ХЭНТИЙ АЙМАГ
ЗАСАГ ДАРГЫН ТАМГЫН ГАЗРЫН
ДАРГЫН ТУШААЛ

2018 оны 09 сарын 02 өдөр Дугаар А/35 Чингис хот

Журам батлах тухай

Монгол Улсын Засаг захиргаа, нутаг дэвсгэрийн нэгж, түүний удирдлагын тухай хуулийн 33 дугаар зүйлийн 33.5, Байгууллагын нууцын тухай хуулийн 5 дугаар зүйлийн 5.1 дэх заалт, Монгол Улсын Засгийн газрын 2018 оны Төрийн мэдээллийн аюулгүй байдлыг хангах зарим арга хэмжээний тухай 138 дугаар тогтоолын заалтыг үндэслэн ТУШААХ нь:

1. Төрийн мэдээллийн нэгдсэн сүлжээний аюулгүй байдлыг хангах байгууллагын интернэтийн зохистой хэрэглээг бий болгох төрийн албан хаагчдын цаг ашиглалт, ажлын бүтээмжийг сайжруулах зорилгоор "Хэнтий аймгийн Засаг даргын Тамгын газрын цахим мэдээллийн аюулгүй байдлыг хангах журам"-ыг хавсралтаар батлсугай

2. "Хэнтий аймгийн Засаг даргын Тамгын газрын цахим мэдээллийн аюулгүй байдлыг хангах журам"-ыг үйл ажиллагаандаа мөрдөж ажиллахыг аймгийн Засаг даргын Тамгын газрын нийт албан хаагчид, хэлтсийн дарга нарт үүрэг болгосугай.

3. Энэхүү журмын хэрэгжилтэд хяналт тавьж ажиллахыг Төрийн захиргааны удирдлагын хэлтсийн дарга /Ж.Гантулга/-д даалгасугай

ДАРГА Ж.ГАНБААТАР

D:\My Documents\Тушаал 2018.doc

Аймгийн Засаг даргын Тамгын газрын
даргын 2018 оны ..07.. дугаар сарын ..02...
өдрийн ...35... дугаар тушаалын хавсралт

ХЭНТИЙ АЙМГИЙН ЗАСАГ ДАРГЫН ТАМГЫН ГАЗРЫН ЦАХИМ МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ЖУРАМ

Нэг. Нийтлэг үндэслэл

1.1. Энэхүү журмын гол зорилго нь Хэнтий аймгийн Засаг даргын Тамгын газрын мэдээллийн аюулгүй байдлын тогтолцоог бий болгох, мэдээллийн сүлжээ, системийн найдвартай ажиллагаа, мэдээллийн сангийн нууцлал, аюулгүй байдлыг хангах, гадна болон дотоодоос учирч болох халдлага, аюул заналаас хамгаалах, эрсдэлийг бууруулах, нэн даруй хариу арга хэмжээ авахад оршино

1.2. Хэнтий аймгийн Засаг даргын Тамгын газрын албан хаагчид ажил үүргээ гүйцэтгэхдээ энэхүү журмыг мөрдлөг болгон ажиллана.

1.3. Энэхүү журамд дурдсан нэр томьёог дор дурдсан утгаар ойлгоно.

1.3.1. "Active Directory" гэж дотоод сүлжээнд холбогдсон нийт албан хаагчийн компьютерыг хэрэглэгчийн эрхээр нь зохион байгуулан төвлөрсөн удирдлагаар хангах систем:

1.3.2. "Хэрэглэгч" гэж байгууллагын мэдээллийн системтэй харьцдаг бүхий л шатны албан хаагч:

1.3.3. "Системийн зохицуулагч" гэж байгууллагын мэдээлэл технологи хариуцсан эрх, үүрэг бүхий албан хаагч

Хоёр. Компьютер болон бусад техник хэрэгслийн аюулгүй байдал

2.1. Албан хаагч бүр албан хэрэгцээнд ашиглаж буй компьютер, тэдгээрт хадгалагдах мэдээллийн аюулгүй байдлыг дараах байдлаар хангаж ажиллана. Үүнд:

2.1.1. Компьютерийг идэвхтэй горимд орхих үед дэлгэц хамгаалах програм заавал ажиллуулах буюу түгжих

2.1.2. Албан хаагч бүр өөрийн компьютерийн системд нэвтрэх нууц үгтэй байх ба түүний нууцлалыг хадгалах

2.1.3. Төрийн болон байгууллагын нууцын зэрэгтэй мэдээ мэдээлэл боловсруулах, хадгалах, хамгаалах зөөврийн болон суурин компьютер нь интернэт сүлжээнд холбогдоогүй, системийн тохиргоонд стандарт оролтуудыг хаасан, хатуу дискнээс мэдээлэл алдагдахаас сэргийлэн лац тэмдэглэгээ хийсэн, процессорын гадна хэсэгт лац, зориулалтын хамгаалалтын нөхцөлийг хангасан байх.

2.1.4. Нууц мэдээлэл агуулсан компьютер болон бусад техник хэрэгсэл авч явах үедээ нэвтрэх эрхээр хамгаалагдсан програм ашиглах, мөн файлд нууцлал хийж хамгаалах

2.2. Байгууллагын мэдээллийн сүлжээнд холбогдсон компьютер бүрт зайлшгүй хортой кодын эсрэг програм хэрэглэнэ. Хортой кодын эсрэг програмын автомат хамгаалалт нь файл нээх болон хаахад давхар шалгалт хийдэг байх ёстой.

2.3. Албан ёсны эрх бүхий хортой кодын эсрэг програм худалдан авах ашиглах хугацааг сунгах зардлыг жил бүрийн төсөвт тусгана.

2.4. Нууц мэдээлэл бүхий зөөврийн хадгалах төхөөрөмжийг найдвартай хамгаалалттай газар хадгална.

2.5. Компьютер болон бусад техник хэрэгслийг гал, шингэн зүйл болон бусад хортойгоор нөлөөлж болзошгүй зүйлээс хол байрлуулна. Компьютерийн дэлгэцийг нарны гэрэл тусахгүй газар байрлуулна. Компьютер, техник хэрэгслийн цахилгааны залгуурыг салгасан тохиолдолд цэвэрлэж байна.

Гурав. Мэдээллийн системийн аюулгүй байдал

3.1. Байгууллагын компьютерийн системийн тасралтгүй үйл ажиллагааг хангах, мэдээллийн нууцлал, аюулгүй байдлыг дээшлүүлэх зорилгоор компьютерийн тохиргоог төвлөрүүлэн зохион байгуулна.

3.2. Байгууллагын мэдээллийн системд нийцүүлэн албан хаагчдын ажлын компьютерууд нь виндоус /Windows/ үйлдлийн системтэй байна

3.3. Байгууллагын албан хаагчдын ажлын компьютерийг системийн зохицуулагч удирдан хянах боломжийг Active Directory бүхий програмын хэрэгслийг ашиглан нэг домэйнд оруулан бий болгоно.

3.4. Active Directory домэйнд холбогдсон компьютерийн системийн нууцлал, аюулгүй байдал, хэвийн үйл ажиллагааг хангах, хяналт шалгалт хийх үйл ажиллагааг системийн зохицуулагч хариуцах бөгөөд энэхүү журамд нийцүүлэн зохион байгуулна.

3.5. Албан хаагчийн системд хандах эрхийг албан хаагчийн ажил үүргийг үндэслэн системийн зохицуулагч тогтооно.

3.6. Хэрэглэгчийг "энгийн" ба "онцгой эрхтэй" хэрэглэгч гэж ангилна Системийн зохицуулагч нь өөрөө администратор эрхтэй байх бөгөөд удирдах бүрэлдэхүүнийг онцгой эрхт хэрэглэгч гэх ба үлдсэн албан хаагчдыг энгийн хэрэглэгч гэж ойлгоно.

3.7. Системийн зохицуулагч нь "Active Directory" домэйнд хэрэглэгчийг шинээр бүртгэж хэрэглэгчийн нэр, нууц үгийг олгоно.

3.8. Системийн зохицуулагч нь комптьютерийн нэрийг тухайн компьютер эзэмшигчийн нэрээр олгоно.

3.9. Системийн зохицуулагч нь хэрэглэгчийн ашиглах шаардлагатай програмуудад тохирох эрхийг нь олгож, сервертэй холбогдох болон хэрэглэгчийн тохиргоог хийнэ.

3.10. Албан хаагч нь 30 минут дотор 5 удаа нууц үгээ буруу оруулбал түүний хэрэглэгчийн эрх нь хаагдахаар системийн нийт компьютерыг тохируулна.

3.11. Хүний нөөцөөс мэдэгдсэний дагуу албан хаагчийн ажлын байр өөрчлөгдөх бүр Active Directory системд шаардлагатай өөрчлөлтүүдийг хийнэ.

3.12. Системийн зохицуулагч нь албаны хэмжээнд ашиглах дотоод сүлжээнд агуулагдах мэдээллийн баазыг 7 хоног бүрийн сүүлийн өдөр архивлах ба гэнэтийн техникийн болон програм хангамжийн гэмтэл, гадны бусад хүчин зүйлээс шалтгаалан устсан үед буцаан сэргээх боломжтой байхаар хадгална.

Дөрөв. Мэдээллийн сүлжээ, интернэтийн аюулгүй байдал

4.1. Албан хаагч нь мэдээллийн болон системийн аюулгүй ажиллагааг хангах, ажлын цагийн үр бүтээлийг дээшлүүлэх үүднээс интернэтийн сүлжээнд ажлын шугамаар бүрэн болон хязгаарлагдмал эрхтэйгээр ашиглана.

4.2. Хязгаарлагдмал эрхээр интернэт ашиглах албан хаагчийн интернэт хандалтыг дараах байдлаар түгээмэл хэрэглэгддэг цахим хуудсуудын хувьд хязгаарлана. Үүнд:

4.2.1. Дуу, дүрс бичлэгийн цахим хуудас
4.2.2. Олон эх үүсвэрээс зэрэг татах боломжтой файл татах програм
4.2.3. Найз нөхөдтэйгөө харилцах, санал бодлоо илэрхийлж, мэдээлэл авах хуудас
4.2.4. Интернэтийн орчинд өөр сервер дээр мэдээлэл түр хугацаагаар хадгалж, өөр газраас татаж авах боломжтой хуудас

4.3. Интернэт сүлжээг дараах зорилгоор ашиглахыг хориглоно. Үүнд:

4.3.1. Арьс өнгө, гарал үүсэл, нас, хүйс, шашин шүтлэг, эрүүл мэнд, үзэл бодол зэргээр ялгаварласан текст болон дүрст мэдээлэлд хандах, түүнийг үүсгэх, дамжуулах, хэвлэх, татаж авах;
4.3.2. Садар самууны холбогдолтой текст, дүрст мэдээлэлд хандах, түүнийг илгээх, хүлээн авах, татаж авах, хэвлэх;
4.3.3. Албаны зориулалтаас бусад текст, зураг, дуу, дүрс бүхий мэдээлэл бүхий файлыг татаж авах.

4.3.4. Хакер /хакердалт, cracking (лицензийг нь эвдэх), бусад хууль бус сайтуудад хандах, програм заавар татаж авах:

4.3.5. Зохиогчийн эрхтэй програм хангамж материалыг зохиогчийн зөвшөөрөлгүйгээр татаж авах, хувилж олшруулах, тараах:

4.3.6. Аливаа програмыг системийн зохицуулагчийн зөвшөөрөлгүйгээр татаж авах, суулгах:

4.3.7. Интернэт үйлчилгээ хэрэглэгчид санаатай болон санамсаргүйгээр сүлжээний ачаалал унагаах үйлдэл, хандалт хийх

4.3.8. Сүлжээний бүтцийг илрүүлэх зорилгоор тандалт хийх:

4.3.9. Байгууллагын сүлжээнээс дотоод болон гадны сүлжээнд мэдээлэл хулгайлах, хорлон сүйтгэх, сүлжээг тагнах зорилгоор хандалт хийх:

4.3.10. Байгууллагын нууцад хамаарагдах мэдээллийг цахим шуудангаар бусдад илгээх, интернэт орчинд байрлуулах.

4.4. Байгууллагын утасгүй интернэт, дотоод сүлжээнд гадны хэрэглэгч болон бусад хэрэглэгч холбогдох тохиолдолд холбогдох удирдлагын зөвшөөрлийн дагуу системийн зохицуулагч өөрийн биеэр очиж тухайн төхөөрөмжид нууц үгийг оруулж өгч сүлжээнд холбоно.

4.5. Сүлжээний хамгаалалтыг зохион байгуулах, мэдээлэлд зөвшөөрөлгүй нэвтрэх оролдлогыг таслан зогсоох, илрүүлэх зориулалтаар хамгаалалт, хяналтын техник, програм хангамжийг нэвтрүүлж байнгын ажиллагаанд ашиглана.

4.6. Албан хаагч нь ажлаас гарсан эсвэл интернэт, цахим шуудангийн үйлчилгээг хаалгах шаардлага гарсан тохиолдолд системийн зохицуулагч дээрх эрхийг хаана.

Тав. Цахим шуудангийн үйлчилгээ

5.1. Байгууллагын албан хаагчид албан хэрэгцээндээ зөвхөн албан ёсны цахим шуудангийн үйлчилгээг ашиглана.

5.2. Байгууллагын хэмжээнд компьютер ашиглаж буй албан хаагч бүр хэрэглэгчийн Жишээ нь: нэр@khentii.gov.mn домэйн нэр бүхий албан цахим шуудангийн хаягтай байна.

5.3. Албан хаагч цахим шуудангийн хаяг үүсгэх холбогдох тохиргоо хийх асуудлыг системийн зохицуулагч гүйцэтгэнэ.

5.4. Албан хаагч цахим шуудангийн хандах нэвтрэх үгийн нууцлал, аюулгүй байдлыг өөрөө хариуцна.

5.5. Цахим шууданг дараах зорилгоор ашиглахыг хориглоно Үүнд:

5.5.1. Интернэтийн нийтээр ашигладаг нөөц /форум, эрдэм шинжилгээний хурал г.м./-д өөрийн болон байгууллагын бусад албан хаагчийн цахим шуудангийн хаягийг тавих:

5.5.2. Нийт 25 мегабайтаас хэтэрсэн хэмжээтэй файл илгээх

5.5.3. Компьютер ба сүлжээний тоног төхөөрөмжийн үйл ажиллагааг хязгаарлах эвдэж устгахад зориулагдсан програм файл, компьютерийн командууд болон хортой код агуулсан материалууд эсвэл интернэтэд хууль бусаар хандахад зориулагдсан програм, худалдахад зориулагдсан програмын серийн нууц дугаар ба тэдгээрийг үүсгэх програм /crack, keygen/, интернэтийн төлбөртэй үйлчилгээг хууль бусаар ашиглахад зориулсан нууц үг, бусад хэрэгслийг цахим шуудангаар дамжуулах:

5.5.4. Зохиогчийн эрх нь хамгаалагдсан материал тараах:

5.5.5. Байгууллагын нэрийн өмнөөс хувийн үзэл бодлоо цахим шуудангаар бусдад илгээх, мэдээний вэб сайт, интернэтэд байрлуулах:

5.5.6. Байгууллагын нууцад хамаарагдах мэдээллийг цахим шуудангаар бусдад илгээх, мэдээний вэб сайт, интернэтэд байрлуулах:

5.5.7. Гинжин цахим шуудан илгээх, пирамид болон бусад хууль бус схемд оролцох. Тухайлбал, тухайн цахим шууданг бусдад олон тоогоор дамжуулснаар мөнгө авах утгатай, бусдын сэтгэл санаанд нөлөөлөх цахим шуудан дамжуулах

5.5.8. Монгол Улсын хууль болон Монгол Улсын нэгдэн орсон олон улсын хууль, тогтоомжоор хориглосон хорлон сүйтгэх ажиллагаа, заналхийлэл гүтгэлэг, зохисгүй мэдээлэл агуулсан мэдээлэл, түүнчлэн бусад этгээдийн-ололт, нэр хүндийг гутаан доромжилсон мэдээлэл, хууль бус үйл ажиллагаанд уриалсан, зэр зэвсэг хэрэглэх арга ажиллагааг тайлбарласан гэх мэт агуулга, чиглэл бүхий материалыг тараах:

5.5.9. Албаны үйл ажиллагааны нууцыг илэрхийлсэн, хандахыг хязгаарласан мэдээллийг тараах:

5.5.10. Улс төрийн сонгуулийн зориулалт бүхий сурталчилгааны материал тавих:

Зургаа. Дотоод сүлжээ, мэдээллийн сан

6.1. Дотоод сүлжээн дэх цахим мэдээллийн санг нийт албан хаагч багтаамж ихтэй файл түргэн шуурхай солилцох, ажлын шугамаар хоорондоо харилцахад хэрэглэнэ.

6.2. Цахим мэдээллийн санг хадгалах автомат системтэй байх бөгөөд уг системийг ашиглан албан хаагч бүр албан ажлын цахим мэдээллийг улирал бүр цахим санд хадгална.

6.3. Мэдээллийн сангийн мэдээллийг дараах байдлаар бүрдүүлж шинэчилнэ Үүнд:

6.4.1. Мэдээллийн санд байршуулах цахим мэдээллийг шинэчлэх ажлыг тухайн мэдээлэл хамаарах хэлтсийн албан хаагч хариуцна.

6.4.2. Байгууллагын үйл ажиллагаатай холбоотой дүрэм журам, заавар шинээр батлагдсан болон өөрчлөлт орсон даруй 2 хоногт багтаан мэдээллийн санд байршуулна.

6.4. Дотоод сүлжээний мэдээллийн аюулгүй байдалд дараах зүйлсийг анхаарч ажиллана. Үүнд:

6.4.1. Мэдээллийн сангийн нууцлал хамгааллыг системийн зохицуулагч хариуцах ба мэдээллийн сан дахь мэдээллийг зөвхөн дотоод ажлын хэрэгцээнд ашиглаж, бусдад задруулахгүй байх үүргийг албан хаагч бүр хүлээнэ.

6.4.2. Мэдээллийн сантай холбоотой аливаа асуудал, санал хүсэлтийг тухай бүрт нь системийн зохицуулагчид мэдэгдэж байна.

6.5. Мэдээллийн санг ашиглахад дараах зүйлсийг хориглоно. Үүнд:

6.5.1. Мэдээллийн санд байгаа мэдээллийг гадагш бусдад дамжуулах, нууцыг задруулах, ажлын бус шаардлагаар хэвлэх, олшруулах, хувийн зорилгоор болон хэсэг бүлэг хүний эрх ашгийн үүднээс ашиглах.

6.5.2. Мэдээллийн санд байгууллагын үйл ажиллагаанд хамааралгүй мэдээлэл байршуулах, хоорондоо солилцох бие биенээ доромжлох, ёс зүй, байгууллагын дотоод журамд харш зураг, мэдээлэл тавих.

6.5.3. Нууцын зэрэгтэй бүхий л мэдээллийн файлуудыг байршуулах

Долоо. Түлхүүр үгийг олгох хамгаалах

7.1. Хэрэглэгчийн түвшний түлхүүр үгийг шаардлагатай тохиолдолд тухай бүр, ердийн нөхцөлд 6 сар тутамд солино.

7.2. Албан хаагч нь мэдээлэл технологийн орчинд аль болох хялбар биш, зөвхөн өөрт амархан тогтоож болох түлхүүр үгийг хэрэглэх шаардлагатай.

Түлхүүр үг нь дараах шинж чанартай. Үүнд:

7.2.1. том жижиг үсгийн аль алинаас бүтсэн байх:

7.2.2. тоо, үсэг, тэмдэглэгээ холилдон орсон байх:

7.2.3. хамгийн багадаа 6 тэмдэгтээс бүтсэн байх:

7.2.4. хувийн мэдээлэл, гэр бүлийн нэрс дээр үндэслэгдээгүй байх:

7.2.5. түлхүүр үгийг бичиж эсвэл онлайн хэлбэрээр хадгалахгүй байх:

7.3. Түлхүүр үгийг хамгаалах үүднээс хэн нэгэнд ямар нэг байдлаар хэлэхгүй байна.

7.4. Албан хаагч нь түлхүүр үг задарч болзошгүй сэжигтэй тохиолдолд системийн зохицуулагчид мэдэгдэн бүх түлхүүр үгсийг солих хэрэгтэй.

Найм. Байгууллагын мэдээллийн аюулгүй байдал хариуцсан албан хаагчийн эрх үүрэг

8.1. Байгууллагын мэдээллийн систем, сүлжээ, мэдээллийн санд заналхийлж буй халдлагыг илрүүлэх, таслан зогсоох болон эмзэг байдлыг тогтоох, эрсдэлийг бууруулах, аюулгүй байдлыг хангах зорилгоор мэдээллийн аюулгүй байдлыг хангах мэргэжилтнийг цаашид систем зохицуулагч гэж ажиллуулна. Байгууллагын нийт албан хаагч болон удирдах бүрэлдэхүүн нь мэдээллийн аюулгүй байдлыг хангахад дэмжлэг үзүүлнэ.

8.2. Системийн зохицуулагчийн эрх:

8.2.1. Ажил үүргийн хуваарийн дагуу мэдээллийн аюулгүй байдлыг шалгах, эмзэг байдлыг бууруулах зорилгоор мэдээллийн систем, албан хаагчдын комльютерт байгууллагын удирдлагад танилцуулж зөвшөөрөл авсны үндсэн дээр нэвтрэх.

8.2.2. Мэдээллийн аюулгүй байдлын талаарх шаардлагыг зөрчиж буй хэрэглэгчийн мэдээллийн санд нэвтрэх эрхийг удирдах тэдгээрийн ажиллагааг хэсэгчлэн болон бүрэн зогсоох.

8.2.3. Аюулгүй байдлын шаардлагыг удаа дараа зөрчигчдөд хариуцлага тооцох талаар байгууллагын удирдлагад санал оруулах.

8.2.4. Байгууллагад ашиглагдах мэдээллийн систем, техник технологи худалдан авах болон шинээр нэвтрүүлэхэд техникийн шийдлийг холбогдох албан хаагчидтай хамтран боловсруулах.

8.2.5. Мэдээллийн систем, цахим мэдээллийн сангийн бүрэн бүтэн байдалд хяналт тавих, мэдээллийн сангийн нөөц хувийг хувилж хадгалах нөхцөлийг хангах.

8.2.6. Байгууллагын компьютерийн систем серверт нэмэлт өөрчлөлт, шинэчлэлт, техникийн үйлчилгээг хийхэд гадны байгууллага, мэргэжилтнийг зайлшгүй ажиллуулах тохиолдолд тухайн ажлыг гүйцэтгэх байгууллагыг сонгох үйл явцад оролцох бөгөөд тухайн гүйцэтгэх явц, гүйцэтгэлд нь хяналт тавих.

8.3. Системийн зохицуулагчийн үүрэг.

8.3.1. Мэдээллийн системийг байгуулах, турших, ашиглах, засвар үйлчилгээг хийх, хэвийн үйл ажиллагааг хангах

8.3.2. Мэдээллийн сан, програм хангамж, компьютерийг хортой кодоос хамгаалах

8.3.3. Байгууллагын мэдээллийн аюулгүй байдлыг хангахад чиглэсэн сургалт, сурталчилгааг зохион байгуулах

8.3.4. Байгууллагын сүлжээ, системд нэвтэрсэн халдлагыг таслан зогсоож хариу үйлдэл хийх хурдан хугацаанд системийг сэргээх арга хэмжээ авах

8.3.5. Байгууллагын мэдээллийн системд ашиглах техник хэрэгсэл, програм хангамжийн гарал үүслийг бүртгэх шаардлагатай тохиолдолд техникийн үзлэг хийх

8.3.6. Байгууллагын мэдээллийн аюулгүй байдлыг хангахад шаардагдах хамгаалалтын системийг бий болгох, түүний ажлын горимыг боловсруулах

8.3.7. Мэдээллийн аюулгүй байдлыг хангах чиглэлээр мэргэжлээ дээшлүүлж байх

8.3.8. Шинээр гарч буй мэдээллийн аюулгүй байдлыг хангах техник. технологийг өөрийн байгууллагын үйл ажиллагаанд нэвтрүүлэх

8.3.9. Систем зохицуулагч нь байгууллагын удирдлагад "нууц"-ын баталгаа гаргаж өгнө.

8.3.10. Байгууллагын нууцыг хангах хамгаалах талаар ажилтнуудаас нууцын баталгааг гаргуулах ажлыг төрийн нууц хариуцсан ажилтантай хамтран зохион байгуулах

Ес. Хяналт, хариуцлага

9.1. Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээг мэргэжлийн байгууллагаар 2 жилд нэг удаа, шаардлагатай тохиолдолд тухай бүр хийлгэх ба холбогдох зардлыг төсөвт тусгана.

9.2. Албан хаагч нь ажлаас чөлөөлөгдсөн тохиолдолд системийн зохицуулагч нь мэдээллийн систем, цахим шуудан, интернэтэд хандах эрхийг хаана

9.3. Энэхүү журмыг зөрчсөн албан хаагчдад холбогдох хуулийн дагуу сахилгын шийтгэл ногдуулна.