“Сэнд Эм Эн ББСБ” ХХК-ийн
ТУЗ-ийн хурлын ..... тоот
тогтоолын хавсралт

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН БОДЛОГО

2026

1. ТАНИЛЦУУЛГА

1.1 “Сэнд Эм Эн ББСБ” ХХК /Цаашид “Сэнд Эм Эн” гэх/ нь “Санхүүгийн Зохицуулах Хороо”-оос авсан “Зээл”, “Валют арилжаа”, “Цахим төлбөр тооцоо, Мөнгөн гуйвуулга”, “Итгэлцэл”-н тусгай зөвшөөрлийн хүрээнд үйл ажиллагаагаа явуулдаг Олон улсын мөнгөн гуйвуулгын финтек компани.

2019 оноос уламжлалт мөнгөн гуйвуулгын үйлчилгээг орчин үеийн мэдээллийн технологийн шийдэлтэй хослуулан “SendMN” аппликейшн зах зээлд нэвтрүүлэн ажиллаж байна.

Финтек компанийн хувьд Сэнд Эм Эн нь харилцагч, хамтран ажиллагчдын болон үйл ажиллагааны онцлогоос хамаарч маш их мэдээ мэдээллийг цуглуулж, хадгалж, дамжуулж, боловсруулж ажиллдаг.

2025 оноос компанийн үйл ажиллагаандаа “Мэдээллийн аюулгүй байдлын менежментийн тогтолцоо”/МАБМТ/-ны, ISO/IEC27001:2022 стандартыг амжилттай нэвтрүүлэн, хэрэгжүүлж байна.

2. МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН БОДЛОГО

2.1 Ерөнхий заалт

“Сэнд Эм Эн ББСБ” ХХК нь мэдээллийн хөрөнгийн нууцлал, бүрэн бүтэн байдал, хүртээмжтэй байдлыг хангах зорилгоор мэдээллийн аюулгүй байдлын удирдлагын тогтолцоог хэрэгжүүлнэ. Энэхүү бодлого нь компанийн мэдээллийн аюулгүй байдлыг хангах үндсэн зарчим, чиглэл, хариуцлага, хамрах хүрээг тодорхойлох дээд түвшний баримт бичиг болно.

2.2 Зорилго

2.2.1 Компанийн мэдээллийн аюулгүй байдлын удирдлагын тогтолцоог ISO/IEC 27001:2022 стандарт, холбогдох хууль тогтоомж, гэрээний шаардлагад нийцүүлэн хэрэгжүүлэх;

2.2.2 Компанийн үйл ажиллагаанд ашиглагдаж буй бүх мэдээлэл, өгөгдөл, баримт бичиг, систем, тоног төхөөрөмж, програм хангамж болон бусад биет болон биет бус хөрөнгийг мэдээллийн хөрөнгө гэж үзэж хамгаалах;

2.2.3 Мэдээллийн аюулгүй байдлын эрсдэлийг тогтмол тодорхойлж, үнэлж, бууруулах арга хэмжээг хэрэгжүүлэх;

2.2.4 Мэдээллийн хөрөнгийн дараах үндсэн зарчмыг хангах:

- **Нууцлал** – мэдээлэлд зөвхөн эрх бүхий этгээд хандах;
- **Бүрэн бүтэн байдал** – мэдээллийг зөвшөөрөлгүй өөрчлөх, устгах, гэмтээхээс хамгаалах;
- **Хүртээмжтэй байдал** – шаардлагатай мэдээлэл, системийг зөвшөөрөгдсөн хэрэглэгч хэрэгцээт үедээ ашиглах боломжтой байлгах;

2.2.5 Ажилтнуудын мэдээллийн аюулгүй байдлын мэдлэг, хариуцлага, ёс зүйг нэмэгдүүлж, компанийн хэмжээнд мэдээллийн аюулгүй байдлын соёлыг төлөвшүүлэх.

2.3 Хамрах хүрээ

Энэхүү бодлого нь “Сэнд Эм Эн ББСБ” ХХК-ийн бүх алба нэгж, ажилтан, гэрээт ажилтан, зөвлөх, ханган нийлүүлэгч, үйлчилгээ үзүүлэгч, хамтран ажиллагч партнер байгууллага болон компанийн мэдээллийн хөрөнгөд хандах эрх бүхий гуравдагч этгээдэд хамаарна.

Бодлого нь дараах хүрээнд үйлчилнэ:

2.3.1 Компанийн бүх физик байршил, салбар, оффис;

2.3.2 Компанийн үндсэн систем, API холболт, санхүүгийн систем, CRM, сүлжээний төхөөрөмж, ажилтны компьютер, POS төхөөрөмж, үүлэн орчин, домэйн, цахим шуудан болон бусад мэдээллийн технологийн систем;

2.3.3 Хувийн мэдээлэл, санхүүгийн мэдээлэл, харилцагчийн мэдээлэл, нууц мэдээлэл, оюуны өмч болон компанийн үйл ажиллагаатай холбоотой бусад бүх мэдээлэл;

2.3.4 Мэдээллийн хөрөнгийн удирдлага, эрсдэлийн удирдлага, зөрчлийн удирдлага, хандалтын хяналт, бизнесийн тасралтгүй байдал, аудит, мониторингийн үйл ажиллагаа.

2.4 Орхилт

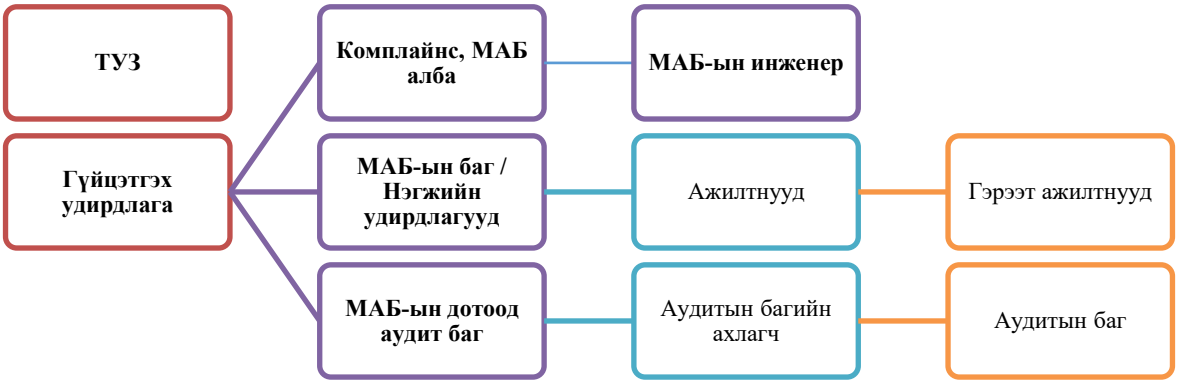
ISO/IEC 27001:2022 стандартын шаардлагын хүрээнд аль нэг бүлэг, дэд бүлгийг орхигдуулаагүй. Хавсралт А-ийн хяналтуудыг Нийцлийн тунхаглалд тусгасны дагуу хэрэгжүүлнэ..

3. МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ЗОХИОН БАЙГУУЛАЛТ

3.1 Компанийн мэдээллийн аюулгүй байдлын зохион байгуулалт дараах зорилготой. Үүнд:

- Мэдээллийн аюулгүй байдлын менежментийн тогтоолцоог манлайлах, хэрэгжүүлэх, хянах,
- Компанийн хөрөнгийг зөвшөөрөлгүй, зүй бусаар ашиглах боломжийг багасгах,
- Мэдээллийн хөрөнгийн нууцлал, бүрэн бүтэн, хүртээмжтэй байдлыг хангах,
- Ашиг сонирхлын болон эрх бүхий байгууллагуудтай компанийг төлөөлж харилцах эрхтэй ажлын байруудыг тодорхойлох юм.

3.2 Компанийн МАБУТ-н бүтцийн зураглал



Зураг 2. Компанийн мэдээллийн аюулгүй байдлын бүтцийн зураглал

4. МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ОРЧИН

4.1 Сэнд Эм Эн нь өөрийн МАБ-ын зорилго, зорьсон үр дүнд хүрэхэд нөлөөлж болох дотоод болон гадаад орчинг “SWOT”, “PESTLE” шинжилгээний аргуудаар тодорхойлж, гүйцэтгэх удирдлагаар батлуулна.

5. МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ҮҮРЭГ ХАРИУЦЛАГА

5.1 Төлөөлөн удирдах зөвлөл

ТУЗ нь компанийн мэдээллийн аюулгүй байдлын бодлогыг батлах, мэдээллийн аюулгүй байдлын хэрэгжилтэд хяналт тавих, мэдээллийн аюулгүй байдлыг хэрэгжүүлэхэд шаардлагатай бодлогын дэмжлэг үзүүлнэ.

5.2 Гүйцэтгэх удирдлага

Гүйцэтгэх удирдлагын баг нь "Гүйцэтгэх захирал", "Мэдээллийн технологи хариуцсан захирал", "Санхүү хариуцсан захирал" гэсэн бүрэлдэхүүнтэй байна.

Гүйцэтгэх удирдлагын баг нь МАБМТ-ны засаглалын үйл ажиллагааг удирдан зохион байгуулах дээд баг бөгөөд компанийн үйл ажиллагааны стратеги төлөвлөгөөний чиглэлтэй нийцүүлэн МАБ-ын бодлого, зорилт, хамрах хүрээг тодорхойлох, тэдгээрийн хэрэгжилтийн үр дүнг шалгах;

МАБМТ-г бий болгох, хэрэгжүүлэх, хянах, хадгалах, сайжруулахад хангалттай нөөцөөр хангах;

МАБ-ын дотоод аудитыг томилох, дотоод аудитаар илэрсэн бүх зөрчлүүдийг холбогдох оролцогч талууд цаг тухайд нь засч, хаасан эсэхийг баталгаажуулах;

Эрсдэлийн үнэлгээний тайлан, эрсдэлийг бууруулах төлөвлөгөө, үлдэгдэл эрсдэлийг батлах, компанид эрсдэлд суурилсан соёлыг сурталчлах;

5.3 Мэдээллийн аюулгүй байдлын баг

МАБ-ын баг нь Санхүү, МТ, комплаенс, ХҮТ, Бизнес хөгжлийн албадын удирдлагуудаас бүрдсэн баг байна.

МАБ-ын баг нь МАБМТ-той холбоотой арга хэмжээг хариуцсан нэгжийн ажилтнуудад цаг алдалгүй мэдээлэх, бодлого журмыг хэрэгжүүлэх, сурталчлан таниулах, компанийн МАБ-ын эрсдэлийн үнэлгээг хийж гүйцэтгэх удирдлагын багт мэдээлэх үүрэгтэй.

5.4 Салбар, алба нэгжийн удирдлага

Компанийн салбар, алба нэгжийн удирдлага нь МАБ-ын хүрээнд дараах үүрэгтэй:

- МАБ-ын холбогдох арга хэмжээг хариуцсан нэгждээ хэрэгжүүлэх;
- Компаниас явуулж буй сургалт, хөтөлбөрт нэгжийн нийт ажилтануудыг хамруулах;
- МАБ-ын багийн зааварын дагуу эрсдэлийн үнэлгээний удирдлагыг хэрэгжүүлэх;
- МАБ-ын бодлого, журмыг алба нэгжийн ажилтнуудад мөрдүүлэх;
- Баримт бичгийг үүсгэх, хувилбар гаргах, хянах, ангилах;
- Бүртгэл үүсгэх, хадгалах, устгах;
- Хөрөнгийн удирдлага;
- Тогтмол хандах эрхийн хяналт шалгалт хийх (нэвтрэх эрх олгох, цуцлах)
- Доголдол, зөрчлийн талаар мэдээлэх,
- Тасралтгүй байдал, гамшгийн нөхөн сэргээлт;
- МАБМТ-д дотоод болон гаднын байгууллагаас хийж буй хяналт шалгалтыг дэмжиж ажиллах, оролцогчийг баталгаажуулах;
- Аудитаар илэрсэн бүх үл нийцлүүдийг төлөвлөгөөт хугацаанд нь үр дүнтэй залруулж хаах үйл явцыг баталгаажуулах;

5.5 Ажилтнууд болон ажилтан бус хүмүүс

Ажилтнууд гэдэгт компантай гэрээний үндсэн дээр хамтран ажиллаж байгаа үндсэн, цагийн, болон түр ажилтнуудыг хамруулна.

Ажилтан бус хүмүүс гэдэгт гэрээт ажилтнуудаас бусад компанийн мэдээлэл, өгөгдөл, мэдээллийн системд хандах эрх олгосон дадлагажигч, зөвлөх, бизнесийн хамтрагчид, түншүүд, зохицуулагч байгууллагын ажилтнууд, аутсорсингийн үйлчилгээ үзүүлэгчийн ажилтнууд болно. Компанийн ажилтан болон ажилтан бус хүмүүс нь дараах үүрэг хариуцлагатай.

- Өөрийн өдөр тутмын ажил үүргээ компаниас батласан МАБ-ын бүх бодлого, журам, зааврын шаардлагын дагуу хийж гүйцэтгэх;
- Хариуцаж буй мэдээллийн хөрөнгө, өгөгдлийг тодорхойлж, МАБ-ын бодлого журмын дагуу баримт бичгийг боловсруулах, ангилах, хадгалах, дамжуулах, бүртгэл үүсгэх;
- МАБ-ын эрсдэлийг тодорхойлох, удирдах ажилтанаас өгсөн заавар, шаардлагын дагуу эрсдлийг бууруулах арга хэмжээг цаг тухайд нь хэрэгжүүлэх;
- Эрсдэл гарах магадлал болон нөлөөлөлийг бууруулах зорилгоор авч хэрэгжүүлсэн арга хэмжээний үр дүнгийн талаар хэлтэс нэгжийн удирдлага болон МАБ-ын багт мэдээлэх.
- Компанийн дотоод хяналт шалгалт, ба хөндлөнгийн баталгаажуулалтын аудитад оролцох, нэгжийг төлөөлөх;
- Хяналт болон аудитын явцад илэрсэн бүх үл нийцлийг залруулах арга хэмжээг хэрэгжүүлэх, үр дүнг салбар, нэгжийн удирдлага болон МАБ-ын багт мэдээлэх;
- Компанийн үйл ажиллагаанд тохиолдсон зөрчлийг мэдээллэх;
- Компаниас зохион байгуулж буй МАБ-н сургалтад хамрагдах;

5.6 Дотоод аудитын баг

МАБУТ-ын дотоод аудитын баг нь аудиторууд болон аудитын багийн ахлагчаас бүрдэнэ. Аудитын багийн ахлагч нь аудиторын бүх үүрэг, хариуцлагыг гүйцэтгэх боловч доор тодорхойлсон нэмэлт үүрэг хариуцлага хүлээх болно.

- МАБМТ-ын үйл явц, хамрах хүрээ, хил хязгаар, дотоод аудитын хөтөлбөр, хуанли дээр үндэслэн аудитыг төлөвлөх;
- Дотоод аудиторын аудит хийхэд шаардагдах ур чадвар, мэдлэгийг баталгаажуулах;
- Ярилцлага, баримт бичиг, ажиглалтын аргаар дотоод аудит хийх;
- Аудитын явцад тохирол, хазайлт, үл нийцэл, сайжруулах талбарыг тодорхойлох;
- Аудитын дүгнэлтийг зохих бодитой нотлох баримт, жишээ, дэлгэрэнгүй мэдээллээр дэмжих, бичиг баримтуудыг цуглуулах;
- Аудитын үр дүнг МАБ-ын баг болон дээд удирдлагад мэдээлэх;
- Аудит дууссаны дараа нэгжүүдийн авах арга хэмжээ, үр дүнтэй байдлыг хангахын тулд хэрэгжүүлсэн арга хэмжээг шалгах;
- Удирдлагын дүн шинжилгээний хурлын үеэр аудитын үр дүн, төлөвлөсөн арга хэмжээ, тэдгээрийг засах, үр дүнтэй байдлын талаар гүйцэтгэх удирдлагад мэдээлэх.
- Дотоод аудитын багийн ахлагч нь дотоод аудиторуудын багийг сонгох;
- Төлөвлөгөөний талаар МАБ-ийн баг, нэгжийн удирдлага нар болон аудит хийлгэж буй хүмүүст хүргэхэд туслах;
- Аудитын үеэр нээлтийн хурал, танилцуулга, хаалтын хурлыг удирдан явуулах;
- Аудитын явцад аудит хийлгэж буй хүмүүс болон аудиторуудаас ирсэн аливаа асуудал, хүсэлтийг шийдвэрлэх;
- Багийн дотор санал зөрөлдөөн гарсан тохиолдолд асуудлыг шийдэж, зөвшилцөлд хүрэх арга хэмжээ авна.

5.7 Гадаад ханган нийлүүлэгчид

Гадны ханган нийлүүлэгчид гэдэгт компанид зөвлөх болон аутсорсинг үйлчилгээ үзүүлэгч, гэрээлэгч, эсвэл бараа бүтээгдэхүүн, засвар үйлчилгээ үзүүлдэг аливаа гуравдагч этгээдүүд болно. Ханган нийлүүлэгчид нь дараах үүрэгтэй.

- Компанид ажил үйлчилгээ нийлүүлэхдээ компанийн МАБ-ын бодлого, журамтай танилцаж, дагаж мөрдөх, ажил үйлчилгээний гэрээний шаардлагуудыг дагаж мөрдөх,
- Компанид санал болгож буй үйлчилгээг гүйцэтгэхдээ туслан гүйцэтгэгч эсвэл аутсорсинг авч байгаа тухай мэдэгдэх;
- Ажил үйлчилгээтэй холбоотой боломжит эрсдэлийг тодорхойлох, эрсдэлийг бууруулах зорилгоор хэрэгжүүлж болох техникийн болон үйл ажиллагааны талаар мэдээлэл өгөх;
- Техникийн сул тал, үйл явдал, зөрчил, доголдол, түүний дотор аюулгүй байдлын зөрчлүүдийг илрүүлсэн эсвэл мэдсэн тохиолдолд компанид цаг тухайд нь мэдээлэх;
- Компанийн эзэмшиж буй мэдээлэл, мэдээллийн хөрөнгө, мэдээлэл боловсруулах хэрэгсэл, мэдээллийн систем гэх мэт зүйлсэд хандах зайлшгүй шаардлагатай тохиолдолд зөвшөөрөл авах, МАБ-ын заавар, бодлого, дүрэмд нийцүүлэн ажиллах;
- Компанид хамаарах мэдээлэл, өгөгдөлтэй харьцах, хадгалах, хуваалцах, задруулах, устгах явцад шаардлагатай зөвшөөрлийг авч баталгаажуулах;

6. ЭРСДЭЛИЙН УДИРДЛАГА

Компани мэдээллийн аюулгүй байдлын эрсдэлийг мэдээллийн хөрөнгийн нууцлал, бүрэн бүтэн, хүртээмжтэй байдалд нөлөөлж болзошгүй үндсэн хүчин зүйл гэж үзэж, эрсдэлд суурилсан мэдээллийн аюулгүй байдлын удирдлагын зарчмыг баримтална. Мэдээллийн аюулгүй байдлын эрсдэлийн удирдлага нь бизнесийн үйл ажиллагаа, мэдээллийн хөрөнгө, мэдээллийн систем, хууль зохицуулалтын шаардлага, гуравдагч талын хамаарал болон технологийн орчинтой уялдсан байна. Компани мэдээллийн аюулгүй байдлын эрсдэлийг хүлээн зөвшөөрөх боломжит түвшинд байлгах зорилгоор зохистой хяналт, хамгаалалт, удирдлагын орчныг бүрдүүлнэ.

7. НИЙЦЛИЙН БОДЛОГО

Компани мэдээллийн аюулгүй байдал болон бизнесийн үйл ажиллагаагаа холбогдох хууль тогтоомж, зохицуулалтын шаардлага, стандарт, болон гэрээний үүрэгт нийцүүлэн хэрэгжүүлнэ. Мэдээллийн аюулгүй байдлын нийцэл нь компанийн бодлого, журам, процесс, гэрээний харилцаа болон гуравдагч талын удирдлагын салшгүй хэсэг байна. Компани нийцлийн шаардлагыг зөрчихөөс урьдчилан сэргийлэх, нийцлийн түвшинг хадгалах, шаардлагатай тохиолдолд сайжруулах хяналттай орчныг бүрдүүлнэ.

8. ХУВИЙН НУУЦ ХАМГААЛАХ БОДЛОГО

Компани бизнесийн үйл ажиллагаандаа ашиглаж буй хүний хувийн мэдээллийг холбогдох хууль тогтоомж, зохицуулалтын шаардлага, стандарт, гэрээний үүрэг болон мэдээллийн аюулгүй байдлын зохих хяналтад нийцүүлэн цуглуулж, боловсруулж, хадгалж, дамжуулж, устгана. Компани хувийн мэдээлэлд зөвшөөрөлгүй хандах, өөрчлөх, задруулах, алдагдуулах, бууруулаар ашиглахаас урьдчилан сэргийлэх хамгаалалттай орчныг бүрдүүлнэ. Хувийн мэдээллийн зөрчил, эрсдэл илэрсэн тохиолдолд компанийн мэдээллийн аюулгүй байдлын зөрчлийн удирдлагын зарчмын дагуу хариу арга хэмжээ авна.

9. БАРИМТ БИЧИГ БҮРТГЭЛ ХЯНАЛТЫН БОДЛОГО

Компани өөрийн үйл ажиллагаа, мэдээллийн аюулгүй байдал болон бизнесийн тасралтгүй байдалд хамаарах баримт бичиг, бүртгэлийг зохих хууль, журам, стандартын дагуу бүрдүүлж, баталгаажуулж, үнэн зөв, бүрэн бүтэн, нууцлалтай, болон хүртээмжтэй байдлыг хангана. Баримт бичиг, бүртгэл, бичлэгийг хууль тогтоомж, зохицуулалт, гэрээний үүрэг болон компанийн дотоод шаардлагад нийцсэн, хяналттай, хамгаалагдсан орчинд хадгална. Компани баримт бичиг, бүртгэл, бичлэгт зохих ангилал, нууцлал, хандалтын зарчмыг хэрэгжүүлж, зөвшөөрөлгүй өөрчлөлт, ашиглалт, задрал, алдагдал, устгалаас хамгаална.

10. СУРГАЛТЫН БОДЛОГО

Компани мэдээллийн аюулгүй байдлыг байгууллагын соёлын салшгүй хэсэг гэж үзэж, ажилтан болон компанийн мэдээллийн хөрөнгөд хандах эрх бүхий этгээд бүр мэдээллийн аюулгүй байдлын зохих мэдлэг, ойлголттой байх нөхцөлийг бүрдүүлнэ. Компани хүний хүчин зүйлээс үүдэлтэй мэдээллийн аюулгүй байдлын эрсдэлийг бууруулах зорилгоор мэдээллийн аюулгүй байдлын мэдлэг олгох, сэрэмжлүүлэх, чиглүүлэх сургалтыг тогтмол хэрэгжүүлнэ. Мэдээллийн аюулгүй байдлын сургалт нь ажилтны үүрэг, хариуцлага, мэдээлэлд хандах эрхтэй уялдсан байна.

11. ЗӨВШӨӨРӨГДСӨН ХЭРЭГЛЭЭНИЙ БОДЛОГО

Компанийн мэдээлэл, мэдээллийн хөрөнгө, систем, төхөөрөмж, сүлжээ болон бусад мэдээллийн технологийн хөрөнгөд хандах эрх бүхий этгээдүүд нь зөвхөн ажлын үүргийн дагуу зөвшөөрөгдсөн хүрээнд, мэдээллийн нууцлал, бүрэн бүтэн, хүртээмжийг алдагдуулахгүйгээр ёс зүйтэй, аюулгүй, ашиглана. Компани зөвшөөрөгдсөн хэрэглээний хэрэгжилтэд зохистой хяналт тавьж, мэдээллийн хөрөнгийг буруугаар ашиглах, зөвшөөрөлгүй хандах, мэдээлэл алдагдах болон мэдээллийн аюулгүй байдлын зөрчлөөс урьдчилан сэргийлэх хамгаалалттай орчныг бүрдүүлнэ. Мэдээллийн хөрөнгө, систем, сүлжээ, имэйл, интернэт, программ хангамж, зөөврийн төхөөрөмж болон ажлын байрны нөөцийг зөвшөөрөлгүй ашиглах, өөрчлөх, дамжуулах, задруулах, гэмтээх, хяналтыг тойрох, компанийн нэр хүндэд сөргөөр нөлөөлөх байдлаар ашиглахыг хориглоно.

12. ЦЭВЭР ШИРЭЭ, ЦЭВЭР ДЭЛГЭЦ

Компани мэдээллийн нууцлал, бүрэн бүтэн, хүртээмжтэй байдлыг хамгаалах зорилгоор Цэвэр ширээ, цэвэр дэлгэцийн зарчим хэрэгжүүлнэ. Компанийн мэдээлэл, баримт бичиг, төхөөрөмж болон систем нь зөвшөөрөлгүй этгээд харах, хандах, авах, ашиглах, өөрчлөх, задруулах боломжгүй байдлаар хамгаалагдсан байна. Ажилтан болон мэдээллийн хөрөнгөд хандах эрх бүхий этгээд нь ажлын орчин, дэлгэц, төхөөрөмж, хэвлэмэл материалтай харьцахдаа мэдээлэл ил задгай үлдэх, алдагдах, буруугаар ашиглагдах эрсдэлээс сэргийлэх хариуцлагатай байна. Цэвэр ширээ, цэвэр дэлгэцийн зарчим нь компанийн мэдээллийн аюулгүй байдлын соёл, дотоод хяналт болон мэдээлэл хамгаалах орчны нэг хэсэг байна.

13. ХАНДАХ ЭРХИЙН ХЯНАЛТЫН БОДЛОГО

Компани мэдээллийн хөрөнгө, систем, сүлжээ, программ хангамж, үүлэн орчин, биет орон зай болон баримт бичигт хандах эрхийг зөвхөн албан үүрэг, бизнесийн хэрэгцээ, мэдээллийн аюулгүй байдлын шаардлагад үндэслэн олгох зарчмыг баримтална. Хандах эрх нь “мэдэх шаардлагатай”, “хамгийн бага эрхийн зарчим”-д суурилсан байна. Дундын болон зөвшөөрөлгүй нэвтрэх эрх ашиглахыг хориглоно. Давуу эрхтэй болон өндөр эрсдэлтэй хандалтад нэмэлт хамгаалалт, баталгаажуулалт, хяналтын шаардлага тавьж, хандах эрхийн ашиглалт, өөрчлөлт, цуцлалт нь хяналттай, бүртгэлтэй, зөвшөөрөгдсөн байна. Хандах эрхийн хяналт нь компанийн мэдээллийн аюулгүй байдлын үндсэн хамгаалалтын нэг хэсэг байна.

14. НУУЦ ҮГ БА БАТАЛГААЖУУЛАЛТЫН БОДЛОГО

Компанийн систем, сүлжээ, програм хангамж болон мэдээллийн хөрөнгөд зөвхөн зөвшөөрөгдсөн хэрэглэгч аюулгүй нэвтрэх нөхцөлийг хангах зорилгоор нууц үгийн удирлагыг хэрэгжүүлнэ. Нууц үг нь шаардлагатай урт, нийлмэл байдлыг хангасан, шифрлэн хадгалагдсан байх бөгөөд бусдад дамжуулах, ил бичих, давтан ашиглахыг хориглоно. Өндөр эрсдэлтэй болон давуу эрхт хандалтад MFA ашиглаж, зөрчил гарсан тохиолдолд хандалтыг хязгаарлах, хариуцлага тооцох арга хэмжээ авна.

15. ЛОГ БҮРТГЭЛИЙН БОДЛОГО

Компани мэдээллийн систем, сүлжээ, сервер, өгөгдлийн сан, программ хангамж, үүлэн үйлчилгээ болон гуравдагч талтай холбогдсон системийн үйл ажиллагааг хяналттай, мөрдөн шалгах боломжтой байлгах зорилгоор лог бүртгэлийн зарчмыг хэрэгжүүлнэ. Лог бүртгэл нь мэдээллийн аюулгүй байдлын зөрчил, зөвшөөрөлгүй хандалт, системийн өөрчлөлт, давуу эрхийн ашиглалт болон сэжигтэй үйлдлийг илрүүлэх, хянах, нотлох баримт болгон ашиглах боломжтой байна. Компанийн лог бүртгэл нь бүрэн бүтэн, үнэн зөв, цаг хугацааны хувьд баталгаатай, зөвшөөрөлгүй өөрчлөх, устгах, хандахаас хамгаалагдсан байна. Компани лог бүртгэлийн мэдээллийг мэдээллийн аюулгүй байдлын хяналт, инцидентийн удирдлага, аудит, нийцлийн баталгаажуулалт болон эрсдэлийн удирдлагын зорилгоор зохистойгоор ашиглана.

16. ЭД ХӨРӨНГИЙН УДИРДЛАГА

Компани мэдээллийн болон мэдээллийн технологийн хөрөнгийг байгууллагын үнэ цэнтэй хөрөнгө гэж үзэж, тэдгээрийн нууцлал, бүрэн бүтэн, хүртээмжтэй байдлыг хамгаална. Мэдээллийн хөрөнгө нь үнэ цэнэ, мэдрэг байдал, бизнесийн ач холбогдол, хууль зохицуулалтын шаардлага болон эрсдэлийн түвшинд үндэслэн зохих ангилал, эзэмшил, хамгаалалттай байна. Компанийн мэдээллийн хөрөнгийг зөвхөн зөвшөөрөгдсөн, хууль ёсны, ажил үүргийн хэрэгцээнд ашиглана. Зөвшөөрөлгүй ашиглах, өөрчлөх, дамжуулах, алдагдуулах, гэмтээх, устгах үйлдлийг хориглоно. Мэдээллийн хөрөнгийг үүсгэх, ашиглах, хадгалах, дамжуулах, буцаах болон устгахдаа мэдээллийн аюулгүй байдлын шаардлага, бизнесийн хэрэгцээнд, нийцсэн хяналттай орчинд хэрэгжүүлнэ.

17. КРИПТОГРАФИЙН БОДЛОГО

Компани мэдээллийн нууцлал, бүрэн бүтэн, баталгаат байдал болон аюулгүй байдлыг хангах зорилгоор криптографийн хамгаалалтын зарчмыг баримтална. Криптографийн хамгаалалт нь мэдээллийн ангилал, системийн эрсдэлийн түвшин, бизнесийн хэрэгцээ, хууль, зохицуулалт, стандарт болон гэрээний шаардлагад нийцсэн байна. Шифрлэлт, цахим гэрчилгээ, дижитал гарын үсэг, VPN, аюулгүй файл дамжуулалт болон баталгаажуулалтын криптографийн хэрэгслийг зөвшөөрөгдсөн, зөвшөөрөлгүй хандах, өөрчлөх, хуулбарлах, задруулах, алдагдахаас хамгаалагдсан найдвартай, хяналттай орчинд ашиглана. Компани криптографийн хамгаалалтыг мэдээлэл хадгалах, дамжуулах, баталгаажуулах, зайнаас хандах болон өндөр эрсдэлтэй мэдээлэл боловсруулах үйл ажиллагаанд зохистойгоор хэрэгжүүлнэ.

18. МЭДЭЭЛЭЛ ДАМЖУУЛАЛТЫН БОДЛОГО

Компани мэдээллийг дотоод болон гадаад орчинд дамжуулахдаа мэдээллийн нууцлал, бүрэн бүтэн, хүртээмжтэй байдал болон хууль, зохицуулалт, гэрээний нийцлийг хангана. Мэдээлэл дамжуулалт нь мэдээллийн ангилал, мэдрэг байдал, бизнесийн хэрэгцээ, хүлээн авагчийн эрх, дамжуулах сувгийн аюулгүй байдал болон эрсдэлийн түвшинд нийцүүлэн зөвхөн зөвшөөрөгдсөн, баталгаажсан, хамгаалагдсан сувгаар дамжуулна. Нууц, эмзэг болон хувийн мэдээллийг зөвшөөрөлгүй этгээдэд дамжуулах, нийтийн болон хамгаалалтгүй сувгаар илгээх, хувийн хэрэгслээр дамжуулахыг хориглоно. Мэдээлэл алдагдах, буруу хүлээн авагчид очих, зөвшөөрөлгүй задрах, өөрчлөгдөх, ашиглагдах эрсдэлийг бууруулах хяналттай орчныг бүрдүүлнэ. Гуравдагч этгээдтэй мэдээлэл солилцохдоо нууцлал, гэрээний үүрэг, мэдээллийн аюулгүй байдлын шаардлага болон зохих зөвшөөрлийн зарчмыг баримтална.

19. МЭДЭЭЛЭЛ БА МЭДЭЭЛЛИЙН ХЭРЭГСЭЛ УСТГАХ БОДЛОГО

Компани цаашид ашиглах шаардлагагүй мэдээлэл, мэдээлэл агуулсан хэрэгслийг аюулгүй, хяналттай, нөхөн сэргээх боломжгүй байдлаар мэдээллийн ангилал, хууль зохицуулалтын шаардлага, гэрээний үүрэг болон стандартад нийцүүлэн устгана. Компани мэдээлэл устгалаас үүдэх мэдээлэл алдагдах, зөвшөөрөлгүй сэргээгдэх, буруу ашиглагдах эрсдэлийг бууруулах хамгаалалттай орчныг бүрдүүлнэ.

20. НӨӨЦЛӨЛТ БА СЭРГЭЭЛТИЙН БОДЛОГО

Компани бизнесийн тасралтгүй ажиллагаа, мэдээллийн бүрэн бүтэн байдал, хүртээмжтэй байдлыг хангах зорилгоор чухал мэдээлэл, систем, өгөгдлийг зохистой нөөцлөх, сэргээх зарчмыг баримтална. Нөөцлөлт ба сэргээлийн шаардлага нь мэдээллийн үнэ цэнэ, системийн чухал байдал, бизнесийн хэрэгцээ, хууль зохицуулалт болон гэрээний үүрэгт нийцсэн байна. Компани мэдээлэл алдагдах, устах, гэмтэх, системийн доголдол үүсэх үед мэдээлэл, системийг сэргээх боломжтой, хамгаалагдсан, хяналттай нөөцлөлтийн орчныг бүрдүүлнэ.

21. ХӨДӨЛГӨӨНТ ТӨХӨӨРӨМЖ АШИГЛАХ БА ЗАЙНААС АЖИЛЛАХ БОДЛОГО

Компанийн ажилтан хөдөлгөөнт төхөөрөмж ашиглах болон зайнаас ажиллах үед мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмжтэй байдлыг хамгаалах зарчмыг баримтална. Компанийн мэдээлэл, систем, сүлжээнд зөвхөн зөвшөөрөгдсөн, баталгаажсан, хамгаалагдсан төхөөрөмж болон аюулгүй холболтоор хандана. Хөдөлгөөнт төхөөрөмж, хувийн төхөөрөмж болон зайнаас ажиллах орчин нь зөвшөөрөлгүй хандалт, мэдээлэл алдагдал, төхөөрөмжийн алдагдал, буруу ашиглалт болон хамгаалалтгүй сүлжээний эрсдэлээс хамгаалагдсан байна. Компани хөдөлгөөнт төхөөрөмж болон зайнаас хандах үйл ажиллагаанд зохих хандалтын хяналт, баталгаажуулалт, шифрлэлт, төхөөрөмжийн хамгаалалт болон мэдээлэл хадгалалт, дамжуулалтын аюулгүй байдлын шаардлагыг хэрэгжүүлнэ.

22. ЭМЗЭГ БАЙДЛЫН УДИРДЛАГЫН БОДЛОГО

Компани мэдээллийн систем, программ хангамж, сүлжээ, төхөөрөмж, үүлэн орчин болон гуравдагч талын технологийн орчинд үүсч болзошгүй эмзэг байдлыг мэдээллийн аюулгүй байдлын эрсдэлийн эх үүсвэр гэж үзэж, эрсдэлд суурилсан байдлаар удирдана. Эмзэг байдлын удирдлага нь системийн чухал байдал, мэдээллийн ангилал, ашиглагдах магадлал, бизнесийн нөлөөлөл болон нийцлийн шаардлагад үндэслэсэн байна. Компани эмзэг байдлаас үүдэх зөвшөөрөлгүй хандалт, мэдээлэл алдагдал, системийн доголдол, халдлагын эрсдэлийг бууруулах зорилгоор зохистой илрүүлэлт, үнэлгээ, засварлалт болон хяналтын орчныг бүрдүүлнэ.

23. ӨӨРЧЛӨЛТИЙН УДИРДЛАГЫН БОДЛОГО

Компани мэдээллийн технологийн систем, дэд бүтэц, программ хангамж, сүлжээ, үүлэн үйлчилгээ болон мэдээллийн аюулгүй байдлын орчинд хийгдэх өөрчлөлтийг хяналттай, эрсдэлд суурилсан, баримтжуулсан зарчмаар удирдана. Өөрчлөлт нь мэдээллийн аюулгүй байдал, бизнесийн тасралтгүй ажиллагаа, системийн найдвартай байдал, хууль зохицуулалтын болон гэрээний шаардлагад сөрөг нөлөө үзүүлэхгүй байх ёстой. Компани өөрчлөлтөөс үүдэх зөвшөөрөлгүй хандалт, системийн доголдол, мэдээлэл алдагдал, үйлчилгээ тасалдах болон тохиргооны алдааны эрсдэлийг бууруулах хяналттай орчныг бүрдүүлнэ.

24. БИЗНЕСИЙН ТАСРАЛТГҮЙ БАЙДЛЫН БОДЛОГО

Компани урьдчилан таамаглах боломжгүй системийн доголдол, кибер халдлага, гамшиг болон бусад онцгой тасалдлын үед бизнесийн үндсэн үйл ажиллагаа, чухал мэдээллийн систем, дэд бүтцийн тасралтгүй, бэлэн байдлыг хангаж ажиллана. Бизнесийн тасралтгүй байдлын удирдлага нь үйл ажиллагааны чухал байдал, мэдээллийн аюулгүй байдал, сэргээх хэрэгцээ, хууль зохицуулалтын болон стандартын шаардлага, харилцагч, түнш байгууллагын өмнө хүлээсэн үүрэгтэй уялдсан байна. Компани тасалдлын нөлөөллийг бууруулах, чухал үйл ажиллагааг сэргээх, мэдээлэл болон системийн хүртээмжтэй байдлыг хадгалах зорилгоор зохистой төлөвлөлт, нөөцлөлт, сэргээх болон хяналтын орчныг бүрдүүлнэ.

25. ПРОГРАМ ХАНГАМЖ АЮУЛГҮЙ ХӨГЖҮҮЛЭЛТИЙН БОДЛОГО

Компани программ хангамж, мэдээллийн системийг хөгжүүлэх, худалдан авах, интеграц хийх, өөрчлөх болон засварлах бүх үе шатанд мэдээллийн аюулгүй байдлын зарчмыг баримтална. Программ хангамжийн хөгжүүлэлт нь системийн эрсдэлийн түвшин, мэдээллийн ангилал, бизнесийн хэрэгцээ, архитектурын шаардлага болон хууль, гэрээний нийцэлтэй уялдсан байна. Компани баталгаажуулалт, эрхийн хяналт, лог бүртгэл, шифрлэлт, аюулгүй кодчилол, тест, эмзэг байдлын шалгалт болон өөрчлөлтийн хяналтыг хөгжүүлэлтийн зохистой хамгаалалтын нэг хэсэг болгон хэрэгжүүлнэ. Дотоод хөгжүүлэлт, гуравдагч талын хөгжүүлэлт, SaaS болон худалдан авсан систем нь компанийн мэдээллийн аюулгүй байдлын шаардлага, интеграцийн аюулгүй байдал, өгөгдлийн хамгаалалт болон тасралтгүй ажиллагааны шаардлагад нийцсэн байна.

26. НИЙЛҮҮЛЭГЧ БА ГУРАВДАГЧ ЭТГЭЭДИЙН ҮЙЛЧИЛГЭЭНД ТАВИХ АЮУЛГҮЙ БАЙДЛЫН БОДЛОГО

Компани нийлүүлэгч, үйлчилгээ үзүүлэгч, аутсорсинг, үүлэн үйлчилгээ болон бусад гуравдагч этгээдтэй харилцахдаа мэдээллийн аюулгүй байдлын эрсдэлийг удирдах зарчмыг баримтална. Гуравдагч этгээдийн үйлчилгээ нь компанийн мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмжтэй байдал, хууль зохицуулалтын шаардлага болон гэрээний үүрэгт нийцсэн байна. Компани гуравдагч этгээдэд мэдээлэл, систем, сүлжээ болон үйлчилгээний орчинд хандах эрх олгохдоо зохих үнэлгээ, гэрээний хамгаалалт, хандалтын хяналт, нууцлал, зөрчлийн мэдэгдэл болон тасралтгүй ажиллагааны шаардлагыг тавина.

27. БОДИТ ОРЧНЫ АЮУЛГҮЙ БАЙДАЛ

Компани мэдээлэл боловсруулах байгууламж, ажлын байр, тоног төхөөрөмж болон биет мэдээллийн хөрөнгийг зөвшөөрөлгүй хандалт, гэмтэл, хулгай, гамшиг орчны аюул болон үйл ажиллагааны тасалдлаас хамгаална. Физик орчны хамгаалалт нь мэдээллийн хөрөнгийн үнэ цэнэ, эрсдэлийн түвшин, нууцлалын шаардлагтай уялдсан байна. Компанийн хамгаалагдсан бүс, тоног төхөөрөмж, сүлжээний холболт болон байгууллагаас гадуур ашиглагдах төхөөрөмж нь хяналттай, зөвшөөрөлтэй, аюулгүй орчинд ашиглагдана. Компани бодит орчноос үүдэх мэдээлэл алдагдах, системийн доголдол, зөвшөөрөлгүй нэвтрэлт болон тоног төхөөрөмжийн гэмтэл, алдагдлын эрсдэлийг бууруулах хамгаалалттай орчныг бүрдүүлнэ.

28. МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ЗӨРЧЛИЙН УДИРДЛАГА

Компани мэдээллийн аюулгүй байдлын зөрчил, сэжигтэй үйл явдал болон сул талыг шуурхай илрүүлэх, мэдээлэх, үнэлэх, хариу арга хэмжээ авна. Компани мэдээллийн аюулгүй байдлын зөрчлөөс үүдэх хохирол, үйлчилгээний тасалдал, мэдээлэл алдагдал, нэр хүндийн эрсдэл болон давтагдах эрсдэлийг бууруулах хяналттай орчныг бүрдүүлнэ. Зөрчлийн дараах сургамж, нотлох баримт, тайлагнал болон сайжруулалтын арга хэмжээ нь мэдээллийн аюулгүй байдлын удирдлагын тогтолцооны тасралтгүй сайжруулалтын нэг хэсэг байна.

29. МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН НИЙЦЭЛ

Компани мэдээллийн аюулгүй байдлын үйл ажиллагааг холбогдох хууль тогтоомж, зохицуулалтын шаардлага, гэрээний үүрэг болон олон улсын стандартын шаардлагад нийцүүлэн хэрэгжүүлэнэ. Мэдээллийн аюулгүй байдлын нийцэл нь компанийн дотоод бодлого, журам, процесс, техникийн болон зохион байгуулалтын хяналтын салшгүй хэсэг байна. Нийцлийн хэрэгжилт, хяналт

шинжилгээ, хэмжилтийн үр дүн нь удирдлагын дүн шинжилгээ болон мэдээллийн аюулгүй байдлын тасралтгүй сайжруулалтын үндэслэл болно.

30. БАРИМТ БИЧГИЙН ХЯНАЛТ

Энэхүү бодлогыг жилд нэг удаа хянаж шаардлагтай тохиолдолд өөрчлөлтийг хийж, компанийн “Төлөөлөн удирдах зөвлөл”-өөр батлуулна.