

# МОНГОЛ УЛСЫН ХУУЛЬ

2008 оны ....дугаар  
сарын ...-ний өдөр

Улаанбаатар  
хот

## МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ТУХАЙ

### НЭГДҮГЭЭР БҮЛЭГ

#### Нийтлэг үндэслэл

#### 1 дүгээр зүйл. Хуулийн зорилт

1.1. Энэ хуулийн зорилт нь Монгол улсын мэдээллийн аюулгүй байдлын тогтолцоог бий болгох, хувь хүн, аж ахуйн нэгж, байгууллага, төрийн мэдээллийн аюулгүй байдлыг хангахтай холбогдон үүсэх харилцааг зохицуулахад оршино.

#### 2 дугаар зүйл. Мэдээллийн аюулгүй байдлын тухай хууль тогтоомж

2.1. Мэдээллийн аюулгүй байдлын тухай хууль тогтоомж нь Үндсэн хууль, Төрийн нууцын тухай хууль, Байгууллагын нууцын тухай хууль, Хувь хүний нууцын тухай хууль, энэ хууль, Үндэсний Аюулгүй Байдлын үзэл баримтлал болон тэдгээртэй нийцүүлэн гаргасан хууль тогтоомжийн бусад актаас бүрдэнэ.

2.2. Монгол Улсын нэгдэн орсон олон улсын гэрээнд энэ хуульд зааснаас өөрөөр заасан бол олон улсын гэрээний заалтыг дагаж мөрдөнө.

#### 3 дугаар зүйл. Хуулийн нэр томъёоны тодорхойлолт

3.1. Энэ хуульд хэрэглэсэн нэр томъёог дор дурдсан утгаар ойлгоно:

3.1.1. "Мэдээлэл" гэж хүн, эд зүйлс, баримт, үйл явдал, юмс үзэгдэл, үйлдэл болон үйл ажиллагааны тухай илэрхийлэгдэх хэлбэрээсээ үл хамаарах мэдээг хэлнэ;

3.1.2. "Мэдээ" гэж ямар нэг объект, үзэгдэл, үйл явдал, хүчин зүйлийн тухай өгөгдөхүүнийг хэлнэ.

3.1.3. "Монгол улсын мэдээллийн аюулгүй байдал" гэж нийгэм, төр, байгууллагын мэдээллийн орчны хамгаалагдсан байдал болон энэхүү хамгаалагдсан байдлыг хангахын тулд хэрэгжүүлж буй цогц арга хэмжээг хэлнэ;

3.1.4. "Мэдээллийн аюулгүй байдлын бүрдэл хэсэг" гэж мэдээллийн нууцлал, хүртээмж, бүрэн бүтэн байдлыг хэлнэ.

3.1.5. "Мэдээллийн аюулгүй байдлын үзэл баримтлал" гэж мэдээллийн аюулгүй байдлыг хангахад баримтлах стратегийг хэлнэ.

3.1.6. "Байгууллагын мэдээллийн аюулгүй байдал" гэж өгөгдөл, мэдээ, мэдээлэл, баримт материал, тоног төхөөрөмж, мэдээллийг дэмжих дэд бүтцэд хандах боломжийг хаах, түүнийг хууль бус, зүй зохисгүй ашиглах, өөрчлөх, устгах гэмтээх аюулаас хамгаалах, эмзэг сул байдлыг буруугаар ашиглахаас сэргийлэх зорилготой урьдчилан сэргийлэх цогц арга хэмжээг хэлнэ;

3.1.7. "Мэдээллийн аюулгүй байдлын харилцаа" гэж мэдээллийн нэгдмэл байдал, хүртээмжтэй байдал, нууцлалыг хангахтай холбоотой үүсэж буй нийгмийн харилцааг хэлнэ;

- 3.1.8. “Мэдээллийн хүртээмжтэй байдал” гэж шаардлагатай мэдээлэл, үйлчилгээг тохиромжтой цагт олж авах боломж, мэдээллийн бүрдэл хэсгүүд болон дэд бүтцийн элементүүд үйлчилгээ бусниулах халдлагаас хамгаалагдсан байхыг хэлнэ;
- 3.1.9. “Мэдээллийн нууцлал” гэж мэдээллийн бүрдэл хэсгүүд, үйлчилгээ болон дэд бүтцийн элементүүд хууль бус нэвтрэлтээс хамгаалагдсан байхыг хэлнэ;
- 3.1.10. “Мэдээллийн бүрэн бүтэн байдал” гэж мэдээлэл цаг үедээ нийцсэн, зөрчилдөөнгүй, хууль бусаар, зөвшөөрөлгүй өөрчлөхөөс хамгаалагдсан байхыг хэлнэ;
- 3.1.11. “Туравдагч тал” гэж байгууллагын бизнес үйл ажиллагаанд ямар нэг байдлаар оролцож, эсхүл үйлчилгээ үзүүлж буй гадны этгээдийг хэлнэ.
- 3.1.12. “Аюул” гэж Мэдээллийн Аюулгүй Байдлыг ямар нэг байдлаар зөрчиж болох боломж, үйлдэл, үйл явдлыг хэлнэ;
- 3.1.13. “Довтолгоон” гэж аюулыг хэрэгжүүлэх оролдлогыг хэлнэ;
- 3.1.14. “Эмзэг байдал” гэж довтолгоон үйлдэж болох боломжит суваг, замыг хэлнэ;
- 3.1.15. “Эрсдэл” гэж хамгаалалт шаардаж буй хор хохирол учрах магадлалыг хэлэх бөгөөд аюул, эмзэг байдлын үр дүнд бий болно;
- 3.1.16. “Эрсдэлийн шинжилгээ, удирдлага” гэж эд хөрөнгийг адилтгах, тодорхойлох, үнэ цэнийг тогтоох, аюул заналхийллийг үнэлэх, эмзэг байдлыг үнэлэх, одоо байгаа болон төлөвлөж буй аюулгүй байдлын арга хэмжээг үнэлэх, эрсдэлийн үнэлгээ хийх, эрсдэлийг зохих түвшинд хүртэл бууруулах үйл ажиллагааны нэгдлийг хэлнэ;
- 3.1.17. “Эд хөрөнгө” гэж мэдээлэл, өгөгдөл, програм хангамж болон мэдээллийг дэмжих дэд бүтцийг бүрдүүлж буй эд зүйлс, хүний нөөц, байгууллагын нэр хүндийг хэлнэ;
- 3.1.18. “Мэдээллийг дэмжих дэд бүтэц” гэж мэдээллийг үүсгэх, боловсруулах, хадгалах, дамжуулахад ашиглагдаж буй тоног төхөөрөмж, байр орчин, үйлчилгээ, хүний нөөц, бусад хангамжийн нийлбэрийг хэлнэ;
- 3.1.19. “Мэдээллийн аюулгүй байдлын бодлого” гэж мэдээллийн аюулгүй байдлын эрсдэлийн шинжилгээ дээр тулгуурлан байгууллагын мэдээллийн аюулгүй байдлын удирдлагын тогтолцоог бий болгох, аюулгүй байдлын дэг, хяналт, удирдлагуудыг бий болгох талаар гаргасан шийдвэр, баримтлах үндсэн чиглэлүүдийг тусгасан баримт бичгийн нэгдлийг хэлнэ;
- 3.1.20. “Мэдээллийн онц чухал дэд бүтэцтэй байгууллага” гэж мэдээллийн сүлжээ, систем, түүний ажиллагаа нь нийгмийн амьдрал, үндэсний аюулгүй байдалд чухал ач холбогдолтой, эсхүл үүсгэж, боловсруулж, хадгалж, дамжуулж буй мэдээлэл, өгөгдөл нь нууцын зэрэглэлд хамаардаг байгууллагуудыг хэлнэ;
- 3.1.21. “Будлиан” гэж мэдээллийн аюулгүй байдлыг ямар нэг хэлбэрээр зөрчиж буй аливаа учрал, тохиолдол, зөрчил, гэмт хэргийг хэлнэ;
- 3.1.22. “Будлианы удирдлага” гэж Мэдээллийн Аюулгүй Байдлын будлианыг илрүүлэх, мэдээлэх, боловсруулах, хариу үйлдэл хийх, цаашид урьдчилан сэргийлэх талаар хэрэгжүүлж буй цогц арга хэмжээг хэлнэ.
- 3.1.23. “Аудит” гэж байгууллагын мэдээллийн хамгаалалт, мэдээлэл дэмжих дэд бүтцийг шалгах, турших, мэдээллийн аюулгүйн байдлын шаардлагад нийцэж байгаа эсэхийг тодруулах, үнэлэх, мэдээллийн аюулгүй байдлын бодлого, дэг, журмыг хэвшүүлсэн эсэхийг нягтлан шалгах цогц үйл ажиллагааг хэлнэ.

3.1.24. “Системийн аюулгүй байдлын үйлчилгээ” гэж мэдээллийн системийн хэвийн ажиллагаа, үйлчилгээнд зайлшгүй шаардлагатай адилтгах, таньж зөвшөөрөх, хандалтыг удирдах, үйл явдлыг бүртгэх, системийг хянах, шифрлэх, бүрэн бүтэн байдлыг хянах, галт хана (сүлжээ хоорондын дэлгэц) суулгах, аюулгүй байдлыг шинжлэх, тасалдалгүй найдвартай байдлыг хангах, сэргээх боломжийг хангах, холболт үүсгэх, удирдах зэрэг нэмэлт үйлчилгээг хэлнэ.

3.1.25. Програм-техникийн хамгаалалтын арга хэмжээ гэж тоног төхөөрөмж, програм, өгөгдлийн бүрэн бүтэн, хэвийн байдал, мөн чанарыг хянахад чиглэсэн арга хэмжээний цогцыг хэлнэ.

3.1.26. “Логик удирдлага” гэж сүлжээ, систем, мэдээллийн дэд бүтцийг програм, тоног төхөөрөмжийн тусламжтайгаар зохион байгуулах, уялдуулах, зохицуулах, хянах, гажуудал, алдааг засах үйл явцыг хэлнэ.

3.1.27. “Криптографын технологи” гэж чухал мэдээллийн нууцлалыг хангах, түүнийг холбооны сувгаар дамжуулах, хадгалах үед өөрчлөх, хууль бусаар хандахаас хамгаалах шифрлэлтийн арга, технологийг хэлнэ.

3.1.28. “Сүлжээ хоорондын галт хана (дэлгэц)” гэж хоёр болон түүнээс дээш сүлжээний хоорондын хилийг хамгаалах зорилгоор үүсгэсэн хамгаалалтын програм-аппаратын системийг хэлнэ. Өгөгдлийн багцыг сүлжээнд хууль бусаар оруулах, гаргахыг урьдчилан сэргийлдэг. Мөн сүлжээний доторхи хандалтыг хязгаарлахад ашиглагддаг.

3.1.29. “Багцлах” гэж системийн аюулгүй байдлын үйлчилгээний нэг бие даасан хэсэг бөгөөд дамжуулж буй өгөгдлийг шинэ “дугтуй”-нд дугтуйлах, шинэ багц болгон хувиргах ажиллагааг хэлнэ.

3.1.30. “Тоон гарын үсэг” гэж мэдээлэл илгээгчийн үнэн зөвийг тогтоож, өөрчлөгдөөгүй гэдгийг баталгаажуулж буй цахим адилтгагч

3.1.31. “Сэргээн ажиллуулах” гэж халдлага, довтолгоон, будлиан, учрал, онцгой байдлын улмаас систем, сүлжээ, дэд бүтцийн үйл ажиллагаа доголдсон, зогссон үед буцааж хэвийн ажиллагаанд оруулах үйл явцыг хэлнэ.

#### **4 дүгээр зүйл. Мэдээллийн аюулгүй байдлыг хангах үйл ажиллагааны зарчим**

4.1. Мэдээллийн аюулгүй байдлыг хангах үйл ажиллагаанд дараахь зарчмыг баримтлана:

4.1.1. Мэдээллийн Аюулгүй Байдлыг хангах үйл ажиллагаанд хувь хүн, нийгэм төрийн эрх, ашиг сонирхлыг хүндэтгэх, хангах;

4.1.2. Мэдээллийн Аюулгүй Байдлыг хангах үйл ажиллагаа хууль тогтоомжид нийцсэн байх;

4.1.3. Мэдээллийн Аюулгүй Байдлыг хангах үйл ажиллагаа хүний эрх, эрх чөлөөг хүндэтгэсэн байх;

4.1.4. Мэдээллийн Аюулгүй Байдлыг хангах үйл ажиллагаа орчин үеийн шинжлэх ухаан, техник, технологийн ололтод тулгарласан байх;

4.1.5. Олон улсын мэдээллийн аюулгүй байдлын тогтолцоотой ойртон нягтрах;

4.1.6. Мэдээллийн аюулгүй байдлыг хангах арга хэмжээ зохистой байх;

4.1.7. Хамгаалалтын арга хэмжээг хянах боломжтой байх.

4.1.8. Мэдээллийн аюулгүй байдлыг хангах арга хэмжээ үр нөлөөтэй байх;

4.1.9. Мэдээллийн ил тод байдлыг хангах;

4.1.10. Чөлөөт өрсөлдөөн, шинжлэх ухаан техникийн дэвшлийг хөхүүлэн дэмжих;

- 4.1.11. Мэдээллийн аюулгүй байдлыг хангах ажиллагаа эрсдэлийн удирдлага, үнэлгээнд тулгуурлах;
- 4.1.12. Мэдээллийн аюулгүй байдлыг хангах ажиллагаа тасралтгүй байх;
- 4.1.14. Будлианыг цаг алдалгүй илрүүлэх, боловсруулах, хор уршиг, нөлөөллийг үнэлэх;
- 4.1.15. Будлиан болон түүний үр дагаврыг таамаглах боломжтой байх;
- 4.1.16. Хамгаалвал зохих өгөгдөл мэдээлэл, дэд бүтцийн үнэ цэнтэй Мэдээллийн аюулгүй байдлын арга хэмжээ дүйцсэн байх.

## **ХОЁРДУГААР БҮЛЭГ**

### **Мэдээлийн аюулгүй байдлыг хангах тогтолцоо**

#### **6 дугаар зүйл. Мэдээллийн аюулгүй байдлыг хангах тогтолцоо**

6.1. Мэдээллийн аюулгүй байдлыг хангах тогтолцоо нь Монгол Улсын Их Хурал, Монгол улсын Ерөнхийлөгч, Засгийн газар, түүний харьяа яам, агентлаг, хууль хамгаалах байгууллага, бусад байгууллагуудаас бүрдэнэ. Байгууллагууд тус тусын эрх хэмжээний хүрээнд мэдээллийн аюулгүй байдлыг хангах арга хэмжээг боловсруулан хэрэгжүүлэх ажлыг зохион байгуулж, биелэлтэд хяналт тавина.

#### **7 дугаар зүйл. Монгол Улсын Их Хурлын бүрэн эрх**

7.1. Монгол Улсын Их Хурал Мэдээллийн аюулгүй байдлыг хангах талаар дараах бүрэн эрхийг хэрэгжүүлнэ:

- 7.1. Мэдээллийн аюулгүй байдлыг хангах эрх зүйн орчныг бий болгох, шаардлагатай хуулиудыг батлан гаргах
- 7.2. Мэдээллийн аюулгүй байдлын талаар Монгол улсын үзэл баримтлал (стратег), төрийн бодлогыг батлах
- 7.3. Мэдээллийн аюулгүй байдлыг хангах төсвийг батлах

#### **8 дугаар зүйл. Монгол Улсын Ерөнхийлөгчийн бүрэн эрх**

8.1. Монгол Улсын Ерөнхийлөгч нь Үндэсний аюулгүй байдлын зөвлөлийн тэргүүний хувьд Мэдээллийн аюулгүй байдлын талаар дараах бүрэн эрхийг хэрэгжүүлнэ;

- 8.1.1. Монгол улсын хэмжээнд хэрэгжүүлж буй мэдээллийн аюулгүй байдлыг хангах арга хэмжээг уялдуулан зохицуулах, хяналт тавих, санал гаргах, чиглэл өгөх;
- 8.1.2. Монгол Улсын Мэдээллийн Аюулгүй Байдлын үзэл баримтлалыг боловсруулах, Улсын Их Хуралд өргөн барих, хэрэгжилтийг нягтлан шалгах, нэмэлт өөрчлөлт оруулах санал гаргах;
- 8.1.4. Хууль тогтоомжид заасан бусад эрх.

#### **9 дүгээр зүйл. Засгийн газрын бүрэн эрх**

9.1. Засгийн газар мэдээллийн аюулгүй байдлыг хангах талаар дараах бүрэн эрхийг хэрэгжүүлнэ;

- 9.1.1 Мэдээллийн аюулгүй байдлыг хангах төрийн бодлого боловсруулж УИХ-д өргөн барих, хэрэгжүүлэх, мэдээллийн аюулгүй байдлын үзэл баримтлалд нэмэлт, өөрчлөлт оруулах талаар санал гаргах;
- 9.1.2. Мэдээллийн аюулгүй байдлыг хангахад чиглэсэн эрх зүй, эдийн засаг, зохион байгуулалт, дэг, програм-техникийн болон бусад арга хэмжээ авах;

9.1.3. Мэдээллийн аюулгүй байдлыг хангах санхүүжилтийг төсвийн хуулинд тусгаж батлуулах;

9.1.4. Төрийн байгууллагууд болон Мэдээллийн онц чухал дэд бүтэцтэй байгууллагад мэдээллийн аюулгүй байдлын бодлого, дэг журмыг боловсруулж, батлан хэрэгжүүлэх ажлыг удирдах, энэ хуулийн хэрэгжилтийг хангах, гарсан зөрчилд хариуцлага тооцох;

9.1.5. Энэ хуулийн 11.1-д заасан төрийн байгууллага болон Мэдээллийн онц чухал дэд бүтэцтэй байгууллагын жагсаалтыг гаргаж батлан мөрдүүлэх;

9.1.6. Мэдээллийн аюулгүй байдлыг хангах технологийг хөгжүүлэх, технологийн хараат байдлыг багасгах судалгаа, эрдэм шинжилгээний ажлыг хөхүүлэн дэмжих;

9.1.7. Мэдээллийн аюулгүй байдлыг хангах чиглэлээр үндэсний хүний нөөцийг бэлтгэх тогтолцоог хөгжүүлэх, боловсронгуй болгох;

9.1.8. Мэдээллийн аюулгүй байдлын талаар олон улсын хамтын ажиллагааг хөгжүүлэх;

9.1.9. Мэдээллийн аюулгүй байдлын будлиан, учралыг мэдээлэх, боловсруулах үндэсний тогтолцоо бүрэлдэн тогтоход бүх талаар дэмжин туслах, хөгжүүлэх;

9.1.10. Төрийн цахим баримт бичиг солилцох (цахим баримт бичгийн эргэлтийн) системийг үүсгэх, аюулгүй байдлыг хангах арга хэмжээ хэрэгжүүлэх;

9.1.11. Мэдээллийн аюулгүй байдлын үндэсний стандартуудыг төрийн байгууллагуудад хэвшүүлэн мөрдүүлэх;

9.1.12. Хууль тогтоомжид заагдсан бусад эрх.

## **10 дугаар зүйл. Үндэсний Мэдээллийн аюулгүй байдлын асуудал эрхэлсэн төрийн захиргааны төв байгууллагын бүрэн эрх**

10.1. Үндэсний мэдээллийн аюулгүй байдлын асуудал эрхэлсэн төрийн захиргааны төв байгууллага нь Мэдээлэл, Шуудан, Харилцаа Холбооны Технологийн Газар байна.

10.2. Мэдээллийн аюулгүй байдлын асуудал эрхэлсэн төрийн захиргааны төв байгууллага дараах бүрэн эрхийг хэрэгжүүлнэ:

10.1.1. Монгол улсын Мэдээллийн Аюулгүй Байдлын үзэл баримтлал, төрийн бодлогод нэмэлт, өөрчлөлт оруулах талаар санал гаргах;

10.1.2. Мэдээллийн аюулгүй байдлын үндэсний стандарт боловсруулан батлуулах, хэрэгжилтэнд нь хяналт тавих;

10.1.8. Мэдээллийн аюулгүй байдлын будлианыг мэдээлэх, боловсруулах үндэсний тогтолцооны үйл ажиллагааг уялдуулах, нийцүүлэх, гэмт хэргийн шинжтэй будлианыг мэдээлэх, боловсруулах журмыг батлан хэрэгжүүлэх;

10.1.9. Мэдээллийн аюулгүй байдалд учирч болзошгүй аюулаас урьдчилан сэргийлэх, техник технологийн талаар гадаадын аль нэг улсын хараат байдалд орохгүй байх арга хэмжээг авч хэрэгжүүлэх, энэ чиглэлээр бусад байгууллагыг арга зүйн зөвлөмж, удирдлагаар хангах, харилцан уялдааг хангах;

10.1.10. Хууль тогтоомжид заасан бусад бүрэн эрх

## **11 дүгээр зүйл. Төрийн мэдээллийн аюулгүй байдлын асуудал эрхэлсэн төрийн захиргааны төв байгууллагын бүрэн эрх**

11.1 Төрийн мэдээллийн аюулгүй байдлын асуудал эрхэлсэн төрийн захиргааны төв байгууллага нь Тагнуулын Ерөнхий Газар байна.

11.2. Төрийн мэдээллийн аюулгүй байдлын асуудал эрхэлсэн төрийн захиргааны төв байгууллага дараах бүрэн эрхийг хэрэгжүүлнэ:

11.1.1. Төрийн цахим баримт бичиг солилцох системийг зохион байгуулах, удирдах, зохицуулах, хяналт тавих;

11.1.2. Цахим засгийн мэдээллийн нэгдсэн сан, Үндэсний дата төв, нөөцлөх төвийн аюулгүй байдлыг нягтлан шалгах, хянах;

11.1.3. Төрийн байгууллагууд болон Мэдээллийн онц чухал дэд бүтэцтэй байгууллагад мэдээллийн аюулгүй байдлын бодлого, дэг журмыг боловсруулж, батлан хэрэгжүүлж буй байдлыг нягтлан шалгах, хэрэгжилтийг хянах;

11.1.4. Төрийн байгууллагууд болон Мэдээллийн онц чухал дэд бүтэцтэй байгууллагад мэдээллийн аюулгүй байдлыг хангах програм-техникийн арга хэмжээг хэрхэн хэрэгжүүлж буй байдлыг хянах, тусгай зөвшөөрөлтэй байгууллагаар дамжуулан аудит хийх, туршин үзэх

11.1.5. Нууцлалын зэрэглэлтэй мэдээллийг нууцлах технологийн горимыг тогтоож, түүний хэрэгжилтэд хяналт тавих;

## **ГУРАВДУГААР БҮЛЭГ**

### **Мэдээллийн аюулгүй байдлыг хангахад аж ахуйн нэгж, төрийн бус байгууллагын оролцоо**

**12 дугаар зүйл. Мэдээллийн аюулгүй байдлыг хангахад аж ахуйн нэгж, төрийн бус байгууллагын оролцоо, эрх үүрэг;**

12.1. Аж ахуйн нэгж, төрийн бус байгууллага өөрсдийн эзэмшиж буй өгөгдөл, мэдээлэл, мэдээллийн дэд бүтцийн аюулгүй байдлыг хангах үүрэгтэй;

12.2. Аж ахуйн нэгж, төрийн бус байгууллага нь олон улсын болон үндэсний мэдээллийн аюулгүй байдлын стандарт, түүнтэй нийцүүлэн гаргасан удирдамж, дүрэм журмыг үйл ажиллагаандаа мөрдлөг болгон ажиллаж болно;

12.3. Аж ахуйн нэгж, төрийн бус байгууллага нь аюулгүй байдлын цогц удирдлага, эрсдлийн удирдлага нэвтрүүлж, эрсдэлийн үнэлгээ, дахин үнэлгээг тодорхой мөчлөгтэйгөөр хийж болно;

12.4. Эзэмшиж буй системийн хэвийн, тасралтгүй ажиллагааг хангах, онцгой байдлын үед ажиллах, сэргээн ажиллуулах төлөвлөгөө боловсруулж, үйл ажиллагаандаа мөрдлөг болгон ажиллаж болно.

## **ДӨРӨВДҮГЭЭР БҮЛЭГ**

### **Мэдээллийн Аюулгүй Байдлын удирдлага**

**13 дүгээр зүйл. Байгууллагын мэдээллийн аюулгүй байдлын удирдлага**

13.1. Төрийн байгууллагууд болон мэдээллийн онц чухал дэд бүтэцтэй бүх байгууллагад мэдээллийн аюулгүй байдлын удирдлагыг хэрэгжүүлсэн байна.

13.2. Энэ хуулийн 11.1-д зааснаас бусад байгууллага энэ хуулинд заасан мэдээллийн аюулгүй байдлын удирдлагыг хэрэгцээ шаардлагадаа тулгуурлан сонгон хэрэгжүүлж болно.

#### **14 дугаар зүйл. Мэдээллийн аюулгүй байдлын удирдах ажилтан**

14.1 Төрийн байгууллагууд болон мэдээллийн онц чухал дэд бүтэцтэй байгууллагын мэдээллийн аюулгүй байдлын удирдлагыг хэрэгжүүлэх албан тушаалтан нь МАБ-ын удирдах ажилтан (CISO) байна.

14.2 Мэдээллийн эмзэг, онц чухал дэд бүтэцтэй байгууллагууд болон яам, агентлагт МАБ-ын удирдах ажилтны орон тоо, цалингийн фондыг баталсан байна.

14.3 МАБ-ын удирдах ажилтны орон тоонд ажиллах хүн мэдээллийн аюулгүй байдал, сүлжээний аюулгүй байдлын мэргэшсэн, зохих сургалт дүүргэж гэрчилгээ авсан байна.

#### **15 дугаар зүйл. Систем, сүлжээний администратор**

15.1 Мэдээллийн эмзэг, онц чухал дэд бүтэцтэй байгууллагууд болон яам, агентлагийн систем, сүлжээний администратороор ажиллах хүн сүлжээний аюулгүй байдал, системийн удирдлагаар мэргэшсэн, зохих сургалт дүүргэж гэрчилгээ авсан байна.

#### **16 дугаар зүйл. Байгууллагын мэдээллийн аюулгүй байдлын үзэл баримтлал**

16.1. Энэ хуулийн 11.1-д заасан байгууллагууд мэдээллийн аюулгүй байдлын үзэл баримтлалаа тодорхойлсон байна.

16.2. Байгууллагын мэдээллийн аюулгүй байдлын үзэл баримтлалд дараах зүйлсийг заавал тусгасан байна:

16.2.1. Мэдээллийн аюулгүй байдлыг хангах талаар байгууллагын баримтлах үндсэн чиглэл

16.2.2. Мэдээллийн аюулгүй байдлыг хангахад баримтлах зарчмууд

16.2.3. Мэдээллийн аюулгүй байдалд заналхийлж буй аюул, эмзэг байдал, эрсдлийн удирдлага, шинжилгээ, довтолгооны загвар

16.2.4. Байгууллагын мэдээллийн аюулгүй байдлын бодлогын бүтэц

16.2.5. Байгууллагын мэдээллийн аюулгүй байдлын тогтолцоо, удирдлага, бүтэц, албан тушаал

16.2.6. Байгууллагын мэдээллийн аюулгүй байдлын мониторинг, хяналтын тодорхойлолт, төрөл,

#### **17 дугаар зүйл. Байгууллагын мэдээллийн аюулгүй байдлын бодлого**

17.1. Энэ хуулийн 11.1-д заасан байгууллага бүр мэдээллийн аюулгүй байдлын бодлогоо боловсруулж, батлан хэрэгжүүлсэн байна.

17.2. Мэдээллийн аюулгүй байдлын бодлогод байгууллагын мэдээллийн аюулгүй байдлыг хангах үндсэн чиглэл, тогтолцоо, хяналт, арга хэмжээг тусгасан байна.

17.3. Байгууллагын мэдээллийн аюулгүй байдлын бодлогод дараах зүйлсийг заавал тусгасан байна.

17.3.1. Бодлогын зорилго, тавигдах шаардлага,

17.3.2. Эрсдэлийн шинжилгээ, үнэлгээ;

17.3.3. Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоо, дотоод зохион байгуулалт, хүн бүрийн хүлээх үүрэг, хариуцлага, үйл ажиллагааны уялдаа холбоо, тоног төхөөрөмжийг шалган зөвшөөрөх бодлого, нууцлалын гэрээ, эрх бүхий байгууллага, сонирхогчдын бүлэгтэй хамтран ажиллах журам, бие даасан нягтлан шалгах ажиллагааг зохион байгуулах, гуравдагч этгээдтэй харилцах харилцааны удирдлага;

17.3.4. Байгууллагын эд хөрөнгийн тооллого, бүртгэлийн журам, ангилал, үнэлгээ, тэмдэглэгээ, эд хөрөнгийн талаар хүлээх үүрэг, хариуцлага, эд хөрөнгийг ашиглах талаар тавигдах шаардлага, удирдлага;

17.3.5. Хамгаалагдах орон зайд тавигдах шаардлага, хил хязгаар, биет хамгаалалтын зохион байгуулалт, аюулаас хамгаалах арга хэмжээ, ажиллах удирдамж, хамгаалах журам, тоног төхөөрөмжийн аюулгүй байдал, тухайлбал байрлал, хамгаалалт, үйлчилгээ, хангамж, кабелийн аюулгүй байдал, аюулгүй захиран зарцуулах, дахин ашиглах үйл явцыг удирдах удирдлага, тавигдах шаардлага;

17.3.6. Хүний нөөцтэй холбоотой мэдээллийн аюулгүй байдлын шаардлагууд, тухайлбал, ажилд шилж сонгох, ажил эрхлэх, ажлаас халагдах, ажлаа өөрчлөх үед тавигдах шаардлага, удирдлага;

17.3.7. Үйл ажиллагааны дэг журам, үүрэг хариуцлага, гуравдагч талын үйлчилгээ үзүүлэх ажиллагааны удирдлага, системийг төлөвлөх, хүлээн авах удирдамж, хортой кодоос хамгаалах, нөөц хуулбар хийх, сүлжээний аюулгүй байдлыг хангах, мэдээлэл тээгчтэй ажиллах, мэдээлэл солилцох, цахим үйлчилгээ, худалдаанд тавигдах мэдээллийн аюулгүй байдлын шаардлагууд, хяналт шалгалт, мониторинг;

17.3.8. Хандалтын хяналтад тавигдах шаардлага, хэрэглэгчийн хандалтын удирдлага, хэрэглэгчийн үүрэг, сүлжээнд хандах хандалтын удирдлага, үйлдлийн системд хандах хандалтын удирдлага, систем болон мэдээлэлд хандах хандалтын удирдлага, Зөөврийн тооцоолох хэрэгсэл ашиглах болон зайнаас ажиллах ажиллагааны удирдлага;

17.3.9. Мэдээллийн системийн аюулгүй байдлын шаардлагууд, хэрэглээнд зөв ажиллах удирдамж, криптографын технологи ашиглах удирдамж, удирдлага, системийн файлын аюулгүй байдлыг хангах удирдамж, боловсруулах, дэмжих үйл явцын аюулгүй байдлыг хангах удирдлага, техникийн эмзэг байдлын удирдлага;

17.3.10. Мэдээллийн аюулгүй байдлын будлианыг илрүүлэх, мэдээлэх, боловсруулах, нотлох баримт цуглуулах, бэхжүүлэх, урьдчилан сэргийлэх удирдлага;

17.3.11. Бизнесийн тасралтгүй ажиллагааны удирдлагын мэдээллийн аюулгүй байдлын асуудлууд, онцгой байдлын үед ажиллах, сэргээн ажиллуулах төлөвлөгөө;

17.3.12. Бодлогын хууль зүйн болон оюуны өмчийн нийцэл.

17.4. Байгууллага өөрийн үйл ажиллагааны онцлог, мэдээллийн технологиос хамаарсан байдал, бусад хүчин зүйлийг харгалзан үзсэний үндсэн дээр Интернеттэй ажиллах бодлого, нууц түлхүүрийн удирдлагын бодлого, тоон гарын үсгийн бодлого, сүлжээний аюулгүй байдлын бодлого гэх мэт шаардлагатай дэд бодлогыг боловсруулан хэрэгжүүлж болно.

17.5. Мэдээллийн аюулгүй байдлын дэд бодлогод байгууллагын үйл ажиллагааны тодорхой чиглэл, хүмүүсийн ажиллагаа, мэдээллийн технологийн үйл ажиллагаанд мэдээллийн аюулгүй байдлыг хангах удирдлагын шийдвэрийг тусгасан байна.

## **18 дүгээр зүйл. Мэдээллийн аюулгүй байдлын хөтөлбөр**

18.1. Энэ хуулийн 11.1-д заасан байгууллага бүр мэдээллийн аюулгүй байдлын бодлогоо хэрэгжүүлэх хөтөлбөр гаргасан байна.

18.2. Мэдээллийн аюулгүй байдлын хөтөлбөрийн үндэс нь байгууллагын мэдээллийн аюулгүй байдлын бодлого байна.

18.3. Шаардлагатай гэж үзвэл дээд түвшний болон ажлын түвшний хөтөлбөр гаргана.

18.4. Дээд түвшний хөтөлбөрийн зорилго нь эрсдлийг удирдах, мэдээллийн аюулгүй байдлын үйл ажиллагааг уялдуулах, санхүүжилтээр хангах, нөөцийг хуваарилах, стратеги төлөвлөгөө боловсруулах, хяналт тавихад оршино. Дээд түвшний хөтөлбөрийг байгууллагын мэдээллийн аюулгүй байдлын захирал юмуу аюулгүй байдлын менежер удирдана.

18.5. Ажлын түвшний хөтөлбөрийн зорилго нь систем, сүлжээ, үйлчилгээний итгэлтэй, хэмнэлттэй хамгаалалт бий болгоход оршино.

### **19 дугаар зүйл. Аюулгүй байдлын хөтөлбөрийг системийн мөчлөгтэй уялдуулах**

19.1. Бага зардлаар үр нөлөөтэй хамгаалалт бий болгохын тулд мэдээллийн аюулгүй байдлын хөтөлбөрийг хамгаалагдаж буй системийг худалдан авах, суурилуулах, суулгах, ашиглах, ашиглалтаас гаргах мөчлөгтэй уялдуулах арга хэмжээг хэрэгжүүлнэ.

### **20 дугаар зүйл. Эрсдлийн удирдлага**

20.1. Эрсдлийн удирдлага дээр мэдээллийн аюулгүй байдлын удирдлага, бодлого, хөтөлбөр суурилна.

20.2. Эрсдлийн удирдлагын хүрээнд эрсдлийн үнэлгээ, шинжилгээ хийх, эрсдлийг саармагжуулах (хамгаалалтын хэрэгсэл, сөрөг арга хэмжээ) үйл ажиллагаа хамаарагдана.

20.3. Эрсдлийг саармагжуулах арга хэмжээний хүрээнд эрсдлийг үгүй болгох, багасгах, хүлээн авах, шилжүүлэх ажиллагаа хийгдэж болно.

20.4. Эрсдлийн удирдлага дараах үе шатад ангилагдана:

20.4.1. Объектийг сонгох, шинжлэх түвшинг тодорхойлох

20.4.2. Эрсдлийг үнэлэх аргачлалаа сонгох

20.4.3. Эд хөрөнгийг тодорхойлох

20.4.4. Аюул, түүний уршиг, хохирлыг шинжлэх, эмзэг байдлыг илрүүлэх

20.4.5. Эрсдэлийг үнэлэх

20.4.6. Хамгаалалтын арга хэмжээг сонгох

20.4.7. Сонгосон арга хэмжээг хэрэгжүүлэх, шалгах

20.4.8. Үлдэгдэл эрсдлийг үнэлэх

### **21 дүгээр зүйл. Мэдээллийн Аюулгүй Байдлын дэг, журам**

21.1. Энэ хуулийн 11.1-д заасан байгууллага бүр мэдээллийн аюулгүй байдлын бодлого, дэд бодлого, хөтөлбөрөө хэрэгжүүлэхийн тулд аюулгүй байдлын дэг, журмыг батлан мөрдүүлнэ.

21.2. Хүний нөөцийг удирдах, биет хамгаалалтыг зохион байгуулах, системийн үйл ажиллагааны чадварыг дэмжих, аюулгүй байдлын будлианыг удирдах, хариу үйлдэл хийх, сэргээн ажиллуулах үйл явцад ажилтнуудын баримтлах зан үйлийг тодорхойлоход мэдээллийн аюулгүй байдлын дэг, журам чиглэгдэнэ.

21.3. Энэ хуулийн 11.1-д заасан байгууллага бүр хүний нөөцийг шилж сонгох, шалгах, үйл ажиллагааг нь удирдах, шинжлэх, сургах хөгжүүлэх, эрх мэдэл олгох, зөрчилдөөнийг шийдвэрлэх, хандалтын эрх олгох, хаах, нууцлалыг хангах, тоног төхөөрөмж хүлээлцэх, түлхүүрийн нууцлалыг хангах, гуравдагч талын үйлчилгээний аюулгүй байдлыг хангах дэг, журмыг батлан мөрдүүлнэ.

21.4. Энэ хуулийн 11.1-д заасан байгууллага бүр нэвтрэн орох, гарах, галын аюулаас сэргийлэх, дэмжих дэд бүтцийг хамгаалах, өгөгдлийг замаас нь барьж авахаас хамгаалах, хөдөлгөөнт систем, тоног төхөөрөмжийг хамгаалах дэг журмыг батлан мөрдүүлнэ.

21.5. Энэ хуулийн 11.1-д заасан байгууллага бүр хэрэглэгчийг дэмжих, програм хангамжтай ажиллах, програмын өөрчлөлтийг удирдах, нөөц хуулбар хийх, тээгчтэй ажиллах, баримтжуулах, тохируулга хийх, Интернетэд ажиллах, нууц үг, түлхүүрийг удирдах дэг журмыг батлан мөрдүүлнэ.

21.6. Энэ хуулийн 11.1-д заасан байгууллага бүр Мэдээллийн аюулгүй байдлын будлианыг цаг алдалгүй таслан зогсоох, саармагжуулах, хор хохирлыг багасгах, зөрчил гаргагчийг

илрүүлэх, дахин үүсэхээс сэргийлэх зорилгоор мэдээллийн аюулгүй байдлын будлианыг мэдээлэх, боловсруулах, хариу үйлдэл хийх, нотлох баримтыг бэхжүүлэх дэг журмыг батлан мөрдүүлнэ.

21.7. Энэ хуулийн 11.1-д заасан байгууллага байгууллага бүр систем, сүлжээний үйл ажиллагааг тасалдуулах осол, аваар, ноцтой нөхцөл байдлын дараа нэн даруй сэргээн ажиллуулах төлөвлөгөө баталсан байна. Төлөвлөгөөнд ослоос сэргийлэх, илрүүлэх, үр дагаварыг нь арилгах ажиллагаа тусгагдана. Энэ ажиллагааны хүрээнд байгууллагын онц чухал чиг үүрэг, тэргүүлэх чиглэлийг тодорхойлох, онц чухал чиг үүргийг гүйцэтгэхэд шаардлагатай нөөцийг адилтгах, боломжит ослын жагсаалт гаргах, сэргээх ажлын стратегийг боловсруулах, стратегийг хэрэгжүүлэх бэлтгэл ажил хийх, стратегийг шалгах үйл явц хамаарна.

## **ТАВДУГААР БҮЛЭГ**

### **Програм-техникийн арга хэмжээ**

#### **22 дугаар зүйл. Мэдээллийн аюулгүй байдлыг хангах програм-техникийн арга хэмжээ**

22.1. Энэ хуулийн 11.1-д заасан байгууллага бүр сүлжээний бүтэц, зохион байгуулалтын (архитектур) аюулгүй байдлын шаардлага, зарчмыг баримтлан сүлжээ, системээ зохион байгуулсан байна.

22.2. Энэ хуулийн 11.1-д заасан байгууллага бүр тоног төхөөрөмж, програм хангамж, өгөгдлийг хамгаалах, хэвийн ажиллагааг хангах, хянах, зөрчил, будлианаас сэргийлэх, илрүүлэх, таслан зогсоох үйлчлэлийн хүрээг хумих, зөрчил гаргагчийг илрүүлэх, сэргээн ажиллуулахад чиглэгдсэн програм-техникийн цогц арга хэмжээг хэрэгжүүлсэн байна.

22.3. Програм-техникийн цогц арга хэмжээнд адилтгах, таньж зөвшөөрөх, хандалтыг удирдах, үйл явдлыг бүртгэх, хянах, шифрлэх, бүрэн бүтэн байдлыг хянах, галт хана зохион байгуулах, хүртээмжтэй, тасалдалгүй найдвартай байдлыг хангах, сэргээх боломжийг хангах, аюулгүй холболт үүсгэх (tunnelling), мониторинг хийх ажиллагаа хамаарна.

#### **23 дугаар зүйл. Адилтгах, таньж зөвшөөрөх тогтолцоо**

23.1. Энэ хуулийн 11.1-д заасан байгууллага бүр нууц үг, дугаар, түлхүүр, карт, төхөөрөмж, тоон гарын үсэг, био хэмжүүрийн болон орчин үеийн бусад аргууд дээр тулгуурласан адилтгах, таньж зөвшөөрөх тогтолцоо, түүний өгөгдлийн солилцоог хамгаалах технологийг хэрэгжүүлсэн байна.

#### **24 дүгээр зүйл. Хандалтын удирдлага**

24.1. Энэ хуулийн 11.1-д заасан байгууллага бүр хэрэглэгчийн үйлдлийг тодорхойлох, хянах, өгөгдөлд хандах хандалтын нууцлал, бүрэн бүтэн байдлыг хангахын тулд хандалтын логик удирдлагыг хэрэгжүүлсэн байна.

#### **25 дугаар зүйл. Системийн орчны үйл явдлыг бүртгэх, хянах**

25.1. Энэ хуулийн 11.1-д заасан байгууллага бүр хэрэглэгч болон администраторын үйлдлийг тайлагнах, дэс дараалсан үйл явцыг шинжлэх, мэдээллийн аюулгүй байдлыг зөрчсөн будлиан, учралыг илрүүлэх, шинжлэхэд шаардлагатай өгөгдөл бий болгохын тулд системийн орчинд болж буй үйл явдлын тухай мэдээллийг бүртгэх, цуглуулах, хадгалах, уг мэдээллийг шинжлэх програм-техникийн арга хэмжээг хэрэгжүүлж, мэдээллийн аюулгүй байдлын бодлого, дэг журамтайгаа уялдуулсан байна.

#### **26 дугаар зүйл. Шифрлэх**

26.1. Энэ хуулийн 11.1-д заасан байгууллага бүр өгөгдөл, мэдээллийн бүрэн бүтэн байдал, нууцлалыг хангах, нууцлалын зэрэглэлтэй мэдээллийг солилцох, таньж зөвшөөрөх тогтолцоог зохион байгуулахын тулд шифрлэлтийн (криптограф) болон тоон гарын үсгийн орчин үеийн технологи ашиглана.

## **27 дугаар зүйл. Сүлжээ хоорондын галт ханыг (дэлгэц) зохион байгуулах**

27.1. Энэ хуулийн 11.1-д заасан байгууллага бүр Мэдээллийн урсгалыг хянах, шүүх, хандалтыг хязгаарлах, мэдээллийн солилцоог бүртгэх зорилгоор сүлжээ хоорондын галт ханыг (дэлгэц) суулгаж, тохируулж, ажиллагааг нь хянаж байна.

## **28 дүгээр зүйл. Хамгаалагдсан байдлыг шинжлэх**

28.1. Энэ хуулийн 11.1-д заасан байгууллага бүр Үйл ажиллагааны явцад гарсан алдаа, доголдлыг цаг алдалгүй илрүүлж байхын тулд хамгаалагдсан байдлыг шинжлэх програмын хэрэгслүүдийг ашиглаж байна.

## **29 дугаар зүйл. Хүртээмжтэй байдлыг хангах**

29.1. Энэ хуулийн 11.1-д заасан байгууллага бүр үйлчилгээний үр нөлөө, хүртээмжтэй байдлыг хангахын тулд системийн бүрдэл хэсэг, явагдаж буй үйл явцыг туршин баталгаажуулж, бүрдэл хэсэг, үйл явцыг нэг мөр болгон уялдуулж, хянадаг байх бөгөөд шийдэл нь энгийн, автоматжсан байх ёстой.

## **30 дугаар зүйл. Сүлжээний мониторинг**

30.1. Энэ хуулийн 11.1-д заасан байгууллага бүр өөрийн сүлжээнд орж ирж буй халдлага, будлиан, довтолгооныг цаг алдалгүй илрүүлж, таслан зогсоохын тулд сүлжээний мониторингийн үйл явцыг хэрэгжүүлсэн байна.

# **ЗУРГААДУГААР БҮЛЭГ**

## **Туршин баталгаажуулах ажиллагаа**

### **31 дүгээр зүйл. Техник хэрэгсэл, тоног төхөөрөмжийг туршин баталгаажуулах**

31.1. Энэ хуулийн 11.1-д заасан Төрийн байгууллага, мэдээллийн онц чухал дэд бүтэцтэй байгууллагад ашиглах мэдээлэл боловсруулах, дамжуулах, хадгалах техник хэрэгсэл, тоног төхөөрөмжийг туршин шалгаж, баталгаажуулсан байна.

31.2. Энэ зүйлийн 1-д зааснаас бусад байгууллага мэдээлэл боловсруулах, дамжуулах, хадгалах зорилгоор ашиглах техник хэрэгсэл, тоног төхөөрөмжөө туршин шалгаж, баталгаажуулж болно.

31.2. Туршин шалгах ажиллагааны явцад байгууллагын найдвартай, тасалдалгүй ажиллагааг уг техник хэрэгсэл, тоног төхөөрөмж хангаж чадах эсэх, хууль ёсны үйлдлийн систем, хэрэглээний програмууд суулгасан эсэх, бүрдэл хэсгүүдэд хортой код байгаа эсэхийг тодруулна.

### **32 дугаар зүйл. Туршин шалгах, баталгаажуулах байгууллага**

32.1. Мэдээлэл боловсруулах, дамжуулах, хадгалах тоног, төхөөрөмжийг туршин шалгах, баталгаажуулах ажиллагааг эрх бүхий байгууллагаас тогтоосон тодорхой шаардлагыг хангасан байгууллага тусгай зөвшөөрлийн үндсэн дээр эрхэлнэ.

32.2. Мэдээлэл боловсруулах тоног, төхөөрөмжийг туршин шалгах, баталгаажуулах тусгай зөвшөөрөл олгох шаардлага, нөхцөл, журмыг Төрийн Холбооны Газар (**МШХХТГ эсхүл Харилцаа, холбооны зохицуулах хороо байж болно**) тогтооно.

### **33 дугаар зүйл. Баталгаажуулсан гэрчилгээ**

33.1. Мэдээлэл боловсруулах тоног төхөөрөмжийг туршин шалгасны үндсэн дээр аюулгүй байдлын шаардлага хангасныг баталгаажуулсан гэрчилгээг төхөөрөмж бүрт олгоно.

# **ДОЛООДУГААР БҮЛЭГ**

## Мэдээллийн аюулгүй байдлын аудит

### 34 дүгээр зүйл. Мэдээллийн аюулгүй байдлын аудитийг зохион байгуулах

34.1. Төрийн болон мэдээллийн онц чухал дэд бүтэцтэй байгууллагуудад мэдээллийн аюулгүй байдлыг хангахын тулд мэдээллийн аюулгүй байдлын аудитийг тодорхой мөчлөгтэйгөөр (**жил бүр, эсхүл 2 жил тутам гэж болно**) хийж байна.

34.2. Мэдээллийн аюулгүй байдлын аудит нь удирдлагын, сүлжээний, системийн, процедурын, вебийн аюулгүй байдлын болон бусад аудит хэмээн ангилагдана.

### 35 дугаар зүйл. Мэдээллийн аюулгүй байдлын аудит хийх байгууллага

35.2. Мэдээллийн аюулгүй байдлын аудитыг зохих шаардлагыг хангаж тусгай зөвшөөрөл авсан байгууллага гүйцэтгэнэ.

35.3. Мэдээллийн аюулгүй байдлын аудит хийх тусгай зөвшөөрөл олгох нөхцөл, журам, тавигдах шаардлагыг Мэдээлэл, Шуудан Харилцаа Холбооны Технологийн Газар (**эсхүл ХХЗХ**) тогтооно.

### 36 дугаар зүйл. Байгууллагын мэдээллийн аюулгүй байдлын аудит

36.1. Энэ хуулийн 11.1-д зааснаас бусад байгууллага мэдээллийн аюулгүй байдлын аудитыг өөрсдийн хүчээр юмуу тусгай зөвшөөрөлтэй байгууллагын тусламжтайгаар зохион байгуулж болно.

## НАЙМДУГААР БҮЛЭГ

### Будлианы удирдлага

### 37 дугаар зүйл. Мэдээллийн аюулгүй байдлын будлианы удирдлага

37.1. Мэдээллийн хүртээмж, нэгдмэл байдал, нууцлалыг хангах, систем, сүлжээний үйл ажиллагааг цаг алдалгүй сэргээх, аливаа учрал, тохиолдол, гэмт халдлага, довтолгооныг таслан зогсоох, учрах хор хохирлыг бууруулах, цаашид урьдчилан сэргийлэхийн тулд байгууллагууд мэдээллийн аюулгүй байдлын будлианыг мэдээлэх, боловсруулах дэг, журам баталж хэрэгжүүлсэн байна.

37.2. Мэдээллийн аюулгүй байдлын будлианы эсрэг хариу үйлдэл хийх багийг байгууллагын, байгууллага дундын, салбарын, үндэсний хэмжээнд зохион байгуулж болно.

37.3. Мэдээллийн аюулгүй байдлын будлианы эсрэг хариу үйлдэл хийх үндэсний багийг улсын төсвийн хөрөнгөөр санхүүжүүлэн ажиллуулна.

### 38 дугаар зүйл. Мэдээллийн аюулгүй байдлын будлианыг мэдээлэх

38.1. Байгууллага бүр мэдээллийн аюулгүй байдлын ноцтой будлианы тухай мэдээллийг үндэсний багт нэн даруй мэдээлж байна.

38.2. Гэмт хэргийн шинжтэй будлианы тухай мэдээллийг үндэсний баг болон хууль хамгаалах байгууллагад нэн даруй мэдээлж байна.

38.3. Мэдээллийн аюулгүй байдлын будлианы статистик мэдээллийг байгууллага бүр сар, улирлаар гаргаж үндэсний багт хүргүүлнэ.

38.4. Мэдээллийн аюулгүй байдлын будлианы эсрэг хариу үйлдэл хийх үндэсний баг Монгол улсын хэмжээнд будлиан учралыг илрүүлэх, мэдээлэх, боловсруулах ажиллагааг нэгтгэн уялдуулж, мэргэжил, арга зүйн удирдлагаар хангана.

## ЕСДҮГЭЭР БҮЛЭГ

### Төрийн цахим баримт бичиг, өгөгдөл **солилцох системийн** аюулгүй байдал

### 39 дугаар зүйл. Төрийн цахим баримт бичгийн систем.

39.1. Төрийн албан ёсны болон нууцлалын зэрэглэлтэй цахим баримт бичгийг үүсгэх, боловсруулах, дамжуулах, хадгалах аюулгүй ажиллагааг хангахын тулд төрийн цахим баримт баримт бичгийн солилцооны системийг зохион байгуулна.

39.2. Төрийн цахим баримт бичгийн солилцооны системийг **төрийн холбооны газар, үндэсний датаа төвтэй хамтран** эрхлэн зохион байгуулна.

39.3. Баримт бичгийн эргэлтийн хэмжээнээс хамаарч цахим баримт бичгийн дэд системийг яам, агентлаг, нутгийн удирдлагын байгууллага дээр байгуулж болно.

39.4. Төрийн цахим баримт бичгийн солилцооны системийн дүрмийг Засгийн Газар батална.

#### **40 дүгээр зүйл. Төрийн цахим баримт бичгийн солилцоог аюулгүй зохион байгуулах**

40.1. Төрийн цахим баримт бичгийн системд үүсгэж, боловсруулж, дамжуулж, хадгалж буй цахим баримт бичгийг тоон гарын үсгийн орчин үеийн технологи ашиглан баталгаажуулна. Хэрэв шаардлагатай гэж үзвэл шифрлэнэ.

40.2. Төрийн нууцлалын зэрэглэлтэй цахим баримт бичгийг солилцоходоо тоон гарын үсгийн орчин үеийн технологи ашиглан баталгаажуулж давхар шифрлэнэ.

40.3 Төрийн цахим баримт бичгийн системд үүсгэж, боловсруулж, дамжуулж, хадгалж буй цахим баримт бичгийг баталгаажуулахын тулд төрийн албан хаагч бүрт тоон гарын үсгийн хувийн түлхүүр, түлхүүрийн гэрчилгээ үүсгэж өгнө.

## **АРАВДУГААР БҮЛЭГ**

### **Үндэсний Дата Төвийн мэдээллийн аюулгүй байдал**

#### **41 дүгээр зүйл. Үндэсний дата төв**

41.1 Төрийн өгөгдөл мэдээллийн аюулгүй байдлыг хангах, нэгдсэн хамгаалалт хэрэгжүүлэх, харилцан уялдаа холбоог хангах, төвлөрүүлэх, бүртгэлийн өгөгдлийг төрийн цахим үйлчилгээний суурь болгох, хамтран ашиглах боломжийг хангахад үндэсний дата төвийн үйл ажиллагаа чиглэгдэнэ.

#### **42 дугаар зүйл. Үндэсний дата төвийн аюулгүй байдал**

42.1 Үндэсний дата төвд байршиж буй төрийн өгөгдлийн аюулгүй байдлыг хангахын тулд энэ хуулийн 4, 5 дугаар бүлэгт заасан арга хэмжээг хэрэгжүүлэхээс гадна дараах нэмэлт шийдлийг хэрэгжүүлсэн байна:

42.1.1 Аюулын эсрэг нэгдмэл удирдлага (UTM), сүлжээний мониторинг, анхааруулгын систем

42.1.2 Сүлжээний халдлага, довтолгооноос сэргийлэх, таслан зогсоох систем

42.1.3 Биометр үзүүлэлт дээр суурилсан биет хандалтын хяналт, 2-оос доошгүй шатлалтай логик хандалтын систем

42.1.4 Хакерын аюул, хортой трафик, эмзэг сул, цоорхой байдлын байнгын шинжилгээ

42.1.5 Төрийн байгууллагуудтай хамтран өгөгдлийг ангилах, шошголох, нууцлалын зэрэглэлийг тогтоох, төрийн албан хаагчдын хандах эрхийн зэрэглэлийг тогтоох

42.1.6 Төрийн байгууллагуудын интернетийн нэгдмэл гарц

42.1.7 Төрийн өгөгдлийн нөөц хуулбарыг бодит горимоор үүсгэх

42.1.8 Сүлжээний үндсэн тоног төхөөрөмжийн нөөц хувь

42.1.9 Хүний нөөцийн чадвар, цогц шинж чанарыг байнга хөгжүүлэх

42.1.10 Хортой кодыг илрүүлэх, устгах, э-мэйл вирус, зүй бус соёлгүй зарыг хаах, тагнах турших програмуудыг (spyware, adware) арилгах, Хакерийн халдлагыг илрүүлэх, довтолж буй сайтуудыг хаах тогтолцоо

## **АРВАН НЭГДҮГЭЭР БҮЛЭГ**

### **Төрийн цахим үйлчилгээний аюулгүй байдал**

#### **43 дугаар зүйл. Төрийн цахим үйлчилгээний аюулгүй байдал**

43.1 Төрийн цахим үйлчилгээний аюулгүй байдлыг хангахын тулд төрийн өгөгдлийг хамтран ашиглах ажиллагааны удирдлагыг дата төв болон төрийн байгууллагууд хамтран хэрэгжүүлсэн байна.

43.2 Төрийн өгөгдлийг хамтран ашиглахын тулд төрийн албан хаагч бүрийн хандалтын эрхийн зэрэглэлийг тогтоож, хандаж болох өгөгдлийг ангилан тодорхойлсон байна.

43.3 Төрийн цахим үйлчилгээний хүрээнд төрийн албан хаагчдын хамтран ашиглах, хандах өгөгдлийг хуулбарлан тусгай тээгч дээр байрлуулсан байна.

43.4 Төрийн цахим үйлчилгээний аюулгүй байдлыг хангахын тулд Төрийн байгууллагуудын хувийн виртуаль сүлжээ байгуулсан байна

43.5 Төрийн цахим үйлчилгээ, түүний төлбөр тооцооны аюулгүй байдлыг хангах орчин үеийн шийдлийг хэрэгжүүлсэн байна.

43.6 Төрийн цахим үйлчилгээний аюулгүй байдлыг хангахын тулд хүсэлт, өргөдлийг боловсруулах системийн аюулгүй байдал, өргөдөл, хүсэлтийг боловсруулж буй төрийн албан хаагчийн компьютерийн аюулгүй байдлыг хангах арга хэмжээг дата төв болон энэ хуулийн 11.1-д заасан байгууллага бүр хэрэгжүүлсэн байна

## **АРВАН ХОЁРДУГААР БҮЛЭГ**

### **Нөөц хуулбар, сэргээн ажиллуулах төлөвлөгөө**

#### **44 дүгээр зүйл. Өгөгдлийн нөөц хуулбар**

44.1 Төрийн өгөгдлийн бүрэн бүтэн, хүртээмжтэй байдлыг хангахын тулд өгөгдлийн нөөц хуулбарын төвийг нийслэл хотоос өөр газар байгуулж ажиллуулна.

44.2 Төрийн өгөгдлийг өгөгдлийн нөөц төвд бодит горимоор хуулбарлахаас гадна дата төв дээрх нөөц хуулбарын серверт хуулбарлан хадгалж байна.

44.3 Энэ хуулийн 11.1-д заасан байгууллагууд өгөгдлийн нөөц хуулбарыг үндэсний дата тав дээрх нөөц хуулбарын серверт үүсгэж өдөр бүр шинэчилж байна. Хэрэв үндэсний дата төвд холбогдох боломжгүй бол өөрийн нөөц бололцоонд тулгуурлан нөөц хуулбарыг үүсгэж, шинэчилж байна.

#### **45 дугаар зүйл. Сэргээн ажиллуулах төлөвлөгөө**

45.1 Дата төв, нөөц хуулбарын төв болон энэ хуулийн 11.1-д заасан байгууллага бүр онцгой нөхцөл байдал үүсэх, халдлага довтолгооны улмаас систем, сүлжээний үйл ажиллагаа доголдох, тасалдах үед тасралтгүй ажиллагааг хангах төлөвлөгөө, систем, сүлжээг сэргээн ажиллуулах төлөвлөгөө боловсруулж баталсан байна.

45.2 Тасралтгүй ажиллагааг хангах төлөвлөгөө, сэргээн ажиллуулах төлөвлөгөөг тодорхой мөчлөгтэйгөөр туршин хэрэгжүүлж, бэлэн байдлыг хангаж байна.

## **АРВАН ГУРАВДУГААР БҮЛЭГ**

### **Бусад зүйл**

#### **46 дугаар зүйл. Мэдээллийн технологийн салбар дахь хараат байдлыг багасгах**

46.1. Мэдээлэл боловсруулах, дамжуулах, хадгалах төхөөрөмж, аппарат хэрэгсэл, технологи, програм хангамж, үйлчилгээний үндэсний үйлдвэрлэлийг хөгжүүлэх, дэмжих тааламжтай нөхцлийг бий болгох, мэдээллийн технологи, аюулгүй байдлын хүрээн дэх суурь болон хавсарга судалгааг дэмжих, дотоод зах зээлээ хамгаалах замаар мэдээллийн технологийн салбар дахь хараат байдлыг багасгах арга хэмжээг төрөөс авч хэрэгжүүлнэ.

#### **47 дугаар зүйл. Маргаан шийдвэрлэх**

47.1. Хуульд өөрөөр заагаагүй бол мэдээллийн аюулгүй байдлыг хангахтай холбогдсон маргааныг шүүх шийдвэрлэнэ.

#### **48 дугаар зүйл. Хууль зөрчигчдөд хүлээлгэх хариуцлага**

48.1. Мэдээллийн аюулгүй байдлын хууль тогтоомж зөрчсөн нь эрүүгийн хариуцлага хүлээлгэхээргүй бол шүүх гэм буруутай этгээдэд дараах захиргааны шийтгэл ногдуулна:

48.1.1. Энэ хуулийн 11, 12, 13, 14, 17, 18, 19 дүгээр зүйлийн заалтыг зөрчсөн байгууллагыг ..... төгрөгөөр, удирдлагыг .....төгрөгөөр торгох;

48.1.2. Энэ хуулийн 20, 21 дүгээр зүйлийн заалтыг зөрчсөн байгууллагыг ..... төгрөгөөр, удирдлагыг .....төгрөгөөр торгох;

48.1.3. Энэ хуулийн .. дугаар зүйлийн заалтыг зөрчсөн байгууллагыг ..... төгрөгөөр, удирдлагыг .....төгрөгөөр торгох;

48.1.4. Энэ хуулийн .. дүгээр зүйлийн заалтыг зөрчсөн байгууллагыг ..... төгрөгөөр, удирдлагыг .....төгрөгөөр торгох;

48.1.5. Энэ хуулийн ..... дугаар зүйлийн заалтыг зөрчсөн байгууллагыг ..... төгрөгөөр, удирдлагыг .....төгрөгөөр торгох;

### **ГАРЫН ҮСЭГ**