Załącznik Nr 2 do Zapytania ofertowego

1. Podstawowe szkolenie budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników UG i OPS.

Forma szkolenia:	Szkolenie stacjonarne w siedzibie zamawiającego
Zakres szkolenia:	- czym jest cyberbezpieczeństwo; - omówienie poprawnych zasad postępowania związanych z cyberbezpieczeństwem; - metody obrony przed atakami komputerowymi oraz zagrożeniami socjotechnicznymi + przykłady i omówienie sposobów przeciwdziałania oraz zabezpieczania się przed powyższymi zagrożeniami; - szczegółowe informacje związane z zagrożeniami w sieci takimi jak phishing, ransomware, malware, socjotechnika, atak telefoniczny, spoofing, atak odwrócony - zmuszenie ofiary do szukania pomocy u atakującego, przekręt nigeryjski, wyłudzenia BLIK, oszustwo na dyrektora/prezesa/współpracownika; - zasady wykonywania przelewów bankowych; - bezpieczne korzystanie z sieci komputerowych; - wykonywanie kopii zapasowych oraz tworzenie i utrzymania polityki ciągłości działania; - bezpiecznie przetwarzanie danych: szyfrowanie, przechowywanie, udostępnianie, komunikacja; - bezpieczne hasła, menedżer haseł, autoryzacja dwuetapowa, klucze sprzętowe; - bezpieczne korzystanie z mediów społecznościowych; - bezpieczne korzystanie ze smartfonów oraz komputerów przenośnych; - w jaki sposób przeciwdziałać kradzieży tożsamości; - ochrona przed zaawansowanymi atakami przez pocztę i strony internetowe; - wskazanie zasad cyberhigieny; - reagowanie na incydenty i włamania;
Czas trwania szkolenia:	3 godziny

2. Szkolenie z zakresu cyberbezpieczeństwa dla wybranych przedstawiciel i kadry UG oraz OPS, istotnych z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwa informacji.

Forma szkolenia:	Szkolenie stacjonarne w siedzibie zamawiającego
Zakres szkolenia:	- omówienie przepisów prawa w zakresie rozporządzenia ogólnego RODO, rozporządzenia o Krajowych Ramach Interoperacyjności oraz ustawy o Krajowym Systemie Cyberbezpieczeństwa ze szczególnym uwzględnieniem zagadnień analizy ryzyka oraz wymagań Dyrektywy NIS2 - omówienie zadań i obowiązków uczestników szkolenia w doskonaleniu Polityki Bezpieczeństwa Informacji Jednostki oraz Systemu Zarządzania

	Bezpieczeństwem Informacji przyjętego w Jednostce - ćwiczenia praktyczne obejmujące sytuacje z zakresu naruszeń zasad cyberbezpieczeństwa w Jednostce - informacje o zasadach bezpieczeństwa fizycznego oraz teleinformatycznego Jednostki - omówienie harmonogramu sporządzania i realizacji planów szkoleń i audytów wewnętrznych - szczegółowe omówienie zasad przeglądu Systemu Zarządzania Bezpieczeństwem Informacji Jednostki z uwzględnieniem ról i odpowiedzialności osób zaangażowanych w szczególności najwyższego kierownictwa
Czas trwania szkolenia:	2 godziny

3. Szkolenie powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcji personelu, w szczególności reagowanie specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami dla UG i OPS.

Forma szkolenia:	Szkolenie stacjonarne w siedzibie zamawiającego
Zakres szkolenia:	- przed realizacją szkolenia opisanego w punkcie numer 2 należy przeprowadzić testy socjotechniczne skierowane do wybranej grupy pracowników (UG) i (OPS) - należy ponowić przeprowadzenie testów socjotechniczne skierowane do pracowników (UG) i (OPS) po realizacji szkolenia opisanego w punkcie numer 2 - omówienie wyników testów socjotechnicznych - identyfikacja potencjalnych słabych punktów w bezpieczeństwie Jednostki związanych z czynnikiem ludzkim - ocena skuteczności procedur bezpieczeństwa Jednostki - omówienie zasad zgłaszania incydentów bezpieczeństwa przez pracowników (ćwiczenia praktyczne) - przykłady najpopularniejszych ataków socjotechnicznych - szczegółowe zapoznanie pracowników z atakami typu „phising” - metody weryfikacji wiadomości e-mail (ćwiczenia praktyczne)
Czas trwania szkolenia:	4 godziny

4. Szkolenie zdalne dla informatyka: Atakowanie i Ochrona Webaplikacji.

Forma szkolenia:	Szkolenie zdalne
Zakres szkolenia:	**Współczesne problemy bezpieczeństwa aplikacji webowych** - zagrożenia wynikające z architektury webaplikacji (np. CGI, SSI, etc.) - zagrożenia wynikające z języków programowania (PHP, JS, etc.) i technologi, np. ASP, JSP - problem styku webaplikacji z bazą danych - interfejsy zewnętrzne webaplikacji

	- zagrożenia po stronie serwera, środowiska, sieci, a zagrożenia po stronie klient - zagrożenia stron tworzonych pod urządzenia mobilne (telefony, tablety) **Ataki na aplikacje webowe** - Wyszukiwanie adresów serwerów deweloperskich - Bezpieczeństwo hostingu i webserwera - Brak obsługi błędów - Manipulacje parametrami (metody GET, POST) - Techniki podsłuchu i manipulowania transmisją - Atak Forcefull browsing - Atak Path Traversal - Technika Google Hacking - Wstrzyknięcie kodu (PHP shell) i komend systemowych do webaplikacji - Problem filtrowania danych wejściowych - Ataki XSS (persistent, reflected) - Omijanie filtrowania danych wejściowych i encodingu wyjściowych - Ataki na sesję aplikacji webowej - Podsłuchiwanie sesji i kradzież ciasteczek http - Jak poprawnie zarządzać sesją w webapikacji? - Ataki CSRF/XSRF - Bezpieczny upload plików - Metody ułatwiające przetrwanie ataków DoS/DDoS - Ataki Clickjacking - Ataki na bazy danych - Ataki SQL injection i Blind SQL injection - Ochrona przed atakami SQL injection - Szyfrowanie połączenia i ataki na SSL - Szyfrowanie danych w webaplikacji - Ochrona przed spamem i enumeracją zasobów oraz haseł - Podsumowanie zagrożeń i przegląd OWASP TOP10 - Pozaprogramistyczne środki ochrony (systemy IDS/IPS, WAF) - Omijanie detekcji przez systemy WAF/IDS/IPS **Problemy przeglądarek** - Same Orgin Policy - Rich Internet Applications - Dziury w przeglądarkach - Ataki DNS-Rebinding - Narzędzia podnoszące bezpieczeństwo i pomagające w testowaniu aplikacji webowych
Czas trwania szkolenia:	2 dni / 14 godzin