БАГАНУУР ХК

“БАГАНУУР” ХУВЬЦААТ КОМПАНИЙН ГҮЙЦЭТГЭХ ЗАХИРЛЫН ТУШААЛ

2026 оны 04 сарын 30 өдөр Дугаар А/167 Багануур дүүрэг

Журам 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 байдлын удирдлагын журам”-ыг хавсралтаар баталсугай.

2.Батлагдсан журмыг нийт ажилтнуудад танилцуулан, мөрдөж ажиллахыг Мэдээллийн технологийн алба (Т.Эрдэнэ-Очир), журмын хэрэгжилтэд хяналт тавьж ажиллахыг Дотоод хяналт, эрсдэлийн удирдлагын алба (Б.Хажидмаа)-д тус тус үүрэг болгосугай.

3.Энэхүү журам батлагдсантай холбогдуулан Гүйцэтгэх захирлын 2010 оны 06 дугаар сарын 14-ний өдрийн 170 тоот тушаалыг хүчингүй болсонд тооцсугай.

ГҮЙЦЭТГЭХ ЗАХИРЛЫН
ҮҮРЭГ ГҮЙЦЭТГЭГЧ Т.ОТГОНБОЛД

БАГАНУУР ХК

Баримт бичгийн нэр:

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН УДИРДЛАГЫН ЖУРАМ

Баримт бичгийн хариуцагч:	Мэдээллийн технологийн алба
Баримт бичгийн дугаар:	Ж26-МТА-34-02
Баталсан огноо:	2026.04.30
Тушаалын дугаар:	А/167
Мөрдөж эхлэх огноо:	2026.04.30
Боловсруулсан:	МТА-ны системийн ахлах 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 “Баганаар” ХК-ийн дотоод хэрэгцээнд ашиглана.

АГУУЛГА

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

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН УДИРДЛАГЫН ЖУРАМ

НЭГ. НИЙТЛЭГ ҮНДЭСЛЭЛ

1.1. Энэхүү журмын зорилго нь “Багануур” ХК (цаашид “компани” гэх)-ийн мэдээллийн систем болон үйлдвэрлэлийн технологийн мэдээллийн аюулгүй байдлыг хангах, кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, хариу арга хэмжээ авах замаар компанийн үйл ажиллагааны тасралтгүй байдлыг баталгаажуулахад оршино.

1.2. Энэхүү журам нь Кибер аюулгүй байдлын тухай хууль, Засгийн газрын 2023 оны 224 дүгээр тогтоолоор батлагдсан "Кибер аюулгүй байдлыг хангах нийтлэг журам", MNS ISO/IEC 27001:2023 (ISO/IEC 27001:2022) стандарт, "Эрдэнэс Монгол" ХХК нэгдлийн МАБ-ын бодлого, "Багануур” ХК-ийн Мэдээллийн аюулгүй байдлын бодлого, “Багануур” ХК-ийн нууцын журам болон хууль тогтоомжийн бусад актаас бүрдэнэ.

1.3. Компани нь олон улсын ISO/IEC 27001:2022 стандартын шаардлагад нийцүүлэн, өөрийн үйл ажиллагааны онцлог, цар хүрээг харгалзан мэдээллийн аюулгүй байдлын менежментийн тогтолцоог зохион байгуулна.

1.4. Энэхүү журмын заалтууд нь Монгол Улсын олон улсын гэрээнд зааснаас өөрөөр заасан бол олон улсын гэрээний заалтыг дагаж мөрдөнө.

1.5. Компани нь энэхүү журмын хэрэгжилт, нийцэл болон үр нөлөөтэй байдлыг хангах зорилгоор Монгол Улсын холбогдох хууль тогтоомж, стандарт, байгууллагын бүтцэд өөрчлөлт орох тухай бүр. эсхүл төлөвлөгөөт хугацаанд (жилд нэгээс доошгүй удаа) хянан үзэж, шинэчлэн сайжруулна. Журмын шинэчлэлтийг Мэдээллийн технологийн алба (МТА) боловсруулж, Гүйцэтгэх захирлын тушаалаар баталгаажуулна.

1.6. Мэдээллийн аюулгүй байдал гэдэгт "Кибер аюулгүй байдал" гэсэн утгыг хамтад нь ойлгоно.

ХОЁР. ХАМРАХ ХҮРЭЭ

2.1. Энэхүү журам нь компанийн мэдээллийн аюулгүй байдлын бодлогын баримт бичигт тодорхойлсон хамрах хүрээний дагуу компанийн үндсэн үйл ажиллагаа болох нүүрс олборлолт, боловсруулалт, тээвэрлэлт, борлуулалтын процесс, түүнийг дэмжих мэдээллийн технологи болон үйлдвэрлэлийн технологийн систем, сүлжээний дэд бүтэц, мэдээллийн хөрөнгийг ашиглаж буй нийт ажилтан хамаарна.

ГУРАВ. НЭР ТОМЬЁОНЫ ТОДОРХОЙЛОЛТ

3.1. **Мэдээлэл**: Компанийн үндсэн болон дэмжих үйл ажиллагааны хүрээнд бий болсон, боловсруулагдсан, дамжуулагдсан, хадгалагдсан болон ашиглагдаж буй бүх төрлийн өгөгдөл, баримт бичиг, мэдээллийн багцыг хэлнэ. Мэдээлэл нь түүнийг агуулж, дамжуулж буй хэрэгсэл, зөөвөрлөгчөөс үл хамааран биет (цаасан баримт, г.м) болон биет бус (цахим файл, тоон өгөгдөл, ажилтны мэдлэг туршлага, оюуны бүтээл, санаа г.м) бүхий бүх л хэлбэрээр оршин байна;

3.2. **Мэдээллийн аюулгүй байдал (МАБ)**: гэдэг нь мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмжтэй байдлыг хангах үйл явц, удирдлага, арга хэмжээ;

3.3. **Мэдээллийн технологи (IT - Information Technology)**: Компанийн 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;

3.4. **Үйлдвэрлэлийн технологи (OT - Operational Technology)**: Компанийн 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;

3.5. **CIA: (CIA triad: Confidentiality, Integrity, Availability)**: Мэдээллийн технологи болон Үйлдвэрлэлийн технологийн системийн Нууцлаг байдал, Бүрэн бүтэн байдал, Хүртээмжтэй байдлыг хангах зарчим;

3.6. **Мэдээллийн технологи хариуцсан үндсэн нэгж**: Мэдээллийн технологийн алба (МТА);

3.7. **Ажилтан**: гэж хөдөлмөр эрхлэлтийн харилцааны үндсэн дээр ажиллаж байгаа Монгол Улсын иргэн, гадаадын иргэн, харьяалалгүй хүнийг;

3.8. **Мэдээлэл эзэмшигч**: гэж албан үүрэг, ажил мэргэжлийн үйл ажиллагааны хүрээнд аливаа мэдээллийг олж мэдсэн, танилцсан, тухайн мэдээллийг эзэмшиж байгаа ажилтныг;

3.9. **Мэдээлэл хариуцагч**: Мэдээллийн хөрөнгийг эзэмшиж буй ажилтан, нэгжийг шууд удирдлагаар хангах, мэдээлэл боловсруулах үйл явц болон аюулгүй байдлын хяналтыг өдөр тутмын түвшинд бодитой хариуцан хэрэгжүүлэх чиг үүрэг бүхий нэгжийн удирдлагыг хэлнэ;

3.10. **Аюул занал**: гэж систем болон компанид хор учруулж болох мэдээллийн аюулгүй байдлыг ямар нэг байдлаар зөрчиж болох боломж, үйлдэл, үйл явдлыг;

3.11. **Эрсдэл**: гэж аюул заналын байгаа магадлал болон түүний үр дагаврыг;

3.12. **Мэдээллийн аюулгүй байдлын тохиолдол**: гэж мэдээллийн аюулгүй байдлын зөрчил гарсан, аюулгүй байдлын арга хэмжээ үр дүнгүй болсон, эсхүл аюулгүй байдалтай холбоотой ямар нэг нөхцөл байдал үүссэн гэдгийг илтгэж буй системийн үйлчилгээ, хэвийн байдалд нөлөөлөх аливаа тохиолдол, үйл явдлыг;

3.13. **Эрсдэлийн үнэлгээ (Risk Assessment)**: гэж эрсдэлийн хэмжээ, ач холбогдлыг тодорхойлох, шинжлэх, тооцоолох процессыг;

3.14. **Эрсдэлийн хариу арга хэмжээ (Risk Treatment)**: гэж эрсдэлийг өөрчлөх (бууруулах, дамжуулах, зайлсхийх, хүлээн зөвшөөрөх) процессыг;

3.15. **Нөөцлөлт (Backup)**: гэж мэдээлэл, тохиргоо, систем алдагдахаас урьдчилан сэргийлэх зорилгоор хуулбар үүсгэх үйл ажиллагааг;

3.16. **Сэргээлт (Recovery)**: гэж алдагдсан эсвэл гэмтсэн мэдээлэл, системийг нөөцөөс буцааж сэргээх үйл ажиллагааг;

3.17. **Хандалтын удирдлага (Access Control)**: гэж мэдээлэл, систем, сүлжээнд хандах эрхийг зохицуулах, хязгаарлах, хянах процессыг;

3.18. **Нууц үг (Password)**: гэж хэрэглэгчийн нэр хүлээн зөвшөөрөх, баталгаажуулалтын зорилгоор ашигладаг нууц мэдээллийг;

3.19. **Олон хүчин зүйлт баталгаажуулалт (Multi-Factor Authentication - MFA)**: гэж хоёр буюу түүнээс дээш баталгаажуулалтын хүчин зүйл (мэддэг зүйл, эзэмшдэг зүйл, биометрик) ашигладаг аюулгүй нэвтрэх аргыг;

3.20. **Хортой код (Malware)**: гэж систем, сүлжээнд халдах, гэмтээх, эсвэл зөвшөөрөлгүй хандалт хийх зорилготой хор хөнөөлтэй программ хангамж (вирус, ransomware, trojan, spyware гэх мэт)-ийг;

3.21. **Фишинг (Phishing)**: гэж хэрэглэгчийг хууран мэхлэх замаар нууц мэдээлэл (нууц үг, кредит картын мэдээлэл гэх мэт) олж авах оролдлогыг;

3.22. **Кибер халдлага**: гэж мэдээллийн систем, сүлжээнд зориудаар гаргасан хууль бус, зөвшөөрөлгүй үйлдлийг;

3.23. **Эмзэг байдал (Vulnerability)**: гэж систем, программ хангамж, сүлжээний аюулгүй байдлын сул тал, алдааг;

3.24. **NAS (Network Attached Storage)**: Сүлжээний хадгалах төхөөрөмж.

ДӨРӨВ. МАБ-ЫН ЭРСДЭЛИЙН ҮНЭЛГЭЭ БА УДИРДЛАГА

4.1. Эрсдэлийн удирдлагын үе шат ба төлөвлөлт

4.1.1. Компани нь эрсдэлийн удирдлагыг “Эрдэнэс Монгол” ХХК-ийн нэгдсэн эрсдэлийн удирдлагын бодлого, аргачлалын дагуу хэрэгжүүлэх бөгөөд энэхүү журмаар МАБ-ын эрсдэлийг тодорхойлох, шинжлэх, үнэлэх болон арга хэмжээ авахад шаардлагатай, олон улсын ISO/IEC 27005 стандартад нийцсэн МАБ-д онцлог шалгуур, арга зүйг тогтооно.

4.1.2. Эрсдэлийн удирдлагыг дараах үе шаттайгаар хэрэгжүүлнэ. Үүнд:

4.1.2.1 Эрсдэлийг тодорхойлох;

4.1.2.2 Эрсдэлийг үнэлэх (Шинжилгээ ба Үнэлэлт);

4.1.2.3 Эрсдэлийг бууруулах (Арга хэмжээ төлөвлөх);

4.1.2.4 Эрсдэлийг тайлагнах, хянах.

4.1.3. МАБ-ын эрсдэлийн үнэлгээг жил тутамд тогтмол, эсвэл дараах тохиолдолд хийнэ:

4.1.3.1. Шинэ систем, үйлчилгээ нэвтрүүлэх үед;

4.1.3.2. Системд томоохон өөрчлөлт орох үед;

4.1.3.3. Шинэ аюул занал илрэх үед;

4.1.3.4. МАБ-ын зөрчил гарсны дараа;

4.1.3.5. Шинэ аюул занал илрэх тохиолдол бүрд ээлжит бусаар гүйцэтгэнэ.

4.2. Мэдээллийн хөрөнгөд суурилан эрсдэлийг тодорхойлох

4.2.1. Компани нь мэдээллийн аюулгүй байдлын эрсдэлийг тодорхойлохдоо “Мэдээллийн хөрөнгийн бүртгэл”-ийг суурь болгон ашиглаж, хөрөнгө тус бүрт холбогдох аюул занал, эмзэг байдал, боломжит нөлөөллийг системтэйгээр тодорхойлно.

4.2.2. Мэдээллийн хөрөнгийг дараах чиглэлээр ангилж, эрсдэлийн эзэмшигчийг тогтооно:

4.2.2.1. Мэдээлэл /цаасан, цахим мэдээлэл/;

4.2.2.2. Программ хангамж, өгөгдлийн сан;

4.2.2.3. Сервер, тоног төхөөрөмж;

4.2.2.4. Сүлжээ;

4.2.2.5. Ажилтан.

4.2.3. Дараах өндөр эрсдэлтэй систем, орчныг эрсдэлийн үнэлгээнд заавал хамруулна:

4.2.3.1. Уурхайн үйлдвэрлэлийн технологийн систем;

4.2.3.2. Хяналтын камер;

4.2.3.3. Жин хэмжүүр болон тээврийн систем;

4.2.3.4. Алслагдсан сүлжээний орчин;

4.2.3.5. Радио холбооны систем;

4.2.3.6. Дотуур холбооны систем.

4.3. Эрсдэлийг үнэлэх

4.3.1. Компани нь эрсдэлийг үнэлэх шалгуурыг дараах байдлаар тогтооно:

4.3.1.1. Эрсдэлийг үнэлэх аргачлал (5х5 матриц);

4.3.1.2. Эрсдэлийн хүлээн зөвшөөрөх түвшин;

4.3.1.3. Нөлөөллийг үнэлэх шалгуур (CIA);

4.3.1.4. Магадлалын үнэлгээний шалгуур.

4.3.2. Эрсдэлийн үнэлгээг давтагдах боломжтой, ижил аргачлалаар хэрэгжүүлж, өмнөх үнэлгээтэй харьцуулах боломжтой байдлаар баримтжуулна.

4.3.3. Эрсдэлийг үнэлэх үйл явц дараах үе шаттай байна.

4.3.3.1. Аюул занал, эмзэг байдлыг тодорхойлох;

4.3.3.2. Мэдээллийн хөрөнгийн үнэ цэнийг үнэлэх;

4.3.3.3. Нөлөөллийг (CIA) үнэлэх;

4.3.3.4. Магадлалыг үнэлэх;

4.3.3.5. Эрсдэлийн түвшинг тооцоолох (Эрсдэл = Магадлал × Нөлөөлөл);

4.3.3.6. Эрсдэлийг эрэмбэлэх.

4.3.4. Эрсдэлийн түвшний ангилал:

4.3.4.1. Өндөр (12-25 оноо);

4.3.4.2. Дунд (6-10 оноо);

4.3.4.3. Бага (1-5 оноо).

4.3.5. Нөлөөллийг үнэлэхдээ мэдээллийн аюулгүй байдлын CIA-ын шинж чанар алдагдсанаас үүсэх эрсдэлийг 1-ээс 5 оноогоор үнэлнэ.

4.3.6. Магадлалыг үнэлэхдээ аюул заналын давтамж болон компанийн техникийн эмзэг байдалд үндэслэн 1-ээс 5 оноогоор үнэлнэ.

4.3.7. Эрсдэлийн үнэлгээний үр дүнг “МАБ-ын эрсдэлийн үнэлгээ ба хариу арга хэмжээний төлөвлөгөө” [Хавсралт №2]-д бүртгэж хадгална.

4.4. Эрсдэлийг бууруулах буюу хариу арга хэмжээг төлөвлөх

4.4.1. Компани нь эрсдэлийг боловсруулах үйл явцыг тодорхойлж, дараах сонголтуудыг хэрэглэнэ:
- 4.4.1.1. Эрсдэлээс зайлсхийх;
- 4.4.1.2. Эрсдэлийг бууруулах;
- 4.4.1.3. Эрсдэлийг шилжүүлэх;
- 4.4.1.4. Эрсдэлийг хүлээн зөвшөөрөх.

4.4.2. Эрсдэлийн хүлээн зөвшөөрөх шалгуурыг дараах байдлаар тогтооно:
- 4.4.2.1. Бага эрсдэл (хүлээн зөвшөөрнө)
- 4.4.2.2. Дунд эрсдэл (удирдлагын шийдвэрээр хүлээн зөвшөөрөх боломжтой)
- 4.4.2.3. Өндөр эрсдэл (хүлээн зөвшөөрөхгүй, заавал бууруулна)

4.4.3. Эрсдэлийг хүлээн зөвшөөрөх шийдвэрийг холбогдох эрсдэлийн эзэмшигч болон дээд удирдлага баталгаажуулна.

4.4.4. Үнэлгээгээр илэрсэн (Өндөр) болон (Дунд) түвшний эрсдэлд “МАБ-ын эрсдэлийн үнэлгээ ба хариу арга хэмжээний төлөвлөгөө” [Хавсралт №2]-ний дагуу боловсруулж, батлуулна.

4.4.5. Эрсдэлийг бууруулах арга хэмжээ болгон сонгосон хяналтууд нь “МАБ-ын хяналтыг хэрэгжүүлэх мэдэгдэл” (SoA) [Хавсралт №1]-д тусгаж, батлуулна.

4.5. Эрсдэлийг тайлагнах, хянах

4.5.1. Эрсдэлийн удирдлагын үр дүнг дараах үзүүлэлтээр хэмжинэ:
- 4.5.1.1. Өндөр эрсдэлийн тоо
- 4.5.1.2. Буурсан эрсдэлийн хувь
- 4.5.1.3. Хугацаандаа хэрэгжсэн арга хэмжээний хувь

4.5.2. МАБ хариуцсан ажилтан нь хариу арга хэмжээний төлөвлөгөөний биелэлт “МАБ-ын эрсдэлийн үнэлгээ ба хариу арга хэмжээний төлөвлөгөө” [Хавсралт №2]-г удирдлагын дүн шинжилгээний хуралд танилцуулж, шаардлагатай нөөцийг (төсөв, хүний нөөц) шийдвэрлүүлнэ.

ТАВ. ӨӨРЧЛӨЛТИЙН УДИРДЛАГА ХЭРЭГЖҮҮЛЭХ ҮЙЛ ЯВЦ

5.1. Өөрчлөлтийн ангилал:

5.1.1. Компани нь өөрчлөлтийг дараах ангиллаар тодорхойлж, эрсдэлийн түвшинд үндэслэн удирдана:
- 5.1.1.1. Энгийн өөрчлөлт: Эрсдэл багатай, өдөр тутмын үйл ажиллагаанд хамаарах өөрчлөлтүүд хамаарна;
- 5.1.1.2. Чухал өөрчлөлт: Үйлдвэрлэлийн технологийн систем, сүлжээний үндсэн дэд бүтэц, мэдээллийн аюулгүй байдалд өндөр нөлөөтэй өөрчлөлтүүд хамаарна;
- 5.1.1.3. Яаралтай өөрчлөлт: Кибер халдлага, системийн ноцтой саатал зэрэг онцгой нөхцөл байдлын үед түргэвчилсэн горимоор хэрэгжүүлэх өөрчлөлтүүд хамаарна.

5.2. Өөрчлөлтийг төлөвлөх, хэрэгжүүлэх үе шат:

5.2.1. Компани нь мэдээлэл боловсруулах байгууламж, систем болон программ хангамж хөгжүүлэх үе шатуудад (Программ хангамж хөгжүүлэлт, нэвтрүүлэлтийн журам) МАБ-ыг хадгалах зорилгоор өөрчлөлтийг төлөвлөх ба дараах дарааллын дагуу удирдаж, хэрэгжүүлнэ:

5.2.1.1. Өөрчлөлтийн хүсэлт: Мэдээллийн систем, сүлжээ, үйлдвэрлэлийн технологийн дэд бүтцэд оруулах аливаа өөрчлөлтийг (шинээр систем нэвтрүүлэх, тохиргоо өөрчлөх, нөхөөс суулгах гэх мэт) албан ёсны "Өөрчлөлтийн хүсэлт"-ийн [Хавсралт №3] дагуу эхлүүлж, бүртгэл хөтөлнө.

5.2.1.2. Нөлөөлөл болон эрсдэлийн үнэлгээ: Өөрчлөлтийг хэрэгжүүлэхээс өмнө түүний МАБ болон үйлдвэрлэлийн үйл ажиллагаанд үзүүлэх нөлөөллийг үнэлнэ. Уурхайн олборлолт, борлуулалтын системд үзүүлэх нөлөөллийг заавал тооцсон байна.

5.2.1.3. Үүрэг тусгаарлалт: Өөрчлөлт оруулах хүсэлт гаргагч, түүнийг хэрэгжүүлэгч болон батлагч этгээдүүд нь ашиг сонирхлын зөрчилгүй, тусдаа байх зарчмыг баримтална.

5.2.1.4. Туршилт ба хүлээн авалт: Өөрчлөлтийг бодит орчинд нэвтрүүлэхийн өмнө түүнтэй ижил төсөөтэй туршилтын орчинд заавал шалгаж, аюулгүй байдал болон гүйцэтгэлийн шаардлагыг хангаж буйг баталгаажуулна.

5.2.1.5. Нөөцлөлт: Өөрчлөлт хийхийн өмнө системийн тохиргоо болон өгөгдлийн нөөц хуулбарыг заавал үүсгэсэн байна. Нөөц хуулбарын сэргээх чадварыг урьдчилан шалгасан байна. Энэ нь өөрчлөлт амжилтгүй болсон тохиолдолд мэдээллийг алдагдахаас сэргийлэх буюу буцаах төлөвлөгөө бэлэн байна.

5.2.1.6. Буцаах төлөвлөгөө: Өөрчлөлт хэрэгжүүлэх явцад алдаа гарсан тохиолдолд системийг өмнөх хэвийн төлөвт нь түргэн шуурхай шилжүүлэх "Буцаах төлөвлөгөө"-г урьдчилан бэлтгэсэн байна.

5.2.1.7. Яаралтай өөрчлөлтийн процесс: Ийнхүү яаралтай өөрчлөлт хийсний дараа холбогдох эрсдэлийн үнэлгээ, зөвшөөрөл болон баримтжуулалтыг зохих журмын дагуу нөхөн гүйцэтгэнэ.

5.2.2. Зөвшөөрөл баталгаажуулалт: Өөрчлөлтийг хэрэгжүүлэх зөвшөөрлийг нөлөөллийн болон эрсдэлийн үнэлгээний үр дүнд үндэслэн эрх бүхий албан тушаалтан баримтжуулан (цахим эсвэл цаасан хэлбэрээр) олгоно.

5.2.2.1. Өөрчлөлтийн зөвшөөрөл олгох шатлалыг эрсдэлийн түвшнээс хамааран дараах байдлаар тогтооно:

a) Бага эрсдэлтэй өөрчлөлт: Холбогдох нэгжийн удирдлага;
b) Дунд эрсдэлтэй өөрчлөлт: МТА-ны дарга болон МАБ хариуцсан ажилтны хамтарсан шийдвэр;
c) Өндөр эрсдэлтэй өөрчлөлт: Компанийн Гүйцэтгэх удирдлага (эсхүл Ерөнхий инженер)

5.2.2.2. Зөвшөөрөлгүй өөрчлөлт хийхээс урьдчилан сэргийлэх, өөрчлөлтийн мөшгөх боломжийг хангах зорилгоор дараах техникийн болон зохион байгуулалтын хяналтын механизмыг хэрэгжүүлнэ:

a) Системийн тохиргооны бүртгэл: Системийн суурь тохиргоонд орсон аливаа өөрчлөлтийг нэг бүрчлэн бүртгэж, архивлаж хадгалах;
b) Хандалтын хязгаарлалт: Хандалтын давуу эрхийг зөвхөн батлагдсан өөрчлөлт хийх хугацаанд, "Мэдэх шаардлагатай" (Need-to-know) зарчмаар түр хугацаагаар олгох;
c) Мониторинг: Үйлдлийн бүртгэл болон хяналтын механизмыг ашиглан өөрчлөлтийн явцад тасралтгүй хяналт тавьж, баримтжуулах.

5.2.3. Сонирхогч талуудад мэдээлэх: Төлөвлөсөн өөрчлөлтийн хуваарь болон гарч болох үр дагаврын талаар холбогдох нэгжүүд, ажилтан болон гадаад сонирхогч талуудад өөрчлөлтийг хэрэгжүүлэхээс өмнө урьдчилан мэдээлнэ.

5.3. Баримт бичгийн шинэчлэл ба бүртгэлжүүлэлт:

5.3.1. Аливаа өөрчлөлт нь Компанийн баталсан системийн тохиргооны суурьд нийцэж байгаа эсэхийг урьдчилан шалгана. Өөрчлөлтийг хэрэгжүүлсний дараа тухайн өөрчлөлт нь төлөвлөсөн үр дүндээ хүрсэн эсэх, МАБ-ын (CIA)-д сөрөг нөлөө үүсгэсэн эсэхийг заавал үнэлж, үр дүнг баримтжуулна. Үнэлгээний үр дүнд үндэслэн холбогдох техникийн зураглал, зааварчилгаа, хөрөнгийн бүртгэл болон үйлдвэрлэлийн тасралтгүй ажиллагааны төлөвлөгөөг нэн даруй шинэчлэн сайжруулна. Өөрчлөлтийн үйл явцтай холбоотой бүх үйлдлийг бүртгэж, дотоод аудит болон мөрдөн шалгах зорилгоор баримтжуулан хадгална.

ЗУРГАА. МЭДЭЭЛЛИЙН ХӨРӨНГИЙН УДИРДЛАГА

6.1. Мэдээллийн хөрөнгийн удирдлага

6.1.1. Мэдээллийн хөрөнгийг дараах байдлаар удирдана:

6.1.1.1. Үүсгэх, бүртгэх: (Мэдээлэл бий болох үед түүнийг хөрөнгийн бүртгэлд тусгаж, өмчлөгчийг тогтоох);

6.1.1.2. Ангилах, шошголох: (Мэдээллийн үнэ цэнэ, нууцлалыг тогтоож, зохих тэмдэглэгээ хийх);

6.1.1.3. Ашиглах, хадгалах: (Зөвшөөрөгдсөн хүрээнд ашиглаж, аюулгүй орчинд хадгалах);

6.1.1.4. Дамжуулах, хуваалцах: (Мэдээллийг дотоод болон гадаадад солилцох, дамжуулахдаа нууцлал, бүрэн бүтэн байдлыг хангах);

6.1.1.5. Архивлах, устгах: (Шаардлагагүй болсон мэдээллийг сэргээх боломжгүйгээр устгах эсвэл архивт шилжүүлэх).

6.1.2. Компани нь МАБ-ын менежментийн тогтолцооны хамрах хүрээнд хамаарах бүх мэдээллийн хөрөнгө, мэдээллийн систем болон үйлдвэрлэлийн технологийн дэд бүтцийг хамарсан “Мэдээллийн хөрөнгийн бүртгэл”-ийг [Хавсралт №4] хөтөлж, мэдээллийн үнэ цэнэ, ач холбогдолд тулгуурлан нууцлалын зэрэглэлийг тогтооно. Хөрөнгө бүрт стратегийн хариуцлага хүлээх мэдээлэл эзэмшигч болон тухайн нэгжийн үйл ажиллагааны хүрээнд өдөр тутмын аюулгүй байдлын хяналтыг бодитой хэрэгжүүлэх мэдээлэл

хариуцагчийг томилж, бүртгэлийн үнэн зөв байдал, нийцлийг жил бүр (эсхүл өөрчлөлт гарах тухай бүр) шалгаж баталгаажуулна.

6.2. Мэдээллийн хөрөнгийн бүртгэл

6.2.1. Компанийн мэдээллийн хөрөнгийг бүртгэхдээ 6.1.2.-т заасны дагуу бүртгэж, МТА болон бусад нэгжүүд хоорондоо давхардал үүсгэхгүй байх зарчмыг баримтална.

6.2.2. Хөрөнгийн ангилал: Компани нь МАБ-ын менежментийн тогтолцооны хүрээнд хамаарах бүх хөрөнгийг дараах чиглэлээр ангилан бүртгэж, эзэмшигчийг тогтоон хөтөлнө:

6.2.2.1. Мэдээлэл: Бүх төрлийн цаасан болон цахим хэлбэрийн өгөгдөл, баримт бичиг;

6.2.2.2. Программ хангамж: Хэрэглээний системүүд, өгөгдлийн сан, эх код;

6.2.2.3. Сервер, техник хэрэгсэл: Серверүүд, компьютер, хадгалах төхөөрөмж болон бусад хөдөлгөөнт болон суурин техник хэрэгсэл, уурхайн талбар дахь техникийн тоног төхөөрөмж;

6.2.2.4. Сүлжээ: Шилэн кабель, дотоод болон гадаад сүлжээний зангилаа цэгүүд, сүлжээний төхөөрөмжүүд, холбооны төхөөрөмжүүд, холбооны шугам, дэд бүтэц;

6.2.2.5. Ажилтан: Мэдээлэл болон системд хандах эрх бүхий нийт ажилтнууд.

6.2.3. Мэдээллийн хөрөнгийн бүртгэлд хөрөнгө тус бүрийн таних тэмдэг (код, нэр), төрөл, эзэмшигчийн мэдээлэл, биет болон логик байршил, хамаарал бүхий бусад хөрөнгийг тусгасан байна. Мөн хөрөнгө бүрийн ач холбогдлын түвшинг CIA гэсэн шалгууруар үнэлж бүртгэлд тусгасан байна.

6.2.4. Хөрөнгө бүрд “мэдээлэл эзэмшигч”-ийг тодорхойлно. Эзэмшигч нь тухайн хөрөнгийн ач холбогдлыг үнэлэх, ангиллыг тогтоох, хандалтын эрхийг зөвшөөрөх, аюулгүй байдалд тогтмол хяналт тавих үүрэг хүлээнэ.

6.2.5. Мэдээллийн эзэмшигч нь дараах үүргийг хүлээнэ:

6.2.5.1. Мэдээллийг ангилах, шошголох;

6.2.5.2. Хандалтын эрхийг тодорхойлох, баталгаажуулах;

6.2.5.3. Эрсдэлийг үнэлэхэд оролцох;

6.2.5.4. Хөрөнгийн бүртгэлийн үнэн зөв байдлыг хангах;

6.2.5.5. Хамгаалалтын шаардлагыг тогтоох.

6.2.6. Нэг мэдээллийн хөрөнгөд зөвхөн нэг үндсэн эзэмшигч томилогдох бөгөөд тухайн хөрөнгийн агуулга, ашиглалт, хамгаалалтын шаардлагыг хариуцна.

6.2.6.1. Хүний нөөцийн мэдээлэл (ХН-ийн нэгж эзэмшигч);

6.2.6.2. Санхүүгийн мэдээлэл (Санхүүгийн нэгж эзэмшигч);

6.2.6.3. Гэрээ, эрх зүйн мэдээлэл (Хангамж, ХН-ийн нэгж эзэмшигч);

6.2.6.4. Систем, сервер, сүлжээ (МТ-ийн нэгж).

6.2.7. МТА нь систем, дэд бүтэц, платформын техникийн өмчлөгч байх бөгөөд мэдээллийн агуулга, үнэ цэнийг хариуцах үндсэн эзэмшигч нь тухайн мэдээллийг бий болгож, ашиглаж буй холбогдох чиг үүргийн нэгж байна' гэж засварлавал яаж байна.

6.3. Мэдээллийн ангилал

6.3.1. Компани нь мэдээллийн нууцлалын зэрэглэлийг холбогдох хууль тогтоомж, эрх зүйн актад нийцүүлэн тогтоох бөгөөд мэдээллийн үнэ цэнэ, ач холбогдол болон нууцлалын шаардлагаас нь хамааран дараах байдлаар ангилна:

6.3.1.1. Нийтэд хүртээмжтэй буюу Олон нийтэд: Олон нийтэд нээлттэй задруулбал компанид хохирол учруулахааргүй мэдээлэл;

6.3.1.2. Дотоод хэрэгцээнд: Компанийн дотоод хэрэглээний мэдээлэл, задруулбал бага хохирол учруулж болох;

6.3.1.3. Нууц: Хуульд заагдсан болон Компанийн нууцын журамд тусгагдсан мэдээллүүд хамаарна;

6.3.1.4. Маш нууц: Задруулбал компанид томоохон хохирол учруулж болох мэдээлэл.

6.3.2. Компанийн удирдлага болон ажилтан нь албан тушаал, ажил мэргэжлийн чиг үүргийн хүрээнд олж мэдсэн “Нууц” болон “Дотоод хэрэгцээний” ангилалтай мэдээллийг, мөн компанийн нууцтай танилцах зөвшөөрөл авсан этгээдүүд олж авсан мэдээллийг компанийн нууцын тухай журамд заасан тусгай горимын дагуу эзэмшиж, ашиглах бөгөөд дараах шаардлагыг чанд мөрдөнө:

6.3.2.1. Нууцын баталгаа: Нууцад хамаарах мэдээлэлтэй харьцаж ажиллахаас өмнө “Нууцын баталгаа”-г заавал үйлдэж, баталгаажуулсан байна;

6.3.2.2. Хадгалалт, хамгаалалт: Биет нууц материалыг ажлын цаг дуусмагц зориулалтын сейф, лац бүхий шүүгээнд буцаан байршуулж, түр эзгүйдээ “Цэвэр ширээ, цэвэр дэлгэцийн бодлого”-ыг хэрэгжүүлнэ;

6.3.2.3. Хуулбарлах, дамжуулах: Нууц мэдээллийг хувилж олшруулах, гадагш гаргах, зөвшөөрөлгүй этгээдэд дамжуулахыг хатуу хориглоно;

6.3.2.4. Компанийн үйл ажиллагаатай холбоотой мэдээллийг зөвшөөрөлгүйгээр нийтэд тараахыг хориглоно.

6.4. Мэдээллийн тэмдэглэгээ ба шошгололт

6.4.1. Мэдээллийн шошго нь мэдээллийн хамгаалалтын шаардлагатай уялдсан байна. Ангилсан мэдээллийг биет (цаасан) болон биет бус цахим хэлбэрээр таних тэмдэг, шошгоор баталгаажуулна Үүнд:

6.4.1.1. Цаасан баримт: Баримт бичгийн эхний хуудасны толгойн баруун дээд өнцөгт [НУУЦ] эсвэл [МАШ НУУЦ] гэж бичнэ;

6.4.1.2. Цахим файл: Цахим мэдээллийн хувьд шошгололтыг файлын нэр ([НУУЦ] эсвэл [МАШ НУУЦ]), мета өгөгдөл (мэдээллийн шинж чанар), системийн тохиргоогоор илэрхийлж болно;

6.4.1.3. Цахим шуудан: Цахим шуудангийн сэдэвт [НУУЦ] гэж тэмдэглэнэ;

6.4.1.4. Хавтас: Хавтсанд нууцлалын ангиллын шошго наана.

6.4.2. Шошгололт нь автомат эсвэл гараар хийгдэж болно.

6.4.2.1. Мэдээллийг үүсгэх, хүлээн авах, шинэчлэх үед нууцлалын ангиллыг тодорхойлж, зохих шошгыг заавал тавина.

6.4.2.2. Мэдээллийн ангилал өөрчлөгдсөн тохиолдолд холбогдох шошгололтыг шинэчилж, өмнөх шошгыг хүчингүй болгоно.

6.4.2.3. Мэдээллийн системүүдэд боломжтой тохиолдолд мэдээллийн ангилалд суурилсан автомат шошгололтыг хэрэгжүүлнэ.

6.4.2.4. Шошготой мэдээллийг дамжуулахдаа тухайн ангилалд тохирсон хамгаалалтын арга хэмжээ (шифрлэлт, хамгаалалттай сувгаар дамжуулах) хэрэгжүүлнэ.

6.4.3. Зөөврийн төхөөрөмж (USB, laptop)-д хадгалагдах нууц мэдээлэл нь тухайн ангиллын шошгололттой байх бөгөөд нэмэлт хамгаалалт (шифрлэлт) хэрэглэнэ.

6.5. Мэдээлэл дамжуулах хяналт

6.5.1. Ерөнхий шаардлага: Компани нь дотоод нэгжүүд болон гадаад сонирхогч талуудын хооронд мэдээлэл дамжуулах, солилцох үйл явцад мэдээллийн нууцлаг байдал, бүрэн бүтэн байдал болон хүртээмжтэй байдлыг баталгаажуулах зорилгоор аюулгүй дамжуулалтын суваг, хяналтын механизмыг тогтоон хэрэгжүүлнэ. Энэхүү зохицуулалт нь албаны цахим шуудан, биет баримт бичиг, зөөврийн хадгалах хэрэгсэл, үүлэн үйлчилгээ болон уурхайн үйлдвэрлэлийн технологийн системүүдийн өгөгдөл солилцох бүх төрлийн техникийн суваг, харилцаа холбооны хэрэгсэлд нэгэн адил хамаарна.

6.5.2. Дамжуулах суваг ба зөвшөөрөл:

6.5.2.1. Нийт ажилтнууд мэдээлэл дамжуулахдаа "Харилцаа холбооны матриц"-д заасан зөвшөөрөгдсөн сувгийг ашиглана;

6.5.2.2. "Нууц" болон "Маш нууц" ангилалтай мэдээллийг сүлжээгээр дамжуулахдаа заавал нууцлалын дамжуулалтын протокол (SSL/TLS гэх мэт) эсвэл VPN ашиглана;

6.5.2.3. Нууц мэдээллийг зөөврийн төхөөрөмжөөр дамжуулах тохиолдолд мэдээллийн нууцлал болон бүрэн бүтэн байдлыг хангах үүднээс AES-256, RSA-2048 зэрэг алгоритмаар шифрлэх буюу криптографын аргаар заавал хамгаалсан байна;

6.5.2.4. Хүлээн авагчийг баталгаажуулах шаардлагыг мөрдөнө.

6.5.3. Цахим шуудан ашиглах:

6.5.3.1. Компанийн цахим шуудан хэрэглэгчдийн бүртгэл хөтлөх, шинээр хэрэглэгч нэмэх, өөрчлөх, хасах, хэрэглэгчдийн бүртгэлийн нууцлал аюулгүй байдлыг хангах асуудлыг МТА зохион байгуулна;

6.5.3.2. Ажилтан нь албаны цахим шууданг зөвхөн албан ажлын хэрэгцээнд ашиглаж, өөрийн цахим шуудангийн нууцлал аюулгүй байдлыг хариуцна;

6.5.3.3. Албаны цахим шуудангийн нэвтрэх нууц үгийг энэхүү журмын нууц үгийн дүрэмд заасны дагуу зохион байгуулна.

6.5.3.4. Албаны цахим шуудангаар мэдээлэл дамжуулахдаа эх үүсвэр нь тодорхойгүй, сэжиг бүхий хаяг руу мэдээлэл явуулахгүй байх, мөн тийм хаягнаас ирсэн файл, холбоосыг нээхгүй байх зарчмыг баримтална. Шаардлагатай тохиолдолд мэдээллийн аюулгүй байдлын мэргэжилтэнд мэдэгдэнэ.

6.5.4. Нийлүүлэгчидтэй харилцах: Гаднын нийлүүлэгч, түнш байгууллагатай мэдээлэл солилцох үед МАБ-ын шаардлагыг хангах үүрэг, хариуцлагыг гэрээ хэлцэлд заавал тусгана.

6.5.5. Зөрчлөөс сэргийлэх: Мэдээллийг бусад этгээдэд зөвшөөрөлгүй дамжуулсан эсвэл мэдээлэл алдагдсан тохиолдол илэрвэл ажилтан нь МАБ хариуцсан ажилтанд нэн даруй мэдэгдэнэ.

6.6. Хөрөнгийн зөвшөөрөгдөх хэрэглээ

6.6.1. Ажилтан нь өөрт хариуцуулсан компанийн мэдээллийн хөрөнгө болох техник хангамж, программ хангамж болон мэдээллийн санг зөвхөн ажлын чиг үүргийн албан хэрэгцээнд ашиглах бөгөөд дараах үйлдлийг хориглоно:

6.6.1.1. Зөвшөөрөлгүй хуулбарлах, тараахгүй, өөрчлөх;

6.6.1.2. Хувийн зорилгоор ашиглах;

6.6.1.3. Гуравдагч этгээдэд дамжуулах.

6.6.2. Ажилтан нь компанийн биет болон мэдээллийн хөрөнгийг хэмнэлттэй зарцуулах, аливаа хэлбэрээр хууль бусаар авах, завших, үрэгдүүлэх, сүйтгэхээс урьдчилан сэргийлэх, хамгаалах үүрэг хүлээнэ.

6.7. Хөрөнгийн буцаалт

6.7.1. Компанийн ажилтан нь хөдөлмөрийн гэрээг цуцлах, дуусгавар болгох, өөр албан тушаалд шилжих тохиолдолд өөрийн эзэмшилд байсан бүх биет хөрөнгө болон хариуцан ажиллаж байсан систем, программ хангамж, мэдээллийн сан, нууцын зэрэгтэй мэдээллийг удирдлагын шийдвэрээр түр орлон гүйцэтгэх ажилтанд “тойрох хуудас”-аар бүрэн хүлээлгэн өгнө. “Мэдээллийн хөрөнгийн бүртгэл”-ийн дагуу мэдээллийг ажил хүлээлцэх комисс заавал хүлээж авна.

6.7.2. Ажил хүлээлцэх явцад мэдээллийн хөрөнгийн бүрэн бүтэн байдал, хандалтын эрхийг цуцалсан эсэхийг МТА-наас хянаж, дараах үйлдлийг хийж баталгаажуулна:

6.7.2.1. Ажлын үнэмлэх картыг буцааж авах;

6.7.2.2. Компанийн бүх мэдээллийн хөрөнгө агуулсан бүх төхөөрөмж (суурин компьютер, зөөврийн компьютер, флаш диск, зөөврийн хард диск)-ийг буцааж авах.

6.8. Мэдээллийн технологийн нэгжийн техникийн үүрэг хариуцлага:

6.8.1. МТА нь компанийн мэдээллийн систем, дэд бүтэц болон платформын техникийн өмчлөгч байх бөгөөд дараах техникийн хяналтыг хэрэгжүүлэх үүрэг хүлээнэ:

6.8.1.1. Техникийн аюулгүй орчинд: Мэдээллийг хадгалах, дамжуулах сервер болон сүлжээний найдвартай ажиллагааг хангах, уурхайн үйлдвэрлэлийн технологийн сүлжээг компанийн дотоод сүлжээнээс тусгаарлах техникийн архитектурыг бүрдүүлнэ;

6.8.1.2. Хандалтын техникийн хяналт: Мэдээлэл эзэмшигчийн баталсан "Хандах эрхийн матриц"-ын [Хавсралт №5] дагуу системд нэвтрэх техникийн хязгаарлалт, Олон хүчин зүйлт баталгаажуулалт (MFA) болон нууц үгийн бодлогыг систем дээр хэрэгжүүлнэ;

6.8.1.3. Нөөцлөлт ба Сэргээлт: Үйлдвэрлэлийн процессын эгзэгтэй өгөгдөл, системүүдийн нөөц хуулбарыг тогтоосон хуваарийн дагуу үүсгэж, нөөцөөс сэргээх туршилтыг тогтмол гүйцэтгэн, бэлэн байдлыг хангана;

6.8.1.4. Үйлдлийн бүртгэл ба Мониторинг: Мэдээллийн системд хийгдсэн үйлдлүүдийг (хэн, хэзээ, ямар үйлдэл) лог файл (Log file) хэлбэрээр бүртгэж, 1-ээс (12 сар) доошгүй жилийн хугацаатайгаар аюулгүй хадгалж, хэвийн бус үйлдлийг хянана.

ДОЛОО. ХАНДАЛТЫН ХЯНАЛТ БА УДИРДЛАГА

7.1. Хандалтын удирдлага

7.1.1. Хандалтын эрхийг олгох, өөрчлөх, цуцлах үйл явцыг энэхүү журмын дагуу нэгдсэн байдлаар удирдаж, баримтжуулан хэрэгжүүлнэ. Хандалтын эрхийн бүх өөрчлөлт нь эрх бүхий албан тушаалтны зөвшөөрөлд үндэслэж, бүртгэлд тусгагдана.

7.1.2. Мэдээлэл, систем, сүлжээнд хандалтыг "Хэрэгцээг мэдэх" (Need-to-know) болон "Хамгийн бага эрх олгох" (Least Privilege) зарчмаар зохицуулна.

7.1.3. Хандалтын эрх олгохдоо албан үүргийн дагуу зөвхөн шаардлагатай эрхийг олгоно.

7.1.4. Ажилтнуудын мэдээллийн санд нэвтрэх эрхийг тухайн нэгжийн удирдлагын албан бичгээр ирүүлсэн зөвшөөрлийг үндэслэн МТА өгнө.

7.1.5. МТА нь улирал тутамд "Хандах эрхийн матриц"-ыг хянаж, ашиглагдаагүй болон илүүдэл эрхийг тухай бүр шаардлагатай өөрчлөлтийг оруулж шинэчилнэ.

7.1.6. Систем хариуцсан хэрэглэгчдэд хандах эрхийг олгохдоо зөвшөөрөгдсөнөөс бусад мэдээлэлд хандах боломжгүй байхаар зохион байгуулна;

7.1.7. Систем хариуцсан мэргэжилтэн өөрийн чиг үүргийн дагуу системд нэвтрэх хандалтын эрхийг эдэлнэ;

7.1.8. Ажилтанд системд хандах эрх олгохоосоо өмнө дараах зүйлсийг хийнэ:

7.1.8.1. Ажилтны албан үүргийн дагуу шаардлагатай хандалтын түвшнийг тогтоох;

7.1.8.2. Шууд удирдлага, мэдээлэл хариуцагчаас зөвшөөрөл авах;

7.1.8.3. МАБ-ын журамтай танилцуулж, гарын үсэг зуруулах;

7.1.8.4. Хандалтын эрхийн бүртгэлд бичих.

7.1.9. Хэрэглэгчийн нэр үүсгэхдээ нэгдсэн стандарт дүрэм мөрдөнө.

7.1.10. Нэг нэрийг олон хүн дундаа ашиглахгүй.

7.2. Хандалтын арга хэмжээ

7.2.1. Ажилтан ажлаас гарах үед дараах МАБ-ын арга хэмжээг авна: Мэдээллийн сан, мэдээллийн системд хандах эрх бүхий ажилтан ажлаас гарсан, халагдсан, өөр ажилд шилжсэн тохиолдолд нэвтрэх эрхийг цуцална. Компанийн хүний нөөцийн холбогдох мэргэжилтэн тухайн ажилтныг ажлаас чөлөөлсөн тухай шийдвэр гармагц МТА-ны программ хангамжийн инженерт бичгээр болон албаны цахим шуудангаар мэдэгдсэн байна.

7.2.1.1. Системд хандах бүх эрхийг нэн даруй хүчингүй болгох;
7.2.1.2. Компанийн мэдээлэл ашигласан хувийн төхөөрөмжөөс мэдээллийг устгуулах;
7.2.1.3. Хандалтын эрхийн бүртгэлээс хасах.
7.2.2. Ажилтан албан тушаал шилжих, эсхүл үүрэг өөрчлөгдсөн тохиолдолд хандалтын эрхийг дахин үнэлж, хаах, өөрчлөх, шинэчлэх арга хэмжээг авна.

7.3. Нууц үгийн бодлого

7.3.1. Нууц үгийн шаардлага:
7.3.1.1. Хамгийн багадаа 8, тохиромжтой нь 12+ тэмдэгт;
7.3.1.2. Том, жижиг үсэг, тоо, тусгай тэмдэгт агуулах;
7.3.2. Нууц үг солих:
7.3.2.1. Нууц үгийг 90 хоног тутамд заавал солих;
7.3.2.2. Анхдагч нууц үгийг эхний нэвтрэлтийн дараа заавал солино;
7.3.2.3. Сүүлийн нууц үгийг давтахгүй байх;
7.3.2.4. Нийтлэг нууц үг ашиглахгүй байх;
7.3.3. Нууц үгийн удирдлага
7.3.3.1. Нууц үгийн менежер программ ашиглахыг зөвшөөрнө;
7.3.3.2. Нууц үгийг цахим шуудан буюу имэйл, мессежээр илгээхийг зөвшөөрөхгүй.

НАЙМ. ҮҮЛЭН ҮЙЛЧИЛГЭЭГ ХЭРЭГЛЭХ ҮЕИЙН МАБ

8.1. Үүлэн үйлчилгээг авахад дараах нийтлэг зарчмыг баримтална

8.1.1. Хуулийн нийцэл: Компани нь үүлэн технологид суурилсан үйлчилгээг авахдаа мэдээллийг Монгол Улсын нутаг дэвсгэр дээрх үндэсний дата төв эсвэл түүнтэй дүйцэхүйц зэрэглэлийн дотоодын дата төвд байршуулах зарчмыг баримтална.
8.1.2. Гэрээний шаардлага: Үүлэн үйлчилгээ үзүүлэгчтэй байгуулах гэрээ болон үйлчилгээний түвшний гэрээнд МАБ-ын тусгай нөхцөлийг заавал тусгана
8.1.3. Мэдэгдэх үүрэг: Үйлчилгээний тасралтгүй ажиллагаанд нөлөөлөх техникийн өөрчлөлт, байршлын өөрчлөлт болон кибер халдлага илэрсэн тохиолдолд Компанид нэн даруй мэдэгдэх талаар гэрээнд тусгана;
8.1.4. Гэрээ дуусгавар болох: Үйлчилгээг зогсоох эсхүл өөрчлөх үед нөөц өгөгдөл, тохиргооны файл, эх кодуудыг Компанийн эзэмшилд бүрэн шилжүүлж авах бөгөөд үйлчилгээ үзүүлэгчийн серверээс өгөгдлийг сэргээх боломжгүйгээр устгах ажиллагааг баталгаажуулна.

8.2. Цахим хуудас байршуулах үйлчилгээ

8.2.1. Компанийн цахим буюу веб хуудсыг гаднын веб хостинг үйлчилгээ үзүүлэгч дээр байршуулахдаа дараах шаардлагыг мөрдөнө:
8.2.1.1. Хариуцлагын зааг: Үйлчилгээ үзүүлэгч тал нь серверийн үйлдлийн систем, веб серверийн программ хангамж, дэд бүтцийн аюулгүй байдлыг хариуцах ба Компани нь веб сайтын эх код, өгөгдлийн сангийн агуулга, хэрэглэгчийн хандалтын эрхийг бүрэн хариуцна;

8.2.1.2. Эх кодын аюулгүй байдал: Веб сайтыг байршуулахын өмнө эх кодод эмзэг байдлын дүн шинжилгээ заавал хийж, илэрсэн алдааг зассан байна;

8.2.1.3. Веб хуудасны өгөгдлийн сан дахь мэдээллийг зөвшөөрөлгүй өөрчлөхөөс хамгаалах, тогтмол нөөцлөлт хийх нөхцөлийг тусгана.

8.3. Цахим хуудас ашиглах

8.3.1. Цахим хуудас ашиглалтад дараах зарчмыг баримтална. Үүнд:

8.3.1.1. Компанийн цахим хуудасны аюулгүй байдал, хэвийн үйл ажиллагаа, шинэчлэлт хөгжүүлэлтийг МТА ханган хариуцан ажиллана;

8.3.1.2. Хандалтын хяналт: Хостинг удирдлагын самбарт нэвтрэхдээ Олон хүчин зүйлт баталгаажуулалт (MFA)-ыг заавал ашиглаж, зөвхөн МТА-ны зөвшөөрөгдсөн IP хаягаас хандахаар хязгаарлана;

8.3.1.3. Цахим хуудас нь өгөгдлийн сангуудыг өргөтгөх, цэс нэмэх, засварлах, устгах боломжтой динамик бүтэцтэй, гар утас, таблет веб хөтөч дээр харагдах дэлгэцийн зохиомжтой байна. (Файл дамжуулах протокол болон өгөгдлийн сангийн хэрэглэгчийн нэвтрэх эрхүүдийг үүсгэж хадгална);

8.3.1.4. Цахим хуудасны мэдээ, мэдээлэл түгээх хэл нь Монгол, Англи хэл байна. Цахим хуудасны Монгол, Англи хувилбар бүтэц агуулгын хувьд ялгаатай байж болно;

8.3.1.5. Олон нийттэй харилцах асуудал хариуцсан ажилтан цахим хуудсанд мэдээ, мэдээллийг оруулах, мэдээллийг шинэчлэх ажлыг хийнэ;

8.3.1.6. Цахим хуудаст хуулийн дагуу олон нийтэд ил тод байх ёстой мэдээ, мэдээлэл заавал байршуулсан байна;

8.3.1.7. Мэдээлэл оруулах эрх бүхий ажилтан нь цахим хуудаст мэдээллийг оруулахдаа тухайн нэгжийн удирдлагын зөвшөөрлөөр мэдээллийг оруулна;

8.3.1.8. Цахим хуудсанд тавигдсан мэдээний үнэн бодит байдлыг тухайн нэгжийн удирдлага хариуцна;

8.3.1.9. Цахим хуудас нь гаднын халдлагад өртсөн тохиолдолд МТА сайтыг түр хаах эрхтэй байна.

8.4. Зогсуур түрээслэх болон хадгалах төхөөрөмж байршуулах үйлчилгээ

8.4.1. Компанийн сүлжээний хадгалах төхөөрөмж (NAS)-ийг дата төвд зогсуур түрээслэх хэлбэрээр байршуулахад дараах шаардлагыг мөрдөнө:

8.4.1.1. Биет аюулгүй байдал: Компанийн сүлжээний хадгалах төхөөрөмж байрлаж буй зогсуурт зөвхөн МТА-ны эрх бүхий ажилтан орох эрхтэй байна. Зогсуурт нэвтэрсэн бүх үйлдлийг дата төвийн дүрст хяналтын системээр баримтжуулна;

8.4.1.2. Техникийн хариуцлагын зааг: Дата төв (үйлчилгээ үзүүлэгч) нь серверийн өрөөний биет орчин болон инженерийн дэд бүтцийн аюулгүй байдлын стандарт (хөргөлт, температур, чийгшлийн хяналт, галын дохиолол ба хийн унтраах систем, тасралтгүй тэжээлийн эх үүсвэр) шаардлагыг хангах, биет хандалтыг хянах үүрэг хүлээнэ.

Харин Компани нь сүлжээний хадгалах төхөөрөмжийн (NAS) үйлдлийн системийн аюулгүй байдал, техникийн тохиргоо, нэвтрэх эрхийн удирдлага болон хадгалагдаж буй өгөгдлийн нууцлаг байдал, бүрэн бүтэн байдлыг хангах логик хяналтын хариуцлагыг бүрэн хүлээнэ.

8.4.1.3. Өгөгдлийг шифрлэх: Сүлжээний хадгалах төхөөрөмж дээр хадгалагдаж буй стратегийн өгөгдлийг заавал алгоритмаар шифрлэх бөгөөд сүлжээгээр дамжуулах үед VPN эсвэл SSL/TLS ашиглана;

8.4.1.4. Мониторинг: Сүлжээний хадгалах төхөөрөмжийн системийн хэвийн бус хандалт, техник хангамжийн гэмтлийн лог файлыг (Log file) тогтмол хянана.

ЕС. МАБ-ЫН ЗӨРЧЛИЙН УДИРДЛАГА

9.1. Зөрчлийн удирдлагын төлөвлөлт ба бэлтгэл

9.1.1. МАБ-н зөрчлийн удирдлагыг хэрэгжүүлэхэд нийт ажилтан, гэрээгээр болон түр хугацаагаар ажиллаж буй ажилтан, гуравдагч талтай холбоотой бусад бүх этгээд оролцож дэмжинэ. Нийт ажилтан энэ журам, түүнд агуулагдаж буй зааврууд ыг заавал баримтална.

9.1.2. МАБ-ын зөрчлийг дараах дарааллаар удирдана:

9.1.2.1. Илрүүлэх (Detection);

9.1.2.2. Бүртгэх, мэдэгдэх (Reporting);

9.1.2.3. Үнэлэх, ангилах (Assessment);

9.1.2.4. Хариу арга хэмжээ авах (Response);

9.1.2.5. Сэргээх (Recovery);

9.1.2.6. Зөрчлөөс суралцах ба сайжруулах (Lessons Learned).

9.1.3. МАБ-ын зөрчлийн үйл явцыг нэгдсэн удирдлагаар хангах зорилгоор “Зөрчлийн хариу арга хэмжээний төлөвлөгөө”-г баталж, хэрэгжүүлнэ.

9.1.4. МТА-ны даргаар ахлуулсан “МАБ-ын зөрчлийн хариу арга хэмжээний баг” (Information Security Incident Response Team - ISIRT)-ийн бүрэлдэхүүнд МТА, МАБ хариуцсан ажилтан, Захиргаа хүний нөөцийн хэлтэс (ЗХНХ) болон үйлдвэрлэлийн технологийн системүүдийг хариуцсан инженер, техникийн ажилтнуудын төлөөлөл оролцоно.

9.1.5. Зөрчлийн үед ажиллах төлөвлөгөөг жилд нэгээс доошгүй удаа туршин шалгаж, гарсан үр дүнд үндэслэн төлөвлөгөөг тогтмол шинэчилж сайжруулна.

9.2. Зөрчлийн мэдэгдэл ба тайлагнал

9.2.1. Компанийн нийт ажилтан, гэрээт болон туслан гүйцэтгэгч талууд МАБ-ын зөрчил болон сэжигтэй тохиолдлыг ажигласан даруйдаа “Зөрчил мэдээлэх” харилцаа холбооны олон талт сувгуудыг (QR код бүхий онлайн маягт, Чатбот, тусгай дугаар, дотоод утас (Hotline), Санал хүсэлтийн хайрцаг, цахим шуудангийн хаяг г.м) ашиглаж нэн даруй мэдэгдэх үүрэгтэй.

9.2.2. Зөрчлийг мэдэгдэх суваг, холбоо барих албан тушаалтны мэдээлэл нь нийт ажилтанд нээлттэй, хүртээмжтэй байна.

9.3. Зөрчлийн ангилал ба төрөл

9.3.1. Компани нь мэдээллийн аюулгүй байдлын зөрчлийг тогтмол хувьсан өөрчлөгдөж буй аюул заналын орчинтой уялдуулан, түүний мэдээллийн аюулгүй байдлын үндсэн шинж чанарт (CIA) үзүүлэх нөлөөлөл, шинж чанараар нь дараах үндсэн төрлүүдэд ангилж, МАБ-ын зөрчлийн бүртгэл [Хавсралт №6] бүртгэнэ. Үүнд:

9.3.1.1. Кибер халдлага: Хортой код (malware), барьцаалагч программ (ransomware), фишинг (phishing), үйлчилгээ тасалдуулах халдлага (DoS/DDoS) зэрэг гаднын болон дотоодын санаатай үйлдлүүд;

9.3.1.2. Хандалтын зөрчил: Мэдээллийн систем болон биет орчинд зөвшөөрөлгүй нэвтрэх, нэвтрэх эрхийг хууль бусаар ашиглах, эрхээ хэтрүүлэх үйлдэл;

9.3.1.3. Мэдээлэл алдагдах, задрах: Компанийн нууцад хамаарах өгөгдөл, геологи хайгуулын мэдээлэл, ажилтны хувийн мэдээллийг зөвшөөрөлгүйгээр хуулбарлах, дамжуулах, задруулах;

9.3.1.4. Системийн доголдол ба саатал: Техник болон программ хангамжийн гэмтэл, сүлжээний тасалдал, үйлдвэрлэлийн технологийн системийн үйл ажиллагааны зогсолт;

9.3.1.5. Хяналтын механизмын бүтэлгүйтэл: Мэдээллийн аюулгүй байдлын бодлого, журам, техникийн хяналт (Firewall, Antivirus г.м) үр дүнгүй болох эсхүл зөрчигдөх тохиолдол;

9.3.1.6. Биет аюулгүй байдлын зөрчил: Тоног төхөөрөмж хулгайлагдах, эвдрэх, серверийн өрөөний хамгаалалт алдагдах зэрэг механик үйлдлүүд.

9.4. Зөрчлийн үнэлгээ ба нөлөөллийн ангилал

9.4.1. Зөрчил илрүүлсэн тохиолдолд МАБ хариуцсан ажилтан “Зөрчлийн үнэлгээний шалгуур”-ын дагуу шинжилж, МАБ-ын зөрчил мөн эсэхийг шийдвэрлэнэ.

9.4.2. Зөрчлийн зэрэглэлийг тогтоохдоо дараах хүчин зүйлсийг цогцоор нь харгалзан үзнэ:

9.4.2.1. Үйл ажиллагааны нөлөөлөл: Компанийн үндсэн процесс (олборлолт, ачилт, борлуулалт) болон үйлдвэрлэлийн технологийн сүлжээний тасралтгүй ажиллагаанд үзүүлэх нөлөө;

9.4.2.2. Хамрах хүрээ: Нөлөөлөлд өртсөн хэрэглэгчийн тоо, системийн нэгж болон газар зүйн байршил;

9.4.2.3. Мэдээллийн ангилал: Нөлөөлөлд өртсөн мэдээллийн үнэ цэнэ, нууцлалын зэрэглэл;

9.4.2.4. Хууль эрх зүйн эрсдэл: Кибер аюулгүй байдлын тухай хууль болон бусад хууль тогтоомж, гэрээний үүргийн нийцэл алдагдах магадлал.

9.4.3. Зөрчлийг компанийн үйл ажиллагаанд үзүүлэх нөлөөллөөр нь дараах байдлаар эрэмбэлнэ:

9.4.3.1. 1-р шатны зөрчил (Бага): Компанийн өдөр тутмын үйл ажиллагааны тодорхой хэсэгт бага хэмжээний аюул учруулах;

9.4.3.2. 2-р шатны зөрчил (Дунд): Компанийн үндсэн үйл ажиллагааг (олборлолт, ачилт) хэсэгчлэн саатуулах;

9.4.3.3. 3-р шатны зөрчил (Өндөр/Гамшиг): Компанийн тогтвортой ажиллагаа, санхүү, нэр хүндэд ноцтой хохирол учруулах, үйлдвэрлэлийн технологийн сүлжээг зогсоож болзошгүй тохиолдол.

9.4.4. Зөрчлийг үнэлэхдээ компанийн баталсан мэдээллийн нууцлалын ангиллыг энэхүү журмын заасан “Мэдээллийн хөрөнгийн удирдлага” суурь болгох бөгөөд “Нууц” болон “Маш нууц” зэрэглэлийн мэдээлэл алдагдсан, өөрчлөгдсөн эсвэл зөвшөөрөлгүй хандалт хийгдсэн тохиолдлыг шууд “3-р шатны зөрчил (Өндөр/Гамшиг)”-д хамааруулан ангилж, онцгой горимоор шийдвэрлэнэ

9.5. Зөрчилд хариу арга хэмжээ авах ба сэргээх

9.5.1. МАБ хариуцсан ажилтан болон “МАБ-ын Зөрчлийн хариу арга хэмжээний баг” (МАБЗХАХБ) нь баталсан төлөвлөгөөний дагуу зөрчлийг арилгах, үр дагаврыг хамгийн бага байлгах зорилгоор дараах үе шаттай арга хэмжээг хэрэгжүүлнэ:

9.5.1.1. Тусгаарлах: Зөрчлийн тархалтыг зогсоох, нөлөөллийг хязгаарлахын тулд халдлагад өртсөн систем, сүлжээний сегментийг (ялангуяа үйлдвэрлэлийн сүлжээ) бусад системээс түр тусгаарлах;

9.5.1.2. Устгах: Зөрчил гарсан үндсэн шалтгааныг тодорхойлж, системээс хортой код (malware), зөвшөөрөлгүй хандалт болон бусад аюул заналыг бүрэн арилгах;

9.5.1.3. Сэргээх: Зөрчилд өртсөн системийг нөөц хуулбараас сэргээх, үйл ажиллагааг хэвийн горимд шилжүүлж, бүрэн бүтэн байдлыг шалгаж баталгаажуулах.

9.5.2. Зөрчлийг арилгах, сэргээн босгох үйл ажиллагааны хүрээнд системийн архитектур, тохиргоо болон программ хангамжид өөрчлөлт хийх зайлшгүй шаардлага гарвал энэхүү журмын заасан “Өөрчлөлтийн удирдлага хэрэгжүүлэх үйл явц”-ыг мөрдөнө.

9.5.3. Хэрэв нөхцөл байдал нь үйлдвэрлэлийн зогсолт үүсгэж болзошгүй “Яаралтай өөрчлөлт” шаардсан тохиолдолд яаралтай өөрчлөлтийн процессын заасан түргэвчилсэн горимоор хэрэгжүүлж, зөрчлийг шийдвэрлэсний дараа холбогдох баримтжуулалт, эрсдэлийн үнэлгээг нөхөн гүйцэтгэнэ.

9.6. Нотлох баримт цуглуулах

9.6.1. Зөрчлийг шинжлэх, хууль хяналтын байгууллагад хандах зорилгоор системийн лог файл (Log file), дүрс бичлэг болон бусад дижитал нотлох баримтыг бүрэн бүтэн байдлыг алдагдуулахгүйгээр цуглуулж, баримтжуулна.

9.6.2. Кибер халдлага, зөрчилд өртсөн мэдээллийн систем, мэдээллийн сүлжээний нотлох баримтыг цуглуулахдаа хөндөхгүй байх, бүрэн бүтэн байдал, хадгалалтын гинжин холбоог хангана.

9.7. Зөрчлөөс суралцах ба сайжруулалт

9.7.1. МАБ-ын зөрчлийг шийдвэрлэсний дараа “Зөрчлийн дараах дүн шинжилгээ” хийж, зөрчил гарсан үндсэн шалтгаан болон үйл явцын үр дүнг бүртгэлийн

хуудсанд тэмдэглэх бөгөөд нэгдсэн тайлан болгон удирдлагын дүн шинжилгээний хурлаар удирдлагад танилцуулна.

9.7.2. Илрүүлсэн МАБ-ын зөрчлийн мэдээлэл нь “МАБ-ын эрсдэлийн үнэлгээ ба хариу арга хэмжээний төлөвлөгөө”-г шинэчлэх болон энэхүү журмын “МАБ-ын эрсдэлийн үнэлгээ ба удирдлага” бүлэгт заасан эрсдэлийн үнэлгээг дахин хийх шууд үндэслэл болно. Зөрчлийн үр дүнд аюул заналын тохиолдох магадлал болон нөлөөллийн зэрэглэлийг бодитойгоор дахин үнэлнэ.

9.7.3. Давтагдсан болон өндөр нөлөө бүхий зөрчлийг эрсдэлийн түвшинг нэмэгдүүлэн авч үзэх ба эрсдэлийг бууруулах төлөвлөгөөний хүрээнд нэмэлт техникийн болон зохион байгуулалтын хяналтын механизмыг нэвтрүүлэх үндэслэл болгон ашиглана.

9.7.4. Компани нь МАБ-ын зөрчлийн удирдлагын үр дүнг дараах гүйцэтгэлийн гол үзүүлэлтүүдээр хэмжиж, удирдлагын дүн шинжилгээний хуралд тайлагнана:

9.7.4.1. Зөрчил илрүүлэх дундаж хугацаа: Зөрчил гарсан мөчөөс түүнийг илрүүлэх хүртэлх хугацаа;

9.7.4.2. Зөрчил шийдвэрлэх дундаж хугацаа: Зөрчлийг илрүүлснээс хойш үйл ажиллагааг бүрэн сэргээх хүртэлх хугацаа;

9.7.4.3. Давтагдсан зөрчлийн хувь: Залруулах арга хэмжээ авсны дараа ижил шалтгаанаар гарсан зөрчлийн эзлэх хувийн жин;

9.7.4.4. Өндөр түвшний зөрчлийн тоо: Компанийн тогтвортой ажиллагаанд нөлөөлөхүйц зөрчлийн тоо.

АРАВ. ХҮНИЙ НӨӨЦИЙН АРГА ХЭМЖЭЭ

10.1. МАБ-ыг хангах чиглэлээр дараах арга хэмжээг авч хэрэгжүүлнэ

10.1.1. Компани нь хүний нөөцтэй холбоотой МАБ-ын эрсдэлийг бууруулахын тулд шинээр ажилд авах, ажиллаж байгаа болон ажлаас гарах үе шат бүрт тохирох арга хэмжээг авч хэрэгжүүлнэ.

10.1.2. МАБ-ын удирдах болон гүйцэтгэх чиг үүргийг ажлын байрны, эсхүл албан тушаалын тодорхойлолтод тусгаж, орон тооны, эсхүл хавсран гүйцэтгэх ажилтныг томилно.

10.1.3. Компани нь цахим орчинд хандаж мэдээлэлтэй ажиллах ажилтан бүртэй компанийн Нууцын журам болон Хөдөлмөрийн дотоод журамд нийцүүлэн “Нууцын баталгаа”-г хөдөлмөрийн гэрээний салшгүй хэсэг болгоно.

10.2. Сургалт, мэдлэгийн үнэлгээ

10.2.1. Нийт ажилтанд зориулсан МАБ-ын мэдлэг, ур чадвар олгох сургалтыг жил бүр тогтмол зохион байгуулж, үр дүнг үнэлж, бүртгэнэ.

10.2.2. МАБ-ын сургалтыг дараах хүрээнд зохион байгуулна:

10.2.2.1. Шинээр ажилд орсон ажилтанд томилогдсоноос хойш 1 сарын дотор “Шинэ ажилтныг чиглүүлэх хөтөлбөр”-ийн хүрээнд МАБ-ын анхны шатны зааварчилгаанд заавал хамруулна;

10.2.2.2. Нийт ажилтанд зориулсан үндсэн МАБ-ын сургалтыг жилд 1 удаа;

10.2.2.3. МТА-ны ажилтнуудад зориулсан техникийн сургалтыг жилд 2 удаа;

10.2.2.4. Мэдээллийн технологи, МАБ хариуцсан ажилтны мэдлэг, ур чадварыг тогтмол дээшлүүлэх арга хэмжээг авах;

10.2.2.5. Удирдах ажилтнуудад зориулсан МАБ-ын удирдлагын сургалтыг жилд 1 удаа;

10.2.2.6. Тусгай зориулалтын программтай ажилладаг эрх бүхий ажилтнуудад жилд 2 удаа;

10.2.3. Сургалтын агуулгад мэдээллийн аюулгүй байдал, кибер эрсдэл, мэдээллийн ангилал, зөрчлийг мэдээлэх зэрэг сэдвүүд багтана.

10.3. Хувийн мэдээллийг хамгаалах

10.3.1. Компани нь ажилтны хувийн мэдээллийг цуглуулах, боловсруулах, ашиглахдаа мэдээллийн эзнээс (ажилтнаас) бичгээр эсхүл цахим хэлбэрээр зөвшөөрөл заавал авна;

10.3.2. Уурхайн талбар болон оффисын нэвтрэх хяналтын системд ажилтныг таньж, баталгаажуулах үйлдлийг хялбарчлах зорилгоор биометрик мэдээллийг (гарын хурууны хээнээс бусад) ашиглахдаа ажилтны зөвшөөрлийг авч, эдгээр мэдээллийг өөрчлөх, бусдад дамжуулахгүй байх үүргийг МТА хүлээнэ.

АРАВ НЭГ. БИЕТ ОРЧНЫ ХАМГААЛАЛТ

11.1. Биет аюулгүй байдлын бүс

11.1.1. Биет аюулгүй байдлын бүсчлэл: Компани нь мэдээллийн хөрөнгө, систем, дэд бүтцийг зөвшөөрөлгүй хандалт, гэмтэл, орчны аюулаас хамгаалах зорилгоор нийт орон зайг ач холбогдлын зэрэглэлээр нь дараах бүсүүдэд ангилж, шаталсан хяналтыг хэрэгжүүлнэ:

Бүс	Нэршил	Объектууд	Хамгаалалтын шаардлага
А бүс	Нээлттэй бүс	Нийтэд мэдээллээр үйлчлэх хэсэг, Хүлээн авах, зочдын хүлээлгийн танхим, нийтийн хурлын заал, уулзалтын өрөө, сургалтын өрөө	Хамгийн бага хяналттай, зочид чөлөөтэй нэвтэрнэ.
В бүс	Хязгаарлагдмал бүс	Компанийн нийт ажилтнуудын ажлын өрөө, санхүүгийн алба, хүний нөөцийн хэлтэс, бичиг хэргийн архив, хангамжийн агуулах	Зөвхөн компанийн ажилтнууд үнэмлэхээр нэвтэрнэ. Хяналтын камераар орох, гарах хэсгийг 24/7 хянах.
С бүс	Техникийн дэд бүтцийн бүс	Уурхайн талбар дахь алслагдсан сүлжээний	Физик хамгаалалт болон орчны хяналт (гал, чийг) чухал.

		зангилаа, АТС-ын өрөө, дэд станц тог баригч, сүлжээний гол зангилаа, шилэн кабелийн хуваарилах хайрцаг хамаарна	Гаднын нөлөөллөөс (гал, ус, тоос, чийг) хамгаалсан байх. Биет хаалт (төмөр тор, хаалга) ба заавал цоожтой байх. Температур, чийгшил, галын мэдрэгч суурилуулж, МТА-ны төв хяналтын самбарт холбох.
D бүс	Хамгаалагдсан бүс	МТА-ны төв серверийн өрөө хамаарна	Хамгийн өндөр хяналт. 24/7 камер, нэвтрэх лог файл, Биометрик эсвэл Карт + Код ашиглах. Камерын бичлэгийг хамгийн багадаа 30 хоног хадгалах. Зөвхөн МТА-ны даргын баталсан жагсаалт дахь эрх бүхий ажилтан нэвтрэх. Бүх орох, гарах үйлдлийг “Биет хандалтын бүртгэл”-ийн [Хавсралт №7] дэвтэр болон “Сервер өрөөний хяналтын хуудас”-д [Хавсралт №8] бүртгэж цахим системд баримтжуулах.

11.1.1.1. Гаднын зочин, гэрээт ажилтан нь хамгаалагдсан бүсэд нэвтрэхдээ бүртгэлд бүртгүүлж, дагалдан нэвтрэх зарчмыг баримтална;

11.1.1.2. ‘C’ болон ‘D’ бүсэд нэвтрэхдээ “Аюултай бүсийн хандалтын бүртгэл” хөтөлж, аюулгүй ажиллагааны зааварчилгааг мөрдөнө;

11.1.1.3. Бүс бүрийн аюулгүй байдлыг тухайн бүсийн нэгжийн удирдлага хариуцна.

11.1.1.4. Биет аюулгүй байдлын зөрчлийг энэхүү журмын “МАБ-ын зөрчлийн удирдлага” бүлэгт заасны дагуу удирдана;

11.1.1.5. Биет орчинд байрлах хөрөнгийг энэхүү журмын “Мэдээллийн хөрөнгийн удирдлага” бүлэгт заасан хөрөнгийн бүртгэлтэй уялдуулан хянаж бүртгэнэ;

11.1.1.6. Биет орчны эрсдэлийг энэхүү журмын “МАБ-ын эрсдэлийн үнэлгээ ба удирдлага” бүлэгт заасан эрсдэлийн үнэлгээнд тусгана.

11.2. Мэдээллийг биет орчинд хадгалах, хамгаалах

11.2.1. Биет мэдээллийн хамгаалалт:

11.2.1.1. B бүсэд: Биет мэдээллийг (цаасан баримт, диск, зөөврийн хадгалах төхөөрөмж) аюул занал, халдлагаас сэргийлж заавал цоожтой шүүгээ, сейфэнд хадгална;

11.2.1.2. D бүсэд: Албаны нууц мэдээллийг гадны нөлөөллөөс хол, тусгай зориулалтын өрөөнд, заавал цоожтой сейфэнд хадгална.

11.2.2. Биет бус (цахим) мэдээллийн хамгаалалт: Мэдээллийг зөвхөн нууц үг бүхий компьютерт хадгалах ба D бүс дэх маш нууц мэдээллийг шаардлагатай

бол сүлжээнд холбогдоогүй эсвэл тусгаарлагдсан нууцлалтай сүлжээнд хадгална.

11.2.3. Бүсийн хариуцлага: Бүс бүрт байршуулсан мэдээлэл, тоног төхөөрөмжийн аюулгүй байдлыг тухайн бүсийг хариуцахаар томилогдсон албан тушаалтан хариуцна.

11.2.4. Нэгжийн ажлын байрны орчин, өрөө тасалгаа, сервер болон мэдээллийн сан хадгалдаг компьютерыг орчны нөлөө (гал, ус, чийг, тоос)-нөөс хамгаалах ажиллагааг тухайн нэгжийн удирдлага хариуцаж, МАБ хариуцсан ажилтан хяналт тавина.

11.3. Серверийн өрөөний хамгаалалт ба нэвтрэх хяналт

11.3.1. Компанийн мэдээллийн систем, систем болон өгөгдлийн сангийн сервер, сүлжээний үндсэн тоног төхөөрөмжүүдийг физик халдлага, орчны аюул заналаас хамгаалах зорилгоор 24/7 харуул хамгаалалт, дүрст хяналтын систем бүхий ‘D бүс’ (Хамгаалагдсан бүс) буюу тусгай зориулалтын серверийн өрөөнд байрлуулна. Уг өрөө нь зөвшөөрөлгүй хандалтаас сэргийлсэн биет хамгаалалттай байхаас гадна орчны хяналтын (гал, чийг, температур) системээр тоноглогдсон байна.

11.3.2. Серверийн өрөөний шаардлага D бүс нь:

a) Цоожтой хаалга (электрон түлхүүр эсвэл код);
b) Дүрст хяналтын камер (24/7 бичлэг);
c) Температур, чийгшил хянах систем (18-24°C, 40-60% чийгшил);
d) Галын дохиолол, унтраах систем;
e) Тасралтгүй тэжээлийн эх үүсвэр (UPS);
f) Цонхгүй эсвэл цонхны хамгаалалттай;
g) Хандах эрхийн бүртгэл (хэн, хэзээ орсон).

11.3.3. Нэвтрэх зөвшөөрөл: D бүсэд зөвхөн мэдээлэл хариуцагч, эзэмшигч эсвэл эрх бүхий ажилтан нэвтэрнэ. Зөвшөөрөлгүй этгээд (зочин, засварчин) нэвтрэх тохиолдолд хариуцсан ажилтны хяналт дор нэвтрүүлж, "Биет хандалтын бүртгэл"-ийг хөтөлнө. [Хавсралт №7]

11.3.4. Жагсаалт батлах: Серверийн өрөөнд нэвтрэх эрхтэй ажилтны жагсаалтыг МТА-ны дарга батална.

11.4. Тоног төхөөрөмжийн аюулгүй байдал

11.4.1. Тогтмол хяналт: D бүсэд байрлуулсан сервер, сүлжээний тоног төхөөрөмжийн хэвийн ажиллагаанд хариуцсан ажилтан тогтмол хяналт тавина.

11.4.2. Мэдээллийн системд холбогдсон сервер, техник хэрэгслүүд нь газардуулгатай өрөөнд байрласан, тэжээлийн нөөц эх үүсвэрт холбогдсон байна.

11.4.3. Засвар үйлчилгээний төлөвлөгөө: Тоног төхөөрөмжийн засвар үйлчилгээг батлагдсан "Засвар үйлчилгээний төлөвлөгөө"-ний дагуу тогтмол хийж, гүйцэтгэлийг баримтжуулна.

11.4.4. Хөрөнгийн бүртгэл: Бүх тоног төхөөрөмжид компанийн өмчийн тэмдэг, (үндсэн хөрөнгийн бүртгэлийн код) дугаар нааж, бүртгэл хөтөлнө.

11.5. Тоног төхөөрөмжийн байрлал

11.5.1. Ажилтан ажлын компьютерын дэлгэцийг бусдад шууд харагдахгүйгээр механик, байгалийн хурц гэрэл буюу нарны гэрэл шууд нөлөөлөхгүй байхаар байрлуулна.

11.5.2. Хэвлэгч, олшруулагч хэрэгслүүдийг хараа хяналттай өрөөнд байрлуулна.

11.5.3. Нэгж дундын болон нэг хүний хэвлэх, олшруулах төхөөрөмжийг ашиглаж болно.

11.6. Ажлын байрны цэвэр ширээ, цэвэр дэлгэцийн бодлого

11.6.1. Компанийн ажилтан бүр ажлын байран дахь мэдээллийг зөвшөөрөлгүй хандалт, алдагдал, гэмтлээс хамгаалах зорилгоор энэхүү дүрмийг өдөр тутмын үйл ажиллагаандаа мөрдөж ажиллана.

11.6.2. **Цэвэр дэлгэцийн бодлого:**

11.6.2.1. Ажилтан ажлын байраа түр орхих эсвэл ажил дуусаж явахдаа компьютерыг заавал түгжих (Win+L) товчлуур ашиглах эсвэл системээс бүрэн гарч (Log-off), (Shut down) унтрааж хэвшинэ;

11.6.2.2. Мэдээллийн системүүд нь 5 минутаас дээш хугацаанд ашиглаагүй тохиолдолд дэлгэц автоматаар (Screen Saver) түгжигдэх (Auto-lock) тохиргоотой байна;

11.6.2.3. Дэлгэц дээрх мэдээлэл хажуугаас болон гаднын хүнд харагдахуйц байрлалтай тохиолдолд нууцлалын шүүлтүүр ашиглана.

11.6.3. **Цэвэр ширээний бодлого:**

11.6.3.1. "Нууц" болон "Дотоод хэрэгцээний" ангилалтай биет баримт бичиг, зөөврийн хадгалах төхөөрөмжийг (USB флаш, хард диск) ашиглаагүй үедээ болон ажлын бус цагаар ширээн дээр ил үлдээхгүй, заавал цоожтой шүүгээ, сейфэнд хадгална;

11.6.3.2. Ажлын байрны ширээ, дэлгэц, хана болон бусад харагдахуйц газарт системд нэвтрэх нэр, нууц үг, хандалтын кодыг бичиж наахыг хатуу хориглоно.

11.6.4. **Хэвлэх, хувилах төхөөрөмжийн аюулгүй байдал:**

Ажилтан хэвлэгч (Printer) болон хувилагч төхөөрөмж дээр хэвлэсэн баримт бичгийг ил үлдээхгүй нэн даруй авч байх.

11.6.5. **Бусад орчны хяналт:**

Хурлын заал, сургалтын танхим дахь цагаан самбар болон проекторын дэлгэц дээрх стратегийн ач холбогдолтой мэдээллийг (геологийн зураг, төлөвлөгөө г.м) уулзалт дуусмагц нэн даруй арилгаж, цэвэрлэнэ.

АРВАН ХОЁР. ТЕХНИК БОЛОН ПРОГРАММ ХАНГАМЖИЙН ЗАСВАР ҮЙЛЧИЛГЭЭ

12.1. Техник болон программ хангамжийн засвар үйлчилгээ

12.1.1. МТА-ны техник хангамж хариуцсан нэгжид засвар үйлчилгээнд ирүүлэх компьютер, тоног төхөөрөмжүүдэд дараах дараах шаардлагыг хангасан байна:

12.1.1.1. Биет бүрэн бүтэн байдал: Төхөөрөмжийн биет битүүмжлэл буюу хамгаалалтын лац нь бүрэн бүтэн, МТА-ны зөвшөөрөлгүйгээр ямар нэгэн задаргаа, механик нөлөөлөл ороогүй байна;

12.1.1.2. Бүртгэл: Компьютер, тоног төхөөрөмж нь (Үндсэн хөрөнгийн бүртгэл) бүртгэлд бүртгэлтэй, үндсэн хөрөнгийн эдийн дугаар болон эзэмшигчийн мэдээлэл, үзүүлэлт бусад шаардлагатай мэдээлэл нь цахим хэлбэрээр бүртгэгдсэн, нэгдсэн сүлжээнд холбогдсон, өөрчлөлтүүд нь тогтмол хөтлөгдсөн байна;

12.1.1.3. Хүсэлт гаргах үйл явц: Техникийн засвар үйлчилгээ авах хүсэлтийг МТА-ны техник хангамж хариуцсан үндсэн нэгжид эсвэл албаны утсанд хандан эвдрэл гэмтлийг албан ёсоор гэмтлийн бүртгэлд бүртгүүлнэ. МТА-ны инженер нь бүртгэл үүсгэхдээ гэмтлийн шинж чанар, ач холбогдлын зэрэглэлийг тогтоож, засвар үйлчилгээний дараалалд оруулна.

12.1.2. Техникийн засвар үйлчилгээ авах тухай албан хүсэлтийг мэдээлэл технологийн техник хангамж хариуцсан үндсэн нэгж нь хүлээн авч, техник хангамжийн инженер нь тухайн төхөөрөмжийн мэдээллийг “Засвар үйлчилгээний бүртгэл” [Хавсралт №9]-д тэмдэглэн компьютер, техникийн засвар үйлчилгээ хариуцсан ажилтан гэмтлийг оношлох, шаардлагатай техник үйлчилгээ хийнэ. Бүх засвар үйлчилгээг зөвхөн МТА-д хандаж шийдвэрлүүлнэ.

12.1.3. Компьютерын техникийн гэмтлийг шуурхай оношлох зорилгоор эд хариуцагчтай холбогдон гэмтэлтэй компьютерыг техникийн засварт дуудаж ирүүлэх, зайнаас зааварчилгаа өгч засварлах эсвэл дуудлагаар ажлын байранд очиж техникийн үзлэг оношилгоо хийж дүгнэлт, гэмтлийн актыг үйлдэнэ.

12.1.4. Гэмтлийн актыг үндэслэн засварт шаардлагатай сэлбэг хэрэгслийн тоо, бараа материалын үйлдвэрийн загвар, техник үзүүлэлтийг тодорхойлон эд хөрөнгө эзэмшигчид өгч хангалт хийсний дараа техникийн засвар үйлчилгээг чанартай шуурхай хийж гүйцэтгэнэ.

12.1.5. МТА-нд засагдах боломжгүй болон баталгаат хугацаандаа байгаа, мэдээлэл хадгалдаг техник тоног төхөөрөмжийг компанийн хамгаалагдсан орон зайнаас гаргаж засварлуулах шилжүүлэх үед мэдээлэл хадгалагдаж буй хатуу дискийг салгаж авч үлдэн засварлуулдаг байна;

12.1.6. Мэдээлэл хадгалагдаж буй хатуу дискийг салгаж авах боломжгүй нөхцөлд дээрх мэдээллийг хуулбарлан нөөцлөн авч энэхүү журмын “Техник хангамжийн засвар үйлчилгээ” дагуу сэргээн ашиглах боломжгүй байдлаар мэдээллийг устгаж засварлуулна.

12.1.7. Мэдээллийн технологи, автоматжуулалттай холбоотой засвар, үйлчилгээг тухайн бүтээгдэхүүн үйлдвэрлэгчээс санал болгосон зааврын дагуу хийж гүйцэтгэнэ.

12.1.8. Программ хангамж суулгах, ашиглах, өөрчлөх үед дараах ангиллын дагуу ашиглана. “Зөвшөөрөгдсөн программ хангамжийн жагсаалт” [Хавсралт №10]

12.1.8.1. Тусгай зориулалтын системүүдийн программ хангамжийн жагсаалт [Хавсралт №11];

12.1.8.2. Хэрэглээний программ хангамжийн жагсаалт [Хавсралт №12].

12.1.9. Компанийн нэгжүүд нь компьютерын нөөц, мэдээллийн технологи, сүлжээ, радио станц, техник тоног төхөөрөмж, тусгай зориулалтын программ хангамжид гарсан эвдрэл гэмтэл, дагалдах хэрэгслийн засвар үйлчилгээг зөвхөн хариуцсан албаны утсанд хандана.

12.2. Компьютер, дагалдах тоног төхөөрөмж ашиглах

12.2.1. Компьютер дээр хэрэглээний программ болон техник хангамж түүний дагалдах тоног төхөөрөмжүүдийн хэвийн ажиллагаа, суурилуулалт, шинэчлэлт болон ажилтны компьютерыг форматлан үйлдлийн системийг дахин суулгах, сүлжээнд холбох ажиллагааг тухайн МТА-ны техник хангамж хариуцсан үндсэн нэгж хариуцна.

12.2.2. Компьютер, техник хэрэгслүүдийн битүүмжлэлийг МТА-ны техник хангамж хариуцсан үндсэн нэгж хариуцаж, хяналт тавьж ажиллана.

12.2.3. Нэгдсэн удирдлагад холбогдсон компьютерын файлын вирусийг шалгах, хамгаалалтын нөхцөлийг МТА-ны техник хангамж хариуцсан үндсэн нэгж хариуцна.

12.2.4. Мэдээлэл устгах: Ашиглалтаас гарсан техник хэрэгслийн хатуу дискийг (HDD, SSD) мэдээлэл сэргээх боломжгүйгээр устгана.

12.2.4.1. Физик устгал: Ашиглагдахгүй болсон тоног төхөөрөмжийн хатуу дискийг физикээр сүйтгэх (Дискийг бутлах - шредер, өрөмдөх, хадаж сүйтгэх);

12.2.4.2. Техникээр устгах: Стандарт устгах "delete" функцийг ашиглах бус, мэдээллийг дахин сэргээгдэхгүй болгох тусгай (Data wiping) программ ашиглаж олон удаа дарж бичих (overwriting);

12.2.4.3. Криптографик устгал: Хэрэв мэдээлэл шифрлэгдсэн (encrypted) бол шифрлэлтийн түлхүүрийг устгах замаар мэдээллийг уншигдах боломжгүй болгох;

12.2.4.4. Салгаж авах: Хэрэв тоног төхөөрөмжийг баталгаат засвар үйлчилгээнд өгч байгаа бол хатуу дискийг (HDD, SSD) заавал салгаж авч үлдэх эсвэл өгөгдлийг шифрлэх хэрэв боломжгүй бол мэдээллийг бүрэн цэвэрлэх.

12.3. Зөөврийн компьютер, зөөврийн төхөөрөмж ашиглах

12.3.1. Зөөврийн компьютерт хадгалагдаж байгаа мэдээллийг хариуцсан ажилтан хамгаална.

12.3.2. Зөөврийн компьютерыг эзэнгүй орхих тохиолдолд нууц үг шаардахаар тохиргоо хийсэн байна.

12.3.3. Компанийн зөөврийн компьютер, төхөөрөмжүүдийг хувийн эзэмшлийн болон бусад гаднын байгууллагын сүлжээнд холбож, ашиглах тохиолдолд аюулгүй байдлыг тухайн ажилтан хариуцна.

12.3.4. Зөөврийн төхөөрөмжийг заавал хортой кодын эсрэг программаар шалгаж ашиглана.

12.3.5. Ажилтнууд хувийн хэрэгцээний зөөврийн компьютер, төхөөрөмжийг дотоод сүлжээнд ашиглах тохиолдолд мэдээллийн технологи хариуцсан

нэгжийн мэдээллийн технологи хариуцсан ажилтанд мэдэгдэж, зөвшөөрөл авна.

12.3.6. Хувийн хэрэгцээний зөөврийн компьютерыг ажлын байран дээр ашиглах зөвшөөрөл авсан тохиолдолд нэгжийн нийтийн бүсийн сүлжээнд холбон ашиглана.

12.3.7. Зөөврийн хадгалах төхөөрөмж, компьютерын ашиглалт:

12.3.7.1. Ажилтан эзэмшиж буй хөрөнгийнхөө бүрэн бүтэн байдалд хяналт тавьж, мэдээлэл устах болон хулгайд алдагдах эрсдэлээс хамгаалах тусгайлсан зааварчилгааны дагуу хариуцлагатай ажиллана;

12.3.7.2. Зөөврийн компьютерт хадгалагдаж байгаа мэдээллийг зохих ёсоор заавал хамгаалах. Аль болох бага мэдээллийг зөөврийн компьютерт байршуулна;

12.3.7.3. Албаны мэдээлэл бүхий зөөврийн компьютертой ажлын байрнаас гадуур ажлаар болон албан томилолтоор явахдаа мэдээллийн нууцлалт, хамгаалалтын асуудлыг судалж мэдсэн байна.

АРВАН ГУРАВ. МЭДЭЭЛЛИЙН СИСТЕМИЙН ХАМГААЛАЛТ

13.1. Аюулгүй танилт

13.1.1. Мэдээллийн хандалтын хяналтад үндэслэн хэрэглэгчийг системд таньж, баталгаажуулах аюулгүй технологи, баталгаажуулалтын аргачлалыг баримтжуулан тогтоож, хэрэгжүүлнэ.

13.1.2. Системд нэвтрэх хэрэглэгчийг баталгаажуулахдаа энэхүү журмын “Хандалтын хяналт ба удирдлага” дагуу Нууц үгийн бодлогыг мөрдлөг болгоно.

13.1.3. Аюулгүй танилтын үйл явцад дараах техникийн хяналтыг хэрэгжүүлнэ:

13.1.3.1. Системд нэвтрэх оролдлого амжилтгүй болсон тохиолдолд хэрэглэгчийн эрхийг тодорхой хугацаагаар түгжих эсхүл хандалтыг хязгаарлах механизмыг бүрдүүлнэ;

13.1.3.2. Баталгаажуулалтын мэдээллийг (нууц үг, токен) сүлжээгээр дамжуулахдаа заавал нууцлалын дамжуулалтын протокол (SSL/TLS гэх мэт) ашиглана.

13.1.4. Системийн зохион байгуулагч болон программ хангамжийн инженер нь системийн аюулгүй танилт, баталгаажуулалтын технологийн хэвийн ажиллагааг хариуцах ба МАБ хариуцсан ажилтан үйл явцын нийцэлд хяналт тавина.

13.1.5. Удирдах албан тушаалтан, систем хариуцсан инженерүүд болон алслагдсан хандалтад олон хүчин зүйлт баталгаажуулалтыг заавал ашиглана

13.1.5.1. Удирдах эрх бүхий ажилтнууд заавал ашиглана;

13.1.5.2. Алслагдсан хандалтад заавал ашиглана;

13.1.5.3. Чухал системд хандахад ашиглана.

13.2. Системийн хандалтын удирдлага

13.2.1. Системийн давуу эрх (admin, root)-тэй хэрэглэгчдийн тоог хамгийн бага байлгана.

13.2.2. Системийн давуу эрхтэй хэрэглэгчийн үйлдэл бүрийг лог файлд (Log file) бүртгэж, хянана.

13.2.3. Системийн өөрчлөлт хийх эрх болон тухайн өөрчлөлтийг батлах/хянах эрхийг нэг хүнд давхар олгохгүй.

13.3. Хортой кодоос хамгаалах

13.3.1. Компанийн хэрэгцээнд ашиглагдаж байгаа компьютер, мэдээлэл хадгалагч болон зөөврийн хэрэгслүүдэд зөвшөөрөгдсөн хортой кодын эсрэг (Вирусийн эсрэг - Antivirus) программ хангамжийг ашиглана.

13.3.2. Хортой кодын эсрэг программын шинэчлэлтийг тогтмол хийнэ.

13.3.3. Тодорхой хугацаанд системийн хортой кодын эсрэг программыг уншуулж, илэрсэн тохиолдолд арилгах арга хэмжээг авна.

13.3.4. Системд гаднаас мэдээлэл оруулах бол сүлжээнд холбогдоогүй компьютерт эхэлж хортой кодын шинжилгээг заавал хийсний дараа системд нэвтрүүлнэ.

13.3.5. Цахим шуудангийн хавсралтыг автоматаар вирусийн эсрэг шалгалт хийнэ.

13.3.6. Интернэтээс программ татахыг хязгаарлана, зөвхөн албан ёсны эх сурвалжаас татахыг зөвшөөрнө.

13.4. Тохиргооны удирдлага

13.4.1. МТА нь компанийн эзэмшилд байгаа техник хангамж, программ хангамж, үйлчилгээ болон сүлжээний аюулгүй байдлын тохиргоог тогтоож, баримтжуулж, хэрэгжүүлж, байнгын мониторинг хийх үйл явцыг тасралтгүй хэрэгжүүлнэ.

13.4.2. Систем тус бүрд тавигдах аюулгүй байдлын стандарт тохиргоог тодорхойлж, шинэ төхөөрөмж нэвтрүүлэх эсвэл техникийн эмзэг байдал илрэх бүрд шинэчлэн батална.

13.4.3. Системийн тохиргоог дараах тохиолдолд шинэчилнэ:

13.4.3.1. Шинэ төхөөрөмж эсвэл программ хангамж нэвтрүүлэх;

13.4.3.2. Техникийн эмзэг байдал илэрсэн эсвэл аюул заналхийлэл өөрчлөгдсөн;

13.4.3.3. Шинэ хувилбар, засвар (нөхөөс - patch) гарсан

13.4.4. Системийн тохиргоог хийх, өөрчлөхдөө дараах зарчмыг баримтална:

13.4.4.1. Хамгийн бага эрх олгох зарчим: Үйлчилгээ, портууд болон функцуудыг зөвхөн компанийн хэрэгцээнд шаардлагатай түвшинд идэвхжүүлж, бусад шаардлагагүй болон эрсдэлтэй функцуудыг хаах;

13.4.4.2. Үйлдвэрлэгчийн анхны (default) тохиргоог өөрчлөх: Анхдагч нууц үг, хэрэглэгчийн нэр болон шаардлагагүй үйлчилгээ, портууд, бусад тохиргоог заавал өөрчилж, систем ашиглалтад орохоос өмнө заавал хаасан байна;

13.4.4.3. Үйлдвэрлэгчийн (OEM) гаргасан аюулгүй байдлын шинэчлэлийг (Patch) суулгахдаа үйлдвэрлэлийн зогсолтоос сэргийлж, эхлээд

туршилтын орчинд шалгасны дараа төлөвлөгөөт засвар үйлчилгээний үеэр хэрэгжүүлнэ.

13.4.5. Үйлдлийн систем болон программ хангамжийн шинэчлэлийг (Patch) суулгахаас өмнө эмзэг байдлын дүн шинжилгээ хийж, зөвхөн баталгаат эх сурвалжаас шинэчилнэ

13.4.6. Системийн тохиргоонд орсон аливаа өөрчлөлтийг “Өөрчлөлтийн бүртгэл”-д [Хавсралт №13] тусгаж, зөвшөөрөлгүй өөрчлөлтийг үйлдлийн бүртгэлээр тогтмол хянана.

13.4.7. Тохиргооны удирдлагын хэрэгжилтэд системийн зохион байгуулагч болон программ хангамжийн инженерүүд хариуцан хяналт тавьж ажиллана.

13.4.8. Тасралтгүй хяналт: Тохиргооны өөрчлөлт болон системийн аюулгүй байдлын үйл ажиллагаанд тасралтгүй хяналт, шинжилгээг хийж, хэвийн бус үйлдлийг цаг алдалгүй илрүүлнэ.

13.4.9. Зөрчлийн уялдаа: Дээрх хяналт, шинжилгээний явцад илэрсэн аливаа системийн аюулгүй байдлын зөрчлийг энэхүү журмын “МАБ-ын зөрчлийн удирдлага” бүлэгт заасан журмын дагуу удирдаж, хариу арга хэмжээ авна.

13.5. Үйлдлийн бүртгэл, хяналт

13.5.1. Мэдээллийн систем, мэдээллийн сүлжээнд дараах үйлдлийн бүртгэлийг хөтөлнө:

13.5.1.1. Системд нэвтрэх оролдлого болон нэвтэрсэн тухай;

13.5.1.2. Давуу эрхийн хандалт;

13.5.1.3. Нууц үгийн өөрчлөлт;

13.5.1.4. Үйлдлийн бүртгэлийг өөрчлөх, устгалт;

13.5.1.5. Хандах эрх олгох, өөрчлөх, хүчингүй болгох.

13.5.2. Мэдээллийн системд ажиллаж байгаа хэрэглэгчийн хийсэн үйлдлүүд, хэзээ, хаашаа нэвтэрсэн, ямар үйлдэл хийсэн зэргийг бүртгэгдэж байхаар тохиргоо хийнэ. Үүнд:

13.5.2.1. Хэрэглэгчийн нэр, системд нэвтрэх нэр буюу ID;

13.5.2.2. Огноо;

13.5.2.3. Хандсан хаяг, төхөөрөмжийн мэдээлэл;

13.5.2.4. Хандалтын үргэлжлэх хугацаа;

13.5.2.5. Гүйцэтгэсэн үйлдэл.

13.5.3. Мэдээллийн системийн үйлдлийн бүртгэлд эрх олгогдсон этгээд зөвшөөрлөөр хандах нөхцөлийг бүрдүүлнэ.

13.5.4. Мэдээллийн систем, мэдээллийн сүлжээний үйлдлийн бүртгэлийн лог файлыг (Log file) сар бүр нөөцөлж, хамгийн багадаа 1 жил (12 сар) буюу түүнээс дээш хугацаагаар хадгална. Хадгалах хугацаа дууссаны дараа нягтлан шинжилж, ямар нэгэн зөрчил байхгүй болохыг баталгаажуулсны үндсэн дээр МТА-ны системийн зохион байгуулагч болон МАБ хариуцсан ажилтны хамтарсан дүгнэлтийг үндэслэн удирдлагын зөвшөөрлөөр устгана.

13.5.5. Лог файлыг (Log file) тогтмол хугацаанд шинжилж, үр дүнг “Лог хяналтын бүртгэл” [Хавсралт №14]-д тэмдэглэн баталгаажуулна.

13.5.6. МАБ-ын бодлого, зорилтын хүрээнд нэгдсэн лог файл, хадгалах, хамгаалах системтэй байхыг зорино.

13.6. Эмзэг байдлын удирдлага

13.6.1. Тогтмол хугацаанд эмзэг байдлын шалгалт (vulnerability scan) хийнэ.

13.6.2. Эмзэг байдлыг эрэмбэлж, хугацаанд нь засна.

13.6.3. Систем, программ хангамжийн шинэчлэлийг (patch) сар бүр хийнэ.

13.7. Цагийн синхрончлол

13.7.1. Компанид ашиглаж байгаа бүх мэдээлэл боловсруулах систем, сервер, сүлжээний төхөөрөмж, компьютер болон хэрэглээний программ хангамжуудын цагийг батлагдсан, хүчин төгөлдөр цагийн эх сурвалжтай заавал синхрончилно (ижилсүүлэх);

13.7.2. Компанийн мэдээллийн системүүдийн цагийн эх сурвалж нь Монгол Улсын Стандартчилал, хэмжилзүйн газрын цаг, давтамжийн эталон цагийн серверийн мастер цаг болон Харилцаа холбооны зохицуулах хорооноос тодорхойлсон сүлжээний цагийн эх сурвалж эсхүл олон улсын стандартын шаардлагыг хангасан өндөр нарийвчлалтай цагийн сервертэй холбогдсон байна.

13.7.3. Цагийн синхрончлолыг хэрэгжүүлэхдээ дараах техникийн шаардлагыг мөрдөнө:

13.7.3.1. Бүх сервер болон сүлжээний тоног төхөөрөмжүүд нь дотоод сүлжээний цагийн сервер (Сүлжээний цагийн протокол: Network Time Protocol - NTP) эсхүл батлагдсан гадаад цагийн эх сурвалжтай автоматаар холбогдож, цагаа ижилсүүлж байх тохиргоог заавал хийнэ;

13.7.3.2. Үйлдлийн бүртгэлд лог файл (Log file) хөтөлдөг бүх системд цаг хугацааны тэмдэглэгээ (timestamp) нь зөрүүгүй, нэгдсэн нэг стандартаар (огноо, цаг, минут, секунд) бичигдэх нөхцөлийг бүрдүүлнэ.

13.7.4. МТА-ны нэгжийн инженерүүд нь өөрийн хариуцсан системүүдийн цагийн синхрончлолын үйл ажиллагааг тогтмол хянаж, зөрүү гарсан тохиолдолд тухай бүр тохируулна;

13.7.5. МАБ-ын зөрчил, будилааныг мөрдөх, шинжлэх, задлан шинжилгээ хийх үед цагийн синхрончлол алдагдсан байх нь нотлох баримтын хүчин төгөлдөр байдалд сөргөөр нөлөөлөх тул цагийн серверийн ажиллагаанд МАБ хариуцсан ажилтан хяналт тавьж ажиллана.

13.8. Давуу эрхтэй хэрэглээний программ хангамжийн хэрэглээ

13.8.1. Систем болон хэрэглээний программын аюулгүй байдлын хяналтыг (хандалтын эрх, лог файл гэх мэт) алгасах, давах чадвартай системийн туслах программ хангамж, хэрэгслүүдийн (давуу эрхтэй хэрэглээний программууд) хэрэглээг хязгаарлаж, хатуу хяналттай байлгана.

13.8.2. Давуу эрхтэй хэрэглээний программ хангамж ашиглах үйл ажиллагаанд дараах шаардлагыг мөрдөнө:

13.8.2.1. Давуу эрхтэй программ хангамжийг ашиглах эрхийг зөвхөн эрх бүхий цөөн тооны ажилтанд (системийн зохион байгуулагч, программ хангамжийн инженер) албан ёсоор олгоно;

13.8.2.2. Эдгээр программ хангамжийг ашиглах хэрэгцээ шаардлага, зорилгыг урьдчилан тодорхойлж, зөвхөн шаардлагатай тохиолдолд түр хугацаагаар ашиглах зарчмыг баримтална;

13.8.2.3. Давуу эрхтэй хэрэглээний программ ашигласан бүх үйлдлийг үйлдлийн бүртгэл лог файлд (Log file) заавал тэмдэглэж, тухай бүр хянана.

13.8.3. Мэдээллийн технологийн асуудал хариуцсан нэгж нь давуу эрхтэй программ хангамжуудын жагсаалтыг гаргаж, тэдгээрийг ашиглах эрх бүхий “Давуу эрхтэй хандалтын матриц”-ыг [Хавсралт №15] батлан мөрдүүлнэ.

13.8.4. Давуу эрхтэй программ хангамжийг ашиглан системийн аюулгүй байдлын хяналтыг өөрчилсөн, устгасан тохиолдолд энэ тухай удирдлага болон МАБ хариуцсан ажилтанд даруй мэдэгдэж, зөрчлийн бүртгэлд бүртгэнэ.

13.9. Сүлжээний хамгаалалт

13.9.1. Компанийн стратегийн өгөгдөл болон үйлдвэрлэлийн процессын тасралтгүй байдлыг хангах зорилгоор Үйлдвэрлэлийн технологийн болон мэдээллийн технологийн орчныг техникийн түвшинд (DMZ, Firewall) тусгаарлан хамгаална.

13.9.2. Компани нь уурхайн үйлдвэрлэлийн хяналтын систем болон техникийн удирдлагын сүлжээг уурхайн мэдээллийн технологийн хэрэглэгчийн сүлжээнээс физик болон логик хэлбэрээр бүрэн тусгаарлана. Хоёр сүлжээний уулзвар дээр Демилитаризацийн бүс (DMZ)-ийг байгуулж, зөвхөн зөвшөөрөгдсөн өгөгдлийн урсгалыг нэвтрүүлнэ.

13.9.3. Техникийн дэд бүтцийн найдвартай байдал: МАБ-ыг хангах, мэдээллийн системийн тасралтгүй ажиллагааг хангах, зөвшөөрөлгүй хандалт болон кибер халдлагаас сэргийлэх зорилгоор хяналтын техникийн систем, программ хэрэгслийг дараах техникийн архитектурын шаардлагыг мөрдөнө:

13.9.3.1. Халдлагаас хамгаалах систем: Сүлжээний хамгаалалтын төхөөрөмжүүд (Firewall) нь үйлдвэрлэгчийн албан ёсны байх бөгөөд халдлага илрүүлэх (IDS), таслан зогсоох (IPS), хандалтын хяналт (Access Control), болон веб агуулгын шүүлтүүр (Content Filter) зэрэг үндсэн модулиудыг идэвхжүүлсэн байна;

13.9.3.2. Сүлжээний үндсэн дэд бүтэц: Сүлжээний төв зангилааны (Core) хуваарилагч свичүүд нь Layer 3 түвшний үзүүлэлттэй, албан ёсны программ хангамжийн дэмжлэгтэй байх бөгөөд үйлдвэрлэлийн процессын тасралтгүй байдлыг хангах үүднээс нөөц төхөөрөмжтэй байна;

13.9.3.3. Хандалтын хамгаалалт: Компанийн дотоод сүлжээ болон системд зайнаас хандах (Remote Access) бүх тохиолдолд заавал нууцлалтай суваг буюу Виртуал хувийн сүлжээ (VPN) болон хандалтыг хязгаарлах Галт хана (Firewall)-ын дүрмийг ашиглан техникийн хамгаалалтыг хэрэгжүүлнэ;

13.9.3.4. Архитектурын баримтжуулалт: МТА-ны сүлжээний инженер нь компанийн сүлжээний архитектурыг (Network Architecture) баримтжуулан хадгалах бөгөөд сүлжээний бүтэц, зохион байгуулалт

болон тоног төхөөрөмжид өөрчлөлт орох тухай бүр топологи зургийг (Network Topology Diagram) тогтмол шинэчилж, баримтжуулна.

13.9.4. Сүлжээний бүсчлэл: Компани нь мэдээллийн хөрөнгийн үнэ цэнэ, эрсдэлийн түвшин болон үйл ажиллагааны чиг үүрэгт үндэслэн нэгдсэн сүлжээг физик болон логик (VLAN, Firewall) хэлбэрээр дараах бүсүүдэд заавал тусгаарлаж хамгаална:

13.9.4.1. Үйлдвэрлэлийн сүлжээ: Уурхайн олборлолт, ачилт, тээвэрлэлтийн технологийн системүүдийг агуулсан хамгийн өндөр зэрэглэлийн хамгаалалттай бүс;

13.9.4.2. Демилитаризацийн бүс (DMZ): Дотоод сүлжээ болон интернэт (эсвэл гаднын сүлжээ)-ний уулзвар дээрх шүүлтүүр бүхий завсрын бүс.

13.9.4.3. Серверийн сүлжээ: Компанийн эгзэгтэй системүүд болон өгөгдлийн сан байрлах бүс;

13.9.4.4. Удирдлага ба Хэрэглэгчийн сүлжээ: ИТА болон захиргааны ажилтнуудын өдөр тутмын үйл ажиллагаанд зориулагдсан бүс;

13.9.4.5. Зочны сүлжээ: Гаднын зочин, төлөөлөгчдөд зориулагдсан дотоод сүлжээнээс бүрэн тусгаарлагдсан бүс.

13.9.5. Утасгүй сүлжээний аюулгүй байдал: Компанийн дотоод сүлжээнд утасгүй технологиор (Wi-Fi) нэвтрэхдээ зөвхөн баталгаат шифрлэлтийн алгоритм (WPA2/WPA3 Enterprise) болон төхөөрөмжийг таних техникийн хяналтыг (802.1X authentication) ашиглана. Утасгүй сүлжээний төхөөрөмжийн тохиргоо, нэвтрэх эрх болон SSID менежментийг МТА хариуцан тогтмол хянаж ажиллана.

13.9.6. Зочны сүлжээний хяналт: Зочны Wi-Fi сүлжээ нь компанийн дотоод сүлжээнээс (IT болон OT) техникийн түвшинд бүрэн тусгаарлагдсан байх бөгөөд зөвхөн интернэтийн шууд хандалтаар хангана. Зочны сүлжээгээр дамжуулан компанийн дотоод нөөцөд хандахыг хатуу хориглох ба уг сүлжээний ачаалал, хандалтын бүртгэлийг МТА тогтмол хянана.

13.10. Сүлжээний холболт ашиглах

13.10.1. Кабель шугамын аюулгүй байдал: Компанийн дотоод болон гадаад сүлжээний кабель, холболтын утсыг физик гэмтэл, замаас нь мэдээлэл чагнах болон зөвшөөрөлгүй хандахаас сэргийлж заавал зориулалтын битүүмжлэл бүхий сувагчлал, кабелийн зам ашиглаж хамгаална. Кабель татах, сувагчлах үйл явцыг мэдээллийн технологи хариуцсан нэгж гүйцэтгэх ба МТА-ны сүлжээний инженер техникийн хяналт тавьж, кабелийн хоёр үзүүрийг тэмдэгжүүлэн баталгаажуулна.

13.10.2. Портын удирдлага: МТА-ны сүлжээний инженер нь сүлжээний кабелийн хаягжуулалт, төгсгөлийн цэгүүдийг бүртгэж, аюулгүй байдлыг дараах байдлаар хангана:

13.10.2.1. Сүлжээний төхөөрөмж болон серверийн ашиглагдаагүй сул портуудыг программын түвшинд хааж, зөвшөөрөлгүй хандахаас хамгаална;

13.10.2.2. Программын түвшинд хаах техникийн боломжгүй портуудыг биет хандалтаас сэргийлж лацдах буюу нэвтрэх боломжгүй болгон баталгаажуулна;

13.10.2.3. Ашиглагдаагүй сүлжээний гаралтууд дээр тэмдэглэгээ хийж, хөндлөнгийн этгээд ашиглах боломжийг техникийн аргаар хязгаарлана.

13.10.3. Холболтын бүрэн бүтэн байдал: Сүлжээнд дундаас нь холбогдох болон эмзэг цэгүүдэд тавих хяналтыг МТА-ны холбогдох нэгж хариуцна.

13.11. Цахим гарын үсгийн хэрэглээ

13.11.1. Компанийн үйл ажиллагаанд ашиглагдаж буй тоон гарын үсэг нь бичмэл гарын үсгийн нэгэн адил хүчинтэй байх бөгөөд Цахим гарын үсгийн тухай хуульд нийцсэн байна.

АРВАН ДӨРӨВ. НӨӨЦЛӨЛТ БА СЭРГЭЭЛТ

14.1. Нөөцлөлтийн нэгдсэн бодлого

14.1.1. Компани нь мэдээллийн систем, техник хангамжийн гэмтэл, кибер халдлага болон байгалийн гамшгийн үед стратегийн өгөгдлийг алдагдуулахгүй байх, үйл ажиллагааг түргэн шуурхай сэргээх зорилгоор мэдээллийн нөөцлөлт, хадгалалт, сэргээлтийн нэгдсэн бодлогыг хэрэгжүүлнэ.

14.1.2. Нөөцлөлтийн үйл ажиллагааг МТА хариуцан гүйцэтгэх бөгөөд нөөцлөх өгөгдлийн жагсаалт, давтамж, хадгалах хугацааг мэдээллийн үнэ цэнэ, эрсдэлийн үнэлгээнд үндэслэн “Нөөцлөлтийн бүртгэл”-ийг [Хавсралт №16] хөтөлнө.

14.2. Нөөцлөх өгөгдлийн хамрах хүрээ

14.2.1. Компанийн үйлдвэрлэлийн үйл ажиллагааны тасралтгүй байдлыг хангах зорилгоор дараах өгөгдөл, системийг заавал нөөцлөлтөд хамруулна:

14.2.1.1. Үйлдвэрлэлийн технологийн өгөгдөл: Уурхайн олборлолт, ачилт, тээвэрлэлтийн процессыг хянах системүүдийн тохиргоо, лог файл болон үйлдвэрлэлийн түүхэн өгөгдөл;

14.2.1.2. Санхүү, борлуулалтын өгөгдөл: Борлуулалтын өгөгдөл, жингийн хэмжилтийн нэгдсэн өгөгдөл, нэхэмжлэх болон нягтлан бодох бүртгэлийн систем (ERP)-ийн өгөгдлийн сангууд;

14.2.1.3. Хүний нөөцийн өгөгдөл: Ажилтны хувийн хэрэг, цалингийн тооцоо болон цагийн бүртгэл;

14.2.1.4. Программ хангамжийн эх код: Худалдан авсан, захиалан хийлгэсэн болон өөрсдийн зохиосон тусгай зориулалтын хэрэглээний программ хангамжийн эх код, хувилбарууд болон лицензийн мэдээллүүд;

14.2.1.5. Системийн тохиргооны файлууд: Серверүүдийн үйлдлийн систем, өгөгдлийн сангийн тохиргоо болон сүлжээний үндсэн төхөөрөмжүүдийн (Firewall, Switch) дүрмийн тохиргооны файлууд.

14.3. Нөөцлөлтийн техник зохион байгуулалт

14.3.1. Компани нь нөөцлөлтөд “3-2-1” зарчмыг баримтална:

14.3.1.1. **3** хувь нөөц үүсгэх: Өгөгдлийн 3-аас доошгүй хувийг (Үндсэн + 2 нөөц) үүсгэх;

14.3.1.2. **2** төрлийн өөр төхөөрөмжид хадгалах: Нөөц хуулбарыг 2 өөр төрлийн тээгч (NAS сервер болон Гадаад хатуу диск) дээр хадгалах;

14.3.1.3. **1** гадуур: Нөөц хуулбарын 1 хувийг компанийн үндсэн байршлаас өөр газарт (Off-site storage) эсхүл шифрлэгдсэн үүлэн хадгалалтад хадгалах;

14.3.2. Нөөц өгөгдлийг хадгалах төхөөрөмж (NAS) нь компанийн сүлжээнээс логик түвшинд тусгаарлагдсан, зөвхөн нөөцлөлтийн эрх бүхий хэрэглэгч хандах хязгаарлалттай байна.

14.4. Нөөцлөлтийн давтамж ба Сэргээх хугацаа

14.4.1. Системийн чухлын зэргээс хамаарч өгөгдөл алдагдлыг тэвчих хугацаа болон системийг эргэн сэргээх хугацааг тодорхойлж, нөөцлөлтийн хуваарийг батална.

14.4.2. Өдөр тутмын өөрчлөлтийг (Incremental) тухай бүр, бүрэн нөөцлөлтийг (Full backup) долоо хоног тутам заавал гүйцэтгэнэ.

14.4.3. Сэргээх туршилт ба Хяналт: Нөөц хуулбараас системийг амжилттай сэргээж болох эсэхийг баталгаажуулах туршилтыг жилд 1-ээс доошгүй удаа, стратегийн эгзэгтэй системүүдийн хувьд хагас жил тутам хийж, тайланг баримтжуулна.

14.4.4. Нөөцлөлт амжилтгүй болсон тохиолдол бүрд МТА-ны холбогдох ажилтанд автоматаар мэдэгдэл очдог байхаар техникийн мониторингийг тохируулна.

14.4.5. Нөөц өгөгдлийн бүрэн бүтэн байдал ба Хадгалалтын удирдлага: Нөөцөлсөн мэдээллийн аюулгүй байдал, ашиглалтыг баталгаажуулах зорилгоор дараах техникийн шаардлагыг мөрдөнө:

14.4.5.1. Стандарт нэршил: Серверт хадгалагдах нөөц өгөгдлийн файлыг нэрлэхдээ латин үсгээр галиглах ба олон улсын тэмдэгт (Unicode) ашиглан огноо, системийн нэрээр системчлэн бүртгэнэ;

14.4.5.2. Бүрэн бүтэн байдлын хяналт: Нөөцөлсөн өгөгдлийг хадгалах тээгч (NAS, Диск) дээрх өгөгдлийн бүрэн бүтэн байдлыг тогтмол шалгаж, зөвшөөрөлгүй өөрчлөлт орохоос техникийн аргаар хамгаална;

14.4.5.3. Хадгалах хугацаа ба Устгал: Хадгалагдсан нөөц өгөгдлийн ач холбогдол алдагдсан эсвэл хадгалах хугацаа дууссан тохиолдолд МТА-ны даргын шийдвэрээр сэргээгдэх боломжгүйгээр устгах замаар серверийн сул зайг чөлөөлнө.

АРВАН ТАВ. ХОРИГЛОХ ЗҮЙЛ

15.1. Техник, программ хангамжийн хэрэглээнд хориглох зүйлс

15.1.1. Хэрэглэгчийн үйл ажиллагаанд хориглох зүйл:

15.1.1.1. Хөрөнгө: Өөрийн эзэмшиж буй компьютерыг албан бус зориулалтаар (зураг, кино, тоглоом г.м) ашиглах, шууд харьяалах

удирдлагын зөвшөөрөлгүйгээр гаднын этгээдийг ажиллуулах, бусдад дамжуулахыг;

15.1.1.2. Зөвшөөрөлгүй зөөврийн төхөөрөмж ашиглахыг;

15.1.1.3. Засвар үйлчилгээ: Техник хэрэгслийн гэмтлийг дур мэдэн засварлах, лац ломбыг хөндөх, хувь хүн болон гаднын байгууллагаар зөвшөөрөлгүй оношилгоо, засвар хийлгэхийг;

15.1.1.4. Мэдээлэл зөөвөрлөх: Хувийн хэрэгцээний зөвшөөрөлгүй зөөврийн компьютер, төхөөрөмжөөр компанийн нууцад хамаарах мэдээлэл зөөвөрлөхийг;

15.1.1.5. Нууц мэдээлэл: Компанийн нууцад хамаарах (нууц, маш нууц) мэдээллийг зөвшөөрөлгүйгээр хуулбарлах, дамжуулах, хадгалахыг;

15.1.1.6. Мэдээлэл дамжуулах: Компанийн нууцад хамаарах мэдээллийг хуулсан зөөврийн хэрэгсэл (USB Flash, Hard drive)-ийг ил задгай авч явах, зөвшөөрөлгүйгээр бусдад дамжуулахыг;

15.1.1.7. Нэвтрэх нэр, нууц үгийг бусдад дамжуулах, хуваалцахыг;

15.1.1.8. Зайнаас ажиллах: Нийт ажилтнуудын хувьд алсын зайнаас ажиллах үед мэдээллийн аюулгүй байдлын эсрэг төрлийн болон системийн хамгаалалтыг эвдэх, зөвшөөрөлгүй хандах зориулалттай аливаа программ хангамжийг ашиглахыг хатуу;

15.1.1.9. Компанийн зөвшөөрөлгүй алсын зайнаас ажиллах (VPN, RDP) хэрэгсэл ашиглахыг;

15.1.1.10. Гаднын этгээдэд систем, мэдээлэлд зөвшөөрөлгүй хандалт олгохыг;

15.1.1.11. Программ хангамж: Компанийн “Зөвшөөрөгдсөн программ хангамжийн жагсаалт”-д ороогүй аливаа программ хангамжийн хэрэгслүүдийг системд суулгах, ажиллуулах болон ашиглахыг хатуу;

15.1.1.12. Мэдээллийн аюулгүй байдлын хяналтыг тойрч гарах оролдлого хийхийг;

15.1.1.13. Өөрийн эрхээс давсан хандалт авах, эрх нэмэгдүүлэх оролдлого хийхийг;

15.1.1.14. Мэдээллийн аюулгүй байдлын зөрчлийг нуух, мэдээлэхгүй байхыг.

15.2. Сүлжээний хэрэглээнд хориглох зүйлс

15.2.1. Систем ба сүлжээний хориглолт:

15.2.1.1. Танилт ба баталгаажуулалт: Аливаа системд нэвтрэх нэр, нууц үгээ бусдад ямар нэгэн хэлбэрээр дамжуулах, дундаа ашиглах, нууц үг бичсэн цаасыг дэлгэц болон ширээн дээр наахыг;

15.2.1.2. Үйлдвэрлэлийн технологи: Технологийн болон үйлдвэрлэлийн зориулалт бүхий компьютерт зөвшөөрөлгүйгээр зөөврийн мэдээлэл тээгч холбохыг хатуу;

15.2.1.3. Үйлдвэрлэлийн технологийн системд зөвшөөрөлгүй хандалт, өөрчлөлт хийхийг;

15.2.1.4. Сүлжээний холболт: Дотоод сүлжээнд гаднаас зөвшөөрөлгүй компьютер, кабель холбох, сүлжээний тоног төхөөрөмж болон кабелиудыг дур мэдэн салгах, тоног төхөөрөмж дээрх хаяглалт болон лацыг оролдохыг хориглоно;

15.2.1.5. Зөрчил, халдлага: Сүлжээний протокол задлагч болон аюулгүй байдлын хяналтыг алгасах зориулалттай программ хангамж ажиллуулах;

15.2.1.6. Тохиргоо: Мэдээллийн систем дээр ажиллахдаа хэрэглэгчдэд өгсөн эрх, зааврааас өөр дур мэдэн илүү үйлдэл, тохиргоо хийхийг;

15.2.1.7. Сүлжээний тохиргоо болон АйПи (IP - Internet Protocol) хаягийг МТА-ны зөвшөөрөлгүйгээр дур мэдэн өөрчлөх;

15.2.1.8. Тухайн ажилтны компьютерын мэдээлэлд ямар нэгэн бусадтай хамтран ашиглах (Sharing folder) хавтас байхыг;

15.2.1.9. Нууц болон Дотоод хэрэгцээний мэдээллийг дотоод сүлжээнд хяналтгүйгээр хамтран ашиглах (Sharing) тохиргоо хийх;

15.2.1.10. Сүлжээнд байгаа бусад компьютер болон сервер компьютерын мэдээлэл, программ хангамж /файл, директор буюу хавтас/-ыг зөөх, устгах, түүнд эвдрэл гэмтэл учруулах;

15.2.1.11. Веб хандалт ба агуулгын хориглолт: Ажилтан нь албаны цахим хөтчөөс хортой кодын эсрэг системийн болон галт ханын (Firewall) шүүлтүүрээр хязгаарласан, хориглосон цахим хуудас болон агуулга руу нэвтрэх, техникийн хамгаалалтыг (Proxy/VPN ашиглан) тойрч гарах оролдлого хийхийг;

15.2.1.12. Хортой кодоос сэргийлэх хэрэглэгчийн хориглолт: Ажилтан нь үйлдвэрлэлийн болон мэдээллийн технологийн системд зохих зөвшөөрөлгүй, хортой кодын шинжилгээ хийгдээгүй зөөврийн төхөөрөмж (USB, Hard drive) холбох, мөн эх үүсвэр нь тодорхойгүй сэжиг бүхий цахим шуудангийн хавсралт болон холбоос хаягийг нээх, ажиллуулахыг.

Зөрчлийн хариуцлага: Энэхүү бүлэгт заасан техник, программ хангамж болон мэдээллийн болон үйлдвэрлэлийн технологийн сүлжээний аюулгүй байдлын хориглосон заалтуудыг зөрчсөн аливаа үйлдэл, эс үйлдэхүйг мэдээллийн аюулгүй байдлын зөрчилд тооцно. Зөрчлийг энэхүү журмын “МАБ-ын зөрчлийн удирдлага” бүлэгт заасан үе шатны дагуу бүртгэж, шийдвэрлэх бөгөөд гэм буруутай этгээдэд Монгол Улсын Хөдөлмөрийн тухай хууль, Кибер аюулгүй байдлын тухай хууль болон компанийн “Хөдөлмөрийн дотоод журам”-д заасны дагуу сахилгын болон хуулийн хариуцлага хүлээлгэнэ.

ХАВСРАЛТЫН ЖАГСААЛТ

1. МАБ-ын хяналтыг хэрэгжүүлэх мэдэгдэл - Statement of Applicability (SoA)
2. МАБ-ын эрсдэлийн үнэлгээ ба хариу арга хэмжээний төлөвлөгөө
3. Өөрчлөлтийн хүсэлт
4. МТ нэгж дэх Мэдээллийн хөрөнгийн бүртгэл
5. Хандах эрхийн матриц
6. МАБ-ын зөрчлийн бүртгэл
7. Биет хандалтын бүртгэл (Нэвтрэх бүртгэлийн дэвтэр)
8. Сервер өрөөний хяналтын хуудас
9. Засвар үйлчилгээний бүртгэл
10. Зөвшөөрөгдсөн программ хангамжийн жагсаалт
11. Тусгай зориулалтын системүүдийн программ хангамжийн жагсаалт
12. Хэрэглээний программ хангамжийн жагсаалт
13. Өөрчлөлтийн бүртгэл
14. Лог хяналтын бүртгэл
15. Давуу эрхтэй хандалтын матриц
16. Нөөцлөлтийн бүртгэл

Хавсралт №1:

МАБ-ын хяналтыг хэрэгжүүлэх мэдэгдэл - Statement of Applicability (SoA)

Д/д	№	Шаардлага	Хяналт	Сонгосон эсэх	Хяналтыг хэрэгжүүлэх үндэслэл
5.Зохион байгуулалтын хяналт /Organizational controls					
6.Хүний нөөцийн аюулгүй байдал / People controls					
7. Биет орчны аюулгүй байдал / Physical controls					
8. Технологийн хяналт / Technological controls					

Хавсралт №2

МАБ-ын эрсдэлийн үнэлгээ ба хариу арга хэмжээний төлөвлөгөө

ID	Хөрөнгө	Аюул	Сул тал	Эрсдэлийн тодорхойлолт	Нууцлалын нөлөөлөл (C), Бүрэн бүтэн байдлын нөлөөлөл (I), Хүртээмжийн нөлөөлөл (A)	Магадлалын түвшин	Нөлөөллийн түвшин	Эрсдэлийн оноо	Annex A	Хариуцагч	Хариу арга хэмжээний төрөл	Хугацаа	Хэрэгжүүлэх арга хэмжээ

Эрсдэлийн бүртгэлд дараах мэдээллийг оруулна:

1) Хөрөнгийн код (ID);
2) Хөрөнгийн нэр (Хөрөнгө);
3) Аюул;
4) Сул тал;
5) Эрсдэлийн тодорхойлолт;
6) CIA (CIA triad: Нууцлалын нөлөөлөл (C) - Confidentiality, Бүрэн бүтэн байдлын нөлөөлөл (I) - Integrity, Хүртээмжийн нөлөөлөл (A) - Availability);
7) Магадлалын түвшин (1-5);
8) Нөлөөллийн түвшин (1-5) (CIA - хамгийн өндөр түвшингөөр Нөлөөллийн түвшинг тооцно);
9) Эрсдэлийн үнэлгээ (Магадлал × Нөлөөлөл = Эрсдэлийн оноо);
10) ISO/IEC 27001 стандартын Annex A-ийн 93 хяналт (МАБ-ын хяналтыг хэрэгжүүлэх мэдэгдэл - Statement of Applicability (SoA))
11) Эрсдэлийн хариуцагч (Хариуцагч);
12) Хариу арга хэмжээний төрөл (Эрсдэлийг бууруулах, хүлээн зөвшөөрөх, шилжүүлэх, зайлсхийх);
13) Хугацаа;
14) Хэрэгжүүлэх арга хэмжээ;

Хавсралт №3

Өөрчлөлтийн хүсэлт

1. ЕРӨНХИЙ МЭДЭЭЛЭЛ			
Өөрчлөлтийн дугаар:		Хүсэлт гаргасан огноо:	
Хүсэлт гаргагч (Нэр, албан тушаал):		Холбогдох нэгж/хэлтэс:	
Өөрчлөлтийн нэр:			

2. ӨӨРЧЛӨЛТИЙН ТАЙЛБАР БА АНГИЛАЛ
Өөрчлөлт хийх үндэслэл, шаардлага: (Яагаад энэ өөрчлөлт хэрэгтэй вэ?)
Хамрах хүрээ: (Аль систем, сүлжээ, тоног төхөөрөмжид өөрчлөлт орох вэ? IT/OT)
Өөрчлөлтийн ангилал (Сонгох): ☐ Энгийн: Эрсдэл багатай, өдөр тутмын ☐ Чухал: Үйлдвэрлэлийн систем, сүлжээний суурь өөрчлөлт ☐ Яаралтай: Кибер халдлага, ноцтой саатал

3. НӨЛӨӨЛЛИЙН БА ЭРСДЭЛИЙН ҮНЭЛГЭЭ
Үйлдвэрлэлд үзүүлэх нөлөө: (Уурхайн олборлолт, борлуулалт зогсох эрсдэл бий юу?)
МАБ-ын эрсдэл (CIA): Нууцлаг байдал (C): ☐ Их ☐ Дунд ☐ Бага Бүрэн бүтэн байдал (I): ☐ Их ☐ Дунд ☐ Бага Хүртээмжтэй байдал (A): ☐ Их ☐ Дунд ☐ Бага

4. ТЕХНИКИЙН ТӨЛӨВЛӨГӨӨ БА АЮУЛГҮЙ БАЙДАЛ
Хэрэгжүүлэх алхмууд: (Хэзээ, хэн, юу хийх вэ?)
Туршилтын үр дүн: (Туршилтын орчинд шалгасан байдал)
Нөөцлөлт (Backup): Өөрчлөлт хийхийн өмнө нөөц хуулбар хийсэн эсэх: ☐ Тийм ☐ Үгүй
Буцаах төлөвлөгөө (Roll-back plan): (Алдаа гарвал системийг хэрхэн хэвийн төлөвт шилжүүлэх вэ?)

5. ЗӨВШӨӨРӨЛ БА БАТАЛГААЖУУЛАЛТ
Хэрэгжүүлэгч этгээд (Нэр):
Батлагч этгээд (Эрсдэлийн түвшнээс хамаарч): ☐ Нэгжийн удирдлага (Бага эрсдэл) ☐ МТА ба МАБ (Дунд эрсдэл) ☐ Гүйцэтгэх удирдлага / Ерөнхий инженер (Өндөр эрсдэл)

6. ӨӨРЧЛӨЛТИЙН ДАРААХ ДҮН ШИНЖИЛГЭЭ
Үр дүн: ☐ Амжилттай ☐ Амжилтгүй (Буцаасан)
Баримт бичгийн шинэчлэл: (Журам, зураглал, хөрөнгийн бүртгэлд өөрчлөлт оруулсан эсэх)

Хавсралт №4

Мэдээллийн хөрөнгийн бүртгэл

Хөрөнгийн ID	Хөрөнгийн нэр	Хөрөнгийн төрөл	Эзэмшигчийн албан тушаал, нэр	Эзэмшигчийн харьяа нэгж	Хөрөнгийн одоогийн байршил	Хөрөнгийн ач холбогдол (CIA Value)	Хөрөнгийн эмзэг байдал (Vulnerability)	Одоогийн хяналт	Эрсдэлийн тодорхойлолт	Нөлөөлөл (1-5)	Магадлал (1-5)	Эрсдэлийн түвшин (Score)	Эрсдэлийн хариу арга хэмжээний санал

Хавсралт №5:

Хандах эрхийн матриц

№	Системийн нэр	Нийлүүлэгчийн төрөл	Ашиглалтыг хариуцагч	Автоматаар тохируулдаг эсэх	Чухлын зэрэг (1-10)	Эрхийн тохиргооны лог үүсдэг эсэх	Лог зам	Access roles			
								Admin	Manager	Worker	Viewer

Хавсралт №6

МАБ-ын зөрчлийн бүртгэл

№	Илрүүлсэн огноо, цаг	Зөрчлийн товч утга	Холбогдох хөрөнгө / Систем	CIA-д үзүүлсэн нөлөө	Зөрчлийн зэрэглэл (Incident Level 1, 2, 3)	Үүссэн шалтгаан	Авсан арга хэмжээ	Хаасан огноо, цаг	Дахин давтагдахаас сэргийлэх арга

Хавсралт №7

Биет хандалтын бүртгэл

№	Огноо	Нэвтэрсэн ажилтны овог нэр	Албан тушаал / Байгууллага	Нэвтрэх зорилго	Орсон цаг	Гарсан цаг	Дагалдан явсан эрх бүхий ажилтан	Гарын үсэг	Тайлбар

Хавсралт №8

Сервер өрөөний хяналтын хуудас

№	Хяналтын үзүүлэлт	Шалгуур үзүүлэлт / Шаардлага	Төлөв (Тийм/Үгүй)	Тайлбар / Илэрсэн үл тохирол
1	Биет хандалт ба Хамгаалалт			
1.1	Нэвтрэх хяналтын систем	Цоожтой хаалга, электрон түлхүүр эсвэл биометрик танилт хэвийн ажиллаж буй эсэх		
1.2	Хандалтын бүртгэл	"Биет хандалтын бүртгэл" тогтмол хөтлөгдөж, зөвшөөрөлгүй хүн нэвтрээгүй эсэх		
1.3	Дүрст хяналтын систем	Камер 24/7 бичлэг хийж байгаа эсэх, бичлэг 30-аас доошгүй хоног хадгалагдсан эсэх		
2	Орчны нөхцөл ба Аюулгүй байдал			
2.1	Температур, Чийгшил	Температур 18-24°C, чийгшил 40-60%-ийн хооронд тогтвортой байгаа эсэх		
2.2	Галын аюулгүй байдал	Галын дохиолол, Гал унтраах хор цэнэгтэй, бэлэн байгаа эсэх		
2.3	Цахилгаан хангамж	UPS болон батарейнууд хэвийн цэнэгтэй, тэжээлийн нөөц эх үүсвэр бэлэн эсэх		
3	Төхөөрөмж ба Дэд бүтэц			
3.1	Кабелийн зохион байгуулалт	Кабелууд тэмдэгжүүлсэн, замбараагүй орооцолдоогүй, сувагчлалтай эсэх		
3.2	Сул портын хамгаалалт	Ашиглагдаагүй сул портуудыг программ эсвэл лацаар хааж хамгаалсан эсэх		
3.3	Тоног төхөөрөмжийн төлөв	Төхөөрөмжүүдийн хэвийн, эвдрэл гэмтэл илрээгүй эсэх		
4	Сахилга бат ба Цэвэрлэгээ			
4.1	Цэвэр ширээ, Цэвэр дэлгэц	Өрөөнд ил бичиг баримт, зөөврийн диск, нууц үг наасан байдал байхгүй эсэх		

4.2	Орчны цэвэрлэгээ	Өрөөнд тоосжилтгүй, хэрэгцээгүй хайрцаг сав, шатах материал байхгүй эсэх		

Хяналт хийсэн: ..... /Албан тушаал, Нэр/ Огноо: 202... / ... / ...

Баталгаажуулсан: ..... /МТА-ны дарга/

Хавсралт №9

Засвар үйлчилгээний бүртгэл

№	Огноо / Цаг	Хөрөнгийн код / Нэр	Төрөл	Гэмтлийн тодорхойлолт	Гүйцэтгэсэн ажил	Солигдсон сэлбэг	Мэдээллийн аюулгүй байдал	Гүйцэтгэсэн ажилтан	Төлөв

Хавсралт №10

Зөвшөөрөгдсөн программ хангамжийн жагсаалт

№	Программ хангамжийн нэр	Хувилбар	Үйлдвэрлэгч / Нийлүүлэгч	Ангилал	Зориулалт	Лицензийн төрөл	Баталсан огноо

Хавсралт №11

Тусгай зориулалтын системүүдийн программ хангамжийн жагсаалт

№	Системийн нэр	Хариуцагч нэгж / Инженер	Ач холбогдлын зэрэг	Өгөгдлийн сангийн төрөл	Нөөцлөлтийн хуваарь	Хандалтын хэлбэр

Хавсралт №12

Хэрэглээний программ хангамжийн жагсаалт

№	Программ хангамжийн нэр	Зөвшөөрөгдсөн нэгж / Албан тушаал	Суурилуулах эрх	Хамгаалалтын шаардлага	Хориглох зүйл

Хавсралт №13

Өөрчлөлтийн бүртгэл

№	Огноо / Цаг	Хөрөнгийн код / Нэр	Өөрчлөлтийн товч утга	Өөрчлөлтийн төрөл (IT / OT / Patch)	Эрсдэлийн түвшин	Зөвшөөрөл олгосон	Гүйцэтгэсэн ажилтан	Шалгаж баталгаажуулсан

Хавсралт №14

Лог хяналтын бүртгэл

№	Хяналт хийсэн огноо	Системийн нэр / Код	Төрөл (IT / OT)	Хянасан үйлдлийн төрөл (Check: Access/Admin/Config/Error)	Лог бүртгэлийн хамрах хугацаа	Илэрсэн хэвийн бус үйлдэл / Зөрчил	Эрсдэлийн түвшин (Risk Level)	Авсан арга хэмжээ	Хянасан ажилтан	Баталгаажуулсан

Хавсралт №15

Давуу эрхтэй хандалтын матриц

№	Ажилтны нэр / Албан тушаал	Систем / Программ хангамж	Эрхийн түвшин (Root/Admin/Superuser)	Ашиглах үндэслэл	Танилтын хэлбэр (Password/MFA)	Хандах хугацаа (Байнгын / Түр)	Зөвшөөрөл олгосон (Огноо/Гарын үсэг)

Хавсралт №16

Нөөцлөлтийн бүртгэл

№	Огноо / Цаг (Backup Date/Time)	Системийн нэр / Код (System Name / ID)	Төрөл (IT/OT)	Нөөцлөлтийн ангилал (Full / Incremental)	Хадгалах байршил (Storage Location)	Төлөв (Success / Failure)	Сэргээх туршилт (Restore Test Date)	Хариуцагч ажилтан (Admin)	Баталгаажуулсан (Verified By)