



## Curriculum – Lietuvių

Žinių, įgūdžių ir gebėjimų, susijusių su informacijos saugumu ir duomenų apsauga MVĮ, mokymosi vienetai



Funded by the  
Erasmus+ Programme  
of the European Union





Funded by the  
Erasmus+ Programme  
of the European Union

Šis dokumentas yra licencijuotas pagal CC BY-SA 4.0.

Šis dokumentas parengtas įgyvendinant ERASMUS+ projektą "Teilzertifizierung im Berufsfeld Informationssicherheit - TeBeiSi", projekto ID: 2018-1-EN02-KA202-005218

Europos Komisijos parama rengiant šį leidinį nėra pritarimas turiniui, kuris atspindi tik autorių požiūrį. Komisija negali būti laikoma atsakinga už bet kokį jame esančios informacijos naudojimą.

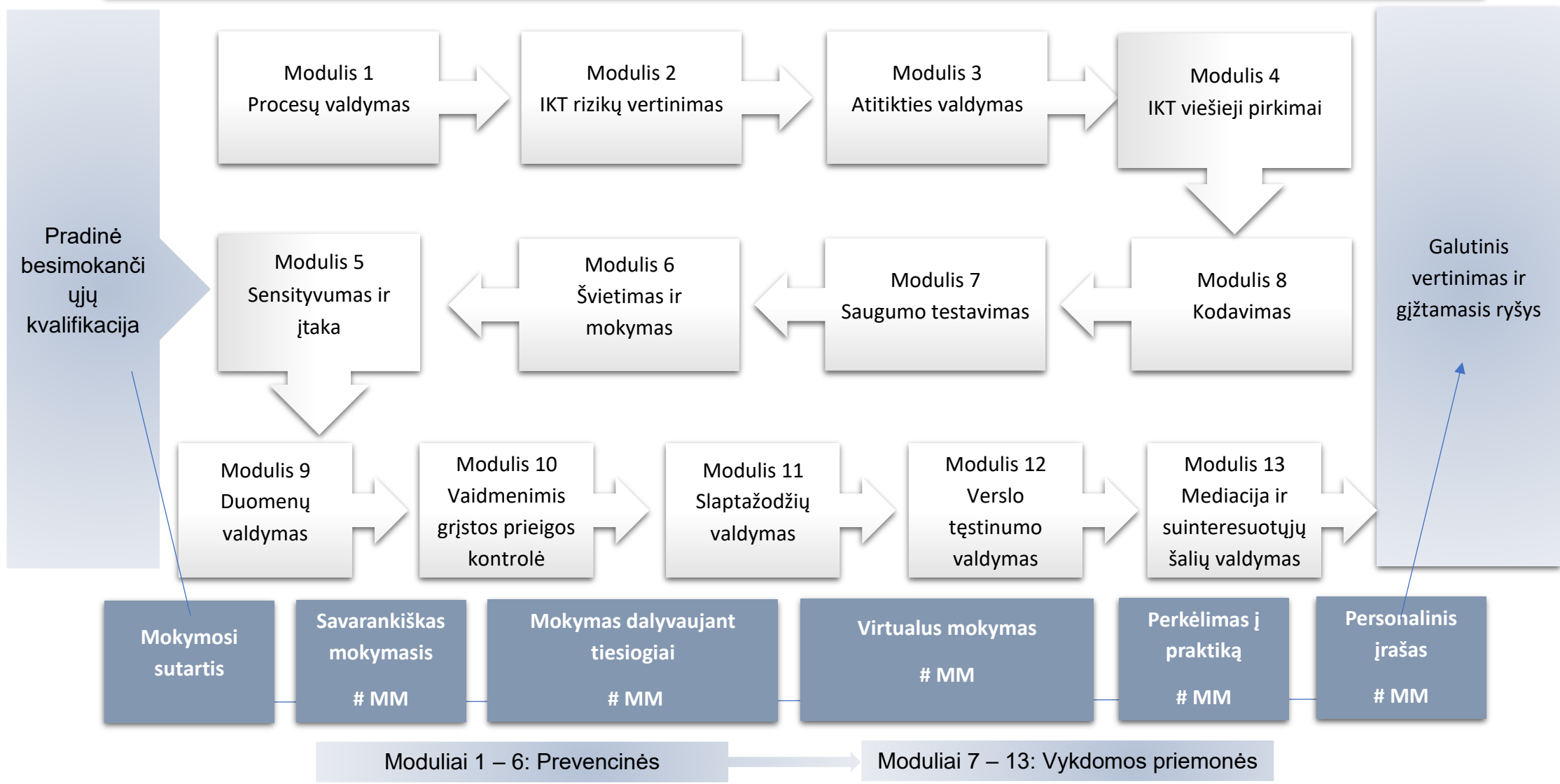


## Turinys

1.1	Mokymų moduliai - apžvalga ir trumpas aprašymas .....	5
2	Išsamus mokymo modulių aprašymas (vadovaujantis ECVET kriterijais) .....	6
2.1	MM1 – Procesų valdymas .....	6
2.2	MM2 - IKT rizikos valdymas .....	8
2.3	MM3 – Atitikties valdymas .....	10
2.4	MM4 – IKT viešieji pirkimai .....	13
2.5	MM5 – Sensityvumas ir įtaka .....	15
2.6	MM6 – Švietimas ir mokymas .....	17
2.7	MM7 – Saugumo testavimas .....	19
2.8	MM8 – Kodavimas .....	21
2.9	MM9 - Duomenų valdymas .....	23
2.10	MM10 - Vaidmenimis grįstos prieigos kontrolė .....	25
2.11	MM11 – Slaptažodžių valdymas .....	27
2.12	MM12 - Verslo tęstinumo valdymas .....	29
2.13	MM13 – Mediacija ir suinteresuotųjų šalių valdymas .....	31



## TeBeSi Mokymų planas (remiantis ECVET kriterijais)





## 1.1 Mokymų moduliai - apžvalga ir trumpas aprašymas

#	Mokymų moduliai	Trumpas aprašymas
MM1	<b>Procesų valdymas</b>	Verslo procesų analizė ir strateginės duomenų apsaugos ir informacijos saugumo ataskaitos rengimas.
MM2	<b>IKT rizikų vertinimas</b>	Įmonės pokyčių, kurie turi įtakos įmonės saugumo strategijai stebėsenai ir ataskaitos kolegoms rengimas.
MM3	<b>Atitikties valdymas</b>	Įmonės gairių, kaip elgtis su konkrečia informacija ir duomenimis parengimas.
MM4	<b>IKT pirkimai</b>	Rekomendacijų dėl įsigyjamų daiktų parengimas, atsižvelgiant į įmonės informacijos saugumo ir duomenų apsaugos reikalavimus.
MM5	<b>Sensityvumas ir įtaka</b>	(Informavimo) veiklų vykdymas, siekiant atkreipti darbuotojų dėmesį į saugumo rizikas ir sužadinant darbuotojų sąmoningumą.
MM6	<b>Švietimas ir mokymas</b>	Įmonės mokymo planų parengimas, siekiant vykdyti reguliarius darbuotojų mokymus informacijos saugumo ir duomenų apsaugos srityse.
MM7	<b>Saugumo testavimas</b>	Antivirusinės programinės įrangos ir užkardos įdiegimas. Atnaujinimų atlikimas ir pagrindinių metodų pritaikymas, užtikrinant įmonėje naudojamos programinės įrangos saugumą ir atitinkamų dokumentų pateikimą.
MM8	<b>Kodavimas</b>	Mobiliųjų prietaisų, ryšio kanalų ir duomenų saugojimo įrenginių sekiuritizacijos pakeitimas naudojant slaptažodžius ar kitas autentifikavimo priemones
MM9	<b>Duomenų valdymas</b>	Įprastinių duomenų atsarginių kopijų rengimas ir taikyti tinkamo duomenų apdorojimo įmonėje metodus pagal BDAR.
MM10	<b>Vaidmenimis grįstos prieigos kontrolė</b>	Sukūrimas administratoriaus paskyros ir apribojimas prieigos teisės tarp darbuotojų, pagal jų padėtį ir pareigas įmonėje.
MM11	<b>Slaptažodžių valdymas</b>	Asmeninių darbuotojų prieigos slaptažodžių sukūrimas ir jų saugojimo ir atkūrimo proceso užtikrinimas.
MM12	<b>Verslo tęstinumo valdymas</b>	Gairių ir procedūrų, dėl nenumatytų atvejų atsiradimo parengimas.
MM13	<b>Mediacija ir suinteresuotųjų šalių valdymas</b>	Įmonės vadovų ir darbuotojų poreikių koordinavimas, teikiant informaciją ir įžvalgas abiem šalims.



## 2 Išsamus mokymo modulių aprašymas (vadovaujantis ECVET kriterijais)

### 2.1 MM1 – Procesų valdymas

Mokymų modulis 1	Procesų valdymas
<b>Bendras aprašymas/ siekiamas rezultatas</b>	Verslo procesų analizė ir strateginės duomenų apsaugos ir informacijos saugumo ataskaitos rengimas
Numeris	MM 1
Tipas	Privalomas – turi būti apibrėžtas
Apimtis	Valandos - turi būti apibrėžtos
<b>Veiklos kompetencijos</b>	Dalyviai mokosi suprasti įmonėje atliekamos struktūrinės procesų analizės svarbą. Geba atpažinti procesus, kuriuos būtina toliau analizuoti atsižvelgiant į jų poveikį duomenų ir informacijos saugumui. Susipažįsta su procesų dokumentacija ir geba stebėti darbo rutinos pokyčius. Geba parengti dokumentus, kurie leidžia formuluoti rekomendacijas dėl veiksmų.
<b>Mokymosi rezultatai</b>	<p><b>Techninė/ profesinė kompetencija</b> Mokymų dalyviai <b>žinos</b>:</p> <ul style="list-style-type: none"> <li>- kaip taikyti BDAR gaires ir gerąją informacijos saugumo praktiką.</li> <li>- kaip nustatyti, dokumentuoti, projektuoti, įgyvendinti, valdyti ir optimizuoti verslo procesus.</li> <li>- kaip strategiškai planuoti procesų dokumentaciją.</li> <li>- apie komunikacijos būdus ir kanalus.</li> </ul> <p>Mokymų dalyviai <b>gebės</b>:</p> <ul style="list-style-type: none"> <li>- įdiegti dokumentus naudojant elektroninio duomenų apdorojimo (EDA) sistemas.</li> <li>- apibendrinti originalią pirminę informaciją,</li> <li>- efektyviai bendrauti su kolegomis siekiant koreguoti darbo eigą.</li> <li>- tinkamai reaguoti į kitų komentarus, pvz., priimti konstruktyvią kritiką ir aktyviai klausytis, siekiant rasti geriausius sprendimus.</li> <li>- rasti tinkamą teisinę ir techninę informaciją bei atitinkamas rekomendacijas iš patikimų šaltinių veiksams atlikti.</li> </ul> <p><b>Asmeninė kompetencija</b></p> <p>Mokymų dalyviai <b>gebės</b>:</p> <ul style="list-style-type: none"> <li>- savarankiškai organizuoti dokumentacijos procesą, dirbant struktūrizuotu būdu, daugiausia dėmesio skiriant detalėms.</li> <li>- savarankiškai bendrauti su kolegomis, bendravimą grindžiant pasitikėjimu.</li> </ul>



	<p>- suprasti su užduotimi susijusią atsakomybę ir atsakomybę ir pasitikėti savimi bendraujant su kitais.</p> <p>-</p>
<b>Rekomendacijos mokymui ir mokymuisi</b>	<p>Procesų dokumentacija grįsta praktiniais pavyzdžiais . EDA sistemos dokumentacijos veiklos laisva forma ir naudojant tekstinius modulius.</p>
<b>Literatūra ir papildomi ištekliai mokymuisi</b>	<p>Nguyen, B. T., Lee, G. M., Sun, K., &amp; Guo, Y. (2019). GDPR-Compliant Personal Data Management: A Blockchain-Based Solution. <i>IEEE Transactions on Information Forensics and Security</i>, 15, 1-13.</p> <p>EU-GDPR. (2019). <i>EU GDPR portal</i>. [Online]. Available: <a href="https://eugdpr.org">https://eugdpr.org</a>.</p> <p>General data protection regulation (2018). Official Journal of the European Union [Online]. Available: <a href="http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679">http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679</a>.</p> <p>Gellert, R. (2015). Understanding data protection as risk regulation. <i>Journal of Internet Law</i>, 18 (11), 3-15.</p>



## 2.2 MM2 - IKT rizikos valdymas

Mokymų modulis 2	IKT rizikos valdymas
<b>Bendras aprašymas/ siekiamas rezultatas</b>	<b>Įmonės pokyčių, kurie turi įtakos įmonės saugumo strategijai stebėsenai ir ataskaitos kolegoms rengimas</b>
Numeris	MM 2
Tipas	Privalomas – turi būti apibrėžtas
Apimtis	Valandos - turi būti apibrėžtos
<b>Veiklos kompetencijos</b>	Dalyviai mokosi suprasti technologinių pokyčių dinamiką ir jų įtaką įmonės strategijai siekiant sumažinti riziką. Geba nuspręsti, kaip skubiai reaguoti į šią riziką. Gebės sekti technologinius pokyčius įmonėje ir už jos ribų bei pateikti įmonės rizikos poveikio vertinimus.
<b>Mokymosi rezultatai</b>	<p><b>Techninė/ profesinė kompetencija</b> Mokymų dalyviai <b>žinos</b>:</p> <ul style="list-style-type: none"> <li>- apie įmonės patiriamos rizikos vertinimą ir esamų priemonių tinkamumą rizikai įveikti.</li> <li>- kaip stebėti technologinius pokyčius įmonėje ir už jos ribų, taip pat personalo pokyčius.</li> <li>- kaip nustatyti tvarkomų asmens duomenų kiekį ir paskirtį.</li> </ul> <p>Mokymų dalyviai <b>gebės</b>:</p> <ul style="list-style-type: none"> <li>- rasti informacijos apie technologijų plėtrą, vadovaujantis informacijos šaltiniais, gautais iš valstybinių ar privačių šios srities institucijų.</li> <li>- aptikti riziką, nepaisant teorinio darbuotojų nenoro atskleisti klaidas ar trūkumus.</li> <li>- remiantis gauta informacija teikti rekomendacijas dėl veiksmų.</li> <li>- įvertinti ir sumažinti su duomenų apsauga susijusią riziką.</li> <li>- nustatyti asmens duomenų saugyklas / tvarkymo operacijas organizacijose ir įvertinti jų kontekstą.</li> <li>- imtis strateginių veiksmų, siekiant sutelkti išteklius ir darbuotojus bendradarbiavimui stiprinti.</li> <li>- demonstruoti atsparumą, kai susiduria su kolegų nenoru bendradarbiauti.</li> </ul> <p><b>Asmeninė kompetencija</b></p> <p>Mokymų dalyviai <b>gebės</b>:</p> <ul style="list-style-type: none"> <li>- demonstruoti atsparumą, kai susiduria su kolegų nenoru bendradarbiauti.</li> <li>- išlikti lanksčiais siekiant rasti sprendimus ir sukurti palankią aplinką.</li> <li>- strategiškai ir organizuotai atlikti užduotis.</li> </ul>
<b>Rekomendacijos mokymui ir mokymuisi</b>	Procesų dokumentacija su realiais pavyzdžiais. EDA sistemos dokumentacijos veiklos laisva forma ir naudojant tekstinius modulius.





<b>Literatūra ir papildomi ištekliai mokymuisi</b>	<p>European Banking Authority (2019). Final Report: EBA Guidelines on ICT and security risk management [Online]. Available: <a href="https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020">https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020</a>.</p> <p>NZ Digital Government (2021). ICT Risk Management Guidance [Online]. Available: <a href="http://www.digital.govt.nz/dmsdocument/130-ict-risk-management-guidance/html">www.digital.govt.nz/dmsdocument/130-ict-risk-management-guidance/html</a>.</p> <p>Commission de Surveillance du Secteur Financier (CSSF) (2020). ICT Risk [Online]. Available: <a href="http://www.cssf.lu/en/ict-risk/">www.cssf.lu/en/ict-risk/</a>.</p> <p>Rothman, T. (2020). Valuations of Early-Stage Companies and Disruptive Technologies: How to Value Life Science, Cybersecurity and ICT Start-ups, and their Technologies. Berlin: Springer.</p>
--	---



## 2.3 MM3 – Atitikties valdymas

Mokymų modulis 3	Atitikties valdymas
<b>Bendras aprašymas/ siekiamas rezultatas</b>	<b>Įmonės gairių, kaip elgtis su konkrečia informacija ir duomenimis parengimas</b>
Numeris	MM 3
Tipas	Privalomas – turi būti apibrėžtas
Apimtis	Valandos - turi būti apibrėžtos
<b>Veiklos kompetencijos</b>	Dalyviai supras, kaip svarbu kodifikuoti įmonės elgesio gaires, kad būtų galima tinkamai elgtis su duomenimis ir informacija. Sužinos, kaip nustatyti gaires, kurios užtikrintų, kad darbuotojai laikytųsi reikalavimų. Supras, kaip svarbu pasirengti numatytiems ir nenumatytiems atvejams ir nustatyti visos įmonės taisykles, kaip elgtis ir kokių priemonių imtis kritinėse situacijose.
<b>Mokymosi rezultatai</b>	<p><b>Techninė/ profesinė kompetencija</b> Mokymų dalyviai <b>žinos</b>:</p> <ul style="list-style-type: none"> <li>- apie BDAR reglamentavimą ir nacionalinius teisės aktus, reglamentuojančius informacijos saugumą ir duomenų apsaugą.</li> <li>- apie informacijos architektūrą ir organizacijos vidaus komunikacijos kanalus</li> <li>- kaip išanalizuoti, aprašyti ir dokumentuoti procesus, dėl kurių gali kilti galimas konfliktas su atitikties politika.</li> <li>- kaip parengti atitikties politikos gaires.</li> <li>- kaip rinkti, tvarkyti ir vertinti duomenų tvarkymo techniką.</li> <li>- kaip analitiškai mąstyti apdorojant kondensuotą informaciją, kuriant sprendimus ir priimant su atitikties valdymu susijusius sprendimus.</li> </ul> <p>Mokymų dalyviai <b>gebės</b>:</p> <ul style="list-style-type: none"> <li>- įgyvendinti teisiniuose dokumentuose aprašytas procedūras.</li> <li>- nustatyti ypatingos svarbos duomenų ir informacijos vienetus, kuriuos reikia ypatingai saugoti ar tvarkyti.</li> <li>- analizuoti ir sudaryti su informacijos srautu susijusių procesų organizacijoje žemėlapi.</li> <li>- atpažinti galimus pavojus ir grėsmes informacijos saugumui ir duomenų apsaugai organizacijos vidaus procesuose.</li> <li>- rengti su atitikties valdymu susijusius praktinių, operatyvinių ar konceptualių problemų sprendimus, susijusius su įvairiomis kasdienio darbo užduotimis.</li> <li>- suprasti atitikties politikos gairių paskirtį ir jas atnaujinti kritiniais atvejais.</li> <li>- taikyti analitinio ir kritinio mąstymo įgūdžius nustatant galimų su atitikties valdymu susijusių problemų sprendimų privalumus ir trūkumus.</li> <li>- patogia ir prasmingai apibendrinti informaciją.</li> </ul> <p><b>Asmeninė kompetencija</b></p>



	<p><b>Mokymų dalyviai gebės:</b></p> <ul style="list-style-type: none"><li>- dirbti struktūrizuotai, daugiausia dėmesio skiriant detalėms.</li><li>- atpažinti su užduotimis susijusią atsakomybę ir pasitikėti savimi bendraujant su kitais.</li><li>- savarankiškai atlikti užduotis ir parodyti norą mokytis..</li></ul>
<b>Rekomendacijos mokymui ir mokymuisi</b>	<p>Procesų dokumentacija su realiais pavyzdžiais. EDA sistemos dokumentacijos veiklos laisva forma ir naudojant tekstinius modulius.</p>
<b>Literatūra ir papildomi ištekliai mokymuisi</b>	<p>Agostinelli S., Maggi F.M., Marrella A., &amp; Sapio F. (2019) Achieving GDPR Compliance of BPMN Process Models. In: Cappiello C., Ruiz M. (eds) Information Systems Engineering in Responsible Information Systems. CAiSE 2019. Lecture Notes in Business Information Processing, 350, 10–22. Springer, Cham. <a href="https://doi.org/10.1007/978-3-030-21297-1_2">https://doi.org/10.1007/978-3-030-21297-1_2</a></p> <p>Basin, D., Debois, S., &amp; Hildebrandt, T. (2018). On purpose and by necessity: compliance under the GDPR. In Proceedings Financial Cryptography and Data Security, 18 [Online]. Available: <a href="https://pure.itu.dk/ws/files/84212312/On_Purpose_and_ny_Necessity.pdf">https://pure.itu.dk/ws/files/84212312/On_Purpose_and_ny_Necessity.pdf</a></p> <p>Besik, S. I., &amp; Freytag, J. C. (2020). Managing Consent in Workflows under GDPR. In J. Manner, S. Haarmann, S. Kolb, O. Kopp (Eds.): 12th ZEUS Workshop, ZEUS 2020, Potsdam, Germany, 20-21 February 2020, (pp. 18-25).</p> <p>Blanco-Lainé, G., Sottet, J. S., &amp; Dupuy-Chessa, S. (2019, November). Using an enterprise architecture model for GDPR compliance principles. In IFIP Working Conference on The Practice of Enterprise Modeling (pp. 199-214). Springer, Cham.</p> <p>EU-GDPR. (2019). EU GDPR portal. [Online]. Available: <a href="https://eugdpr.org">https://eugdpr.org</a>.</p> <p>Kammüller, F., Ogunyanwo, O.O., &amp; Probst, C.W. (2019). Designing data protection for GDPR compliance into IoT healthcare systems. Computer Science. arXiv:1901.02426.</p> <p>Torre, D., Soltana, G., Sabetzadeh, M., Briand, L. C., Auffinger, Y., &amp; Goes, P. (2019). Using Models to Enable Compliance Checking Against the GDPR: An Experience Report. In 2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems (MODELS), Munich, Germany, 2019, (pp. 1-11). doi: 10.1109/MODELS.2019.00-20.</p> <p>Wichmann, J., Sandkuhl, K., Shilov, N., Smirnov, A., Timm, F., &amp; Wißotzki, M. (2020). Enterprise Architecture Frameworks as Support for Implementation of Regulations: Approach and Experiences from</p>



	GDPR. Complex Systems Informatics and Modeling Quarterly, (24), 31-48.



## 2.4 MM4 – IKT viešieji pirkimai

Mokymų modulis 4	IKT viešieji pirkimai
<b>Bendras aprašymas/ siekiamas rezultatas</b>	<b>Rekomendacijų dėl įsigyjamų daiktų parengimas, atsižvelgiant į įmonės informacijos saugumo ir duomenų apsaugos reikalavimus.</b>
Numeris	MM 4
Tipas	Privalomas – turi būti apibrėžtas
Apimtis	Valandos - turi būti apibrėžtos
<b>Veiklos kompetencijos</b>	<p>Dalyviai supras viešųjų pirkimų svarbą informacijos saugumo ir duomenų apsaugos įgyvendinimui.</p> <p>Žinos, kaip pozicionuoti savo kompetenciją įmonės viešųjų pirkimų procese.</p> <p>Gebės daryti įtaką naujų technologijų ir technikos pirkimui bei įvertinti jų tinkamumą naudoti, atsižvelgiant į įmonės duomenų apsaugos ir informacijos saugumo gaires.</p>
<b>Mokymosi rezultatai</b>	<p><b>Techninė/ profesinė kompetencija</b></p> <p>Mokymų dalyviai <b>žinos</b>:</p> <ul style="list-style-type: none"> <li>- apie įmonės saugumo ir specifikacijos reikalavimus, susijusius su nauja įranga.</li> <li>- apie esamos techninės įrangos specifikacijas ir būtinybę jas skubiai pakeisti naujomis technologijomis.</li> <li>- apie paslaugų teikėjų ir įrangos apgaulę dėl BDAR pažeidimų.</li> </ul> <p>Mokymų dalyviai <b>gebės</b>:</p> <ul style="list-style-type: none"> <li>- parengti ir pristatyti trumpą pristatymą (reportažą, procedūrą, procesą, strategiją), skirtą technologijai ar technikai, kurią reikia įsigyti, įvertinti.</li> <li>- perduoti informaciją iš įvairių darbuotojų, skyrių apie jų poreikius ir pateikti rekomendaciją dėl įsigijimo.</li> <li>- surinkti išsamią informaciją apie perkamą technologiją, mašinas.</li> <li>- surasti atitinkamą teisinę ir techninę informaciją ir, remdamiesi šia užklausa, priimti sprendimus.</li> <li>- imtis veiksmų, susijusių su strateginiu lygmeniu nustatytais tikslais ir procedūromis, siekiant sutelkti išteklius ir įgyvendinti nustatytas strategijas.</li> <li>- planuoti ir valdyti išteklius, atsižvelgiant į biudžeto ir laiko apribojimus, ir siekti nustatytų tikslų, naudojantis projekto eigos stebėjimo ir kokybės kontrolės priemonėmis.</li> </ul> <p><b>Asmeninė kompetencija</b></p> <p>Mokymų dalyviai <b>gebės</b>:</p> <ul style="list-style-type: none"> <li>- sužinoti apie rinkoje egzistuojantį įmonės problemos sprendimą.</li> <li>- skirti dėmesio detalėms (teisinėms ir techninėms).</li> <li>- rodyti pasitikėjimą ir atsakomybę bendraujant su suinteresuotomis šalimis.</li> </ul>



<b>Rekomendacijos mokymui ir mokymuisi</b>	Procesų dokumentacija su realiais pavyzdžiais. EDA sistemos dokumentacijos veiklos laisva forma ir naudojant tekstinius modulius.
<b>Literatūra ir papildomi ištekliai mokymuisi</b>	<p>Australian Government: Digital Transformation Agency (2021). ICT procurement [Online]. Available: <a href="http://www.dta.gov.au/help-and-advice/ict-procurement">www.dta.gov.au/help-and-advice/ict-procurement</a>.</p> <p>Moses, M. (2019). Procurement Process and ICT. Zerite Network [Online]. Available: <a href="http://zeritenetwork.com/procurement-process-and-ict/">http://zeritenetwork.com/procurement-process-and-ict/</a>.</p> <p>European Commission (2016). Best practices for ICT procurement based on standards in order to promote efficiency and reduce lock-in: 2-year project completed [Online]. Available: <a href="http://ec.europa.eu/digital-single-market/en/news/">ec.europa.eu/digital-single-market/en/news/</a>.</p> <p>Dovgalenko, S. (2020). The Technology Procurement Handbook: A Practical Guide to Digital Buying. London: Kogan Page.</p>



## 2.5 MM5 – Sensityvumas ir įtaka

Mokymų modulis 5	Sensitivityvumas ir įtaka
<b>Bendras aprašymas/ siekiamas rezultatas</b>	<b>Veiklų (Informavimo) vykdymas, siekiant atkreipti darbuotojų dėmesį į saugumo rizikas ir sužadinant darbuotojų sąmoningumą.</b>
Numeris	MM 5
Tipas	Privalomas – turi būti apibrėžtas
Apimtis	Valandos - turi būti apibrėžtos
<b>Veiklos kompetencijos</b>	<p>Mokymų dalyviai supras, kaip svarbu informuoti darbuotojus ir įmonės vadovus apie duomenų apsaugos ir informacijos saugumo problemas. Išmoks skleisti informaciją apie dažniausiai pasitaikančias grėsmes ir ugdyti darbuotojų gebėjimus aptikti tikėtinas grėsmes jų kasdienėje profesinėje veikloje.</p> <p>Gebės atlikti informuotumo lygio įmonėje analizę ir įgyvendinti atitinkamas informuotumo didinimo priemones.</p>
<b>Mokymosi rezultatai</b>	<p><b>Techninė/ profesinė kompetencija</b> Mokymų dalyviai <b>žinos:</b></p> <ul style="list-style-type: none"> <li>- apie pagrindines BDAR gaires.</li> <li>- kaip elgtis su galimais procesais ir darbuotojais, kurie gali būti pažeidžiami dėl atakų ar neskelbtinos informacijos bei duomenų praradimo.</li> <li>- kaip galima įgyvendinti audito priemones</li> <li>- apie komunikacijos būdus ir kanalus</li> <li>- kaip įgyvendinti pokyčių strategijas</li> </ul> <p>Mokymų dalyviai <b>gebės:</b></p> <ul style="list-style-type: none"> <li>- rasti tinkamą teisinių žinių šaltinį.</li> <li>- bendradarbiauti su kitais asmenimis, siekiant nustatyti pokyčių poreikį ir juos įgyvendinti</li> <li>- veiksmingai bendrauti su kitais, pasirenkant ne tik pranešimo tipą, bet ir jo apimtį bei svarbą atsižvelgiant į aplinkybes.</li> </ul> <p><b>Asmeninė kompetencija</b> Mokymų dalyviai <b>gebės:</b></p> <ul style="list-style-type: none"> <li>- prisitaikyti prie besikeičiančių sąlygų ir aplinkybių, dirbant organizuotai ir išlaikant atstumą, leidžiantį tinkamai save įvertinti.</li> <li>- būti pavyzdžiu kitiems darbuotojams, laikytis profesinės etikos kodekso ir demonstruoti atsakomybę.</li> </ul>
<b>Rekomendacijos mokymui ir mokymuisi</b>	<p>Iliustruokite teoriją praktiniais pavyzdžiais, pvz., pasitikrinimo priemonėmis ir atvejų analize. Galimų praktinių atvejų pavyzdžiai:</p> <ul style="list-style-type: none"> <li>- suklastotos USB atmintinės,</li> <li>- žmogaus inžinerijos atvejai,</li> <li>- suklastotų elektroninių laiškų siuntimas.</li> </ul>



	<p>Taikykite interaktyvius mokymo metodus (pvz., darbas grupėse, diskusijos, atvejų analizė, simuliaciniai vaidmenų žaidimai ir kt.)</p>
<b>Literatūra ir papildomi ištekliai mokymuisi</b>	<p>IT Governance Privacy Team (2020). EU General Data Protection Regulation (GDPR) – An implementation and compliance guide (4th ed.).</p> <p>Clarke, N., Furnell, S. (2020). Human Aspects of Information Security &amp; Assurance (14th ed.). Plymouth: Centre for Security, Communication &amp; Network Research.</p> <p>i-scoop (o.J.). GDPR awareness: a matter of people, culture, leadership and acting now [Online]. Available: <a href="https://www.i-scoop.eu/gdpr/gdpr-awareness/">https://www.i-scoop.eu/gdpr/gdpr-awareness/</a>.</p> <p>Kefron - The Information Management People (o.J.). Why Maximizing Staff Awareness Is The Key To A Smooth GDPR Transition [Online]. Available: <a href="https://www.kefron.com/blog/why-maximizing-staff-awareness-is-the-key-to-a-smooth-gdpr-transition/">https://www.kefron.com/blog/why-maximizing-staff-awareness-is-the-key-to-a-smooth-gdpr-transition/</a>.</p> <p>European Union Agency for Cybersecurity (2017). Handbook on Security of Personal Data Processing [Online]. Available: <a href="http://www.enisa.europa.eu">www.enisa.europa.eu</a></p> <p>General Data Protection Regulation (2021). Complete guide to GDPR compliance [Online]. Available: <a href="https://gdpr.eu/">https://gdpr.eu/</a></p>





## 2.6 MM6 – Švietimas ir mokymas

Mokymų modulis 6	Švietimas ir mokymas
<b>Bendras aprašymas/ siekiamas rezultatas</b>	Įmonės mokymo planų parengimas, siekiant vykdyti reguliarius darbuotojų mokymus informacijos saugumo ir duomenų apsaugos srityse.
Numeris	MM 6
Tipas	Privalomas – turi būti apibrėžtas
Apimtis	Valandos - turi būti apibrėžtos
<b>Veiklos kompetencijos</b>	<p>Mokymų dalyviai supras švietimo svarbą duomenų apsaugos ir informacijos saugumo srityje. Mokės mokytis ir mokyti kitus įmonės darbuotojus.</p> <p>Gebės konsultuodamiesi ir bendraudami su darbuotojais išsiaiškinti jų mokymo(si) poreikius.</p> <p>Išmoks rengti mokymo medžiagą ir mokyti darbuotojus į savo kasdienę profesinę veiklą įtraukti tinkamas darbo procedūras.</p>
<b>Mokymosi rezultatai</b>	<p><b>Techninė/ profesinė kompetencija</b></p> <p>Mokymų dalyviai <b>žinos</b>:</p> <ul style="list-style-type: none"> <li>- kur rasti nacionalinius teisinius dokumentus, reglamentuojančius informacijos saugumą ir duomenų apsaugą (BDAR pagrindai).</li> <li>- kaip parengti mokymų medžiagą ir kaip vykdyti mokymus, kad į juos būtų įtraukta tinkama darbo tvarka.</li> <li>- kaip individualiai konsultuoti darbuotojus</li> </ul> <p>Mokymų dalyviai <b>gebės</b>:</p> <ul style="list-style-type: none"> <li>- supažindinti darbuotojus, kaip praktiškai taikyti nacionalinius teisinius dokumentus informacijos saugumo ir duomenų apsaugos srityje, vadovaujantis BDAR gairėmis.</li> <li>- ugdyti darbuotojų nuostatas sąmoningai ir nuolatos tobulėti abiejose srityse.</li> <li>- teikti pagalbą ir individualiai konsultuoti darbuotojus dėl nustatytų mokymų poreikio.</li> <li>- rengti praktinių, veiklos ar konceptualių problemų, kylančių atliekant darbą įvairiuose kontekstuose, sprendimus.</li> </ul> <p><b>Asmeninė kompetencija</b></p> <p>Mokymų dalyviai <b>gebės</b>:</p> <ul style="list-style-type: none"> <li>- savarankiškai organizuoti mokymus įmonėje, atsižvelgiant į nustatytus darbuotojų poreikius.</li> <li>- savarankiškai bendrauti su kolegomis ir užmezgant pasitikėjimu grįstą santykį..</li> <li>- pripažinti su užduotimis susijusią atsakomybę ir motyvuoti darbuotojus mokytis.</li> <li>-</li> </ul>



<b>Rekomendacijos mokymui ir mokymuisi</b>	Informacijos saugumo ir duomenų apsaugos sunkumų, su kuriais susiduriama kasdieniame darbe, dokumentavimas, siekiant suplanuoti ir įgyvendinti tinkamas mokymo priemones.
<b>Literatūra ir papildomi ištekliai mokymuisi</b>	<p>Pipkin, D. (2000). Information security: Protecting the global enterprise. New York: Hewlett-Packard Company.</p> <p>Da Veiga, A., Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. <i>Computers &amp; Security</i>, (49), 162–176. doi: 10.1016/j.cose.2014.12.006.</p> <p>Peacock, M., Steward, E. B., &amp; Belcourt, M. (2019). <i>Understanding Human Resources Management</i>. Nelson: Nelson College Indigenous.</p> <p>Ryan, L. (2010). <i>Corporate Education: A Practical Guide to Effective Corporate Learning</i>. Salisbury: Griffin Press.</p> <p>Osborne, B. (2020). 10 Benefits of Security Awareness Training [Online]. Available: <a href="https://resources.infosecinstitute.com/topic/10-benefits-of-security-awareness-training/">https://resources.infosecinstitute.com/topic/10-benefits-of-security-awareness-training/</a>.</p> <p>GDPR informer (2017). Data Protection Training: 10 Tips for Your Staff [Online]. Available: <a href="https://gdprinformer.com/gdpr-articles/data-protection-training-10-tips-staff">https://gdprinformer.com/gdpr-articles/data-protection-training-10-tips-staff</a>.</p>



## 2.7 MM7 – Saugumo testavimas

Mokymų modulis 7	Saugumo testavimas
<p><b>Bendras aprašymas/ siekiamas rezultatas</b></p>	<p>Antivirusinės programinę įrangos ir užkardos įdiegimas. Atnaujinimų atlikimas ir pagrindinių metodų pritaikymas, užtikrinant įmonėje naudojamos programinės įrangos saugumą ir atitinkamų dokumentų pateikimą.</p>
<p>Numeris</p>	<p>MM 7</p>
<p>Tipas</p>	<p>Privalomas – turi būti apibrėžtas</p>
<p>Apimtis</p>	<p>Valandos - turi būti apibrėžtos</p>
<p><b>Veiklos kompetencijos</b></p>	<p>Dalyviai supras esamos IKT infrastruktūros pažeidžiamumo, atsižvelgiant į technologijų plėtrą, patikrinimo svarbą. Išmoks naudotis (arba su išorės pagalba suprasti) įsiskverbimo testavimo priemonėmis, kad užtikrintų ugniasienių (firewalls) ir ryšių kanalų saugumą.</p> <p>Yra begalė būdų, kaip įsilaužti į programą. Ir saugumo testavimas pats savaime nėra vienintelis (ar geriausias) rodiklis, parodantis, kiek saugi yra programa. Tačiau labai rekomenduojama, kad saugumo testavimas būtų įtrauktas į standartinį programinės įrangos kūrimo procesą.</p>
<p><b>Mokymosi rezultatai</b></p>	<p><b>Techninė/ profesinė kompetencija</b></p> <p>Mokymų dalyviai <b>žinos</b>:</p> <ul style="list-style-type: none"> <li>- apie tinklo saugumą: tai reiškia, kad reikia ieškoti pažeidimų tinklo infrastruktūroje (ištekliuose ir politikoje).</li> <li>- apie sistemos programinės įrangos saugumą: tai apima įvairios programinės įrangos (operacinės sistemos, duomenų bazių sistemos ir kitos programinės įrangos), nuo kurios priklauso taikomoji programa, silpnųjų vietų vertinimą.</li> <li>- apie kliento programinės įrangos saugumą: tai susiję su kliento (naršyklės ar kitos panašios priemonės) apsaugos nuo manipuliacijų užtikrinimu.</li> <li>- apie serverio saugumą: Tai susiję su užtikrinimu, kad serverio kodas ir jo technologijos būtų pakankamai patikimos ir apsaugotų nuo bet kokio įsilaužimo.</li> </ul> <p>Mokymų dalyviai įgis <b>gebės</b>:</p> <ul style="list-style-type: none"> <li>- kurti testus, skirtus programinės įrangos saugumui nustatyti.</li> <li>- pritaikyti esamą sistemą.</li> <li>- prisijungti prie kompiuterių sistemos ar tinklo turint leidimą.</li> <li>- užtikrinti sistemas, kad nebūtų duomenų vagystės ar sunaikinimo.</li> <li>- atlikti didžiąją dalį nutraukimo veiklos gavus vadovo leidimą.</li> </ul> <p><b>Asmeninė kompetencija</b></p> <p>Mokymų dalyviai <b>gebės</b>:</p> <ul style="list-style-type: none"> <li>- pripažinti, kad procesų dokumentavimas yra atspirties taškas tolesniems darbo veiksmams.</li> <li>- dirbti struktūrotai, daugiausia dėmesio skiriant detalėms.</li> </ul>



	<ul style="list-style-type: none"><li>- pripažinti atsakomybę, susijusią su užduotimi, ir pasitikėti savimi bendraujant su kitais.</li></ul>
<b>Rekomendacijos mokymui ir mokymuisi</b>	Dauguma saugumo testavimo tipų apima sudėtingus veiksmus ir nestandartinį mąstymą, tačiau kartais reikia atlikti paprastus testus, kurie padeda atskleisti rimčiausius saugumo pavojus.
<b>Literatūra ir papildomi ištekliai mokymuisi</b>	<p>Dekkers, C., McCurley, J., &amp; Zubrow, D. (2013). Measures and Measurement for Secure Software Development. Pittsburgh: Carnegie Mellon University.</p> <p>Dowd, M., McDonald, J., &amp; Schuh, J. (2007). The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities. Boston: Addison-Wesley.</p>



## 2.8 MM8 – Kodavimas

Mokymų modulis 8	Kodavimas
<b>General Description / Output</b>	<b>Work on securitisation of mobile devices, communication channels and data storage units via passwords or other means of authentication.</b>
Code number	LU 8
Type	Mandatory – to be defined
Volume	Hours - to be defined
<b>Action Competences</b>	<p>The participants learn to understand the importance of password encoding for their vulnerability in the face of technological developments. They learn to use (or understand with an external support) password encoding tools to ensure the security of firewalls and communication channels.</p> <p>Password Encoding is the process in which a password is converted from a literal text format into a humanly unreadable sequence of characters. If done correctly, it is very difficult to revert back to the original password and so it helps secure user credentials and prevent unauthorized access to a website.</p>
<b>Learning Outcomes</b>	<p><b>Technical Competence</b></p> <p>The participants</p> <p><b>Know</b></p> <ul style="list-style-type: none"> <li>- about Literal Values: Passwords were stored in literal text format in databases without any encoding or hashing. As databases need authentication, which nobody except the admins and the application had, this was considered safe.</li> <li>- about Encryption: It is a safer alternative and the first step taken towards password security.</li> <li>- about Hashing: To combat these attacks, developers had to come up with a way to protect passwords in a database in such a way that they cannot be decrypted.</li> <li>- about Salting: To combat the appearance of rainbow tables, developers started adding a random sequence of characters to the beginnings of the hashed passwords.</li> <li>- about Password Encoders: It provides multiple password encoding implementations to choose from. Each have their advantages and disadvantages, and a developer can choose which one to use depending on the authentication requirement of their application.</li> </ul> <p><b>Can</b></p> <ul style="list-style-type: none"> <li>- educate the team on password encoding best practice.</li> <li>- educate the team on cyber security.</li> <li>- decide what password types not to use.</li> <li>- define the right way to generate encoding processes.</li> <li>- eliminate complex passwords.</li> </ul>



	<ul style="list-style-type: none"> <li>- strongly reduce the risk of copying a password.</li> <li>- ensure password auditing and accountability.</li> </ul> <p><b>Personal Competence</b></p> <p><b>The participants are able to</b></p> <ul style="list-style-type: none"> <li>- recognize the documentation of processes as a starting point for further working steps.</li> <li>- work in a structured way with a focus on details.</li> <li>- recognize the responsibility belonging to the task and be confident in the interaction with others.</li> <li>- manage the main requested tasks with a good level of autonomy.</li> <li>- emphasise their social competences (soft skills, empathy and communication in particular).</li> </ul>
<p><b>Recommendations for Learning &amp; Teaching</b></p>	<p>Most types of encoding processes involve complex steps and out-of-the-box thinking but, sometimes, it is simple tests like the one above that help expose the most severe encoding risks.</p>
<p><b>Literature &amp; Further Resources</b></p>	<p>Kaliski, B. (2000). Password-Based Cryptography Specification Version 2.0. RFC Editor, US. <a href="https://doi.org/10.17487/RFC2898">https://doi.org/10.17487/RFC2898</a>.</p> <p>Mourouzis, T., Pavlou, K. E., &amp; Kampakis, S. (2018). The Evolution of User-Selected Passwords: A Quantitative Analysis of Publicly Available Datasets. Computer Science. arXiv:1804.03946.</p> <p>Barbero, G., Trasselli, F. (2015). Manus OnLine and the Text Encoding Initiative Schema. Journal of the Text Encoding Initiative, (8), 1-16. doi: 10.4000/jtei.1054.</p>



## 2.9 MM9 - Duomenų valdymas

Mokymų modulis 9	Duomenų valdymas
<b>Bendras aprašymas / Rezultatai</b>	<b>Atlikti įprastines atsargines duomenų kopijas ir laikytis BDAR reikalavimų apdorojant duomenis įmonėje.</b>
Kodo numeris	MD 9
Tipas	Privaloma nurodyti
Apimtis	Nurodyti valandų skaičių
<b>Veiklos kompetencijos</b>	Dalyviai mokosi suprasti duomenų ir informacijos saugojimo bei apdorojimo pagal numatytas gaires svarbą. Jie išmoksta kaip tinkamai elgtis su duomenimis laikantis BDAR reikalavimų. Dalyviai gali įvertinti fizinių ir elektroninių duomenų saugojimą ir apdorojimą įmonėje bei nustatyti galimą netinkamą elgesį. Siekiant sušvelninti šią riziką dalyviai išmoks pasiūlyti pakeitimus įmonės procesuose.
<b>Mokymosi rezultatai</b>	<p><b>Techninės kompetencijos</b></p> <p>Dalyviai</p> <p><b>Žino</b></p> <ul style="list-style-type: none"> <li>- kaip apibrėžti sėkmingam procesui reikalingus informacijos poreikius: kokie duomenys yra tvarkomi organizacijoje ir kokie saugojimo būdai turėtų atitikti esamas taisykles.</li> <li>- taisykles, kaip nustatyti asmens duomenų saugojimo ir apdorojimo operacijų apimtį ir tikslą.</li> <li>- kaip organizuoti ir taikyti duomenų valdymą įmonėje: prisitaikyti prie pokyčių, taikyti analitinį mąstymą, kurti sprendimus; savarankiškai atlikti projekto valdymo užduotis.</li> <li>- įvairius būdus ir bendravimo stilius, siekiant gauti reikiamos informacijos apie saugojimą.</li> </ul> <p><b>Geba</b></p> <ul style="list-style-type: none"> <li>- nustatyti organizacijoje saugomų / tvarkomų asmens duomenų apimtį ir paskirtį.</li> <li>- reguliariai kurti atsargines duomenų kopijas siekiant sumažinti riziką prarasti vertingus duomenis ir informaciją.</li> <li>- dirbti grupėje, siekiant efektyvaus procesų pagerinimo.</li> <li>- siekiant konkretaus tikslo planuoti ir valdyti įvairius išteklius bei stebėti duomenų valdymo procesą.</li> </ul> <p><b>Asmeninės kompetencijos</b></p> <p><b>Dalyviai gali</b></p> <ul style="list-style-type: none"> <li>- dirbti struktūrizuotai, daug dėmesio skiriant detalėms.</li> <li>- atpažinti su užduotimis susijusias atsakomybes ir pasitikėti savimi bendraujant su kitais.</li> <li>- savarankiškai atlikti užduotis ir noriai mokytis.</li> </ul>



<b>Mokymosi ir mokymo rekomendacijos</b>	Susiekite teorines žinias su praktiniais pavyzdžiais. Taikykite interaktyvius mokymo metodus (pvz., grupinį darbą, diskusijas, atvejų analizę, vaidmenų modeliavimą ir t. t.)
<b>Literatūra ir kiti šaltiniai</b>	<p>Calabro, A., Daoudagh, S., &amp; Marchetti, E. (2020). Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. <i>Information Systems</i> (91) [Online]. Available: <a href="https://www.sciencedirect.com/science/article/pii/S0306437919305216">https://www.sciencedirect.com/science/article/pii/S0306437919305216</a>.</p> <p>Guide on Good Data Protection Practice in Research (2019) [Online]. Available: <a href="https://www.eui.eu/documents/servicesadmin/deanofstudies/researchethics/guide-data-protection-research.pdf">https://www.eui.eu/documents/servicesadmin/deanofstudies/researchethics/guide-data-protection-research.pdf</a>.</p> <p>EU-GDPR. (2019). EU GDPR portal. [Online]. Available: <a href="https://eugdpr.org">https://eugdpr.org</a>.</p> <p>General data protection regulation (2018). Official Journal of the European Union [Online]. Available: <a href="http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679">http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679</a>.</p>





## 2.10 MM10 - Vaidmenimis grįstos prieigos kontrolė

Mokymų modulis 10	Vaidmenimis grįstos prieigos kontrolė
<b>Bendras aprašymas / Rezultatai</b>	<b>Sukurti administratoriaus paskyras ir apriboti darbuotojų prieigos teises atsižvelgiant į nustatytus apsaugos lygius.</b>
Kodo numeris	MD 10
Tipas	Privaloma nurodyti
Apimtis	Nurodyti valandų skaičių
<b>Veiklos kompetencijos</b>	Dalyviai mokosi suprasti, kaip svarbu, esant galimybėms, apriboti prieigą prie duomenų, informacijos ar fizinės infrastruktūros ir suteikti prieigą tik tam tikrai darbuotojų grupei. Jie išmoksta kaip nustatyti tinkamus apribojimus atsižvelgiant į nustatytą saugumo lygį. Dalyviai gebės priskirti tinkamus vaidmenis įmonėje prie saugumo prieigos lygių ir prireikus sukurti prieigą prie konkrečios atsekamos informacijos.
<b>Mokymosi rezultatai</b>	<p><b>Techninė kompetencija</b></p> <p>Dalyviai</p> <p><b>Žino</b></p> <ul style="list-style-type: none"> <li>- kaip nustatyti organizacijoje atliekamas pagrindines su asmens duomenimis susijusias operacijas.</li> <li>- kaip nustatyti informacijos prieinamumą konkrečioms darbuotojų grupėms.</li> <li>- kaip, esant reikalui, nustatyti tinkamus apribojimus atsižvelgiant į apibrėžtus ir sulgytus saugumo lygius.</li> </ul> <p><b>Geba</b></p> <ul style="list-style-type: none"> <li>- išskirti atskirų darbuotojų ir grupių vaidmenis, siekiant nustatyti jų poreikius įvairiems saugumo lygiams (remiantis vadovybės patvirtintais priskirtais saugumo lygiais).</li> <li>- rasti tinkamus sprendimus atskiriems darbuotojams ar jų grupėms leidžiančius ar ribojančius tam tikrą prieigą ir geba juos pagrįsti.</li> <li>- valdyti individualias vartotojo teises priskiriant tinkamas roles vartotojo paskyrai, kai šios rolės yra apibrėžtos vadovybės.</li> </ul> <p><b>Asmeninės kompetencijos</b></p> <p>Dalyviai gali</p> <ul style="list-style-type: none"> <li>- savarankiškai paskirti atitinkamas roles pagal vadovybės reikalavimus (priskirtus saugumo lygius).</li> <li>- savarankiškai ir su pasitikėjimu bendrauti su kolegomis ir vadovybe.</li> </ul>



	<p>- Savarankiškai atpažinti atsakomybes susietas su užduotimi gerbiant kitų poreikius.</p>
<b>Mokymosi ir mokymo rekomendacijos</b>	<p>Sužinokite / mokykite apie tris pagrindines taisykles, apibrėžtas rolėmis grįstame prieigos valdyme (RBAC): 1) vaidmens priskyrimas, 2) vaidmens teisių suteikimas, 3) leidimo suteikimas. Pagalvokite apie jautrumo svarbą priskiriant vaidmenį ir tai aiškiai aptarkite su vadovybe.</p>
<b>Literatūra ir kiti šaltiniai</b>	<p>Blokdyk, G., (2017). Role-based Access Control: A Successful Design Process.</p> <p>D Ferraiolo, DR Kuhn, R Chandramouli, (2003), Role-based access control.</p> <p>Benantar, M., (2006)., Access Control Systems: Security, Identity Management and Trust Models. New York: Springer.</p> <p>Zhang, E. (2020). What is Role-Based Access Control (RBAC)? Examples, Benefits, and More [Online]. Available: <a href="https://digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more">https://digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more</a>.</p>



## 2.11 MM11 – Slaptažodžių valdymas

Mokymų modulis 11	Slaptažodžių valdymas
<b>Bendras aprašymas / Rezultatas</b>	<b>Sukurti atskirų darbuotojų prieigos slaptažodžius ir užtikrinti saugų saugojimo ir atkūrimo procesą.</b>
Kodo numeris	MD 11
Tipas	Privaloma nurodyti
Apimtis	Nurodyti valandų skaičių
<b>Veiklos kompetencijos</b>	Dalyviai mokosi suprasti kaip svarbu centralizuoti slaptažodžių naudojimo valdymą įmonėje. Jie sužinos, kaip nustatyti slaptažodžius, užtikrinančius autentifikavimą (tarp darbuotojų) ir kaip atstatyti slaptažodžius. Dalyviai mokosi struktūriškai kurti, naudoti / valdyti, saugoti ir pakeisti darbuotojų slaptažodžius.
<b>Mokymosi rezultatai</b>	<p><b>Techninės kompetencijos</b></p> <p>Dalyviai</p> <p><b>Žino</b></p> <ul style="list-style-type: none"> <li>- apie slaptažodžių saugojimą.</li> <li>- apie slaptažodžio perdavimą.</li> <li>- apie slaptažodžio spėjimą.</li> <li>- apie slaptažodžių atskleidimą.</li> <li>- apie slaptažodžio pakeitimą.</li> </ul> <p><b>Geba</b></p> <ul style="list-style-type: none"> <li>- supažinti komandą su geriausiomis slaptažodžių praktikomis.</li> <li>- supažindinti komandą su kibernetinio saugumo klausimais.</li> <li>- nuspręsti, kokių slaptažodžių tipų nenaudoti.</li> <li>- sukurti sudėtingus slaptažodžius.</li> <li>- panaudoti automatizavimo pajėgumus.</li> <li>- pašalinti sudėtingus slaptažodžius.</li> <li>- pašalinti slaptažodžio atkūrimo poreikį.</li> <li>- užtikrinti slaptažodžių auditą ir atskaitomybę.</li> </ul> <p><b>Asmeninės kompetencijos</b></p> <p><b>Dalyviai gali</b></p> <ul style="list-style-type: none"> <li>- atpažinti procesų dokumentaciją kaip atskaitos tašką tolesniems darbo etapams.</li> <li>- dirbti struktūrizuoti, daug dėmesio skiriant detalėms.</li> <li>- atpažinti su užduotimis susijusias atsakomybes ir pasitikėti savimi bendraujant su kitais.</li> <li>- savarankiškai vykdyti pagrindines prašomas užduotis.</li> <li>- pabrėžti savo socialines kompetencijas (ypač minkštus įgūdžius, empatiją ir bendravimą).</li> </ul>



<b>Mokymosi ir mokymo rekomendacijos</b>	Slaptažodžių valdymas naudojant realius pavyzdžius. Laisvos formos dokumentacijos pratimai su teksto modulių pagalba.
<b>Literatūra ir kiti šaltiniai</b>	Luca, M. (2008). Password Management for Distributed Environments. Saarbrücken: VDM Verlag Dr. Müller.  Smith, S. B. (2017). Password Manager: Keep Record of Internet User ID and Passwords in the Password Manage. Keep your internet login info in a safe offline location. CreateSpace: North Charleston.



## 2.12 MM12 - Verslo tęstinumo valdymas

Learning Unit 12	Business Continuity Management
<b>Bendras aprašymas / Rezultatas</b>	<b>Gairių ir procedūrų, dėl nenumatytų atvejų atsiradimo parengimas.</b>
Kodo numeris	MD 12
Tipas	Privaloma nurodyti
Apimtis	Nurodyti valandų skaičių
<b>Veiklos kompetencijos</b>	Dalyviai išmoks suprasti scenarijų „kas būtų, jei būtų“ svarbą. Jie mokosi analizuoti teorinius nenumatytus atvejus ir atsižvelgiant į tai parengti strategines gaires. Dalyviai galės nustatyti gaires ir iš anksto numatyti priemones, kad esant reikalui būtų pasirengę ir koordinuotai reaguotų į iškilusias naujas situacijas. -
<b>Mokymosi rezultatai</b>	<p><b>Techninės kompetencijos</b></p> <p>Dalyviai</p> <p><b>Žino</b></p> <ul style="list-style-type: none"> <li>- kaip rasti nacionalinius dokumentus ir kaip ieškoti informacijos nacionaliniuose teisiniuose dokumentuose, reglamentuojančiuose saugumą ir duomenų apsaugą.</li> <li>- simuliacijos metodus skirtus galimiems duomenų pažeidimams numatyti.</li> <li>- kaip elgtis su rizikos vertinimo taisyklėmis.</li> </ul> <p><b>Geba</b></p> <ul style="list-style-type: none"> <li>- nustatyti rizikas naudojant skirtingas technikas ir bendravimo stilius.</li> <li>- įgyvendinti rizikos vertinimo taisykles pritariant vadovybei.</li> <li>- planuoti ir kurti sprendimus, prisitaikant prie organizacijoje esančių aplinkybių ir pokyčių, ir juos įgyvendinti vadovybei pritarus.</li> <li>- rasti naujų sprendimų, pagrįstų ankstesnių įvykių analize.</li> </ul> <p><b>Asmeninės kompetencijos</b></p> <p><b>Dalyviai gali</b></p> <ul style="list-style-type: none"> <li>- dirbti nepalankiomis sąlygomis išlaikant dėmesį detalėms.</li> <li>- lengvai prisitaikyti prie naujų aplinkybių.</li> </ul>



	<ul style="list-style-type: none"><li>- būti pavyzdžiu kitiems darbuotojams laikantis jų etikos elgesio kodekso ir parodyti atsakomybę.</li></ul>
<b>Mokymosi ir mokymo rekomendacijos</b>	Teorinė skirtingų grėsmių ir rizikos situacijų scenarijų praktika. Darbas su realių situacijų pavyzdžiais.



## 2.13 MM13 – Mediacija ir suinteresuotųjų šalių valdymas

Mokymų modulis 13	Mediacija ir suinteresuotųjų šalių valdymas
<b>Bendras aprašymas / Rezultatas</b>	Įmonės vadovų ir darbuotojų poreikių koordinavimas, teikiant informaciją ir įžvalgą abiem šalims.
Kodo numeris	MD 13
Tipas	Privaloma nurodyti
Volume Apimtis	Nurodyti valandų skaičių
<b>Veiklos kompetencijos</b>	Dalyviai mokosi suprasti koordinavimo su visais įmonės suinteresuotais asmenimis svarbą atsižvelgiant į jų vaidmenį ir įtaką susijusių su duomenų apsauga ir informacijos saugumu. Jie išmoksta efektyviai bendrauti su skirtingais hierarchijos lygmenimis (darbuotojais ir vadovybe) ir pasikeitus organizacinei tvarkai pritaikyti prie jos savo poreikius bei interesus. Dalyviai gebės diplomatiškai bendrauti su suinteresuotosiomis šalimis ir susidoroti su galimu pasipriešinimu savo įtakai.
<b>Mokymosi rezultatai</b>	<p><b>Techninės kompetencijos</b></p> <p>Dalyviai</p> <p><b>Žino</b></p> <ul style="list-style-type: none"> <li>- kaip rasti nacionalinius teisinius dokumentus, reglamentuojančius informacijos saugumą ir duomenų apsaugą, ir kaip ieškoti informacijos.</li> <li>- kokie vidiniai ir išoriniai komunikacijos kanalai gali būti naudojami vadovybei pritarus, ir kokia yra su jais susijusi rizika.</li> <li>- kokios priemonės gali būti taikomos norint stebėti, išbandyti ir įvertinti procesus organizacijoje.</li> <li>- kokios priemonės gali būti taikomos rizikai įvertinti ir kaip elgtis vertinant riziką.</li> </ul> <p><b>Geba</b></p> <ul style="list-style-type: none"> <li>- įgyvendinti vidaus audito priemones (vadovybei pritarus).</li> <li>- planuoti ir plėtoti strateginius sprendimus bei juos įgyvendinti gavus vadovybės pritarimą.</li> <li>- vadovybei pritariant įdiegti prevencinę kultūrą.</li> <li>- nustatyti, įvertinti ir prioretizuoti rizikas.</li> <li>- sukurti vidaus taisykles visai organizacijai ir jas įgyvendinti (vadovybei patvirtinus).</li> </ul> <p><b>Asmeninės kompetencijos</b></p> <p>Dalyviai gali</p>



	<ul style="list-style-type: none"><li>- susidoroti su pokyčiais ir prisitaikyti.</li><li>- būti kūrybiški ir siekti tolesnio tobulėjimo.</li><li>- remtis savo etikos kodeksu, kad kiti galėtų vadovautis jų pavyzdžiu.</li><li>-</li></ul>
<b>Mokymosi ir mokymo rekomendacijos</b>	Susiekite teorines žinias su praktiniais pavyzdžiais. Taikykite interaktyvius mokymo metodus (pvz., darbas grupėse, diskusijos, atvejų analizė, vaidmenų modeliavimas ir t. t.)
<b>Literatūra ir kiti šaltiniai</b>	<p>IT Governance Privacy Team (2020). EU General Data Protection Regulation (GDPR) – An implementation and compliance guide (4th ed.).</p> <p>General data protection regulation (2021). Complete guide to GDPR compliance [Online]. Available: <a href="https://gdpr.eu/">https://gdpr.eu/</a>.</p> <p>Gorondutse, A. H., &amp; Hilman, H. (2016). Mediation effect of organizational culture on the relationship between perceived ethics and SMEs. Journal of Industrial Engineering and Management 2016, 9(2), 505-529.</p> <p>Straight, J. (2018). GDPR compliance: Identifying an organization's unique profile [Online]. Available: <a href="https://www.helpnetsecurity.com/2018/05/14/gdpr-compliance-profile/">https://www.helpnetsecurity.com/2018/05/14/gdpr-compliance-profile/</a></p>