Załącznik nr 8 do SWZ

Szczegółowy opis przedmiotu zamówienia

Specyfikacja Warunków Zamówienia w przetargu Cyfrowa Gmina

W związku z już używanymi od lat w Urzędzie Gminy Aleksandrów Kujawski programami dziedzinowymi z zakresu wymiaru i księgowości zobowiązań podatkowych oraz wymiaru i księgowości opłat lokalnych Zamawiający zaplanował wdrożenie usług domenowych Active Directory, aby ujednolicić i podnieść poziom bezpieczeństwa tego systemu. W urzędzie wdrożony i używany jest również system wydruku podążającego i skanowania z różnych urządzeń. Jednostki komputerów – stanowiska pracy poszczególnych pracowników wyposażone są w system operacyjny rodziny Microsoft Windows. Wszystko to potwierdza, że Zamawiający powinien wdrożyć oprogramowanie serwerowe rodziny Microsoft Windows, aby już posiadane i planowane do zakupu elementy systemu teleinformatycznego poprawnie współpracowały ze sobą w ramach usługi Active Directory oferowanej przez serwerowy system operacyjny Microsoft Windows Serwer.

Zamawiający wymaga więc, aby wyspecyfikowane poniżej urządzenia posiadały zainstalowany i skonfigurowany system operacyjny z rodziny Microsoft Windows Serwer w możliwie najnowszej wersji lub były w 100% kompatybilne z takim systemem i bez problemów z nim współpracowały.

1. ZAKUP:

Serwer wraz z oprogramowaniem – 2 (dwie) sztuki

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2,5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	Zainstalowany jeden procesor min. 16-rdzeniowy, min. 2.4 GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 258 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	Minimum 256GB DDR4 RDIMM 3200MT/s w modułach o pojemności minimum 64GB, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Funkcjonalność pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
Gniazda PCI	- minimum jeden slot PCIe x16 generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 porty 25GbE SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) Wraz z karta należy dostarczyć minimum 2 przewody typu DAC o długości minimum 3 m Dodatkowa karta: Dwuportowa karta 32GB FC
Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD Zainstalowane 2 dyski SSD SATA o pojemności min. 480 GB, 6Gb, 2,5" Hot-Plug. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480 GB z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Kontroler RAID	Sprzętowy kontroler z pojemnością cache min. 4GB, możliwe konfiguracje poziomów RAID: 0,1,5,6,10,50,60, JBOD

System operacyjny/dodatkowe oprogramowanie	Windows Server 2022 Standard (licencja musi zostać dobrana tak aby przy zaproponowanych procesorach umożliwić uruchomienie min. 4 maszyn wirtualnych)
Wbudowane porty	4 x USB z czego nie mniej niż 1x USB 3.0, 2xVGA z czego jeden na panelu przednim.
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	Redundantne, Hot-Plug min. 800W każdy.
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.

Warunki gwarancji	Urządzenie objęte co najmniej 4 letnią gwarancją realizowaną na terenie Polski przez producenta lub wyznaczony przez producenta autoryzowany serwis, z czasem reakcji do następnego dnia roboczego od dnia przyjęcia zgłoszenia, możliwość zgłaszania awarii w każdy dzień tygodnia 24 godziny na dobę poprzez e-mail/platformę lub ogólnopolską dedykowaną linię telefoniczną. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Wraz z serwerami należy dostarczyć licencje kompatybilne z oprogramowaniem (systemem operacyjnym) serwera umożliwiające:

- **równoczesny** dostęp do serwera dla minimum **70 użytkowników**.
- **równoczesny** dostęp do serwera dla minimum **10 urządzeń.**
- **równoczesny** dostęp do pulpitu zdalnego serwera dla minimum **10 użytkowników.**

Macierz dyskowa – 1 (jedna) sztuka

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Do instalacji w standardowej szafie RACK 19”, macierz musi zajmować maksymalnie 2U i pozwalać na instalacje 24 dysków 2.5” (uzyskana ilość slotów na dyski może zostać osiągnięta poprzez stosowanie dodatkowych półek dyskowych, jednak całe zaproponowane rozwiązanie nie może przekroczyć 2U)
Kontrolery	Dwa kontrolery RAID pracujące w układzie active-active posiadające łącznie minimum osiem portów 32GB FC
Kable/wkładki	Wraz z macierzą należy dostarczyć min. 4 wkładki SFP 16GB FC oraz 4 kable MM LC-LC o długości minimum 2m
Cache	16GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, podtrzymywana bateryjnie przez min. 72h w razie awarii.

Dyski	Zainstalowane: 6 dysków Hot-Plug o pojemności 2.4TB SAS 12Gbps 2,5”, 6 dysków Hot-Plug o pojemności 1.92TB SSD SAS 12Gbps 2,5”, Możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych do łącznie minimum 276 dysków. Możliwość mieszania typów dysków w obrębie macierzy oraz pojedynczej półki.
Oprogramowanie/ /Funkcjonalności	Zarządzanie macierzą poprzez minimum przeglądarkę internetową, GUI oparte o HTML5. Macierz powinna zostać dostarczona z licencją umożliwiającą utworzenie minimum 512 LUN’ów oraz 1024 kopii migawkowych na całą macierz. Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane między rożnymi typami dysków. Możliwość wykorzystania dysków SSD jako cache macierzy, możliwość rozbudowy pamięci cache do min. 8TB poprzez dyski SSD. Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 8 hostów bez konieczności zakupu dodatkowych licencji. Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie asynchronicznym.
Wsparcie dla systemów operacyjnych/wirtualizatorów	• Windows Server 2022, 2019 and 2016 • RHEL 8.2 and 7.8 • SLES 15.2 and 12.5 • VMware 7.0 and 6.7 • Citrix Xen 8.x and 7.x • VMware vSphere (ESXi) • vCenter; SRM • Microsoft Hyper-V
Bezpieczeństwo	Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne.
Warunki gwarancji dla macierzy	Urządzenie objęte co najmniej 4 letnią gwarancją realizowaną na terenie Polski przez producenta lub wyznaczony przez producenta autoryzowany serwis, z czasem reakcji do następnego dnia roboczego od dnia przyjęcia zgłoszenia, możliwość zgłaszania awarii w każdy dzień tygodnia 24 godziny na dobę poprzez e-mail/platformę lub ogólnopolską dedykowaną linię telefoniczną. *D*yski twarde w macierzy dyskowej z co najmniej 3 letnią gwarancją realizowaną na terenie Polski przez producenta lub wyznaczony przez producenta autoryzowany serwis Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji macierzy. • Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu.

	• Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części I transportu. • W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim
Certyfikaty	Macierz musi być wyprodukowany zgodnie z normą ISO 9001:2015.

Zasilacz awaryjny UPS – 1 (jedna) sztuka

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Do instalacji w standardowej szafie RACK 19”
Wymiary	2 U
Poziom hałasu	Mniej niż 40 dB w odległości 1 m
Minimalna moc wyjściowa	3,0 kW / 3,0 kVA
Złącza wyjściowe	Co najmniej 2 x IEC 320 C19, co najmniej 8 x IEC 320 C13
Napięcie wyjściowe	230V
Topologia	Włączony / podwójna konwersja
Typ przebiegu	Sinusoida
Minimalny czas przełączania	6 ms
Minimalny czas podtrzymania dla obciążenia 50% / 100%	9 min / 3min
Typ gniazda wejściowego	IEC 320 C20
Komunikacja i zarządzanie	Złącze USB, port szeregowy, port RJ-45. Panel sterowania: wyświetlacz statusu led ze wskaźnikiem pracy online: zasilanie akumulatorowe: wskaźniki wymień baterię i przeciążenie, Wielofunkcyjna konsola sterownicza i informacyjna lcd. Alarm dźwiękowy: alarm przy zasilaniu akumulatora: alarm przy bardzo niskim poziomie naładowania akumulatora: konfigurowalne opóźnienia. Awaryjny wyłącznik zasilania. Analiza uszkodzeń akumulatorów z funkcją wczesnego ostrzegania. Okresowy autotest akumulatora. Zdalne zarządzanie zasilaniem podtrzymywacza napięcia przez sieć. Prognozowanie daty wymiany akumulatora.
Certyfikaty i zgodności z normami	CE, EAC, EN/IEC 62040-1, EN/IEC 62040-2, ENERGY STAR, UL 1778
Gwarancja	Urządzenie UPS z co najmniej 2 letnią gwarancją realizowaną na terenie Polski przez producenta lub wyznaczony przez producenta autoryzowany serwis (akumulatory według specyfikacji producenta z co najmniej 2 lata realizowanej na terenie Polski przez producenta lub wyznaczony przez producenta autoryzowany serwis).

Przełącznik sieciowy – 2 (dwie) sztuki

Parametr	Charakterystyka (wymagania minimalne)
Ilość i rodzaj portów	12 portów SFP+ oraz 12 portów 10GBaseT niezależne
Chłodzenie urządzenia	od przodu do tyłu obudowy
Montaż	Wysokość 1 U, możliwość ułożenia przy sobie dwóch urządzeń w szafie RACK 19”
Tablica MAC	min. 16 K
Bufor	32 Mb
Średni czas bezawaryjnej pracy	MTBF min. 192 tys. godzin
Wydajność	min. 357 Mp/s
Przepustowość	min. 480 Gp/s
Przekazywanie	Store-and-forward
Zarządzanie, dostęp	Port USB, miniUSB, Port zarządzania poza pasmem, Web GUI, HTTPs, CLI, Telnet, SSH, SNMP, MIB RSPAN, Radius, TACACS+, DiffServ
Zarządzenie, kontrola przepływu danych, dostępu, zarządzanie i konfiguracja sieci i urządzeń	Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram, IPv4/Ipv6 Multicast filtering, IGMPv3 MLDv2 Snooping, ASM & SSM, IGMPv1, v2 Querier, Auto-VoIP, Auto-iSCSI, Policy-based routing (PBR), LLDP-MED, Spanning Tree, Green Ethernet, STP, MTP, RSTP, PVISTP, BPDU/STRG Root Guard, EEE (802.3az), GVRP/GMRP, Q in Q, Private VLAN, DOT1X, MAB, DHCP Snooping, DHCPv6 Snooping, Dynamic ARP, Inspection, IP Source Guard
Sieć gościnna – Captive Portal	tak
Procesor	min. 800 MHz
Pamięć	1 GB RAM, min. 256 MB Flash
Min ilość obsługiwanych VLAN	4000
DHCP Server	2000 rezerwacji
Wsparcie dla sFlow	tak
Minimalna ilość przełączników w stosie	8
Możliwość łączenia w stos za pomocą interfejsów 10Gb/s	tak
Możliwość łączenia przełączników w stos w konfiguracji:	pierścień, podwójny pierścień, mesh
Agregacja łączy, interfejsów	Non-stop forwarding (NSF), Distributed Link Aggregation (LAGs across the stack),
Ilość interfejsów IP	128
Sieci wirtualne	Double VLAN Tagging (QoQ),

Routing między warstwami, sieciami, urządzeniami	PIM-DM (Multicast Routing – dense mode), PIM-DM (Ipv6), PIM-SM (Multicast Routing – sparse mode), PIM-SM (Ipv6), RIPv2, OSPFv2, RFC 2328, RFC 1583, OSPFv2 min. sąsiadów 400, OSPFv3 min. Sąsiadów 400, OSPFv3 min. Sąsiadów na interfejs 100, UDLD, LLPF, MMRP
Wysyłanie alertów i komunikatów na e-mail	tak
Ilość list kontroli dostępu ACL	min. 100
Ilość reguł na listę	min. 1023 na wejściu i 511 na wyjściu
Standardy EMC	CE, FCC 15 A, VCCI A, A EN 55022, (CISPR 22) A, EN 50082-1, EN 55024
Gwarancja	Urządzenie objęte co najmniej 4 letnią gwarancją realizowaną na terenie Polski przez producenta lub wyznaczony przez producenta autoryzowany serwis, z czasem reakcji do następnego dnia roboczego od dnia przyjęcia zgłoszenia, możliwość zgłaszania awarii w każdy dzień tygodnia 24 godziny na dobę poprzez e-mail/platformę lub ogólnopolską dedykowaną linię telefoniczną w systemie door-to-door. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji.

2. W ramach zamówienia przeprowadzone zostaną następujące prace wdrożeniowe, wsparcie serwisowe, instalacyjne, konfiguracyjne sprzętu, szkolenia oraz dokumentację:

A) Wdrożenie/konfiguracyjne:

- Projekt realizacyjny:
  - Analiza przedwdrożeniowa
  - Przedstawienie szczegółowej architektury wdrożenia
  - Dokumentacja projektowa
- Przygotowanie środowiska zgodnie z dokumentacją projektową:
  - Instalacja fizyczna serwerów, switchy, macierzy oraz UPS
  - Aktualizacja oprogramowania systemowego urządzeń, jeśli wymagane
  - Konfiguracja przełączników LAN - stack, konfiguracja do 3 VLAN
- Wdrożenia klastra HA
  - Instalacja oprogramowania serwerowego na dostarczanych serwerach
  - Konfiguracja sieci i klastra HA w oparciu o środowisko Microsoft Hyper-V
  - Testy poprawności konfiguracji klastra HA
- Konfiguracja domeny :
  - Utworzenie kontrolera domeny,
  - Dopisanie użytkowników do domeny
  - Konfiguracja 2 przykładowych polityk GPO
  - Dodanie 3 przykładowych urządzeń do domeny
- Dokumentacja powdrożeniowa
- Odbiór prac przez Zamawiającego
- Omówienie sposobu zarzadzania domeną i klastrem HA, oraz UTM w ramach rozwiązania na podstawie przeprowadzonego wdrożenia w zakresie minimum 10 godzin

B) Wsparcie serwisowe

Wykonawca zagwarantuje wsparcie serwisowego dla lokalnych administratorów IT w wymiarze 8 godzin pracy, do wykorzystania w przeciągu 1 miesiąca. Wsparcie Wykonawcy będzie stanowić bezpośrednie wsparcie działu IT w problemach które nie będą mogły z przyczyn technicznych być rozwiązane lokalnie.

C) Szkolenia:

- Szkolenie z Windows Server + zarządzanie domeną + HyperV- 2 dni (dla dwóch osób)

- Szkolenie z konfiguracji zapory sieciowej typu UTM (Fortigate) – 2 osoby

D) Dokumentacja: przygotowanie / ustanowienie i wdrożenie

I. SZBI z uwzględnieniem wymagań i norm w tym:

1. Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz wsparcie merytoryczne w procesie wdrożenia.

2. Opracowanie dokumentacji SZBI przez osoby posiadające odpowiednie kwalifikacje w tym co najmniej certyfikat Audytora wiodącego Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO 27001 oraz weryfikacja i aktualizacja już funkcjonujących Polityk Bezpieczeństwa Informacji (PBI) oraz Instrukcji Zarządzania Systemem Informatycznym (IZSI).

3. Przeprowadzenie szkolenia i warsztatów uwzględniających konsultacje w zakresie doskonalenia, monitorowania i wdrożenia zmian w SZBI.

4. Przygotowanie i przeprowadzenie szkolenia i warsztatów z zakresu Systemu Zarządzania Bezpieczeństwem Informacji dla pracowników Urzędu, obejmujących co najmniej następujące obszary:

4.1. omówienie podstawowych zasad bezpieczeństwa informacji wynikających z SZBI;

4.2. objaśnienie definicji powiązanych z systemem zarządzania bezpieczeństwem informacji;

4.3. konteksty i potrzeby stron z uwzględnieniem wymagań prawnych i regulacyjnych;

4.4. zakres i polityka Systemu Zarządzania Bezpieczeństwem Informacji;

4.5. cel Systemu Zarządzania Bezpieczeństwem Informacji;

4.5 klasyfikacja informacji;

4.6 metodyka szacowania ryzyka w ramach Systemu Zarządzania Bezpieczeństwem Informacji;

4.7. metodyka szacowania szansę w ramach Systemu Zarządzania Bezpieczeństwem Informacji;

4.8. omówienie zasad i zabezpieczeń w ramach deklaracji stosowania;

4.9. nadzór nad udokumentowana informacja;

4.10. przeglądy Oraz doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji;

4.11. metodyka ewidencjonowania aktywów informacyjnych;

4.12. zarządzanie dostępem użytkowników;

4.13. Omówienie technik, standardów i oprogramowania wspomagającego kryptografię;

4.14. polityki bezpieczeństwa informacji;

4.15. budowanie procedur w ramach Systemu Zarządzania Bezpieczeństwem Informacji;

4.16. odpowiedzialność za naruszenie zasad SZBI;

4.17. zasady zgłaszania i reagowania na incydenty;

4.18. bezpieczeństwo informatyczne w miejscu pracy.

Szkolenia dla pracowników zostaną przeprowadzone w formie stacjonarnej/online. Szkolenie zrealizowane będzie w dwóch grupach: pracownicy administracyjni i kadra kierownicza. Celem części warsztatowej jest opracowanie przykładowych wzorów polityk, procedur i ram Systemu Zarządzania Bezpieczeństwem Informacji:

a. Przewodnik SZBI;

b. Definicje SZBI;

c. Konteksty i potrzeby stron;

d. Zakres i Polityka SZBI;

e. Cele SZBI;

f. Szacowanie ryzyka z uwzględnieniem zabezpieczeń wynikających z Deklaracji stosowania SZBI;

g. Deklaracja stosowania SZBI;

h. Nadzór nad udokumentowaną informacją;

i. Protokół z przeglądu zarządzania;

j. Rejestr niezgodności;

k. Ramy ewidencji aktywów informacyjnych;

l. Zarządzanie dostępem użytkowników;

m. Klauzule umowne: odpowiedzialności stron, zakończenie zatrudnienia lub zmiana zakresu umowy, bezpieczne przesyłanie informacji, bezpieczeństwo usług sieciowych, zapisy związane z poufnością informacji, wymagania odnoszące się do ryzyk;

n. Ogólne techniki, standardy kryptograficzne;

o. Ogólne standardy bezpieczeństwa informacji;

p. Ramy rejestru incydentów;

q. Procedury i polityki bezpieczeństwa informacji: Procedury szyfrowania transmisji danych w pracy zdalnej, Polityka pracy zdalnej i stosowania urządzeń mobilnych, Procedury weryfikacji kandydatów do pracy, Procedury postępowań dyscyplinarnych, Ewidencja aktywów informacyjnych, Polityka zarządzania aktywami informacyjnymi, Polityka klasyfikacji informacji, Procedury oznaczania informacji zgodnie z klasyfikacją, Procedury postępowania z aktywami informacyjnymi, Procedury zarządzania nośnikami informacji, Polityka kontroli dostępu, Procedury nadawania i odbierania uprawnień, Zarządzanie dostępem użytkowników, Polityka haseł, Procedury bezpiecznego logowania, Polityka stosowania zabezpieczeń kryptograficznych, Procedury pracy w obszarach bezpiecznych, Procedury konserwacji sprzętu, Procedury przekazywania sprzętu, Procedury zarządzania sprzętem komputerowym, Polityka czystego biurka i czystego ekranu, Polityka zarządzania zmianą, Procedury monitorowania i wykorzystania zasobów, Procedury separacji środowisk pracy, Procedury ochrony przed szkodliwym oprogramowaniem, Polityka kopii zapasowych, Procedury tworzenia kopii zapasowych, Procedury rejestrowania zdarzeń i monitorowania, Procedury nadzoru nad instalacją oprogramowania, Procedury instalowania oprogramowania, Procedury zabezpieczenia audytu systemów informacyjnych, Polityka monitorowania sieci w trybie ciągłym, Polityka przesyłania informacji, Procedury przesyłania informacji, Polityka pozyskiwania, rozwoju i utrzymania systemów, Procedury przeglądu i kontroli zmian w systemach, Polityka bezpieczeństwa informacji w relacjach z dostawcami, Procedury zarządzania incydentem, Polityka ciągłości działania, Procedury zachowania ciągłości działania, Procedury zachowania zgodności, Procedury przeglądu bezpieczeństwa informacji;

r. Przegląd polityk bezpieczeństwa informacji (Audyty wewnętrzne): Program audytów, Raport z audytu wewnętrznego.

II. <u>Polityka Bezpieczeństwa</u>

III. <u>Instrukcja Zarządzania Systemem Teleinformatycznym</u>

Szkolenie oraz wzory polityk, procedur i ram Systemu Zarządzania Bezpieczeństwem Informacji powinny – zgodnie z §20 ust. 2 pkt 14 KRI - odnosić się do SZBI wdrożonego zgodnie z Polskimi Normami PN-ISO/IEC 27001 - w odniesieniu do SZBI, PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem, PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.