INFORMATIKOS IR RYŠIŲ DEPARTAMENTO
PRIE LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTERIJOS
INFORMACIJOS SAUGOS VALDYMO SISTEMOS
INFORMACIJOS SAUGOS POLITIKA

1. Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos informacijos saugos valdymo sistemos nuostatai (toliau – ISVS nuostatai) reglamentuoja pagrindinius Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Departamentas) informacijos saugos užtikrinimo ir valdymo principus, siekiant užtikrinti Departamento tvarkomos informacijos, įskaitant jo teikiamų paslaugų gavėjų ir kitų suinteresuotų šalių informacijos, saugą.

2. Informacija – Departamento veiklai strategiškai svarbus turtas, todėl Departamento informacijos praradimas, neteisėtas atskleidimas ar pakeitimas arba kiti neteisėti Departamento informacijos tvarkymo veiksmai gali sutrikdyti Departamento veiklą. Atsižvelgiant į tai, informacijos saugos politika nustato pagrindinius, bendruosius saugos reikalavimus, kuriais siekiant apsaugoti Departamento informaciją privalo vadovautis visi Departamento darbuotojai, tiekėjai ir kitos suinteresuotos šalys.

3. ISVS nuostatai taikomi ir privalomi visiems Departamento valstybės tarnautojams ir darbuotojams, dirbantiems pagal darbo sutartis, (toliau – darbuotojai), kitiems fiziniams ir juridiniams asmenims bei jų atstovams, kuriems sutartinių santykių pagrindu yra suteikta prieiga prie Departamento tvarkomos informacijos ar informacijos apdorojimo priemonių sutartyse numatytoms funkcijoms atlikti.

4. Informacijos sauga apima tris pagrindinius elementus:

4.1. informacijos konfidencialumą – informacijos apsaugą nuo nesankcionuoto atskleidimo;

4.2. informacijos vientisumą – informacijos apsaugą nuo nesankcionuoto ar atsitiktinio pakeitimo;

4.3. informacijos pasiekiamumą – užtikrinimą, kad Departamento informacija prieinama tada, kai ji yra reikalinga.

5. Bendrieji informacijos saugos tikslai:

5.1. užtikrinti tinkamą ir efektyvų informacijos valdymą, siekiant išvengti veiklos sutrikdymo dėl informacijos konfidencialumo, vientisumo ir pasiekiamumo pažeidimų bei įgyvendinant gerąją praktiką atitinkančias organizacines ir technines saugumo priemones;

5.2. užtikrinti atitiktį ISVS nuostatuose nurodytiems teisės aktų reikalavimams, atliekant kasmetinį atitikties vertinimą ir šalinant nustatytus trūkumus;

5.3. užtikrinti efektyvų rizikos valdymą ir tinkamų rizikos valdymo priemonių naudojimą, siekiant suvaldyti riziką iki priimtino lygio, atliekant kasmetinį rizikos vertinimą ir įgyvendinant

rizikos valdymo priemonių planą;

5.4. užtikrinti Departamento tvarkomų informacinių sistemų ir registrų veiklos tęstinumą, atliekant periodinį veiklos tęstinumo valdymo plano veiksmingumo išbandymą ir jo peržiūrą.

6. Pamatuojami informacijos saugos gerinimo uždaviniai ir priemonės kiekvieniems metams nustatomi Departamento vadovybės atliekamos analizės metu ir įtraukiami į strateginį bei veiklos planus, atsižvelgiant į bendruosius informacijos saugos valdymo tikslus.

7. Reikalavimai Departamento informacijos saugai nustatomi:

7.1. vadovaujantis teisės aktų reglamentuotais informacijos saugos, kibernetinio saugumo ir asmens duomenų apsaugos reikalavimais;

7.2. vadovaujantis Departamento veiklos tikslais ir veiklos reikalavimais;

7.3. atsižvelgiant į suinteresuotų šalių lūkesčius ir poreikius, išreikštus informacijos saugą reglamentuojančiuose teisės aktuose, duomenų teikimo ar kitokio pobūdžio sutartyse;

7.4. vertinant informacijos saugos riziką.

8. Departamento informacijos saugos politikos įgyvendinimas užtikrinamas ir valdomas nuosekliai planuojant, įgyvendinant, vertinant ir tobulinant ISVS, vadovaujantis standarto LST ISO/IEC 27001 reikalavimais.

9. Departamento vadovybė įsipareigoja:

9.1. nustatyti bendruosius informacijos saugos valdymo tikslus;

9.2. nustatyti informacijos saugos tobulinimo uždavinius ir priemones, įtraukiant juos į strateginį bei veiklos planus;

9.3. laikytis visų informacijos saugos įsipareigojimų, reglamentuotų Europos Sąjungos ir Lietuvos Respublikos teisės aktuose bei sutartyse;

9.4. užtikrinti efektyvų ISVS aprūpinimą reikiamais ištekliais;

9.5. sudaryti sąlygas Departamento darbuotojams tobulinti žinias informacijos saugos srityje.

10. Departamento darbuotojai įsipareigoja būti susipažinę su Departamento ISVS nuostatų reglamentuota informacijos saugos politika ir jos laikytis.

11. Departamentas nuolat gerina ISVS veiksmingumą, įgyvendinamas informacijos saugos politiką ir tikslus, organizuodamas ISVS vidaus auditus, nustatydamas neatitiktis ir jas šalindamas, vykdydamas ISVS korekcinius veiksmus ir reguliariai aptardamas informacijos saugos klausimus vadovybės pasitarimuose.

12. Informacijos saugos politika skelbiama suinteresuotoms šalims joms prieinama ir suprantama forma. Informacijos saugos politika peržiūrima periodiškai, ne rečiau kaip kartą per metus, ir esant poreikiui tikslinama.

_____