INFORMACIJOS SAUGUMO POLITIKA

Tikslas:	**Šios politikos tikslas yra nustatyti būdus, kuriais „Affidea“ saugo verslo informaciją kaip įmonės turtą, taikydama aukšto lygio taisykles ir išsamias gaires.** **Tikslas – apsaugoti informaciją iš trijų perspektyvų: konfidencialumo (pvz., prieiga suteikiama tik turint teisę), vientisumo (pvz., tiksli ir išsami informacija) ir prieinamumo (pvz., prieiga suteikiama, kai reikia). Be to, įvykus bet kokiam saugumo įvykiui, kuris sutrikdo veiklą, atkuriama žinoma, tinkamos būklės informacija.**

Autorius (SME): ..... **Data:** **2020-07-09**

Daiva Adomaitienė

Kokybės vadovė/Duomenų apsaugos pareigūnė

Proceso savininkas: ..... **Data:** **2020-07-09**

Giedrius Frankas

IT vadovas

Patvirtina: ..... **Data:** **2020-07-09**

Vitalijus Orlovas

Direktorius

Galioja nuo:	**2020 m. liepos 10 d.**

1. Apimtis

Politikos savininkas yra atsakingas ir turi įgaliojimus sukurti ir įgyvendinti informacijos saugumo valdymo sistemą (ISMS).

ISMS yra valdoma pagal šią politiką, bet išsamiausiai ji aprašyta „Informacijos saugumo gairėse“.

Ši politika taikoma visiems „Affidea“ darbuotojams, paslaugoms, vietovėms, rangovams/konsultantams ir (arba) trečiosioms šalims, teikiančioms paslaugas.

Ši politika taikoma „Affidea“ informacijos saugumo (IS) įrašams visais formatais, įskaitant elektroninius ir spausdintus įrašus.

Politikoje numatytas strategijos įgyvendinimas, vadovaujantis vartotojų, administratorių ir vadovų priimamais sprendimais ir informuojant šiuos asmenis apie jų atsakomybę už saugumą.

Politikoje taip pat nurodomi mechanizmai, kuriais remiantis galima įgyvendinti įsipareigojimus, ir patarimai apie informacinių sistemų įgijimą, ir konfigūravimą.

Pagrindiniai veiksmai, kuriais prisidedama prie saugumo politikos sėkmės:

- Politikos įgyvendinimas pasitelkiant saugumo priemones ir sankcijas;
- Apibrėžtos naudotojų, administratorių ir vadovų atsakomybės sritys;
- Aiškiai ir suprantamai informuojamos visos suinteresuotosios šalys;
- Darbuotojų patvirtinimai, kad jie perskaitė ir suprato politiką.

Ši politika galioja visai UAB „Affidea Lietuva“ įmonių grupei, t.y. visiems šią grupę sudarantiems juridiniams asmenims ir jų visiems darbuotojams. UAB „Affidea Lietuva“ įmonių grupę sudaro: UAB „Affidea Lietuva“, kodas 300542299; UAB „Medicinos paslaugų grupė“, kodas 304148323; UAB „Alytaus Medea klinika", kodas 300566791; UAB „Šilutės MCT“, kodas 300150444; UAB „MCT kompiuterinė tomografija", kodas 302032665; UAB „Endemik", kodas 220509380; UAB „Endemik didmena“, kodas 302244593, UAB “Kuncų ambulatorinė klinika”, kodas 141292840.

2. Terminai

CIO	Asmuo, atsakingas už tinkamą turto apsaugos įgyvendinimą, kaip apibrėžta Saugumo politikoje, kartu su Informacijos saugumo vadovu (CISO).
Informacijos saugumo vadovas (CISO)	Vadovas, atsakingas už saugumo iniciatyvų, susijusių su įmonių programomis ir verslo tikslais, laikymąsi, užtikrinant tinkamą informacijos turto ir technologijų apsaugą.

3. Politika

4.1 INFORMACIJOS SAUGUMAS

Pagrindinis informacijos saugumo tikslas – užtikrinti tinkamą ir efektyvų informacijos saugumo valdymą ir išvengti veiklos sutrikdymo dėl informacijos konfidencialumo, vientisumo bei prieinamumo pažeidimų.

Reikalavimai informacijos saugumo vadybos sistemai nustatomi:

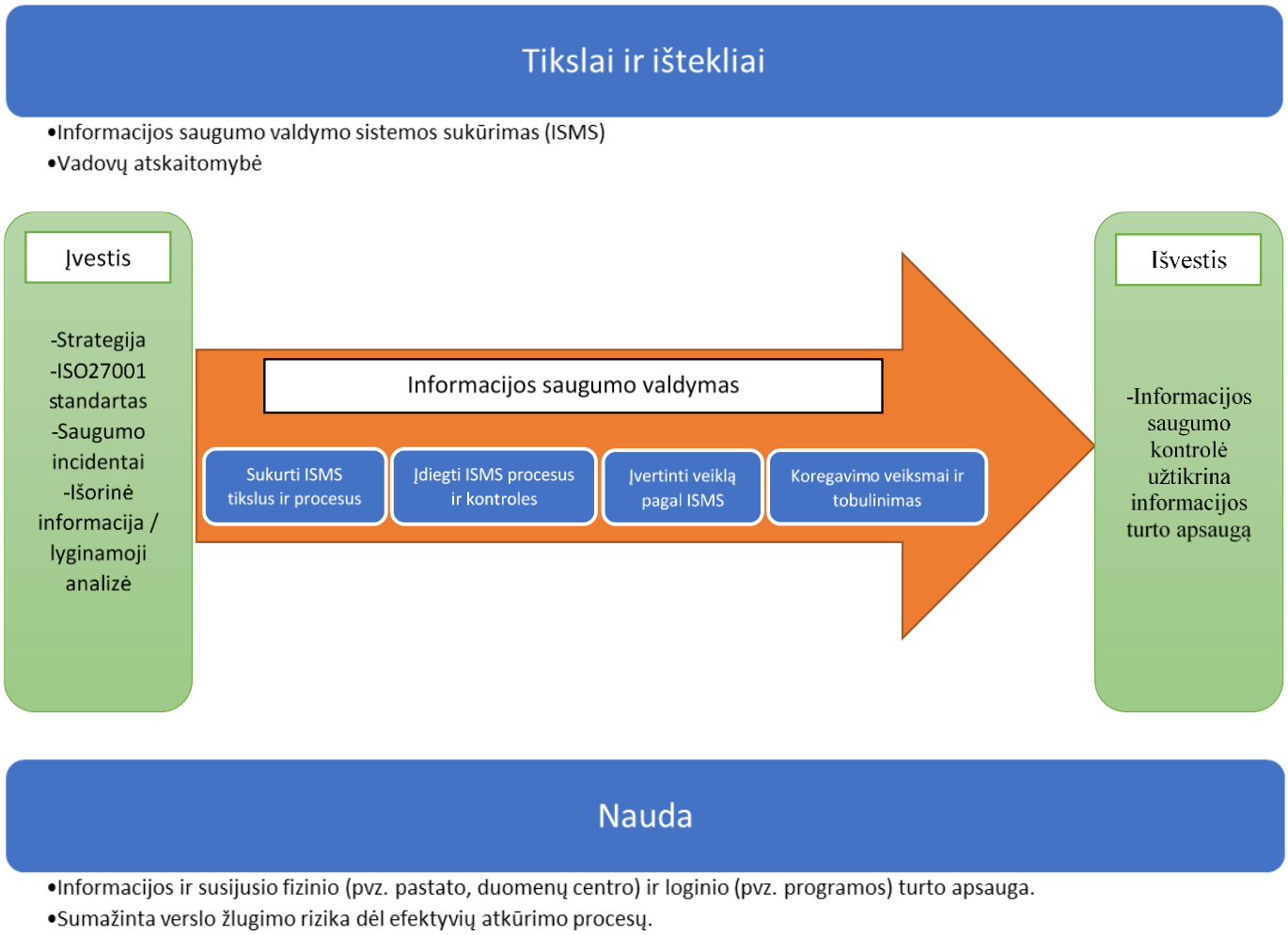
- vadovaujantis suinteresuotų šalių keliamais reikalavimais bei lūkesčiais, išreikštais informacijos saugą reglamentuojančiuose teisės aktuose, duomenų teikimo ar kitokio pobūdžio sutartyse, išoriniais ir vidiniais informacijos keitimosi būdais (raštais, elektroniniais laiškais ir pan.);

- vertinanti riziką informacijos saugumui;
- vadovaujantis nustatytais veiklos tikslais ir reikalavimais.

Vadovybė įsipareigoja:

- ✓ nustatyti tikslus informacijos saugumo vadybos sistemai;
- ✓ laikytis visų įsipareigojimų informacijos saugumui, nurodytų EN ISO 27001:2013 standarte, teisės aktuose, sutartyse;
- ✓ užtikrinti efektyvų aprūpinimą reikiamais ištekliais;
- ✓ sudaryti sąlygas darbuotojams tobulinti savo žinias informacijos saugumo srityje.

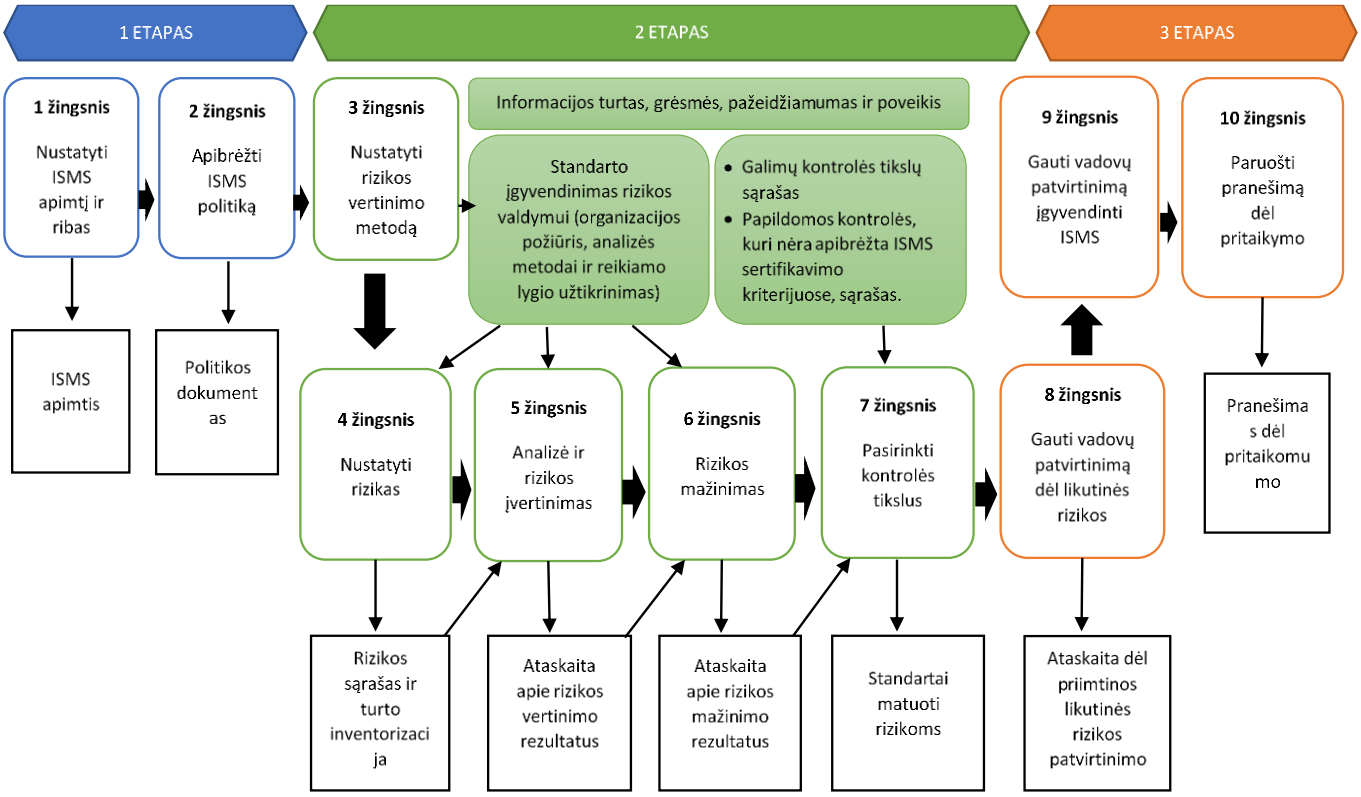
4.2 PROCESO APŽVALGA



4.3 PAGRINDINĖ VEIKLA

4.3.1 Sukurti informacijos saugumo vadybos sistemą – tikslai ir procesai

ISMS bus sukurta kartu su jos tikslais, procesais ir standartinės veiklos procedūromis (SOP), susijusiomis su rizikos valdymu ir informacijos saugumo tobulinimu, kad rezultatai būtų pasiekti vadovaujantis bendra organizacijos politika ir tikslais.



4.3.2 Įgyvendinti informacijos saugumo vadybos sistemą – procesai ir kontrolė

Sukūrus ISMS, jos procesai ir kontrolė turi būti įgyvendinami ir valdomi.
Įgyvendinimas apima technologijų įsigijimą ir eksploatavimą, specifinį pareigų ir atsakomybės paskirstymą vadovams ir darbuotojams, atitinkamos rizikos kontrolės diegimą ir užtikrinimą, kad vadovybė ir darbuotojai suprastų savo pareigas ir turėtų žinių, įgūdžių ir motyvacijos, reikalingų jų pareigoms atlikti. Tai apima visapusiškos informuotumo didinimo programos planavimą ir vykdymą.

4.3.3 Veiklos vertinimas / matavimas

Nuolat renkama ir analizuojama informacija, susijusi su naujomis grėsmėmis ir pažeidžiamumu, faktiniais išpuoliais institucijoje arba kitur, kartu su esamų saugumo kontrolės priemonių veiksmingumo palaikymu.
Reguliarus ISMS tinkamumo vidinio audito užbaigimas yra proceso dalis, o ataskaitų išvados pateikiamos vadovybės vertinime.

4.3.4 Prevenciniai, koregavimo veiksmai ir tobulinimas

Imamasi koregavimo ir prevencinių veiksmų, pagrįstų:

- vertinimų (matavimų) rezultatais,
- bet kokiais ISMS auditais, kurie galėjo įvykti,
- vadovybės peržiūra ir
- kita svarbia informacija,

siekiant nuolatinio ISMS tobulinimo.

4.4 PROCESO KONTROLĖ

Turi būti nustatyti ir stebimi rodikliai, kaip laikomasi pagrindinių korporacijos verslo aspektų:

- Atitikties duomenys;
- Finansiniai duomenys;

- Išteklių duomenys;
- Duomenys apie incidentus;
- Pažeidžiamumo duomenys;
- Grėsmės duomenys.

4.5 KOMUNIKACIJA

Rodiklių ataskaitos rengiamos reguliariai ir perduodamos atitinkamoms suinteresuotosioms šalims.
Iš anksto nustatyti informacijos saugumo sistemos aspektai yra rengiami metinėje vadybos apžvalgos ataskaitoje.

4. Mokymų reikalavimai

Su dokumentu supažindinami ar apmokinami šių funkcijų darbuotojai:

- Visi darbuotojai.

Įrašai apie supažindinimą su dokumentu ar mokymus atliekami ir laikomi pagal SOP-QM-LT-003 Kokybės įrašų kontrolė.

5. Auditas / Metrikai

Šalies vadovas yra atsakingas už tai, kad būtų vykdomas vidinis (valstybės lygmens) auditas, skirtas įvertinti atitiktį šiai politikai.
Atitiktis politikai apima darbuotojų mokymų ir sąmoningumo įrodymą.
Siekiant įvertinti atitiktį politikai, gali būti vykdomas išorinis auditas (centrinio biuro arba trečiųjų šalių).

6. Nuorodos / Susiję dokumentai

P-IT-LT-001	Informacijos saugumo politika
SOP-IT-LT-001	Informacijos saugumo incidentų valdymo procedūra

7. Versijų istorija

Versija	Pakeitimo aprašymas	Pakeitimo priežastis
01	Pirminis dokumentas	
02	Išplėsta politikos taikymo apimtis	Įmonių prisijungimas