Załącznik nr 1a do SWZ

Szczegółowy opis przedmiotu zamówienia na audyt wdrożonego systemu bezpieczeństwa informacji oraz cykl szkoleń w ramach konkursu grantowego „Cyberbezpieczny Samorząd”

Załącznik nr 1a do SWZ

Spis treści

Wstępny audyt KRI

Usługa: „Wstępnego audytu bezpieczeństwa informacji, którego kryterium jest Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (zwanym dalej „Rozporządzeniem KRI")"

Przedmiotem zamówienia jest usługa wykonania wstępnego audytu bezpieczeństwa informacji dla Zamawiającego

LP	Parametr lub warunek	Minimalne wymagania
1.	**Opis przedmiotu zamówienia**	Przedmiotem zamówienia jest przeprowadzenie: a) Audytu bezpieczeństwa zgodnie z § 20 ust. 2 pkt 14 Rozporządzenia KRI; b) Audyt musi być przeprowadzony przez: • co najmniej dwóch audytorów posiadających uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu. Audyt musi być zrealizowany w siedzibie Zamawiającego, w wymiarze co najmniej 1 dnia roboczego (tj. 8 godzin). Audyt ma obejmować weryfikację bezpieczeństwa fizycznego (sprawdzenie ochrony pomieszczeń, sprzętów, infrastruktury oraz personelu przed bezpośrednim działaniem czynników fizycznych i zdarzeń takich jak kradzież, nieuprawniony dostęp), bezpieczeństwa informatycznego (analiza bezpieczeństwa systemu teleinformatycznego) oraz bezpieczeństwa organizacyjnego i osobowego (stosowane procedury bezpieczeństwa), w tym przegląd

		dokumentacji dotyczącej systemu zarządzania bezpieczeństwem informacji. Audyt musi obejmować weryfikację: a. systemu zarządzania bezpieczeństwem informacji, b. zapewnienia aktualizacji regulacji wewnętrznych w zakresie bezpieczeństwa informacji, c. utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, d. przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, e. podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia, f. zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji, g. zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, h. ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, i. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie, j. zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji, k. ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży, l. zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, m. bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji, n. zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji.

		Kryteriami audytu są: • Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych; • Ustawa o Krajowym Systemie Cyberbezpieczeństwa; • Norma ISO/IEC 27001; • Norma PN-EN ISO/IEC 22301. Wykonawca zobowiązany jest do dostarczenia Zamawiającemu: • raportu z audytu bezpieczeństwa systemu informacyjnego, • rekomendacji do wdrożenia w celu poprawy cyberbezpieczeństwa Zamawiającego.

Obowiązkowy (końcowy) audyt KRI

Usługa: „Audytu bezpieczeństwa informacji, którego kryterium jest Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (zwanym dalej „Rozporządzeniem KRI")"

Przedmiotem zamówienia jest usługa wykonania audytu dla Zamawiającego zgodnego z warunkami określonymi w:

• Regulaminie Konkursu Grantowego „Cyberbezpieczny Samorząd".

LP	**Parametr lub warunek**	**Minimalne wymagania**
1.	**Opis przedmiotu zamówienia**	1. Przedmiotem zamówienia jest przeprowadzenie: a) Audytu bezpieczeństwa zgodnie z § 19 ust. 2 pkt 14 Rozporządzenia KRI; b) Audyt musi być przeprowadzony przez: •co najmniej dwóch audytorów posiadających uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.

		Audyt musi być zrealizowany w siedzibie Zamawiającego, w wymiarze co najmniej 1 dnia roboczego (tj. 8 godzin). Audyt ma obejmować weryfikację bezpieczeństwa fizycznego (sprawdzenie ochrony pomieszczeń, sprzętów, infrastruktury oraz personelu przed bezpośrednim działaniem czynników fizycznych i zdarzeń takich jak kradzież, nieuprawniony dostęp), bezpieczeństwa informatycznego (analiza bezpieczeństwa systemu teleinformatycznego) oraz bezpieczeństwa organizacyjnego i osobowego (stosowane procedury bezpieczeństwa), w tym przegląd dokumentacji dotyczącej systemu zarządzania bezpieczeństwem informacji. Audyt musi obejmować weryfikację: a. systemu zarządzania bezpieczeństwem informacji, b. zapewnienia aktualizacji regulacji wewnętrznych w zakresie bezpieczeństwa informacji, c. utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, d. przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, e. podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia, f. zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji, g. zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, h. ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, i. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie, j. zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji,

		k. ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży, l. zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, m. bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji, n. zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji. Kryteriami audytu są: • *Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;* • *Ustawa o Krajowym Systemie Cyberbezpieczeństwa;* • *Norma ISO/IEC 27001;* • *Norma PN-EN ISO/IEC 22301.* Wykonawca zobowiązany jest do dostarczenia Zamawiającemu: • raportu z audytu bezpieczeństwa systemu informacyjnego, • rekomendacji do wdrożenia w celu poprawy cyberbezpieczeństwa Zamawiającego.

System zarządzania bezpieczeństwem informacji

Usługa: „Opracowania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, zwanego dalej „SZBI", zgodnie z Rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (zwanym dalej „Rozporządzeniem KRI").

LP	**Parametr lub warunek**	**Minimalne wymagania**
1.	**Opis przedmiotu zamówienia**	1. Przedmiotem zamówienia jest: a) usługa opracowania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji dla Zamawiającego, zgodnie z warunkami określonymi w § 19 Rozporządzenia KRI oraz § 3 ust.

		2 pkt. 1 Regulaminu Konkursu Grantowego „Cyberbezpieczny Samorząd”. b) Przeprowadzenie szkolenia dla zespołu wdrożeniowego SZBI Zamawiającego c) Wsparcie merytoryczne zespołu wdrożeniowego SZBI Zamawiającego, 2. Dokumentacja musi obejmować bezpieczeństwo fizyczne (ochrona pomieszczeń, sprzętów, infrastruktury oraz personelu przed bezpośrednim działaniem czynników fizycznych i zdarzeń takich jak kradzież, nieuprawniony dostęp), bezpieczeństwo informatyczne (bezpieczeństwo systemu teleinformatycznego) oraz bezpieczeństwo osobowe i organizacyjne (stosowane procedury bezpieczeństwa). Dokumentacja musi obejmować następujące obszary: a. ustanowienie polityki bezpieczeństwa informacji oraz polityk tematycznych, b. aktualizacji regulacji wewnętrznych w zakresie bezpieczeństwa informacji, c. utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, d. przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, e. podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia, f. zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji, g. zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, h. ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,

		i. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie, j. zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji, k. ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży, l. zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, m. bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji, n. zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji. Dokumentacja musi uwzględniać wymagania następujących aktów prawnych oraz norm: • *Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;* • *Ustawa o Krajowym Systemie Cyberbezpieczeństwa;* • *Norma PN-EN ISO/IEC 27001:2023;* • *Norma PN-EN ISO/IEC 27002:2023;* • *Norma PN-EN ISO/IEC 22301:2020.* Wykonawca zobowiązany jest do dostarczenia Zamawiającemu: • Kompleksowej dokumentacji systemu zarządzania bezpieczeństwem informacji, • rekomendacji do wdrożenia w celu poprawy cyberbezpieczeństwa Zamawiającego. 3. W ramach usługi Wykonawca przeprowadzi szkolenie zespołu wdrożeniowego Zamawiającego w zakresie systemu zarządzania bezpieczeństwem informacji. 4. W ramach usługi Zamawiający zapewni wsparcie zespołu wdrożeniowego SZBI Zamawiającego, które odbywać się będzie

		w formie konsultacji, od poniedziałku do piątku, realizowanych w trakcie wdrożenia, poprzez bezpieczne formy komunikacji, takie jak: rozmowa telefoniczna, poczta e-mail, telekonferencja lub stacjonarnie w siedzibie Zamawiającego.

Szkolenie z podstaw cyberbezpieczeństwa dla pracowników

Usługa: „przeprowadzenia szkoleń w zakresie cyberbezpieczeństwa skierowanych do osób zatrudnionych u Zamawiającego w zakresie ataków cybernetycznych oraz metod obrony przed tymi atakami”

Przedmiotem zamówienia jest usługa wykonania szkoleń, zgodnie z wymogiem § 90 ust. 6 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

Liczba wymaganych jednostek szkoleniowych: 3 grupy po 2 tury

LP	**Parametr lub warunek**	**Minimalne wymagania**
1.	**Opis przedmiotu zamówienia**	1. Przedmiotem zamówienia jest przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa. Szkolenie musi być zrealizowane w siedzibie Zamawiającego. W ramach szkolenia, uczestnicy muszą otrzymać konkretne porady do zastosowania w praktyce, tak aby możliwe było ich sprawne i zarazem bezpieczne funkcjonowanie w cyberprzestrzeni. Program kursu musi skupiać się na najważniejszych w danym obszarze aspektach. Trenerzy muszą zapewnić wysoki poziom merytoryczny oraz komunikacyjny. Szkolenie ma zapoznać uczestnika z zagrożeniami, technikami ataków cyberprzestępczych oraz metodami socjotechnicznymi, ukierunkowanymi na osoby pracujące na co dzień przed komputerem. Uczestnicy mają dowiedzieć się jak działa rynek cyberprzestępczy, jakimi kwotami operują współcześni przestępcy, jakimi sposobami próbują uzyskać dostęp do sieci teleinformatycznej oraz jak w czasie rozmowy osobistej, telefonicznej lub mailowej oszuści potrafią wyłudzić informację od nieświadomego pracownika. Podczas szkolenia uczestnik ma być również edukowany ze skutków, dla których wykorzystywanie komputera służbowego do celów prywatnych zwiększa ryzyko ataku na całą organizację. Szkolenie musi być skierowane do każdego pracownika w organizacji bez względu na jego wiedzę i umiejętności informatyczne. Korzyści po szkoleniu:

		• zdobycie wiedzy obejmującej bezpieczne zarządzanie miejscem pracy oraz danymi • zdobycie wiedzy umożliwiającej ochronę przed atakami socjotechnicznymi Wykonawca zobowiązany jest do: • wydania imiennych zaświadczeń / certyfikatów dla każdego uczestnika, • zapewnienia dla każdego uczestnika materiałów szkoleniowych w formie elektronicznej. 2. Szczegółowy wykaz szkoleń: a) Szkolenie - podstawy cyberbezpieczeństwa dla pracowników (wymiar szkolenia: 2 h na turę), o następującej tematyce: • Co to jest cyberprzestępczość? • Opis funkcjonowania zorganizowanych grup cyberprzestępczych • Czy jestem atrakcyjnym „klientem” dla cyberprzestępcy? • Jakie zyski może mieć cyberprzestępca atakując moje dane? • Straty wynikające z udanego ataku • Rodzaje ataków skierowane w użytkowników Internetu • Jak bronić się przed cyberprzestępcami? • Spam jako niegroźny sposób na groźne ataki • Handel adresami e-mail • Kampanie Phishingowe • Opłacalność ataków DoS/DDoS wymierzonych w konkretną instytucję • Groźne ataki 0-day • Nieopłacona FV jako sposób przemycenia wirusa do naszego komputera • Ataki socjotechniczne - czyli niewinne „wyłudzanie” danych • Przekazywanie haseł dostępowych znajomym • Fizyczne bezpieczeństwo danych osobowych • Znaleziony pendrive na parkingu jako pozwolenie na atak dla cyberprzestępcy • Aktualne zagrożenia wynikające z wojny w Ukrainie • Podsumowanie szkolenia, pytania, dyskusja

Załącznik nr 1a do SWZ

Szkolenie z podstaw cyberbezpieczeństwa dla kadry kierowniczej

Usługa: „przeprowadzenia szkoleń w zakresie cyberbezpieczeństwa skierowanych do osób zatrudnionych u Zamawiającego w zakresie ataków cybernetycznych oraz metod obrony przed tymi atakami”

Przedmiotem zamówienia jest usługa wykonania szkoleń, zgodnie z wymogiem § 19 ust. 6 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Liczba wymaganych jednostek szkoleniowych: 2 grupy po 3 tury

LP	Parametr lub warunek	Minimalne wymagania
1.	**Opis przedmiotu zamówienia**	1.Przedmiotem zamówienia jest przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa. Szkolenia muszą być zrealizowane w siedzibie Zamawiającego. W ramach szkolenia, uczestnicy muszą otrzymać konkretne porady do zastosowania w praktyce, tak aby możliwe było ich sprawne i zarazem bezpieczne funkcjonowanie w cyberprzestrzeni. Program kursu musi skupiać się na najważniejszych w danym obszarze aspektach. Trenerzy muszą zapewnić wysoki poziom merytoryczny oraz komunikacyjny. Szkolenie ma zapoznać uczestnika z zagrożeniami, technikami ataków cyberprzestępczych oraz metodami socjotechnicznymi, ukierunkowanymi na osoby pracujące na co dzień przed komputerem. Uczestnicy mają dowiedzieć się jak działa rynek cyberprzestępczy, jakimi kwotami operują współcześni przestępcy, jakimi sposobami próbują uzyskać dostęp do sieci teleinformatycznej oraz jak w czasie rozmowy osobistej, telefonicznej lub mailowej oszuści potrafią wyłudzić informację od nieświadomego pracownika. Podczas szkolenia uczestnik ma być również edukowany ze skutków, dla których wykorzystywanie komputera służbowego do celów prywatnych zwiększa ryzyko ataku na całą organizację. Szkolenie musi być skierowane do każdego pracownika w organizacji bez względu na jego wiedzę i umiejętności informatyczne. Korzyści po szkoleniu: • zdobycie wiedzy obejmującej bezpieczne zarządzanie miejscem pracy oraz danymi

		• zdobycie wiedzy umożliwiającej ochronę przed atakami socjotechnicznymi Wykonawca zobowiązany jest do: • wydania imiennych zaświadczeń / certyfikatów dla każdego uczestnika, • zapewnienia dla każdego uczestnika materiałów szkoleniowych w formie elektronicznej. Szkolenie dla kadry zarządzającej z zakresu cyberbezpieczeństwa (wymiar szkolenia: 2 h na turę), o następującej tematyce: • Wstęp do bezpieczeństwa w cyberprzestrzenii; • Akty Prawne; • Krajowy System Cyberbezpieczeństwa; • Analiza ataków cybernetycznych; • Najpopularniejsze zagrożenia; • Przewodnik po metodach obrony instytucji; • Cyberbezpieczeństwo osobiste; • Postępowanie w pracy; • ABC higieny pracy w cyberprzestrzeni; • Bezpieczeństwo pracy zdalnej; • Ataki socjotechniczne - czyli niewinne „wyłudzanie” danych • Kampanie Phishingowe • Opłacalność ataków DoS/DDoS wymierzonych w konkretną instytucję • Aktualne zagrożenia wynikające z wojny w Ukrainie· • Dyskusja;

Testy socjotechniczne oraz penetracyjne

Usługa: „wykonania testów socjotechnicznych wobec pracowników Zamawiającego”

Przedmiotem zamówienia jest usługa wykonania prób ataków socjotechnicznych za pomocą poczty e-mail.

Załącznik nr 1a do SWZ

Ilość usług: 2

LP	Parametr lub warunek minimalny	Minimalne wymagania
1.	**Opis przedmiotu zamówienia**	I. Opis przedmiotu zamówienia: 1. Przedmiotem zamówienia jest przeprowadzenie: a) Testów socjotechnicznych pracowników Zamawiającego; Testy muszą być zrealizowane w wymiarze co najmniej 7 dni roboczych (tj. 16 godzin). Przeprowadzenie prób ataków socjotechnicznych polega na wywieraniu wpływu na ludzi i stosowaniu perswazji w celu oszukania ich tak, aby uwierzyli, że socjotechnik jest osobą o sugerowanej przez siebie, a stworzonej na potrzeby manipulacji, tożsamości. Dzięki temu socjotechnik jest w stanie wykorzystać swoich rozmówców, przy dodatkowym (lub nie) użyciu środków technologicznych, do zdobycia poszukiwanych informacji. Przeprowadzane próby w Organizacji miały na celu zweryfikowanie świadomości pracowników i zabezpieczeń przed atakami socjotechnicznymi. Testy muszą składać się z następujących faz: 1. Rozpoznanie (biały wywiad, obserwacja pracy pracowników). 2. Budowanie więzi i zaufania (użycie wewnętrznych informacji, podawanie się za kogoś innego, wspominanie nazwisk osób znanych ofierze, zgłoszenie potrzeby pomocy lub zasugerowanie posiadania władzy). 3. Wykorzystanie zaufania (prośba o informację lub działanie skierowana do ofiary). Testy muszą być przeprowadzone za pomocą aktualnych narzędzi, wykorzystujących najnowsze możliwości w zakresie symulacji złośliwych kampanii socjotechnicznych. Zakres testów: Próba wyrywkowego przeprowadzenia testów socjotechnicznych za pomocą e-maila - próba będzie polegała na wysłaniu wiadomości e-mail na adresy służbowe pracowników Organizacji i przeprowadzeniu ataku socjotechnicznego.

		Przygotowane przez testerów wiadomości muszą odpowiadać realnym atakom, realizowanym aktualnie przez przestępców. Wykonawca musi uwzględnić: • Ataki typu phishing, • Ataki typu spear phishing • Phishing typu whaling • Phishing przez klonowanie • Angler phishing Wykonawca zobowiązany jest do wykrycia (w stosunku do konkretnego adresu email): • otwieranych wiadomości, • otwieranych stron za pomocą linków umieszczonych w wiadomościach, • podawanych poświadczeń na stronach mających na celu wyłudzanie informacji, przygotowanych przez testerów, • pobieranie plików w popularnych formatach, takich jak „docx.", czy „xlsx", • otwierania plików w popularnych formatach, takich jak „docx.", czy „xlsx".

Szkolenia dla pracownika IT z obecnych i dostarczonych rozwiązań oraz z zakresu cyberbezpieczeństwa

Z uwagi na istniejącą infrastrukturę, Zamawiający wymaga dostarczenia dwóch voucherów na szkolenia on-line, które zostaną zrealizowane przez certyfikowaną jednostkę szkoleniową, zapewniającą odpowiednią jakość i zgodność z obowiązującymi standardami.

LP	**Parametr lub warunek minimalny**	**Minimalne wymagania**
1.	**Opis przedmiotu zamówienia**	1. MS-55371 Windows Server Administration 5-dniowy kurs prowadzony przez instruktora, stworzony dla pracowników sektora IT, którzy szukają doświadczenia w zarządzaniu Windows Server. Szkolenie przeznaczone dla osób

		odpowiedzialnych za zarządzanie tożsamością, zasobami, siecią i obliczanie za pomocą Windows Server. Podczas szkolenia, uczestnik pozna różne scenariusze, wymagania i opcje dostępne w Windows Server i dowie się jak je poprawnie zastosować w organizacji. Po ukończeniu szkolenia, uczestnik będzie umiał: Używać technik i narzędzi do administracji Windows Server Wdrażać usługi tożsamości Zarządzać infrastrukturą sieci Konfigurować serwery plików i jego zasoby Zarządzać maszynami wirtualnymi przy użyciu wirtualizacji Hyper-V i kontenerów Zarządzać systemem wysokiej niezawodności i rozwiązaniami odnowy Stosować funkcje bezpieczeństwa w celu zabezpieczenia krytycznych danych Konfigurować usługi zdalnego centrum pomocy technicznej Konfigurować wdrażanie infrastruktury pulpitu bazując na maszynach wirtualnych Wdrażać zdalny dostęp i usługi sieciowe Wdrażać monitorowanie usług i wydajności, oraz rozwiązywać powiązane problemy Wprowadzać aktualizacje i migracje związane z AD DS. i zasobami 2. FortiGate - kompleksowa ochrona każdej sieci I (CCE-FGI) Zdobycie umiejętności samodzielnej konfiguracji poszczególnych modułów bezpieczeństwa takich, jak: AntyVirus, AntySpam, WebFilter, IPS. Poznanie funkcjonalności modułu umożliwiającego kontrolę aplikacji. Zaprezentowanie dostępnych rozwiązań VPN. Szkolenie przeprowadzane w formie warsztatów ze znaczną liczbą praktycznych laboratoriów. Zakres tematyczny oraz część warsztatowa dostosowana zostanie do potrzeb uczestników szkolenia. Szkolenie oparte jest o FortiOS w wersji 6.x.