүүлж, манлайлан ажиллана.

6.3. Энэхүү бодлого нь МАБ-ын менежментийн тогтолцооны үндэс болох бөгөөд нийт ажилтнуудад хүртээмжтэй байхаас гадна сонирхогч талуудад нээлттэй байна.

ДОЛОО. МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ЗОРИЛТ

7.1. **Бодлогыг хэрэгжүүлэх:** Компанийн хэмжээнд МАБ-ын бодлого, журам, стандартыг хэрэгжүүлэх, дотоод аудит, хяналтын механизмыг бий болгох;

7.2. **Кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, илрүүлэх, хариу арга хэмжээ авах:** Мэдээллийн систем, сүлжээний тасралтгүй, найдвартай ажиллагааг хангахын тулд эрсдэлийн үнэлгээ, аудит, хяналт үнэлгээ, шинжилгээний тогтолцоог бий болгох, кибер халдлагыг сөрөн зогсоох чадавхыг бэхжүүлэх;

7.3. **Нууцлал аюулгүй байдлыг хангах:** Шифрлэлт, тоон гарын үсэг, аюулгүй холболт зэрэг орчин үеийн шийдлүүдийг эрсдэлийн үнэлгээнд суурилан хэрэгжүүлж, мэдээллийн аюулгүй байдлыг баталгаажуулах;

7.4. **Онцгой байдлын төлөвлөлт:** Онцгой нөхцөлд мэдээллийн системийг нөхөн сэргээх, нүүлгэн шилжүүлэх төлөвлөгөөтэй байх, бизнесийн тасралтгүй ажиллагааг хангах стратеги боловсруулах, хэрэгжүүлэх;

7.5. **Олон Улсын стандарт нэвтрүүлэх:** Цаасан болон цахим мэдээллийн нууцлал, бүрэн бүтэн болон хүртээмжтэй (CIA: Confidentiality, Integrity, Availability) байдлыг хангах, Компанийн хэмжээнд ОУ-ын ISO27001:2022 МАБМТ-ны стандартыг үр дүнтэй нэвтрүүлэхэд чиглэсэн байна;

7.6. **Мэргэжлийн хүний нөөцийг бэлтгэх:** МАБ, мэдээллийн технологийн чиглэлээр өндөр түвшний мэргэшсэн, чадварлаг мэргэжилтнүүдийг бэлтгэх, тогтмол сургалтад хамруулах;

7.7. **МАБ, хамгаалалтын дэвшилтэт технологийг нэвтрүүлэх (Хиймэл оюун ухаан AI, машин сургалт ML, Их өгөгдөл Big data, Юмсын интернэт IoT гэх мэт):** МАБ-ын систем, тоног төхөөрөмжийн дэд бүтэц, орчин үеийн дэвшилтэт технологи, хамгаалалтын шийдлийг хэрэгцээ шаардлагад үндэслэн нэвтрүүлнэ;

7.8. **Хамтын ажиллагаа:** МАБ-ын чиглэлээр туршлага солилцох, дэвшилтэт технологи нэвтрүүлэх, хүний нөөц бэлтгэх, кибер халдлага зөрчлөөс урьдчилан сэргийлэх, таслан зогсоох зэрэг чиглэлээр гадаад, дотоодын байгууллага болон нэгдлийн компаниуд хоорондын хамтын ажиллагааг хөгжүүлж, бэхжүүлнэ;

Дээрх зорилтуудыг Гүйцэтгэх захирал жилд нэг удаа хянаж, шаардлагатай бол өөрчлөлт оруулна. Зорилтуудыг хэрэгжүүлэх арга хэмжээний гүйцэтгэлийг МАБМТ-ны удирдлагын дүн шинжилгээний хурлаар жил бүр хянаж, шаардлагатай тохиолдолд өөрчлөлт оруулна. “МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ЗОРИЛТОД ХҮРЭХ ТӨЛӨВЛӨГӨӨ” Хавсралт №1.

НАЙМ. БАРИМТЛАХ ЗАРЧИМ

8.1. Бодлого нь холбогдох хууль тогтоомж, стандарт, гэрээний шаардлагыг бүрэн хангасан байна.

8.2. Компанийн нэгдсэн менежментийн тогтолцооны шаардлагууд, үйл ажиллагаатай уялдсан байна.

8.3. Удирдлагын манлайллын дэмжлэгтэйгээр нийт ажилтнуудын оролцоо, хамтын ажиллагаанд суурилсан байна.

8.4. Олон улсын менежментийн арга зүй, дэвшилтэт технологи, мэргэжлийн туршлагад тулгуурлан мэдээллийн аюулгүй байдлыг хангана.

8.5. Эрсдэлд суурилсан хяналтыг хэрэгжүүлж, тасралтгүй сайжруулалтыг хийдэг байна.

8.6. Компанийн хэмжээнд МАБ-ын чиглэлээр мэдээллийн нэгдсэн, анхдагч эх үүсвэрийг бий болгож, мэдлэгийн менежментийн тогтолцоогоор дамжуулан шилдэг туршлага, дэвшилтэт технологийг нэгдлийн хэмжээнд харилцан солилцох замаар хамтын ажиллагааг бэхжүүлж, хамгаалалт, хяналтын нэгдсэн тогтолцоонд шилжинэ.

Хавсралт №1

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ЗОРИЛТОД ХҮРЭХ ТӨЛӨВЛӨГӨӨ

Д/д	Зорилтод хүрэх арга хэмжээ	Шаардлагатай нөөц	Хариуцах эзэн	Гүйцэтгэлийн түвшин /хувиар/			Үр дүнг үнэлэх арга / KPI	Хүрэх үр дүн
				2026 он	2027 он	2028 он		
1	**МАБ-ын бодлогыг хэрэгжүүлэх**							**Аюулгүй байдлын түвшин дээшилнэ** Энэхүү бодлого хэрэгжсэнээр байгууллагын мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмжтэй байдал олон улсын стандартын түвшинд хүрнэ. Системийн хяналт, аудитын давтамж нэмэгдсэнээр сул талуудыг эрт илрүүлж, урьдчилан сэргийлэх боломж бүрдэнэ. Үүний үр дүнд байгууллагын нийт эрсдэлийн түвшин буурч, мэдээллийн найдвартай хамгаалалт тогтоно.
	МТА-ны ажиллах журмыг Эрдэнэс Монгол нэгдлийн МАБ бодлого, ISO/IEC 27001:2022 стандарттай бүрэн уялдуулан мөрдүүлэх	МАБМТ-ны төслийн зөвлөх үйлчилгээний төсөв, МТА-ны инженерүүд	Гүйцэтгэх захирал, МТА-ны дарга	50%	70%	80%	Журмын нийцлийн үнэлгээ > 80% (Хуулийн нийцлийн маягт), Шинэчлэгдсэн журмуудын тоо	
	Мэдээллийн аюулгүй байдлын менежментийн тогтолцоо (ISMS)-г байгууллагын түвшинд хэрэгжүүлэх	Дотоод мэдээллийн суваг, сургалтын систем	Гүйцэтгэх захирал, МТА-ны баг, МАБМТ-ны ажлын хэсэг	50%	70%	80%	Ажилтнуудын МАБ-ын мэдлэгийн түвшин; CMMI төлөвшлийн түвшин	
	МАБ-ын эрсдэлийн үнэлгээ, эрсдэлийн бүртгэл (Risk Register) хөтлөх	Эрсдэлийн үнэлгээний аргачлал, программ хангамж	Эрсдэлийн эзэд (Нэгжийн удирдлагууд), МАБ хариуцсан ажилтан	50%	70%	80%	Эрсдэлийн бүртгэлийн шинэчлэл; Өндөр эрсдэлийн бууралтын хувь	
	Дотоод аудит, удирдлагын дүн шинжилгээг тогтмол хийх	Хараат бус аудитын баг, хурлын протоколын сан	ДХЭУ-ын алба, компанийн МАБ-ын дотоод аудиторууд	50%	70%	80%	Аудитын дүгнэлтийн дагуу хийгдсэн залруулах арга хэмжээний биелэлт	
	МАБ-ын бодлогын хэрэгжилтийг жил бүр тайлагнах	KPI мониторингийн өгөгдөл, тайлангийн загвар	МТА-ны дарга	50%	70%	80%	ТУЗ-өөр хэлэлцүүлсэн тайлан; Сонирхогч талуудын сэтгэл ханамж	
2	**Кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, илрүүлэх, хариу арга хэмжээ авах**							**Кибер халдлага, өгөгдөл алдагдах эрсдэл буурна** Тогтмол эрсдэлийн үнэлгээ болон эмзэг
	Сүлжээ, сервер, системийн логийг төвлөрүүлэн хянах мониторингийн тогтолцоо бий болгох	SIEM программ хангамж, хадгалах төхөөрөмж,	МТА-ны дарга, Системийн зохицуулагч, Сүлжээний	30%	50%	80%	Лог цуглуулалтын хамрах хүрээ 100%; Сэжигтэй үйлдлийг мэдээлэх хугацаа (MTTD) < 30 минут	

			инженер					байдлын шалгалтыг хийснээр халдлагын гол замуудыг илрүүлж, хамгаалалтыг сайжруулахад түлхэц болох бөгөөд хортой код, программ хангамж, хуурамч хандалт /ransomware, phishing/ зэрэг халдлагын төрлүүдийг эрт илрүүлэх хамгаалалтын шийдлүүд, сүлжээний хамгаалалтын аргуудыг хэрэглэж кибер халдлагад өртөх, өгөгдөл алдагдахаас хамгаална. Ингэснээр байгууллага мэдээлэл алдах, үйл ажиллагаа доголдох, гаднын халдлагын улмаас санхүүгийн болон нэгдлийн нэр хүнд унах эрсдэлийг бууруулах боломжтой. Мөн мэдээлэл алдагдсанаас үүсэх шууд зардлуудыг хэмнэх боломжтой /нөөцийг сэргээх, үйл ажиллагаа доголдох гэх мэт/
	Penetration test, эмзэг байдлын үнэлгээг жил бүр зохион байгуулах	МАБМТ-ны төслийн төсөв,	МТА-ны дарга, Системийн зохицуулагч	30%	50%	80%	Илэрсэн өндөр эрсдэлтэй эмзэг байдлын засварлалтын хувь = 100%; Аудитын тайлан баталгаажсан байх	
	Кибер инцидент илрүүлэх, мэдээлэх, хариу арга хэмжээ авах журам хэрэгжүүлэх	Зөрчлийн удирдлагын журам, мэдээлэх суваг (холбогдох дугаар утас, имэйл), багийн сургалт	МТА-ны дарга, Зөрчлийн хариу арга хэмжээний баг	30%	50%	80%	Зөрчлийг шийдвэрлэх дундаж хугацаа (MTTR); Жил бүрийн зөрчлийн нэгдсэн тайлангийн чанар	
	Антивирус, firewall, endpoint хамгаалалтыг сайжруулах	Нээлттэй эх болон лицензтэй программ хангамж, Next-Gen Firewall шинэчлэл.	Системийн зохицуулагч, Сүлжээний инженер, Техник хангамжийн инженер.	30%	50%	80%	Хортой кодоос хамгаалагдсан төхөөрөмжийн хувь 100%; Зөвшөөрөлгүй хандалтын оролдлого хаагдсан тоо	
3	**Нууцлал аюулгүй байдлыг хангах**							
	Мэдээллийг нууцлал–хүртээмж–бүрэн бүтэн байдлаар ангилах	Мэдээллийн хөрөнгийн бүртгэл (Asset Inventory), ангиллын зааварчилгаа, шошгожуулах хэрэгсэл.	Мэдээлэл эзэмшигч (нэгжийн удирдлагууд), МАБ хариуцсан ажилтан.	20%	40%	60%	Бүртгэгдсэн нийт мэдээллийн хөрөнгийн ангилагдсан байдлын хувь = 100%	
	Шифрлэлт, MFA, VPN, аюулгүй холболтын шийдлүүд нэвтрүүлэх	MFA, VPN систем, шифрлэлтийн түлхүүр удирдлагын шийдэл.	МТА-ны дарга, Системийн зохицуулагч, Программын инженер	20%	40%	60%	Критик системд MFA нэвтрүүлсэн хувь = 100%; Зөвшөөрөлгүй хандалтын оролдлого илрүүлсэн тоо.	
4	**Онцгой байдлын төлөвлөлт**							

	Үйлдвэрлэлийн тасралтгүй ажиллагаа (BCP), сэргээн босголтын (DR) төлөвлөгөө боловсруулах	Бизнесийн нөлөөллийн шинжилгээ (BIA) аргачлал, удирдлагын дэмжлэг, мэргэжлийн зөвлөх үйлчилгээ.	Гүйцэтгэх захирал, МТА-ны дарга	30%	50%	80%	Батлагдсан BCP/DRP төлөвлөгөө; Критик системийн RTO < 4 цаг, RPO < 1 цаг байх	**Хууль эрх зүй, стандартын нийцэл сайжирна** Монгол Улсын Кибер аюулгүй байдлын тухай хууль, Төрийн болон албаны нууцын тухай хууль, Хувийн мэдээлэл хамгаалах тухай хууль зэрэг холбогдох хууль тогтоомжтой нийцсэн, ISO/IEC 27001:2022 стандартын шаардлага хангасан байгууллагын мэдээллийн аюулгүй байдлын менежментийн тогтолцоог үйл ажиллагаандаа нэвтрүүлснээр нэгдлийн мэдээллийн аюулгүй байдлын түвшин олон улсын хэмжээнд баталгаажиж шинэ шатанд гарах нөхцөл бүрдэнэ.
	Нөөц дата, нөөц холбооны сувгийг бэлэн байлгах	Нөөц дата төвийн техник, нөөц холбооны суваг (Satellite/Radio), радио холбооны төхөөрөмж.	МТА-ны дарга, Системийн зохицуулагч, Т/Х-ийн инженер, Сүлжээ, Холбооны инженер.	30%	50%	80%	Нөөц дэд бүтцийн бэлэн байдлын хувь > 99.9%; Нөөцлөлтийн амжилтын хувь (сар бүр)	
	Сэргээх туршилт, сургалт хийх	Туршилтын орчин, дадлага сургуулилтын төлөвлөгөө, сургалтын материал.	МТА-ны дарга, МТА-ны ИТА нар.	30%	50%	80%	DR Туршилтын тайлан; Ажилтнуудын онцгой байдлын бэлэн байдлын үнэлгээ	
5	**Олон Улсын стандарт нэвтрүүлэх**							
	ISO/IEC 27001:2022 стандартын gap analysis хийх	МАБМТ-ны төслийн төсөв, мэргэшсэн зөвлөх үйлчилгээ, MNS ISO/IEC 27001:2023, ОУ-ын ISO/IEC 27001:2022 стандарт	МТА-ны баг, МАБМТ-ны ажлын хэсэг	50%	70%	80%	Батлагдсан "Зөрүүний шинжилгээний тайлан" (Gap Analysis Report).	
	Баримт бичгийн багц бүрдүүлэх	ISO 27001:2022 Toolkit загвар файлууд, дотоод нэгжүүдийн оролцоо	Нэгжийн удирдлагууд.	50%	70%	80%	Батлагдсан баримт бичгийн нийцлийн хувь (100%); Хэрэглэх тухай мэдэгдэл (SoA)	

	Үе шаттай нэвтрүүлэх төлөвлөгөө хэрэгжүүлэх	Ажилтнуудын ажлын цаг, Техникийн хяналтын механизм нэвтрүүлэх, үндсэн хөрөнгө оруулалт ба үйл ажиллагааны зардал	Гүйцэтгэх захирал, МТА.	50%	70%	80%	Дотоод аудитын дүн; МАБМТ-ны төлөвшлийн түвшин (CMMI) (Зорилтот түвшин: 3-4)	**Хүний нөөцийн мэдлэг, чадавх дээшилнэ:** Байнгын сургалт, мэдлэгийн үнэлгээ, дотоод аудит нь ажилтнуудын мэдээллийн аюулгүй байдлын талаарх мэдлэгийг системтэйгээр дээшлүүлж цэвэр ширээ/дэлгэцийн бодлого, нууцлал хадгалах дадал, фишинг таних чадвар зэрэг нь ажилтан төдийгүй байгууллагын өдөр тутмын соёл болж төлөвшинө. Үүний үр дүнд ажилтнууд зөрчил үүсгэх магадлал эрс багасаж, байгууллагын хамгаалалтын хамгийн чухал хэсэг болох “хүний хүчин зүйл”-ийн чадавх бэхэжнэ. **Технологийн шинэчлэл хийгдэнэ:** Дараа үеийн мэдээллийн аюулгүй байдлын систем, үүлэн технологи, хиймэл оюун ухаан, машин сургалт гэх мэт
6	**Мэргэжлийн хүний нөөцийн бэлтгэл**							
	МАБ, кибер аюулгүй байдлын сургалтыг тогтмол зохион байгуулах	Сургалтын платформ, гарын авлага, зөвлөмж, сургалтын төсөв	Захиргаа хүний нөөцийн хэлтэс, МТА	20%	50%	70%	Ажилтнуудын сургалтын хамрагдалт > 95%	
	Фишинг тест, мэдлэгийн үнэлгээ хийх	Фишинг симулятор программ, тестийн асуулгын сан	Захиргаа хүний нөөцийн хэлтэс, МТА	20%	50%	70%	Тестийн дундаж оноо > 80%; Фишинг халдлагад өртөх магдлалтай ажилтны хувь буурсан байх	
	Дотоод мэргэжилтэн бэлтгэх	Мэргэшүүлэх сургалтын төсөв, гэрчилгээний шалгалтын зардал.	Гүйцэтгэх захирал, ЗХНХ, МТА-ны дарга	20%	50%	70%	Гэрчилгээжсэн дотоод мэргэжилтний тоо (Зорилтот түвшин: 3-5 ажилтан).	
7	**Мэдээллийн аюулгүй байдал, хамгаалалтын дэвшилтэт технологийг нэвтрүүлсэн байдал (Хиймэл оюун ухаан AI, машин сургалт ML, Их өгөгдөл Big data, Юмсын интернэт IoT гэх мэт)**							
	AI, ML-д суурилсан илрүүлэлтийн шийдэл судлах	МТА-ны техникийн өгөгдөл, салбарын судалгааны материал, Судалгааны баг, хөндлөнгийн технологийн зөвлөх үйлчилгээ, Лабораторийн орчин, тест өгөгдлийн багц, туршилтын лиценз, (NDR - Network Detection and Response)	МТА-ны дарга, МТА-ны ИТА нар, Зөвлөх баг.	20%	40%	60%	Батлагдсан Техникийн даалгавар, Техник эдийн засгийн үндэслэл, POC (Proof of Concept) үр дүнгийн тайлан	

	Камер + AI ашиглан суурь судалгаа	AI дэмждэг Хяналтын камерын систем, хөндлөнгийн технологийн зөвлөх.	МТА-ны дарга, П/Х-ийн инженер, Т/Х-ийн инженер, Сүлжээ, Холбооны инженер.	20%	40%	60%	Зөвшөөрөлгүй биет нэвтрэлтийг илрүүлсэн нарийвчлал > 95%.	өндөр технологид суурилсан халдлага илрүүлэх систем нэвтрүүлэн сэжигтэй үйлдлийг шуурхай илрүүлж, урьдчилан сэргийлэх, их өгөгдлийн урсгалаас хэвийн бус зан үйлдэл, халдлагын ул мөрийг нарийн тооцоолох, юмсын интернэтийн шинэ шийдлүүд ашиглан уул уурхай, үйлдвэрлэлийн шатанд урьдчилан сэргийлэх, аюулгүй ажиллагааг хангаж ажилласанаар кибер халдлага болон зөрчлийг илрүүлэх хурд, нарийвчлал нэмэгдэж, мэдээллийн хамгаалалт илүү найдвартай болно.
	IoT орчны аюулгүй байдлыг хангах	IoT аюулгүй байдлын галт хана, төхөөрөмжийн бүртгэлийн систем.	МТА-ны дарга, БТС-ийн инженер	20%	40%	60%	IoT төхөөрөмжөөс үүдэлтэй зөрчлийн тоо = 0; Үйлдвэрлэлийн системийн хэвийн ажиллагаа (Uptime) > 99.9%.	
8	**Хамтын ажиллагаа**							
	Нэгдлийн компаниудтай туршлага солилцо	Хамтын ажиллагааны санамж бичиг, томилолтын зардал.	Гүйцэтгэх захирал, ЗХНХ, МТА-ны дарга	20%	30%	40%	Хамтын ажиллагааны уулзалтын тоо (жилд 2-оос доошгүй); Нэгдлээс авсан зөвлөмжийн хэрэгжилтийн хувь.	
	Мэргэжлийн байгууллагатай хамтарсан сургалт зохион байгуулах	Сургалтын төсөв, мэргэшсэн сургагч багш нар, лабораторийн орчин.	ЗХНХ, МТА	20%	30%	40%	Хамтарсан сургалт, дадлагад хамрагдсан ажилтны тоо; Сургалтын дараах ур чадварын ахиц (> 20%).	
	Кибер дасгал, хамтарсан арга хэмжээ хэрэгжүүлэх	Дасгал сургуулилтын техник орчин, зөрчил илрүүлэх системүүд	МТА-ны дарга	20%	30%	40%	Кибер дасгалын үр дүнгийн тайлан; Зөрчилд хариу үзүүлэх дундаж хугацаа (MTTR) буурсан үзүүлэлт.	

Тайлбар: CMMI (Capability Maturity Model Integratoion) Системийн үйл ажиллагааны боловсронгуй байдал, чадавхыг үнэлэх төлөвшлийн загварын 5 түвшин. • **1** - Анхан шат (Initial): Үйл ажиллагааны хэрэгжилт тогтворгүй, системтэй бус, ихэвчлэн зохион байгуулалтгүй. Тогтолцооны бодлого, хяналт хангалтгүй, осол, эрсдэлийг удирдах үйл явц дутмаг. • **2** - Удирдлагатай (Managed): Системийн зарим хэсэг төлөвлөгдөж, хэрэгжиж эхэлсэн ч бүрэн бус. Зарим бодлого, үйл ажиллагаа, хяналт бий боловч тогтвортой бус. • **3** - Тодорхойлогдсон (Defined): Үйл явц тодорхойлогдож, байгууллагын хэмжээнд стандартчилагдсан. Технологи, аюулгүй байдлын бодлого, хяналт үйл ажиллагаа тогтвортой хэрэгждэг. • **4** -Удирдлага, хяналттай (Quantitatively Managed): Үйл ажиллагаа бүрэн хяналттай, тоон үзүүлэлтэд суурилсан удирдлагаар хэрэгждэг. Гүйцэтгэлийг хэмжиж чаддаг, сайжруулалт тогтмол хийгддэг. • **5 -** Оновчлогдсон (Optimized): Тогтолцоо бүрэн боловсронгуй, тасралтгүй сайжруулалттай, бүх талын (хүн, баримт бичиг, үйл явц, технологи) хамрах хүрээтэй. Эрсдэлийг бүрэн хянаж, урьдчилан сэргийлдэг, үйл ажиллагаа бүрэн тогтвортой, найдваржилт өндөр. Эдгээр түвшин нь байгууллагын мэдээллийн технологийн болон мэдээллийн аюулгүй байдлын удирдлагын хэрэгжилтийн боловсронгуй байдлыг харуулдаг бөгөөд хүн, баримт бичиг, үйл явц, технологи гэсэн дөрвөн талын амжилтын хүчин зүйлд суурилна.