Załącznik nr 5

**Tematyka szkolenia pracowników z zakresu cyberbezpieczeństwa**

1. Wstęp
	* Co to jest cyberbezpieczeństwo - definicja cyberprzestrzeni i cyberbezpieczeństwa, dlaczego to jest ważne
	* Polityka bezpieczeństwa - czym jest w organizacji polityka bezpieczeństwa i jaka jest jej rola
	* Incydenty bezpieczeństwa - co należy rozumieć jako incydent bezpieczeństwa i jak z nim postępować
2. Ataki „na człowieka” tzw. SOCJOTECHNIKA (stosowane techniki manipulacji)
	* Ataki socjotechniczne - techniki manipulacji wykorzystywane przez cyberprzestępców
	* Sposoby - pod jakimi pretekstami wyłudza się dane
	* Wykrywanie - jak rozpoznać, że jest się celem ataku socjotechnicznego
	* Reakcja - jak prawidłowo reagować na ataki socjotechniczne
	* Jak i skąd atakujący zbierają dane na twój temat
	* Miejsca, w których zostawiamy swoje dane świadomie i nieświadomie - jak świadomie udostępniać informacji w sieci
3. Atak „na komputery” - objaśnienia, które przedstawią użytkownikowi potencjalne zagrożenia
	* Przegląd aktualnych ataków komputerowych wykorzystywanych przez cyberprzestępców
	* Ataki przez sieci bezprzewodowe (WiFi, Bluetooth, NFC) oraz metody zabezpieczania
	* Ataki przez pocztę e-mail (fałszywe e-maile) oraz metody zabezpieczania
	* Ataki przez strony WWW - jak nie dać się zainfekować, fałszywe strony
	* Ataki przez komunikatory (Skype, Facebook) oraz metody zabezpieczania
	* Ataki przez telefon (fałszywe SMS-y, przekierowania rozmów, itp.) oraz metody zabezpieczania
	* Ataki APT, phishing, smishing, spear-phishing, pharming, spoofing, spam, spim, scam jak się chronić przed takim typem ataku.
4. Dobre praktyki związane z bezpiecznym korzystaniem z systemu informatycznego urzędu
	* Polityka haseł - jakie hasło jest bezpieczne, jak nim zarządzać, wykorzystanie 2FA, oraz menadżera haseł
	* Bezpieczeństwo fizyczne - urządzenia, nośniki danych, dokumenty, „czyste biurko”
	* Bezpieczna praca z urządzeniami mobilnymi (smartfon, tablet, laptop)
	* Problem aktualnego oprogramowania i kopii zapasowych
	* Bezpieczna praca z pakietem biurowym Microsoft Office
	* Bezpieczna praca z programem pocztowym
	* Bezpieczna praca z przeglądarką internetową
	* Zastosowanie technik kryptograficznych (szyfrowanie, certyfikaty)
5. Praca zdalna – bezpieczeństwo
	* Organizacja pracy zdalnej
	* Miejsce pracy zdalnej – zabezpieczenia fizyczne i organizacja
	* Sposoby zabezpieczania urządzeń przed utratą danych / kradzieżą
	* Nieświadome naruszenia bezpieczeństwa informacji
6. Aspekty prawne
	* Odpowiedzialność pracownika przed pracodawcą za ujawnienie informacji
	* Nieautoryzowane użycie systemów komputerowych
	* Rażące zaniedbania związane z wykorzystywaniem sprzętu komputerowego
	* Dane osobowe i dane wrażliwe