Załącznik nr 9 do zarządzenia nr 35/23 Rektora Collegium
Witelona Uczelnia Państwowa z dnia 09 maja 2023 r.

KARTA MODUŁU

I. OGÓLNE INFORMACJE O MODULE								
COLLEGIUM WITELONA UCZELNIA PAŃSTWOWA WYDZIAŁ NAUK SPOŁECZNYCH I HUMANISTYCZNYCH								
Kierunek studiów:		Administracja						
Poziom studiów:		pierwszego stopnia						
Profil studiów:		praktyczny						
Forma studiów:		stacjonarne/niestacjonarne						
Nazwa modułu:		**Wprowadzenie do cyberbezpieczeństwa**						
Rodzaj modułu:		obowiązkowy						
Język wykładowy:		Język polski*						
Rok studiów:	1	**Formy prowadzenia zajęć wraz z liczbą godzin dydaktycznych:**						
Semestr:	2	Wykład S/N	Warsztat S/N	**	**	**	**	**
Liczba punktów ECTS ogółem:	2	10/10	10/20	S/N	S/N	S/N	S/N	S/N
Forma zaliczenia:		Zaliczenie z oceną						
Wymagania wstępne:		brak						

II. CELE KSZTAŁCENIA
Cele kształcenia:
Cel 1: przekazanie studentom wiedzy o podstawowych problemach cyberbezpieczeństwa w obszarach życia prywatnego i zawodowego. **Cel 2:** wykształcenie wśród studentów umiejętności właściwego reagowania na różnego rodzaju zagrożenia pojawiające się w sieci internetowej, umiejętności rozstrzygania dylematów związanych z administrowaniem oraz uzupełniania i doskonalenia nabytej wiedzy i umiejętności w warunkach postępu procesów cyfryzacji w administracji publicznej.

III. EFEKTY UCZENIA SIĘ WRAZ Z ODNIESIENIEM DO EFEKTÓW KIERUNKOWYCH ORAZ METODY WERYFIKACJI EFEKTÓW			
Efekt	Student, który zaliczył moduł w zakresie:	Odniesienie do efektów kierunkowych	Metody weryfikacji
wiedzy:			
W01	w zaawansowanym stopniu zna i rozumie procedury właściwe działaniu administracji publicznej i ich praktyczne zastosowanie.	K1A_W13	test wiedzy
W02	Student w zaawansowanym stopniu zna fakty i zjawiska zachodzące w obrębie instytucji polskich i europejskich, realizujących zadania z zakresu administracji i gospodarki rynkowej, różnorodne i złożone formy aktywności administracji publicznej państwa i samorządu, jej organów i instytucji, zna i rozumie procesy zachodzące w administracji państwa i samorządu oraz regulacje prawa w tym zakresie	K1A_W15	test wiedzy
umiejętności:			
U01	potrafi samodzielnie stosować uwarunkowania organizacyjne, techniczne, prawne i inne z zakresu administrowania w praktyce.	K1A_U17	prezentacja problemu, dyskusja
kompetencji społecznych:			
K01	jest gotów by współdziałać i pracuje w określonej organizacji przyjmując w niej różne role a nadto by w tym zakresie zasięgać opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem zadania.	K1A_K03	obserwacja i ocena postaw studenta.

IV. TREŚCI PROGRAMOWE
Treści programowe (tematyka zajęć, zaprezentowana z podziałam na poszczególne formy zajęć z określeniem liczby godzin potrzebnych na ich realizację)
Wykład

Kod	Tematyka zajęć	Liczba godzin 10/10
W1	Cyberprzestrzeń i cyberbezpieczeństwo – definicja, cechy.	2/2
W2	Rola organów państwowych w zapewnieniu bezpieczeństwa cyberprzestrzeni	1/1
W3	Współpraca krajowa i międzynarodowa jako gwarancja cyberbezpieczeństwa.	1/1
W4	Internet i jego zastosowanie w administracji publicznej.	1/1
W5	Sieci lokalne i Internet– podstawy techniczne funkcjonowania współczesnych sieci.	2/2
W6	E-społeczeństwo, dostępne usługi – szanse i zagrożenia	1/1
W7	Cyberbezpieczeństwo w dobie sztucznej inteligencji	1/1
Warsztaty:		
Kod	Tematyka zajęć	Liczba godzin 20/10
WT1	Internet – powstanie i rozwój. Wpływ na funkcjonowanie człowieka.	4/2
Wt2	Praca i nauka zdalna – rekomendacje bezpieczeństwa, typy zagrożeń w cyberprzestrzeni, minimalizacja ryzyka.	4/2
WT3	Przemoc w sieci – sposoby reagowania. Inne zagrożenia w sieci.	4/2
WT4	Zachowanie bezpieczeństwa w e-administracji.	4/2
WT5	E – administracja wobec e- społeczeństwa. Aktualne problemy i wyzwania.	4/2

V. METODY KSZTAŁCENIA, NARZĘDZIA DYDAKTYCZNE

1. Metody kształcenia: Wykład: informacyjny (konwencjonalny) prowadzony w formie konwencjonalnej lub zdalnie, konwersatoryjny. Warsztaty: metoda problemowa; metoda ćwiczeniowa oparta na wykorzystaniu różnych źródeł wiedzy; metoda projektu; studium przypadku; dyskusja.
2. Narzędzia (środki) dydaktyczne: wykorzystanie urządzeń mulimedialnych, sieci internetowej, bibliografii, tekstów aktów prawnych i innych materiałów źródłowych.

VI. FORMA I KRYTERIA ZALICZENIA MODUŁU

Forma zaliczenia przedmiotu – zaliczenie z oceną.

Kryteria oceny formującej:
1. Zaliczenie pisemne – kryteria oceny:
- 51% - 60% - ocena dostateczna,
- 61% - 70% - ocena dostateczna plus,
- 71% - 80% - ocena dobra,
- 81% - 90% - ocena dobra plus,
- 91% - 100% - ocena bardzo dobra.

2. Obserwacja i ocena postaw studenta wynikających z:
- realizacji zadań przygotowanych w ramach warsztatów,
- zaangażowania w pracę grupy,
- zachowań i aktywności w trakcie wykładów i warsztatów,
- prowadzenia merytorycznej dyskusji,
- potrzeby ciągłego rozwoju osobistego i zawodowego.

Kryteria oceny podsumowującej:
- średnia ocen formujących.

VII. BILANS PUNKTÓW ECTS - NAKŁAD PRACY STUDENTA

Kategoria	**Obciążenie studenta**
Liczba godzin realizowanych przy bezpośrednim udziale nauczyciela (godziny kontaktowe)	**30/20**
Udział w wykładach	10/10
Udział w innych formach zajęć (**)	
Samodzielna praca studenta (godziny niekontaktowe)	**20/30**
Przygotowanie do wykładu	5/5
Przygotowanie do innych form zajęć – warsztaty	10/15

Przygotowanie do zaliczenia wykładu	5/10
Przygotowanie do zaliczenia innych form zajęć	
Łączna liczba godzin	**50**
Punkty ECTS za moduł	**2**

VIII. ZALECANA LITERATURA

Literatura podstawowa:

1.Cisco Introduction to cybersecurity – platforma Cisco NetAcad
2. Cyberbezpieczeństwo: zarys wykładu / redakcja naukowa Cezary Banasiński ; [autorzy] Cezary Banasiński, Cezary Błaszczyk, Jacek M. Chmielewski, Władysław Hydzik, Dariusz Jagiełło, Filip Krzyżankiewicz, Arwid Mednis, Włodzimierz Nowak, Marcin Rojszczak, Adam Szafrański, Ryszard Szpyra, Kazimierz Waćkowski, Paweł Widawski, Joanna Worona, Zofia Zawadzka, Wolters Kluwer , Warszawa 2018.
3. Cyberbezpieczeństwo: podejście systemowe, Jerzy Krawiec, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2019.
4. E-administracja : szanse i zagrożenia, red. Tadeusz Stanisławski, Bogusław Przywora, Łukasz Jurek, Wydawnictwo KUL, Lublin 2013.

Literatura uzupełniająca:

1. Dominika Lisiak – Felicka, Maciej Szmit, Cyberbezpieczeństwo w administracji publicznej w Polsce, European Association for Security, Kraków 2016, e-book:
https://www.google.pl/books/edition/Cyberbezpiecze%C5%84stwo_administracji_publi/5f3wCwAAQBAJ?hl=pl&gbpv=1&pg=PA1&printsec=frontcover

2. Zachowania jednostki w sytuacjach zagrożenia w kontekście doznawanych emocji : ujęcie cybernetyczne, Wilsz Jolanta, Biblioteka Narodowa 2018.