

TIPINIŲ ASMENS DUOMENŲ APSAUGOS PRIEMONIŲ SĄRAŠAS

1. Fizinė prieiga prie kompiuterinės įrangos:

- 1.1. patalpos rakinamos;
- 1.2. įrengta patalpų signalizacijos sistema;

2. Programinės įrangos naudotojai:

- 2.1. nustatyta naudotojų prieigos teisių suteikimo tvarka;
- 2.2. valdoma naudotojų teisė naudotis programine įranga;
- 2.3. registruojama informacija apie paskutinius informacinių sistemų ir jose esančių duomenų pakeitimus, juos atlikusius naudotojus, ir pakeitimų laiką.

3. Prieiga prie vidinio tinklo:

- 3.1. vidinis tinklas apsaugotas ugniasienėmis;
- 3.2. nutolę įrenginiai prie vidinio tinklo jungiasi saugiu ryšio kanalu (VPN, skirtinėmis linijomis ir pan.);
- 3.3. kontroliuojama naudotojų prieiga prie vidinio tinklo;
- 3.4. tinklu siunčiama informacija šifruojama;
- 3.5. naudojamos ryšio ir tinklo srautų atakų prevencijos priemonės.

4. Atsarginių duomenų kopijų ir laikmenų naudojimas:

- 4.1. patvirtintos duomenų atsarginio kopijavimo ir laikmenų naudojimo tvarkos;
- 4.2. atsarginės duomenų kopijos saugomos atskirose apsaugotose patalpose, kitame pastate;
- 4.3. kompiuterinė įranga ir laikmenos valdomos centralizuotai;
- 4.4. atsarginės duomenų kopijos ir laikmenos yra šifruojamos.

5. Apsauga nuo vagystės:

- 5.1. apribota fizinė prieiga prie tarnybinių stočių ir kompiuterinių darbo vietų;
- 5.2. apribota programinė prieiga prie tarnybinių stočių, kompiuterinių darbo vietų ir jose esančių duomenų;
- 5.3. kompiuterinėse darbo vietose pagrindiniai duomenys nesaugomi.

6. Apsauga nuo piktnaudžiavimo duomenų perdavimo tinklu:

- 6.1. veikia duomenų perdavimo tinklo valdymo sistema;
- 6.2. nustatyti griežti duomenų perdavimo tinklo srauto apribojimai;
- 6.3. įdiegta speciali duomenų perdavimo tinklo srauto stebėjimo įranga;
- 6.4. nuolat stebima duomenų perdavimo tinklo būklė.

7. Programinės įrangos klaidos:

- 7.1. naudojama tik legali programinė įranga, kuri prižiūrima laikantis gamintojo reikalavimų;
- 7.2. diegiami operacinių sistemų ir naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai;
- 7.3. pakeista programinė įranga testuojama atskiroje tarnybiniame stotyje ar stotyse;
- 7.4. veikia informacinių sistemų infrastruktūros stebėjimo sistema.

8. Apsauga nuo kenkėjiškos programinės įrangos:

- 8.1. tarnybiniame stotyje ir kompiuterinėse darbo vietose įdiegta antivirusinė programinė įranga;
- 8.2. viešai prieinamos informacinių sistemų dalys yra atskirame potinklyje – demilitarizuotoje zonoje;
- 8.3. darbuotojai supažindinti su vidaus tvarkomis ir žino, kaip elgtis pastebėjus kenkėjišką programinę įrangą.

9. Duomenų atstatymo gebėjimai:

- 9.1. numatyta duomenų atstatymo iš atsarginių kopijų procedūra.

10. Programinės įrangos naudojimas:

- 10.1. naudojama tik legali ir leistina programinė įranga;
- 10.2. nuolat atliekama kompiuterinėse darbo vietose naudojamos programinės įrangos kontrolė;
- 10.3. naudotojai patys negali diegti programinės įrangos;
- 10.4. kompiuterinės darbo vietos valdomos centralizuotai.

11. Naudotojų švietimas:

- 11.1. naudotojai mokomi dirbti su programine įranga;
- 11.2. naudotojams parengtos tikslios ir išsamios darbo instrukcijos.

12. Apsauga nuo duomenų perdavimo tinklo įrangos gedimų:

- 12.1. įranga prižiūrima pagal gamintojo rekomendacijas;
- 12.2. priežiūrą ir gedimų šalinimą atlieka kvalifikuoti specialistai;
- 12.3. didžiausią įtaką duomenų perdavimui turinti kompiuterinė įranga dubliuota;
- 12.4. veikia duomenų perdavimo tinklo valdymo sistema;
- 12.5. stebima duomenų perdavimo tinklo būklė.

13. Apsauga nuo kompiuterinės įrangos gedimų:

- 13.1. įranga prižiūrima pagal gamintojo rekomendacijas;
- 13.2. priežiūrą ir gedimų šalinimą atlieka kvalifikuoti specialistai;
- 13.3. svarbiausia kompiuterinė įranga dubliuota;
- 13.4. svarbiausios kompiuterinės įrangos techninė būklė nuolat stebima;
- 13.5. svarbiausiai kompiuterinei įrangai yra įsigyta garantinės priežiūros paslauga.

14. Apsauga nuo užliejimo:

- 14.1. tinkamai suplanuotos ir įrengtos svarbiausios kompiuterinės įrangos laikymo patalpos;
- 14.2. įrengta vandens nutekėjimo sistema ir vandens nuotėkio davikliai.

15. Apsauga nuo gaisro:

- 15.1. patalpose yra ugnies gesintuvai;
- 15.2. įrengti dūmų ir karščio davikliai;
- 15.3. dokumentai ir bylos laikomi nedegiose metalinėse spintose;
- 15.4. atsarginės duomenų kopijos laikomos atskirose apsaugotose patalpose, kitame pastate;
- 15.5. tarnybinių stočių patalpoje yra įrengta automatinio gesinimo sistema.

16. Apsauga nuo temperatūros ir drėgmės svyravimų:

- 16.1. tarnybinių stočių patalpose įrengta kondicionavimo sistema;
- 16.2. nuolat stebimi temperatūros ir drėgmės svyravimai;
- 16.3. kondicionavimo įranga prižiūrima pagal gamintojo reikalavimus;
- 16.4. kondicionavimo įrangos priežiūrą ir gedimų šalinimą atlieka kvalifikuoti specialistai.

17. Apsauga nuo stichinių nelaimių:

- 17.1. parengtas Bendrasis veiklos tęstinumo planas.

18. Apsauga nuo elektros srovės tiekimo sutrikimų:

- 18.1. svarbiausiai kompiuterinei įrangai skirti nenutrūkstamo maitinimo šaltiniai (UPS);
- 18.2. stebima elektros srovės tiekimo būklė.

19. Apsauga nuo maitinimo ir ryšio linijų gedimų:

- 19.1. kabeliai yra izoliaciniuose vamzdžiuose;
 - 19.2. elektros ir duomenų kabeliai saugiai atskirti.
-