



Curriculum – Polskie

Jednostki szkoleniowe w zakresie wiedzy, umiejętności i kompetencji dotyczących bezpieczeństwa informacji i ochrony danych w MŚP



Funded by the
Erasmus+ Programme
of the European Union





Funded by the
Erasmus+ Programme
of the European Union



Ten dokument jest udostępniony na licencji CC BY-SA 4.0.

Niniejszy dokument został opracowany w ramach projektu ERASMUS+ "Teilzertifizierung im Berufsfeld Informationssicherheit - TeBeiSi", ID projektu: 2018-1-EN02-KA202-005218

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiegokolwiek wykorzystanie informacji w niej zawartych.

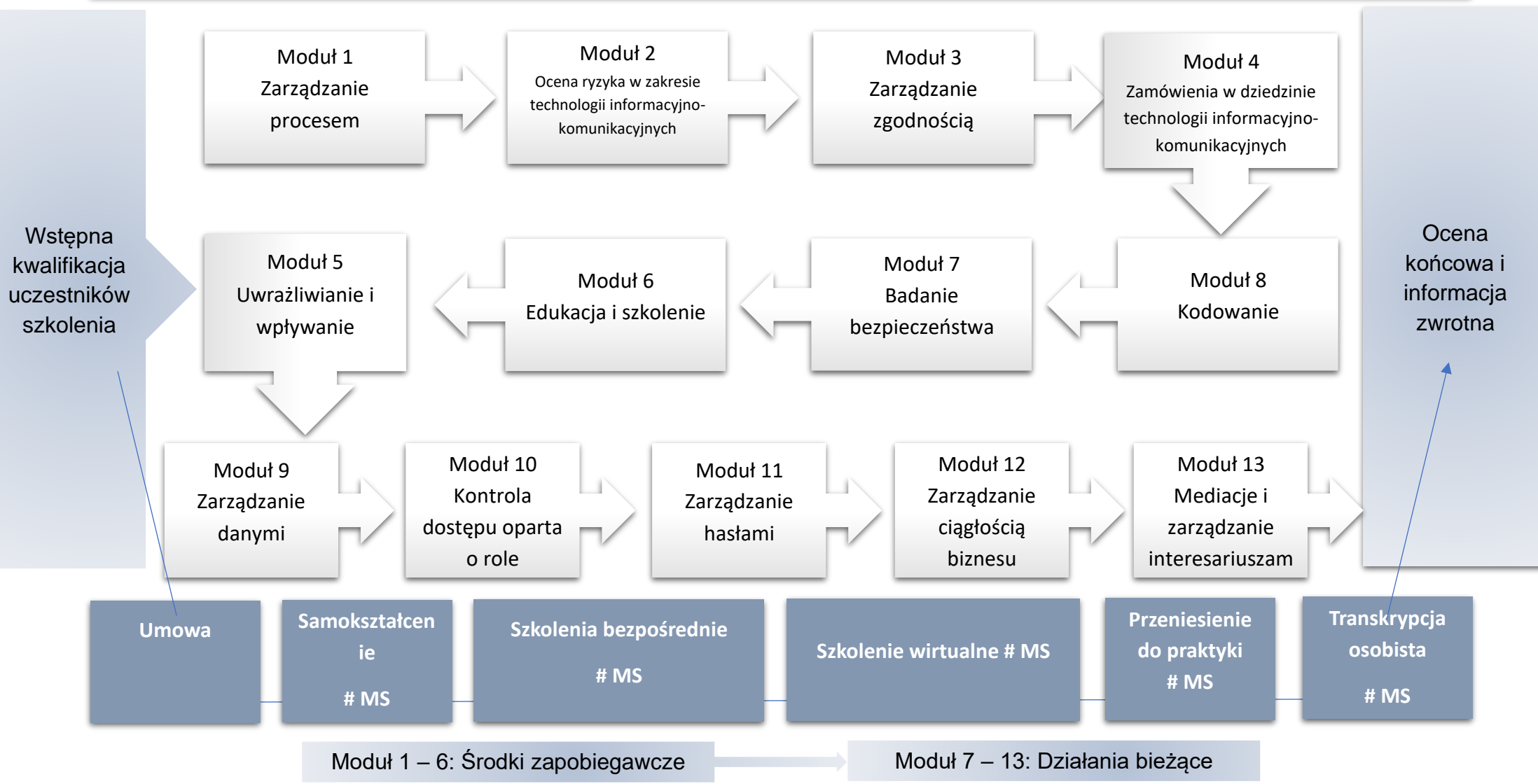


Content

| | | |
|------|--|----|
| 1.1 | Moduły szkoleniowe – przegląd i krótki opis | 5 |
| 2 | Szczegółowy opis modułów szkoleniowych (w oparciu o ECVET)..... | 6 |
| 2.1 | LU1 – Zarządzanie procesem | 6 |
| 2.2 | LU2 – Ocena ryzyka w zakresie technologii informacyjno-komunikacyjnych | 8 |
| 2.3 | LU3 – Zarządzanie zgodnością | 10 |
| 2.4 | LU4 – Zamówienia w dziedzinie technologii informacyjno-komunikacyjnych | 13 |
| 2.5 | LU5 – Uwrażliwianie i wpływanie | 15 |
| 2.6 | LU6 – Edukacja i szkolenie | 17 |
| 2.7 | LU7 – Badanie bezpieczeństwa | 19 |
| 2.8 | LU8 – Kodowanie | 21 |
| 2.9 | LU9 – Zarządzanie danymi..... | 23 |
| 2.10 | LU10 – Kontrola dostępu oparta o role | 25 |
| 2.11 | LU11 – Zarządzanie hasłami | 27 |
| 2.12 | LU12 – Zarządzanie ciągłością biznesu | 29 |
| 2.13 | LU13 – Mediacje i zarządzanie interesariuszami | 31 |



Program szkolenia TeBeISi (w oparciu o kryteria ECVET)





1.1 Moduły szkoleniowe – przegląd i krótki opis

| # | Moduły szkoleniowe | Krótki opis |
|------|---|---|
| MS1 | Zarządzanie procesem | Analiza procesów biznesowych i opracowanie raportu strategicznego dotyczącego ochrony danych i bezpieczeństwa informacji. |
| MS2 | Ocena ryzyka w zakresie technologii informacyjno-komunikacyjnych | Śledzenie zmian w firmie i poza nią, które mają wpływ na strategię bezpieczeństwa firmy i tworzenie raportów dla podwładnych. |
| MS3 | Zarządzanie zgodnością | Opracowanie wytycznych firmowych dotyczących postępowania z określonymi informacjami i danymi. |
| MS4 | Zamówienia w dziedzinie technologii informacyjno-komunikacyjnych | Przygotowywanie rekomendacji dotyczących produktów, które należy nabyć z uwzględnieniem wymogów bezpieczeństwa informacji i ochrony danych firmy. |
| MS5 | Uwrażliwianie i wpływanie | Prowadzenie działań (informacyjnych) mających na celu uwrażliwienie pracowników na zagrożenia bezpieczeństwa w ich rutynowej pracy oraz szerzenie świadomości wśród pracowników. |
| MS6 | Edukacja i szkolenie | Tworzenie planów szkoleniowych dla firmy, aby móc regularnie szkolić pracowników w zakresie bezpieczeństwa informacji i ochrony danych. |
| MS7 | Badanie bezpieczeństwa | Instalowanie zapory sieciowej i oprogramowania antywirusowego. Przeprowadzanie aktualizacji i stosowanie podstawowych metod testowania bezpieczeństwa oprogramowania wykorzystywanego w firmie oraz sporządzanie odpowiedniej dokumentacji. |
| MS8 | Kodowanie | Zabezpieczanie urządzeń mobilnych, kanałów komunikacyjnych i nośników danych za pomocą haseł lub innych środków uwierzytelniania. |
| MS9 | Zarządzanie danymi | Wykonywanie rutynowych kopii zapasowych danych i stosowanie metod właściwego postępowania zgodnych z RODO w odniesieniu do przetwarzania danych w firmie. |
| MS10 | Kontrola dostępu oparta o role | Utworzenie kont administratorów i ograniczenie praw dostępu dla pracowników zgodnie ze zdefiniowanymi poziomami bezpieczeństwa. |
| MS11 | Zarządzanie hasłami | Ustanowienie haseł dostępu dla poszczególnych pracowników oraz umożliwienie bezpiecznego przechowywania i procesu odzyskiwania danych. |
| MS12 | Zarządzanie ciągłością biznesu | Ustanowienie wytycznych i procedur na wypadek pojawienia się możliwych sytuacji awaryjnych. |
| MS13 | Mediacje i zarządzanie interesariuszami | Koordynowanie potrzeb kadry zarządzającej i pracowników firmy, dostarczanie obu stronom informacji i spostrzeżeń pochodzących z wewnątrz firmy. |



2 Szczegółowy opis modułów szkoleniowych (w oparciu o ECVET)

2.1 LU1 – Zarządzanie procesem

| Moduł 1 | Zarządzanie procesem |
|---------------------------------------|---|
| Opis ogólny / Rezultat | Analiza procesów biznesowych i tworzenie raportów strategicznych dotyczących ochrony danych i bezpieczeństwa informacji. |
| Numer kodu | LU 1 |
| Rodzaj | Obowiązkowe - należy określić |
| Ilość | Godziny - do ustalenia |
| Kompetencje w zakresie działań | Uczestnicy uczą się rozumieć znaczenie ustrukturyzowanej analizy procesów w firmie. Są w stanie rozpoznać procesy, które wymagają dalszej analizy ze względu na narażenie danych i bezpieczeństwa informacji. Uczestnicy zapoznają się z dokumentacją procesów i są w stanie monitorować zmiany w rutynie pracy. Potrafią przygotować dokumentację, która pozwala na sformułowanie rekomendacji działań. |
| Efekty kształcenia | Kompetencje techniczne Uczestnicy Wiedzę <ul style="list-style-type: none">- jak stosować wytyczne RODO i dobre praktyki w zakresie bezpieczeństwa informacji.- jak identyfikować, dokumentować, projektować, wdrażać, zarządzać i optymalizować procesy biznesowe.- jak strategicznie planować dokumentację procesów.- jakie są techniki i kanały komunikacji. Są w stanie <ul style="list-style-type: none">- wdrażać dokumentację za pomocą systemów EDP (Electronic Data Processing).- streszczać oryginalne informacje bez utraty pierwotnego przekazu.- efektywnie komunikować się ze współpracownikami w celu dostosowania przepływu pracy.- odpowiednio reagować na wypowiedzi innych, np. przyjmować konstruktywną krytykę i aktywnie słuchać, aby znaleźć najlepsze rozwiązania.- znajdować odpowiednie informacje prawne i techniczne oraz odpowiednie zalecenia dotyczące działania z zaufanych źródeł. Kompetencje osobiste Uczestnicy są w stanie |



| | |
|--|--|
| | <ul style="list-style-type: none">- samodzielnie organizować proces tworzenia dokumentacji, pracując w sposób uporządkowany i skupiając się na szczegółach.- samodzielnie komunikować się ze współpracownikami i być pewnym siebie w interakcjach z nimi.- rozpoznawać odpowiedzialność związaną z zadaniem i być pewnym siebie w interakcji z innymi. |
| Zalecenia dotyczące uczenia się i nauczania | Dokumentacja procesów z wykorzystaniem autentycznych przykładów. Ćwiczenia na dokumentację w systemie EDP (Electronic Data Processing) w formie swobodnej i za pomocą modułów tekstowych. |
| Literatura i inne zasoby | <p>Nguyen, B. T., Lee, G. M., Sun, K., & 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: https://eugdpr.org.</p> <p>General data protection regulation (2018). Official Journal of the European Union [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/uri=CELEX:32016R0679.</p> <p>Gellert, R. (2015). Understanding data protection as risk regulation. <i>Journal of Internet Law</i>, 18 (11), 3-15.</p> |
| | |



2.2 LU2 – Ocena ryzyka w zakresie technologii informacyjno-komunikacyjnych

| Moduł 2 | Ocena ryzyka w zakresie technologii informacyjno - komunikacyjnych |
|---------------------------------------|---|
| Opis ogólny / Rezultat | Śledzenie zmian w firmie i poza nią, które mogą mieć wpływ na strategię bezpieczeństwa firmy i tworzenie raportów dla pracowników. |
| Numer kodu | LU 2 |
| Rodzaj | Obowiązkowe - należy określić |
| Ilość | Godziny - do ustalenia |
| Kompetencje w zakresie działań | Uczestnicy uczyć się rozumieć dynamikę zmian technologicznych i ich wpływu na strategię firmy w zakresie ograniczania ryzyka. Są w stanie decydować o konieczności reagowania na te ryzyka. Uczestnicy będą w stanie śledzić rozwój technologiczny wewnątrz i na zewnątrz firmy oraz dokonywać oceny narażenia firmy na ryzyko. |
| Efekty kształcenia | Kompetencje techniczne Uczestnicy Wiedzę <ul style="list-style-type: none">- o ocenie narażenia firmy na ryzyko i adekwatności obecnych środków do sprostania związanemu z tym ryzyku.- jak monitorować rozwój technologiczny w firmie i poza nią, a także zmiany w zespole pracowników.- jak określić ilość i cel przetwarzanych danych osobowych. Są w stanie <ul style="list-style-type: none">- znajdować informacje o rozwoju technologicznym, wykorzystując odpowiednie źródła wiadomości oraz informacje od publicznych lub prywatnych instytucji z danej dziedziny.- wykrywać zagrożenia pomimo teoretycznej niechęci pracowników do ponownego ujawniania błędów lub słabości.- przedstawiać zalecenia dotyczące działań w oparciu o uzyskane informacje.- oceniać i ograniczać ryzyko związane z ochroną danych.- identyfikować operacje przechowywania/przetwarzania danych osobowych w organizacjach i oceniać ich kontekst.- podejmować działania związane z celami ustalonymi na poziomie strategii, aby zmobilizować zasoby i pracowników w celu wzmocnienia współpracy. Kompetencje osobiste Uczestnicy są w stanie <ul style="list-style-type: none">- wykazać się wytrwałością w obliczu braku chęci współpracy ze strony współpracowników. |



| | |
|--|---|
| | <ul style="list-style-type: none">- zachować elastyczność, aby znaleźć rozwiązania i stworzyć sprzyjające środowisko.- Wykonywać zadania w sposób strategiczny i zorganizowany. |
| Zalecenia dotyczące uczenia się i nauczania | Dokumentacja procesów z pomocą rzeczywistych przykładów. Ćwiczenia na dokumentację w systemie EDP (Electronic Data Processing) w formie swobodnej i za pomocą modułów tekstowych. |
| Literatura i inne zasoby | <p>European Banking Authority (2019). Final Report: EBA Guidelines on ICT and security risk management [Online]. Available: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020.</p> <p>NZ Digital Government (2021). ICT Risk Management Guidance [Online]. Available: www.digital.govt.nz/dmsdocument/130-ict-risk-management-guidance/html.</p> <p>Commission de Surveillance du Secteur Financier (CSSF) (2020). ICT Risk [Online]. Available: www.cssf.lu/en/ict-risk/.</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 LU3 – Zarządzanie zgodnością

| Moduł 3 | Zarządzanie zgodnością |
|---------------------------------------|---|
| Opis ogólny / Rezultat | Tworzenie wytycznych firmowych dotyczących postępowania z konkretnymi informacjami i danymi. |
| Numer kodu | LU 3 |
| Rodzaj | Obowiązkowe - należy określić |
| Ilość | Godziny - do ustalenia |
| Kompetencje w zakresie działań | Uczestnicy uczą się rozumieć znaczenie kodyfikacji wytycznych dotyczących zachowań w firmie w celu ustalenia właściwego postępowania z danymi i informacjami. Uczą się, jak ustalać wytyczne, które zapewniają zgodność wśród pracowników. Rozumieją znaczenie przygotowania się na przewidywane i nieprzewidziane sytuacje awaryjne oraz ustalenia ogólnofirmowych zasad zachowania się i działań, które należy podjąć w sytuacjach krytycznych. |
| Efekty kształcenia | Kompetencje techniczne Uczestnicy Wiedzę <ul style="list-style-type: none">- o obszarze regulacji GDPR i krajowych dokumentów prawnych, regulujących bezpieczeństwo informacji i ochronę danych.- o architekturze informacji i kanałach komunikacji wewnętrznej organizacji- jak analizować, mapować i dokumentować procesy, które mogą powodować potencjalny konflikt z polityką zgodności.- jak przygotować wytyczne polityki zgodności.- jak gromadzić, zarządzać i oceniać techniki przetwarzania danych.- jak myśleć analitycznie w procesie kondensacji informacji, opracowywania rozwiązań i podejmowania decyzji związanych z zarządzaniem zgodnością. Są w stanie <ul style="list-style-type: none">- wdrożyć procedury opisane w dokumentach prawnych.- zidentyfikować krytyczne dane i jednostki informacji, które wymagają szczególnej ochrony lub szczególnego traktowania.- analizować i mapować procesy związane z przepływem informacji w organizacji.- rozpoznawać potencjalne ryzyka i zagrożenia dla bezpieczeństwa informacji i ochrony danych w procesach wewnętrznych organizacji.- opracowywać rozwiązania związane z zarządzaniem zgodnością dla problemów praktycznych, operacyjnych lub koncepcyjnych w szerokim zakresie codziennej pracy.- rozumieć cel wytycznych polityki zgodności i aktualizować je w sytuacjach awaryjnych. |



| | |
|--|---|
| | <ul style="list-style-type: none">- stosować umiejętności analitycznego i krytycznego myślenia w identyfikowaniu mocnych i słabych stron potencjalnych rozwiązań problemów związanych z zarządzaniem zgodnością.- podsumowywać informacje w wygodny i sensowny sposób. <p>Kompetencje osobiste</p> <p>Uczestnicy są w stanie</p> <ul style="list-style-type: none">- pracować w sposób uporządkowany, skupiając się na szczegółach.- rozpoznawać odpowiedzialność związaną z zadaniami i być pewnym siebie w kontaktach z innymi.- samodzielnie radzić sobie z zadaniami i wykazywać chęć do nauki.- |
| Zalecenia dotyczące uczenia się i nauczania | Dokumentacja procesów z wykorzystaniem rzeczywistych przykładów. Ćwiczenia na dokumentację w systemie EDP (Electronic Data Processing) w formie swobodnej i za pomocą modułów tekstowych. |
| Literatura i inne zasoby | <p>Agostinelli S., Maggi F.M., Marrella A., & 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. https://doi.org/10.1007/978-3-030-21297-1_2</p> <p>Basin, D., Debois, S., & Hildebrandt, T. (2018). On purpose and by necessity: compliance under the GDPR. In Proceedings Financial Cryptography and Data Security, 18 [Online]. Available: https://pure.itu.dk/ws/files/84212312/On_Purpose_and_ny_Necessity.pdf</p> <p>Besik, S. I., & 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., & 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: https://eugdpr.org.</p> <p>Kammüller, F., Ogunyanwo, O.O., & 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., & 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., & Wißotzki, M. (2020). Enterprise Architecture Frameworks as Support for Implementation of Regulations: Approach and Experiences from GDPR. <i>Complex Systems Informatics and Modeling Quarterly</i>, (24), 31-48.</p> |
| | |



2.4 LU4 – Zamówienia w dziedzinie technologii informacyjno-komunikacyjnych

| Moduł 4 | Zamówienia w dziedzinie technologii informacyjno - komunikacyjnych |
|---------------------------------------|--|
| Opis ogólny / Rezultat | Przygotowywanie rekomendacji dotyczących zamówień z uwzględnieniem wymogów bezpieczeństwa informacji i ochrony danych firmy. |
| Numer kodu | LU 4 |
| Rodzaj | Obowiązkowe - należy określić |
| Ilość | Godziny - do ustalenia |
| Kompetencje w zakresie działań | Uczestnicy uczą się rozumieć znaczenie zamówień publicznych dla wspierania wdrażania bezpieczeństwa informacji i ochrony danych. Uczą się, jak pozycjonować własne kompetencje w procesie zaopatrzenia firmy. Uczestnicy są w stanie wywierać wpływ na zakup nowych technologii i maszyn oraz oceniać ich adekwatność i użyteczność w odniesieniu do wytycznych firmy w zakresie ochrony danych i bezpieczeństwa informacji. |
| Efekty kształcenia | Kompetencje techniczne Uczestnicy Wiedzę <ul style="list-style-type: none">- o wymaganiach firmy dotyczących bezpieczeństwa i specyfikacji nowego sprzętu.- o specyfikacjach istniejącego sprzętu i pilnej potrzebie ich zmiany przy użyciu nowej technologii.- o oszustwach dostawców usług i sprzętu w odniesieniu do naruszeń RODO. Są w stanie <ul style="list-style-type: none">- skutecznie komunikować się z innymi.- przygotować i przedstawić krótką prezentację (raport/ procedura/ proces/ strategia) poświęconą ocenie technologii lub maszyn, które muszą zostać zakupione.- przekazać informacje od różnych pracowników/ działów na temat ich potrzeb, a następnie wydać rekomendację dotyczącą zakupu.- zebrać wyczerpujące informacje na temat zakupionej technologii/maszyny.- znaleźć odpowiednie informacje prawne i techniczne oraz podjąć decyzje na podstawie tych informacji.- podejmować działania w zakresie celów i procedur określonych na poziomie strategicznym w celu mobilizacji zasobów i realizacji ustalonych strategii.- planować i zarządzać zasobami w ramach ograniczeń budżetowych i czasowych oraz osiągać wyznaczone cele, korzystając z monitorowania postępów projektu i kontroli jakości. |



| | |
|--|---|
| | <p>Kompetencje osobiste</p> <p>Uczestnicy są w stanie</p> <ul style="list-style-type: none">- poznać istniejące na rynku rozwiązanie problemu firmy.- poświęcić uwagę szczegółom (prawnym i technicznym).- wykazać się pewnością siebie i odpowiedzialnością w komunikacji z interesariuszami. |
| Zalecenia dotyczące uczenia się i nauczania | <p>Dokumentacja procesów z wykorzystaniem rzeczywistych przykładów. Ćwiczenia z dokumentacji w systemie EDP (Electronic Data Processing) w formie swobodnej i za pomocą modułów tekstowych.</p> |
| Literatura i inne zasoby | <p>Australian Government: Digital Transformation Agency (2021). ICT procurement [Online]. Available: www.dta.gov.au/help-and-advice/ict-procurement.</p> <p>Moses, M. (2019). Procurement Process and ICT. Zerite Network [Online]. Available: http://zeritenetwork.com/procurement-process-and-ict/.</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: ec.europa.eu/digital-single-market/en/news/.</p> <p>Dovgalenko, S. (2020). The Technology Procurement Handbook: A Practical Guide to Digital Buying. London: Kogan Page.</p> |



2.5 LU5 – Uwrażliwianie i wpływanie

| Moduł 5 | Uwrażliwianie i wpływanie |
|--------------------------------|---|
| Opis ogólny / Rezultat | Prowadzenie działań (informacyjnych) mających na celu uwrażliwienie pracowników na zagrożenia bezpieczeństwa w ich rutynowej pracy oraz szerzenie świadomości wśród pracowników. |
| Numer kodu | LU 5 |
| Rodzaj | Obowiązkowe - należy określić |
| Ilość | Godziny - do ustalenia |
| Kompetencje w zakresie działań | Uczestnicy poznają znaczenie uwrażliwiania pracowników i członków zarządu na kwestie związane z ochroną danych i bezpieczeństwem informacji. Nauczą się podnosić świadomość w zakresie typowych zagrożeń i budować wśród pracowników zdolność do wykrywania prawdopodobnych zagrożeń w ich codziennej pracy. Uczestnicy będą w stanie przeprowadzić analizę poziomu świadomości w firmie i wdrożyć odpowiednie środki zwiększające świadomość. |
| Efekty kształcenia | Kompetencje techniczne Uczestnicy Wiedzę <ul style="list-style-type: none">- o podstawowych wytycznych RODO.- jak radzić sobie z potencjalnymi procesami i personelem narażonym na ataki lub utratę wrażliwych informacji i danych.- w jaki sposób można wdrożyć środki audytu.- o technikach i kanałach komunikacji.- jak wdrażać strategię zmian. Są w stanie <ul style="list-style-type: none">- znaleźć odpowiednie źródło wiedzy prawnej.- współpracować z innymi w szerokim tego słowa znaczeniu w celu określenia potrzeby zmian, inspirowania i instruowania oraz pomocy w ich wprowadzaniu.- skutecznie komunikować się z innymi, wybierając nie tylko rodzaj komunikatu, ale także jego zakres i znaczenie w zależności od okoliczności. Kompetencje osobiste Uczestnicy są w stanie <ul style="list-style-type: none">- adaptować się do zmieniających się warunków i okoliczności, pracując w sposób zorganizowany i zachowując dystans, który pozwala na właściwą samoocenę.- być przykładem dla innych pracowników poprzez przestrzeganie kodeksu etycznego postępowania i wykazywanie się odpowiedzialnością. |



| | |
|--|---|
| | |
| Zalecenia dotyczące uczenia się i nauczania | <p>Połączenie wiedzy teoretycznej i podejścia z praktycznymi przykładami, takimi jak środki ostrożności i sposoby inscenizacji zdarzeń, np:</p> <ul style="list-style-type: none">- Falszywe USB- Przypadki inżynierii ludzkiej- Wysyłanie fałszywych e-maili <p>Stosowanie interaktywnych metod nauczania (np. praca w grupach, dyskusje, analiza przypadków, odgrywanie ról w symulacjach, itp.)</p> |
| Literatura i inne zasoby | <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 & Assurance (14th ed.). Plymouth: Centre for Security, Communication & Network Research.</p> <p>i-scoop (o.J.). GDPR awareness: a matter of people, culture, leadership and acting now [Online]. Available: https://www.i-scoop.eu/gdpr/gdpr-awareness/.</p> <p>Kefron - The Information Management People (o.J.). Why Maximizing Staff Awareness Is The Key To A Smooth GDPR Transition [Online]. Available: https://www.kefron.com/blog/why-maximizing-staff-awareness-is-the-key-to-a-smooth-gdpr-transition/.</p> <p>European Union Agency for Cybersecurity (2017). Handbook on Security of Personal Data Processing [Online]. Available: www.enisa.europa.eu</p> <p>General Data Protection Regulation (2021). Complete guide to GDPR compliance [Online]. Available: https://gdpr.eu/</p> |



2.6 LU6 – Edukacja i szkolenie

| Moduł 6 | Edukacja i szkolenie |
|--------------------------------|--|
| Opis ogólny / Rezultat | Tworzenie planów szkoleniowych dla firmy, aby móc regularnie szkolić pracowników w zakresie bezpieczeństwa informacji i ochrony danych. |
| Numer kodu | LU 6 |
| Rodzaj | Obowiązkowe - należy określić |
| Ilość | Godziny - do ustalenia |
| Kompetencje w zakresie działań | Uczestnicy uczą się rozumieć znaczenie edukacji w zakresie ochrony danych i wymogów bezpieczeństwa informacji. Nauczą się edukować zarówno siebie, jak i pracowników firmy. Uczestnicy będą potrafili korzystać z wiarygodnych źródeł i określać potrzeby szkoleniowe na podstawie konsultacji lub interakcji z pracownikami. Uczestnicy nauczą się przygotowywać materiały szkoleniowe i szkolić pracowników w zakresie włączania odpowiednich procedur roboczych do ich codziennej pracy. |
| Efekty kształcenia | Kompetencje techniczne Uczestnicy Wiedzę <ul style="list-style-type: none">- gdzie znaleźć krajowe dokumenty prawne regulujące bezpieczeństwo informacji i ochronę danych (podstawy RODO).- jak przygotować materiały szkoleniowe i jak przeprowadzić szkolenie, aby wdrożyć odpowiednie procedury pracy.- jak udzielać mentoringu poszczególnym pracownikom. Są w stanie <ul style="list-style-type: none">- przedstawić pracownikom, jak praktycznie stosować krajowe dokumenty prawne w zakresie bezpieczeństwa informacji i ochrony danych zgodnie z wytycznymi RODO.- przekonać pracowników o znaczeniu ciągłego szkolenia w obu obszarach poprzez aktywne podnoszenie świadomości.- wspierać i doradzać poszczególnym pracownikom w zakresie zidentyfikowanych potrzeb szkoleniowych.- opracowywać rozwiązania praktycznych, operacyjnych lub koncepcyjnych problemów, które pojawiają się w trakcie wykonywania pracy w różnych kontekstach. Kompetencje osobiste Uczestnicy są w stanie <ul style="list-style-type: none">- samodzielnie organizować szkolenia w firmie w sposób ustrukturyzowany, koncentrując się na aktualnych potrzebach. |



| | |
|--|---|
| | <ul style="list-style-type: none">- samodzielnie komunikować się ze współpracownikami i kierownictwem, będąc pewnym siebie w interakcjach.- dostrzegać odpowiedzialność związaną z zadaniem i motywować pracowników do nauki. |
| Zalecenia dotyczące uczenia się i nauczania | Rejestrowanie trudności związanych z bezpieczeństwem informacji i ochroną danych napotykanymi w codziennej pracy w celu zaplanowania i wdrożenia odpowiednich działań szkoleniowych. |
| Literatura i inne zasoby | <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 & Security</i>, (49), 162–176. doi: 10.1016/j.cose.2014.12.006.</p> <p>Peacock, M., Steward, E. B., & Belcourt, M. (2019). Understanding Human Resources Management. Nelson: Nelson College Indigenous.</p> <p>Ryan, L. (2010). Corporate Education: A Practical Guide to Effective Corporate Learning. Salisbury: Griffin Press.</p> <p>Osborne, B. (2020). 10 Benefits of Security Awareness Training [Online]. Available: https://resources.infosecinstitute.com/topic/10-benefits-of-security-awareness-training/.</p> <p>GDPR informer (2017). Data Protection Training: 10 Tips for Your Staff [Online]. Available: https://gdprinformer.com/gdpr-articles/data-protection-training-10-tips-staff.</p> |



2.7 LU7 – Badanie bezpieczeństwa

| Moduł 7 | Badanie bezpieczeństwa |
|--------------------------------|---|
| Opis ogólny / Rezultat | Instalowanie zapory sieciowej i oprogramowania antywirusowego. Przeprowadzanie aktualizacji i stosowanie podstawowych metod testowania bezpieczeństwa oprogramowania wykorzystywanego w firmie oraz sporządzanie odpowiedniej dokumentacji. |
| Numer kodu | LU 7 |
| Rodzaj | Obowiązkowe - należy określić |
| Ilość | Godziny - do ustalenia |
| Kompetencje w zakresie działań | <p>Uczestnicy uczą się rozumieć znaczenie testowania istniejącej infrastruktury ICT pod kątem jej podatności na zmiany technologiczne. Uczą się używać (lub rozumieć przy wsparciu zewnętrznym) narzędzi do testów penetracyjnych w celu zapewnienia bezpieczeństwa firewalle i kanałów komunikacyjnych.</p> <p>Istnieje nieskończona liczba sposobów na złamanie aplikacji. I, testy bezpieczeństwa, same w sobie, nie są jedyną (lub najlepszą) miarą tego, jak bezpieczna jest aplikacja. Ale jest wysoce zalecane, aby testy bezpieczeństwa były włączone jako część standardowego procesu rozwoju oprogramowania.</p> |
| Efekty kształcenia | <p>Kompetencje techniczne</p> <p>Uczestnicy</p> <p>Wiedzę</p> <ul style="list-style-type: none"> - o bezpieczeństwie sieci: obejmuje ono poszukiwanie słabych punktów w infrastrukturze sieciowej (zasobach i politykach). - o bezpieczeństwie oprogramowania systemowego: obejmuje ono ocenę słabych punktów w różnych programach (system operacyjny, system baz danych i inne oprogramowanie), od których zależy aplikacja. - o bezpieczeństwie aplikacji po stronie klienta: dotyczy zapewnienia, że klient (przeglądarka lub inne podobne narzędzie) nie może być manipulowany. - o bezpieczeństwie aplikacji po stronie serwera: obejmuje ono upewnienie się, że kod serwera i jego technologie są wystarczająco odporne, aby odeprzeć wszelkie włamania. <p>Są w stanie</p> <ul style="list-style-type: none"> - tworzyć testy w celu określenia bezpieczeństwa produktu oprogramowania. - dostosować istniejący szablon. - uzyskać dostęp do systemu komputerowego lub sieci z autoryzacją. - zabezpieczyć systemy przed kradzieżą lub zniszczeniem danych. - wykonywać większość czynności związanych z łamaniem zabezpieczeń za zgodą właściciela. |



| | |
|--|---|
| | <p>Kompetencje osobiste</p> <p>Uczestnicy są w stanie</p> <ul style="list-style-type: none">- uznać dokumentację procesów jako punkt wyjścia do dalszych kroków roboczych.- pracować w sposób uporządkowany, skupiając się na szczegółach.- rozpoznawać odpowiedzialność związaną z zadaniem i być pewnym siebie w interakcji z innymi. |
| Zalecenia dotyczące uczenia się i nauczania | <p>Większość rodzajów testów bezpieczeństwa wymaga złożonych kroków i nieszablonowego myślenia, ale czasami chodzi o proste testy, które pomagają ujawnić najpoważniejsze zagrożenia bezpieczeństwa.</p> |
| Literatura i inne zasoby | <p>Dekkers, C., McCurley, J., & Zubrow, D. (2013). Measures and Measurement for Secure Software Development. Pittsburgh: Carnegie Mellon University.</p> <p>Dowd, M., McDonald, J., & Schuh, J. (2007). The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities. Boston: Addison-Wesley.</p> |



2.8 LU8 – Kodowanie

| Moduł 8 | Kodowanie |
|---------------------------------------|--|
| Opis ogólny / Rezultat | Prace nad zabezpieczeniem urządzeń przenośnych, kanałów komunikacyjnych i jednostek przechowywania danych za pomocą haseł lub innych środków uwierzytelniania. |
| Numer kodu | LU 8 |
| Rodzaj | Obowiązkowe - należy określić |
| Ilość | Godziny - do ustalenia |
| Kompetencje w zakresie działań | <p>Uczestnicy uczą się rozumieć znaczenie kodowania haseł dla ich podatności na zagrożenia w obliczu rozwoju technologicznego. Uczą się używać (lub rozumieć przy wsparciu zewnętrznym) narzędzi do kodowania haseł w celu zapewnienia bezpieczeństwa firewalli i kanałów komunikacyjnych.</p> <p>Kodowanie haseł to proces, w którym hasło jest przekształcane z dosłownego formatu tekstowego w ciąg znaków nieczytelny dla człowieka. Jeśli jest to zrobione poprawnie, bardzo trudno jest powrócić do oryginalnego hasła, dlatego pomaga zabezpieczyć dane użytkownika i zapobiec nieautoryzowanemu dostępowi do strony internetowej.</p> |
| Efekty kształcenia | <p>Kompetencje techniczne</p> <p>Uczestnicy</p> <p>Wiedzę</p> <ul style="list-style-type: none"> - o wartościach dosłownych: hasła były przechowywane w literalnym formacie tekstowym w bazach danych bez żadnego kodowania czy haszowania. Ponieważ bazy danych wymagają uwierzytelnienia, którego nikt poza administratorami i aplikacją nie posiadał, uznano to za bezpieczne. - o szyfrowaniu: jest to bezpieczniejsza alternatywa i pierwszy krok podjęty w kierunku bezpieczeństwa haseł. - o hashingu: aby zwalczyć te ataki, programiści musieli wymyślić sposób ochrony haseł w bazie danych w taki sposób, aby nie można było ich odszyfrować. - o saltingu: aby zwalczyć pojawianie się tęczy tablic (technologia ułatwiająca łamanie haseł), programiści zaczęli dodawać losowy ciąg znaków do początków haseł. - o koderach haseł: zapewniają wiele implementacji kodowania haseł do wyboru. Każdy z nich ma swoje wady i zalety, a programista może wybrać, której z nich użyć w zależności od wymagań uwierzytelniania jego aplikacji. <p>Są w stanie</p> <ul style="list-style-type: none"> - zapoznać zespół z najlepszymi praktykami kodowania haseł. - przeszkolić zespół w zakresie cyberbezpieczeństwa. - decydować, jakich typów haseł nie należy używać. |



| | |
|--|---|
| | <ul style="list-style-type: none">- zdefiniować właściwy sposób generowania procesów kodowania.- wyeliminować skomplikowane hasła.- zdecydowanie zmniejszyć ryzyko skopiowania hasła.- zapewnić audyt i rozliczalność haseł. <p>Kompetencje osobiste</p> <p>Uczestnicy są w stanie</p> <ul style="list-style-type: none">- uznać dokumentację procesów jako punkt wyjścia do dalszych kroków roboczych.- pracować w sposób uporządkowany, skupiając się na szczegółach.- rozpoznawać odpowiedzialność związaną z zadaniem i być pewnym siebie w interakcji z innymi.- radzić sobie z głównymi wymaganymi zadaniami z dobrym poziomem autonomii.- podkreślać swoje kompetencje społeczne (umiejętności miękkie, w szczególności empatię i komunikację). |
| Zalecenia dotyczące uczenia się i nauczania | Większość typów procesów kodowania wymaga złożonych kroków i nieszablonowego myślenia, ale czasami to właśnie proste testy pomagają ujawnić najpoważniejsze zagrożenia związane z kodowaniem. |
| Literatura i inne zasoby | <p>Kaliski, B. (2000). Password-Based Cryptography Specification Version 2.0. RFC Editor, US. https://doi.org/10.17487/RFC2898.</p> <p>Mourouzis, T., Pavlou, K. E., & 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 LU9 – Zarządzanie danymi

| Moduł 9 | Zarządzanie danymi |
|---------------------------------------|---|
| Opis ogólny / Rezultat | Wykonywanie rutynowych kopii zapasowych danych i stosowanie metod właściwego postępowania zgodnych z RODO w odniesieniu do przetwarzania danych w firmie. |
| Numer kodu | LU 9 |
| Rodzaj | Obowiązkowe - należy określić |
| Ilość | Godziny - do ustalenia |
| Kompetencje w zakresie działań | Uczestnicy uczą się rozumieć znaczenie przechowywania i przetwarzania danych i informacji zgodnie z ustalonymi wytycznymi. Dowiedzą się o właściwym postępowaniu z danymi w świetle RODO. Uczestnicy będą w stanie ocenić sposób przechowywania i przetwarzania danych fizycznych i elektronicznych w firmie oraz zidentyfikować potencjalne nadużycia. Uczestnicy nauczą się sugerować zmiany w procesach firmy w celu złagodzenia tych zagrożeń. |
| Efekty kształcenia | Kompetencje techniczne Uczestnicy Wiedzę <ul style="list-style-type: none">- jak zdefiniować potrzeby informacyjne niezbędne do pomyślnego przeprowadzenia procesu: jakie dane są przetwarzane w ramach organizacji i jakie techniki przechowywania powinny być zgodne z odpowiednimi przepisami.- jak określić objętość i cel przechowywania i przetwarzania danych osobowych.- jak organizować i stosować zarządzanie danymi w firmie: dostosowywać się do zmian; stosować analityczne myślenie; opracowywać rozwiązania; samodzielnie wykonywać zadania związane z zarządzaniem projektami.- jakie są techniki i style komunikacji w celu uzyskania niezbędnych informacji na temat przechowywania danych. Są w stanie <ul style="list-style-type: none">- określić ilość i cel danych osobowych, które są przechowywane/przetwarzane w organizacji.- tworzyć regularne kopie zapasowe w celu zminimalizowania ryzyka utraty cennych danych i informacji.- pracować w grupie w celu efektywnego pozyskiwania informacji dla usprawnienia procesów.- planować i zarządzać różnymi zasobami oraz monitorować proces zarządzania danymi w celu osiągnięcia określonego celu. Kompetencje osobiste |



| | |
|--|--|
| | <p>Uczestnicy są w stanie</p> <ul style="list-style-type: none">- pracować w sposób uporządkowany, skupiając się na szczegółach.- rozpoznawać odpowiedzialność związaną z zadaniem i być pewnym siebie w interakcji z innymi.- samodzielnie wykonywać zadania i wykazywać gotowość do nauki.- |
| Zalecenia dotyczące uczenia się i nauczania | <p>Łączenie wiedzy teoretycznej i podejścia z praktycznymi przykładami. Stosowanie interaktywnych metod nauczania (np. praca w grupach, dyskusje, analiza przypadków, odgrywanie ról w symulacjach, itp.)</p> |
| Literatura i inne zasoby | <p>Calabro, A., Daoudagh, S., & 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: https://www.sciencedirect.com/science/article/pii/S0306437919305216.</p> <p>Guide on Good Data Protection Practice in Research (2019) [Online]. Available: https://www.eui.eu/documents/servicesadmin/deanofstudies/researchethics/guide-data-protection-research.pdf.</p> <p>EU-GDPR. (2019). EU GDPR portal. [Online]. Available: https://eugdpr.org.</p> <p>General data protection regulation (2018). Official Journal of the European Union [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.</p> |



2.10 LU10 – Kontrola dostępu oparta o role

| Moduł 10 | Kontrola dostępu oparta o role |
|---------------------------------------|--|
| Opis ogólny / Rezultat | Tworzenie kont administratorów i ograniczanie praw dostępu dla pracowników zgodnie ze zdefiniowanymi poziomami bezpieczeństwa. |
| Numer kodu | LU 10 |
| Rodzaj | Obowiązkowe - należy określić |
| Ilość | Godziny - do ustalenia |
| Kompetencje w zakresie działań | Uczestnicy uczą się rozumieć, jak ważne jest ograniczanie dostępu do danych, informacji lub infrastruktury fizycznej, gdy jest to możliwe, oraz przyznawanie dostępu tylko grupie odpowiednich pracowników. Dowiedzą się, jak ustanowić odpowiednie ograniczenia zgodnie ze zdefiniowanym poziomem bezpieczeństwa. Uczestnicy będą w stanie przypisać role w firmie do poziomów bezpieczeństwa i w razie potrzeby umożliwić śledzenie dostępu do określonych informacji. |
| Efekty kształcenia | Kompetencje techniczne Uczestnicy Wiedzę <ul style="list-style-type: none">- jak zidentyfikować kluczowe operacje na danych osobowych, które są wykonywane w organizacji.- jak ustalić dostępność informacji dla określonych grup pracowników.- jak ustanowić odpowiednie ograniczenia zgodnie z określonymi i uzgodnionymi poziomami bezpieczeństwa, gdy zostanie to uznane za konieczne. Są w stanie <ul style="list-style-type: none">- rozróżniać role poszczególnych pracowników i grup w celu określenia ich potrzeb w zakresie różnych poziomów bezpieczeństwa (w oparciu o uzgodnione z kierownictwem poziomy bezpieczeństwa).- znajdować odpowiednie rozwiązania dla poszczególnych pracowników lub grup w zakresie dostępu lub ograniczeń i umieć je uzasadnić.- zarządzać uprawnieniami poszczególnych użytkowników, co staje się kwestią prostego przypisania odpowiednich ról do konta użytkownika, gdy role są jasno zdefiniowane (przez kierownictwo). Kompetencje osobiste Uczestnicy są w stanie |



| | |
|--|---|
| | <ul style="list-style-type: none">- samodzielnie przydzielać odpowiednie role zgodnie z wymaganiami kierownictwa (przypisane poziomy bezpieczeństwa).- samodzielnie komunikować się ze współpracownikami i kierownictwem, będąc pewnym siebie w interakcjach.- autonomicznie rozpoznawać odpowiedzialność związaną z zadaniem i szanować potrzeby innych. |
| Zalecenia dotyczące uczenia się i nauczania | Poznanie trzech podstawowych reguł zdefiniowanych dla RBAC: 1) Przypisywanie ról, 2) Autoryzacja ról, 3) Autoryzacja uprawnień. Uświadom znaczenie uwrażliwienia w przypisywaniu ról i dokonaj jasnych uzgodnień z kierownictwem. |
| Literatura i inne zasoby | <p>Błokdyk, 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: https://digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more.</p> |



2.11 LU11 – Zarządzanie hasłami

| Moduł 11 | Zarządzanie hasłami |
|---------------------------------------|--|
| Opis ogólny / Rezultat | Ustanowienie haseł dostępu dla poszczególnych pracowników oraz umożliwienie bezpiecznego przechowywania i procesu odzyskiwania danych. |
| Numer kodu | LU 11 |
| Rodzaj | Obowiązkowe - należy określić |
| Ilość | Godziny - do ustalenia |
| Kompetencje w zakresie działań | Uczestnicy poznają znaczenie centralizacji zarządzania wykorzystywaniem haseł w firmie. Dowiedzą się, jak definiować hasła zapewniające uwierzytelnienie (wśród pracowników) oraz jak resetować hasła. Uczestnicy uczą się, jak strukturalnie tworzyć, używać/zarządzać, przechowywać i zmieniać hasła pracowników. |
| Efekty kształcenia | Kompetencje techniczne Uczestnicy Wiedzą <ul style="list-style-type: none">- o przechowywaniu haseł.- o przekazywaniu haseł.- o odgadywaniu haseł.- o łamaniu haseł.- o zastępowaniu haseł. Są w stanie <ul style="list-style-type: none">- zapoznać zespół z najlepszymi praktykami dotyczącymi haseł.- przeszkolić zespół w zakresie bezpieczeństwa cybernetycznego.- decydować, jakich typów haseł nie używać.- generować złożone hasła.- wykorzystywać możliwości automatyzacji.- wyeliminować skomplikowane hasła.- wyeliminować konieczność resetowania haseł.- zapewnić audyt i rozliczalności haseł. Kompetencje osobiste Uczestnicy są w stanie <ul style="list-style-type: none">- uznać dokumentację procesów jako punkt wyjścia do dalszych kroków roboczych.- pracować w sposób uporządkowany, skupiając się na szczegółach.- rozpoznawać odpowiedzialność związaną z zadaniem i być pewnym siebie w interakcji z innymi.- radzić sobie z głównymi zadaniami z dobrym poziomem autonomii. |



| | |
|--|---|
| | <ul style="list-style-type: none">- podkreślać swoje kompetencje społeczne (umiejętności miękkie, empatia, a w szczególności komunikacja). |
| Zalecenia dotyczące uczenia się i nauczania | Zarządzanie hasłami z pomocą rzeczywistych przykładów. Ćwiczenia na dokumentację w formie swobodnej i za pomocą modułów tekstowych. |
| Literatura i inne zasoby | 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 LU12 – Zarządzanie ciągłością biznesu

| Moduł 12 | Zarządzanie ciągłością biznesu |
|--------------------------------|--|
| Opis ogólny / Rezultat | Ustanowienie wytycznych i procedur na wypadek pojawienia się możliwych sytuacji awaryjnych. |
| Numer kodu | LU 12 |
| Rodzaj | Obowiązkowe - należy określić |
| Ilość | Godziny - do ustalenia |
| Kompetencje w zakresie działań | Uczestnicy uczą się rozumieć znaczenie przeprowadzania scenariuszy "co by było gdyby". Uczą się analizować teoretyczne możliwości i przygotowywać strategiczne wytyczne. Uczestnicy będą w stanie ustalić wytyczne i wstępnie zdefiniować środki, aby być przygotowanym i reagować w sposób skoordynowany na nowe sytuacje, gdy takie się pojawią. |
| Efekty kształcenia | <p>Kompetencje techniczne</p> <p>Uczestnicy</p> <p>Wiedzę</p> <ul style="list-style-type: none">- jak znaleźć dokumenty krajowe i jak szukać wiedzy w krajowych dokumentach prawnych regulujących bezpieczeństwo i ochronę danych.- jakie są techniki symulacyjne pozwalające przewidzieć potencjalne naruszenia danych.- jak radzić sobie z zasadami oceny ryzyka. <p>Są w stanie</p> <ul style="list-style-type: none">- identyfikować ryzyko z wykorzystaniem różnych technik i stylów komunikacji.- wdrażać zasady oceny ryzyka działając za zgodą kierownictwa.- planować i opracowywać rozwiązania dostosowujące się do okoliczności i zmian w skali organizacji oraz wdrażać je, działając za zgodą kierownictwa.- znajdować nowe rozwiązania w oparciu o analizę wcześniejszych zdarzeń. <p>Kompetencje osobiste</p> <p>Uczestnicy są w stanie</p> <ul style="list-style-type: none">- pracować w niesprzyjających okolicznościach, przywiązując wagę do szczegółów.- łatwo przystosować się do nowych okoliczności.- być przykładem dla innych pracowników poprzez przestrzeganie kodeksu etycznego i wykazywanie się odpowiedzialnością.- |



| | |
|--|---|
| Zalecenia dotyczące uczenia się i nauczania | Teoretyczne przeciwienie scenariuszy różnych zagrożeń i sytuacji ryzyka. Praca na przykładach z rzeczywistych sytuacji. |
| Literatura i inne zasoby | <p>Irwin, L. (2019). Why risk assessments are essential for GDPR compliance [Online]. Available: https://www.itgovernance.co.uk/blog/why-risk-assessments-are-essential-for-gdpr-compliance.</p> <p>European Data Protection Board (2021). Guidelines 01/2021 on Examples regarding Data Breach Notification [Online]. Available: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf.</p> <p>European Union Agency for Cybersecurity (2017). Handbook on Security of Personal Data Processing [Online]. Available: www.enisa.europa.eu.</p> <p>Green, A. (2020). GDPR Data Breach Guidelines - COMPLIANCE & REGULATION [Online]. Available: https://www.varonis.com/blog/guide-eu-gdpr-breach-notification-rule/.</p> <p>General data protection regulation (2021). Complete guide to GDPR compliance [Online]. Available: https://gdpr.eu/.</p> |
| | |



2.13 LU13 – Mediacje i zarządzanie interesariuszami

| Moduł 13 | Mediacje i zarządzanie interesariuszami |
|--------------------------------|---|
| Opis ogólny / Rezultat | Koordinowanie potrzeb kadry zarządzającej i pracowników firmy, dostarczanie obu stronom informacji i spostrzeżeń z wewnątrz firmy. |
| Numer kodu | LU 13 |
| Rodzaj | Obowiązkowe - należy określić |
| Ilość | Godziny - do ustalenia |
| Kompetencje w zakresie działań | Uczestnicy poznają znaczenie koordynacji działań ze wszystkimi interesariuszami w firmie w zakresie ich roli i wpływu na ochronę danych i bezpieczeństwo informacji. Dowiedzą się, jak skutecznie komunikować się z różnymi szczeblami hierarchii (pracownicy i kierownictwo) oraz jak dostosować ich potrzeby i interesy do zmian w rutynowych działaniach organizacji. Uczestnicy będą potrafili w sposób dyplomatyczny współdziałać z interesariuszami i radzić sobie z ewentualnym oporem wobec własnego wpływu. |
| Efekty kształcenia | Kompetencje techniczne Uczestnicy Wiedzę <ul style="list-style-type: none">- jak znaleźć krajowe dokumenty prawne, regulujące bezpieczeństwo informacji i ochronę danych oraz jak szukać wiedzy na ten temat.- jakie kanały komunikacji wewnętrznej i zewnętrznej można stosować działając za zgodą kierownictwa i jakie ryzyko jest z nimi związane.- jakie środki mogą być stosowane do obserwacji, testowania i oceny procesów w organizacji.- jakie środki mogą być stosowane do oceny ryzyka i jak radzić sobie z oceną ryzyka. Są w stanie <ul style="list-style-type: none">- wdrażać środki audytu wewnętrznego (z aprobatą kierownictwa).- planować i rozwijać rozwiązania strategiczne, a następnie wdrażać je, działając za zgodą kierownictwa.- wprowadzać kulturę prewencyjną przy wsparciu kierownictwa.- identyfikować, oceniać i nadawać priorytety ryzyku.- tworzyć wewnętrzne regulacje w skali organizacji i wdrażać je (za zgodą kierownictwa). Kompetencje osobiste Uczestnicy są w stanie |



| | |
|--|--|
| | <ul style="list-style-type: none">- radzić sobie ze zmianami i adaptacją.- być kreatywnym i dążyć do dalszego rozwoju.- polegać na własnym kodeksie etycznym, aby inni mogli brać z nich przykład. |
| Zalecenia dotyczące uczenia się i nauczania | Łączenie wiedzy teoretycznej i podejścia z praktycznymi przykładami. Stosowanie interaktywnych metod nauczania (np.: praca w grupach, dyskusje, analiza przypadków, odgrywanie ról w symulacjach, itp.) |
| Literatura i inne zasoby | <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: https://gdpr.eu/.</p> <p>Gorondutse, A. H., & 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: https://www.helpnetsecurity.com/2018/05/14/gdpr-compliance-profile/</p> |