Cyberbezpieczne Wodociągi

Program „Cyberbezpieczne Wodociągi” (KPO, Inwestycja C3.1.1)

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Kompleksowe usługi w zakresie cyberbezpieczeństwa oraz dostawa i wdrożenie urządzeń cyberbezpieczeństwa sieci OT/IT

Zamawiający: Przedsiębiorstwo Wodociągów i Kanalizacji Dolina Bobru Sp. z o.o., ul. Łasicka 17, 59-700 Bolesławiec, NIP 6120004423, REGON 230051249, KRS 0000295640 (forma własności: jednostki samorządu terytorialnego lub samorządowe osoby prawne).

Kontakt: e-mail e.gorczyca@pwik.boleslawiec.pl; tel. +48 75 734 10 00; ePUAP /PWiKwBoleslawcu/domyslna.

Osoba do kontaktu: **Agnieszka Turowska, Specjalista ds. technicznych, tel. 75 734 10 20, e-mail: a.turowska@pwik.dolinabobru.eu**

Znak sprawy: **PWiK/23/JRP/2026** Data publikacji: **04 września 2026 r.**

Niniejszy OPZ stanowi Załącznik nr 1 do Zapytania ofertowego i obejmuje całość przedmiotu zamówienia (usługi organizacyjne oraz dostawy i wdrożenie urządzeń OT/IT). Obejmuje: Część A — postanowienia ogólne; Część B — dostawy (urządzenia OT/IT); Część C — zakres usługowy (organizacyjny, Zadania 1–4); Część D — usługi wdrożeniowe urządzeń; Część E — zbiorcze zestawienie pozycji do wyceny. Podane parametry i wymagania są minimalne — Wykonawca może zaoferować parametry lepsze. Ocena metodą „spełnia / nie spełnia”.

KRAJOWY PLAN ODBUDOWY | Rzeczpospolita Polska | Sfinansowane przez Unię Europejską NextGenerationEU | CENTRUM PROJEKTÓW POLSKA CYFROWA

CZĘŚĆ A — POSTANOWIENIA OGÓLNE

A.0. Opis ogólny przedmiotu zamówienia

Przedmiotem zamówienia jest podniesienie poziomu cyberbezpieczeństwa Zamawiającego poprzez inwestycję w środki trwałe, oprogramowanie oraz kompetencje pracowników w trzech wzajemnie powiązanych obszarach: organizacyjnym, kompetencyjnym oraz technicznym (IT i OT). Przedsięwzięcie obejmuje realizację kompletu zadań usługowych (organizacyjnych) wraz z dostawą sprzętu i urządzeń z odpowiednim oprogramowaniem oraz ich wdrożeniem — zgodnie z charakterystyką i wymaganiami niniejszego OPZ. Zamówienie realizowane jest w ramach projektu grantowego „Cyberbezpieczne Wodociągi" (KPO, Inwestycja C3.1.1 — Cyberbezpieczeństwo), nr naboru **KPOD.05.10-CW.01-001/25**, nr umowy o powierzenie grantu **KPOD.05.10-CW.01-001/25/0225/KPOD.05.10-CW.01-001/25/2026 z dnia 18.03.2026 r.**.

Poszczególne obszary są wzajemnie powiązane: procedury organizacyjne (SZBI, ciągłość działania) znajdują odzwierciedlenie w konfiguracji i eksploatacji dostarczanych systemów oraz w szkoleniach pracowników, dzięki czemu efekt w postaci podniesienia cyberbezpieczeństwa osiągany jest łącznie. Zamawiający wymaga realizacji zgodnie z zasadami horyzontalnymi KPO (m.in. zasada „nie czyń poważnych szkód" DNSH, równość szans i niedyskryminacja, dostępność) — na zasadach określonych w Zapytaniu ofertowym, wzorze umowy i formularzu ofertowym, bez uszczegóławiania ponad zobowiązania wynikające z wniosku o dofinansowanie.

A.1. Klauzula równoważności i wymagania ogólne dla dostaw

Zgodnie z art. 99 ust. 5 i 6 oraz art. 101 ust. 4 ustawy Prawo zamówień publicznych, w każdym miejscu, w którym w niniejszym OPZ przywołano znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces charakteryzujący produkty lub usługi, odwołania te służą wyłącznie doprecyzowaniu przedmiotu zamówienia. Zamawiający każdorazowo dopuszcza zaoferowanie rozwiązania równoważnego — każde takie odniesienie należy odczytywać łącznie ze sformułowaniem „lub rozwiązanie równoważne". Ciężar wykazania równoważności spoczywa na Wykonawcy.

1. Sprzęt fabrycznie nowy, nieużywany, wolny od wad fizycznych i prawnych, nie może pochodzić z ekspozycji, zwrotów ani rynku wtórnego.
2. Sprzęt i oprogramowanie muszą pochodzić z legalnego, autoryzowanego kanału dystrybucji producenta, przeznaczonego na rynek Rzeczypospolitej Polskiej.
3. Oznaczenie CE oraz zgodność z obowiązującymi normami (m.in. RoHS, kompatybilność elektromagnetyczna), pełna identyfikowalność producenta (numer seryjny).
4. Dostawa obejmuje komplet elementów montażowych, okablowania i akcesoriów niezbędnych do uruchomienia.

Okresy gwarancji i wsparcia określono indywidualnie dla poszczególnych pozycji w Części B. Usługi wdrożeniowe urządzeń, odbiory oraz dokumentacja powykonawcza — Część D; zakres usługowy (organizacyjny) — Część C. Wszystkie wymagania oznaczone jako obowiązkowe muszą być spełnione łącznie; ocena spełnienia wymagań następuje metodą „spełnia / nie spełnia".

A.2. Źródło finansowania, kwalifikowalność wydatków i termin realizacji

Zamówienie realizowane jest w ramach programu „Cyberbezpieczne Wodociągi", finansowanego ze środków Krajowego Planu Odbudowy i Zwiększania Odporności (KPO), Inwestycja C3.1.1. Dofinansowanie do 100% kosztów kwalifikowalnych netto; kwalifikowalne są wyłącznie koszty netto, podatek VAT stanowi wydatek niekwalifikowalny. Okres kwalifikowalności wydatków: od 1 stycznia 2025 r. do 15 grudnia 2026 r.

Termin realizacji: rozpoczęcie od dnia podpisania umowy; zakończenie całości przedmiotu zamówienia do 15 grudnia 2026 r.

A.3. Kody CPV

1. Główny: 72000000-5 — Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia.
2. Dodatkowy: 72224000-1 — Usługi doradcze w zakresie zarządzania projektem.
3. Dodatkowy: 79421200-3 — Usługi w zakresie audytów projektów.
4. Dodatkowy: 80511000-9 — Usługi szkolenia personelu.
5. Dodatkowe — dla części dostawowej (urządzenia, oprogramowanie i licencje).
   a) 48820000-2 — Serwery (serwery wirtualizacyjne, serwer kopii zapasowych).
   b) 30200000-1 — Urządzenia komputerowe (szafa RACK 19", elementy montażowe i akcesoria).
   c) 32420000-3 — Urządzenia sieciowe (firewalle UTM/NGFW, przełączniki przemysłowe, routery LTE, system IPS, dioda danych).
   d) 30233000-1 — Urządzenia do przechowywania i odczytu danych (napęd taśmowy LTO-7).
   e) 30234000-8 — Nośniki do przechowywania (nośniki i taśma czyszcząca LTO-7).
   f) 48620000-0 — Systemy operacyjne (Microsoft Windows Server 2025 Standard).
   g) 48710000-8 — Pakiety oprogramowania do kopii zapasowych i odzyskiwania (oprogramowanie backupu klasy Enterprise).
   h) 48730000-4 — Pakiety oprogramowania zabezpieczającego (MFA, PAM, VMP, SIEM).
   i) 48000000-8 — Pakiety oprogramowania i systemy informatyczne (system monitoringu IT/OT, wirtualizacja oraz pozostałe licencje).

CZĘŚĆ B — DOSTAWY (urządzenia, oprogramowanie, licencje)

B.1. Firewalle sprzętowe UTM „Next-Gen” (klaster HA) — 2 szt.

Dostawa 2 (dwóch) fabrycznie nowych urządzeń UTM „Next-Gen” do pracy w klastrze wysokiej dostępności (HA), z 12-miesięcznym wsparciem producenta (aktualizacje, wersja business) dla każdego urządzenia. Parametry minimalne:

1. Typ / model referencyjny: firewall „Next-Gen” Rack Appliance — Deciso DEC2770 (z systemem OPNsense, wersja business) lub równoważne.
2. Obudowa: Rack 19", maks. 1U.
3. Porty: min. 2× SFP+; min. 7× 2,5 GbE RJ45; 1× USB 3.0; port konsolowy.
4. Wyposażenie: SSD M.2 min. 256 GB; min. 8 GB DDR4; CPU min. 4 rdzenie / 8 wątków.
5. Parametry fizyczne: maks. 43,8 × 482,6 × 242 mm; masa maks. 2,75 kg; pobór mocy typ. ok. 20 W.
6. Zgodność: co najmniej FCC part 15 Class A, CE, RoHS.
7. Wydajność — firewall: throughput min. 10 Gbps; min. 830 Kpps; port-to-port maks. 8,5 Gbps oraz 719 Kpps; sesje równoległe min. 7 000 000; nowe połączenia/s min. 50 000; opóźnienie średnio ≤ 150 µs.
8. Wydajność — VPN: IPsec (AES-256-GCM-16) min. 1,2 Gbps oraz min. 178 Kpps.
9. Funkcje (F.01–F.14): Stateful Firewall L3–L7; IPS; Application Control; SSL Deep Inspection; IPsec i SSL-VPN; Secure SD-WAN; routing statyczny/dynamiczny (BGP/OSPF/RIP), NAT; VLAN 802.1Q i VRF; HA Active-Passive; integracja z AP i przełącznikami; MFA/2FA dla administracji i VPN; GUI HTTPS i CLI; logowanie syslog.

KRAJOWY PLAN ODBUDOWY | Rzeczpospolita Polska | Sfinansowane przez Unię Europejską NextGenerationEU | CENTRUM PROJEKTÓW POLSKA CYFROWA

10. Ochrona L7: kontrola i blokowanie aplikacji/protokołów w czasie rzeczywistym; filtrowanie WWW (kategorie + reputacja chmurowa); ochrona przed malware/phishingiem/botnetami/exploitami; inspekcja TLS/SSL; polityki użytkownika (AD/LDAP/Captive Portal); raportowanie w czasie rzeczywistym; opcjonalna integracja z chmurowym panelem centralnego zarządzania bez dodatkowych opłat.
11. Zakres ochrony: min. 50 urządzeń z możliwością wykluczania.
12. Wsparcie (W.01–W.06): 12 miesięcy wsparcia producenta (aktualizacje, wersja business).
13. Model licencyjny (KK.01–KK.03): wszystkie funkcje zainstalowane i gotowe do konfiguracji; cena obejmuje dostawę, akcesoria i 12-mies. wsparcie bez dodatkowych kosztów.
14. Dostawa: elementy montażowe Rack 19", kable, karta katalogowa, dokumentacja wsparcia, wszystkie klucze licencyjne.

B.2. Przełączniki przemysłowe zarządzalne z oprogramowaniem do zarządzania — 5 szt.

Dostawa 5 (pięciu) fabrycznie nowych przełączników zarządzalnych do automatyki przemysłowej, gwarancja 60 miesięcy, wraz z licencją oprogramowania do zdalnego monitoringu i diagnostyki (auto wykrywanie topologii, monitorowanie podsieci, alarmowanie, raportowanie, zdalna konfiguracja via SNMP), On-Premises. Parametry minimalne:

1. Typ / model referencyjny: przełącznik przemysłowy — MOXA EDS-4008-2GT-2GS-HV-T z oprogramowaniem MX View lub równoważne.
2. Porty: min. 6× 10/100BaseT(X) RJ45 oraz min. 2× 100/1000Base SFP.
3. Normy: IEC 62443-4-1 oraz IEC 62443-4-2.
4. Standardy: IEEE 802.3/802.3u/802.3ab/802.3z; 802.3x; 802.3ad (LACP); 802.1Q; 802.1D-2004 (STP); 802.1w (RSTP); 802.1p; 802.1X.
5. Zarządzanie: IPv4/IPv6, flow control, back-pressure, DHCP Server/Client, ARP/RARP, LLDP, fiber check, port mirroring (SPAN/RSPAN), SMTP, SNMP Trap/Inform, SNMP v1/v2c/v3, RMON, TFTP, SFTP, HTTP, HTTPS, Telnet, Syslog, Private MIB.
6. Redundancja L2: STP, RSTP, Turbo Ring v2, Turbo Chain, Ring Coupling, Dual Homing, Link Aggregation, MSTP, MRP.
7. Protokoły przemysłowe: EtherNet/IP, Modbus TCP, PROFINET IO Device.
8. Bezpieczeństwo: broadcast storm protection, rate limit, trusted access control, static port lock, MAC sticky, HTTPS/SSL, SSH, RADIUS, TACACS+, polityka logowania/haseł, ACL, DHCP snooping.
9. Oprogramowanie do zarządzania: autowykrywanie topologii, monitorowanie podsieci, alarmowanie, raportowanie, zdalna konfiguracja via SNMP; interfejs WWW; instalacja On-Premises.
10. Gwarancja: 60 miesięcy.

B.3. Routery przemysłowe LTE (IEC 62443-4-2 SL1) — 17 szt.

Dostawa 17 (siedemnastu) routerów LTE zgodnych z IEC 62443-4-2 SL1 z oprogramowaniem do zarządzania (centralne zarządzanie, dashboardy, VPN WireGuard/DMVPN/GRE, zero-touch provisioning, masowa aktualizacja, audyt), On-Premises. Licencja min. 17 urządzeń. Parametry minimalne:

1. Typ / model referencyjny: router LTE zgodny z IEC 62443-4-2 SL1 — Advantech ICR-2834-S1 z platformą WebAccess/DMP lub równoważne.
2. Porty: min. 2× 10/100BaseT(X) RJ45; min. 2× slot SIM; min. 2× RS-232/RS-485; min. 4× DI i 2× DO.
3. Normy: IEC 62443-4-2 level 1 (SL1).
4. Standardy VPN: OpenVPN, WireGuard, IPsec, GRE.
5. Funkcje sieciowe: DHCP, NAT, VRRP, VLAN, SNMP, NTP, DynDNS, firewall, DMZ.

KRAJOWY PLAN ODBUDOWY | Rzeczpospolita Polska | Sfinansowane przez Unię Europejską NextGenerationEU | CENTRUM PROJEKTÓW POLSKA CYFROWA

6. Protokoły przemysłowe: Modbus RTU/TCP, DNP3, MQTT, IEC 101/104.
7. Bezpieczeństwo: secure boot; system plików tylko do odczytu; wykrywanie włamań (AIDE); silne algorytmy (SHA-256+, RSA-3072+, ED25519); utwardzony OS; polityka silnych haseł (min. 12 znaków, 3 klasy) i blokada konta; wyłączone FTP/Telnet, dostęp administracyjny wyłącznie przez HTTPS.
8. Oprogramowanie do zarządzania: centralne zarządzanie; dashboardy z mapowaniem GPS; zarządzanie VPN (WireGuard/DMVPN/GRE); zero-touch provisioning; cyfrowy bliźniak; masowa aktualizacja i profile konfiguracyjne (eksport/import CSV); 2FA, szyfrowanie PKI, kontrola uprawnień; audyt i historia zdarzeń; multi-tenancy; dostępność SaaS i On-Premises — dla podwyższonych wymagań bezpieczeństwa wdrożenie On-Premises.

B.4. Przemysłowy system IPS z DPI — 2 szt.

Dostawa 2 (dwóch) przemysłowych systemów IPS z DPI dla protokołów przemysłowych, z ochroną sygnaturową i konfigurowalnym trybem bypass. Parametry minimalne:

1. Typ / model referencyjny: TXOne Networks EdgeIPS 103F lub równoważne.
2. Porty: min. 2× 10/100/1000BaseT(X) RJ45; min. 1× port zarządzania.
3. Przepustowość: min. 850 Mbps (IMIX) / 1,2 Gbps+ (UDP 1518 B).
4. Opóźnienie: < 500 µs (średnio, ruch mieszany).
5. Protokoły ICS: Modbus, EtherNet/IP, CIP, FINS, S7Comm, S7Comm+, SECS/GEM, IEC 61850-MMS, IEC-104.
6. Funkcjonalność: dwukierunkowa ochrona zasobów (HMI, PLC); transparentne monitorowanie; aktualizacja sygnatur; wykonanie przemysłowe; konfigurowalny LAN Bypass; wdrożenie in-line lub pasywne (SPAN); wykrywanie assetów i protokołów; autolearning; tryby IDS/IPS; DPI; współpraca z SIEM/SOC.

B.5. Dioda danych — jednokierunkowa separacja OT→IT z integracją SCADA — 1 szt.

Dostawa i konfiguracja 1 szt. diody sieciowej zapewniającej jednokierunkowy transfer danych OT→IT z oprogramowaniem towarzyszącym oraz oprogramowaniem dla systemu klasy TelWin SCADA (lub równoważnego), wraz z usługą wdrożenia.

1. Typ / model referencyjny: **TXOne Networks | EdgeIPS 103F lub równoważne**
2. Jednokierunkowy przepływ danych: wyłącznie OT→IT; architektura wyklucza przepływ zwrotny (IT→OT) na poziomie fizycznym. Niedopuszczalna realizacja wyłącznie programowa (firewall/ACL/filtry) — wymagana fizyczna, sprzętowa separacja.
3. Sprzętowa realizacja separacji: brak jakiejkolwiek ścieżki sygnałowej (elektrycznej/optycznej) umożliwiającej transmisję zwrotną IT→OT.
4. Protokół transmisji: UDP lub równoważny protokół bezpołączeniowy, jednokierunkowy, bez ACK po stronie nadawcy.
5. Obsługa danych procesowych: wartości pomiarowe (PLC, RTU, przeliczniki, liczniki), stany alarmowe i zdarzenia, dane archiwalne/historyczne, dane diagnostyczne/statusowe — bez ingerencji z IT w dane/konfigurację SCADA po stronie OT.
6. Niezależność od systemu SCADA: zdolność pracy niezależnie od konkretnego systemu SCADA po stronie OT; niedopuszczalne urządzenia wymagające dedykowanego oprogramowania pośredniczącego (middleware) po stronie SCADA, nieobjętego standardową licencją systemu eksploatowanego przez Zamawiającego.
7. Kompatybilność SCADA: potwierdzone, produkcyjne współdziałanie z systemem klasy TelWin SCADA (TEL-STER Sp. z o.o.) lub równoważnym, bez modyfikacji istniejącego SCADA i bez wpływu na jego dostępność/stabilność.

KRAJOWY PLAN ODBUDOWY | Rzeczpospolita Polska | Sfinansowane przez Unię Europejską NextGenerationEU | CENTRUM PROJEKTÓW POLSKA CYFROWA

8. Definicja systemu równoważnego (SCADA): akwizycja danych z użyciem co najmniej Modbus RTU/TCP, DNP3, IEC 60870-5-104, OPC UA (lub równoważnych); dane odbieralne bezpośrednio bez middleware po stronie OT; archiwizacja z rozdzielczością ≤ 1 s; środowisko MS Windows 64-bit; architektura klient-serwer z rozproszeniem w LAN.
9. Wykonanie przemysłowe: praca 24/7 w środowisku o podwyższonych zakłóceniach EMC (stacje uzdatniania, węzły cieplne, stacje redukcyjno-pomiarowe, obiekty energetyczne/gazownicze).
10. EMC: certyfikat akredytowanej jednostki, co najmniej EN 55032, EN 55035, EN IEC 61000 (lub równoważne).
11. Interfejsy: co najmniej dwa fizycznie odseparowane (wejściowy OT, wyjściowy IT); konstrukcja uniemożliwia odwrócenie kierunku transmisji przez zmianę konfiguracji lub przełożenie kabli.
12. Certyfikacja produktu: Zamawiający nie wymaga na etapie składania ofert certyfikacji bezpieczeństwa produktu wg IEC 62443 ani Common Criteria (brak takiego obowiązku w NIS2 i uoKSC); zastrzega natomiast prawo żądania na etapie oceny ofert dokumentacji technicznej potwierdzającej sprzętową realizację jednokierunkowego przepływu danych.
13. Granice zakresu (poza dostawą diody, po stronie Zamawiającego): segmentacja VLAN w infrastrukturze sieciowej, polityki firewall i kontrola dostępu zdalnego (VPN), monitoring ruchu po stronie IT oraz procedury raportowania incydentów do właściwego CSIRT (art. 23 NIS2, art. 11 uoKSC).
14. Gwarancja i serwis: gwarancja min. 12 miesięcy od odbioru; wsparcie 24/7 dla zgłoszeń krytycznych przez cały okres gwarancji; aktualizacje firmware w terminie do 5 dni; dostępność części zamiennych min. 3 lata.
15. Wymagania podmiotowe i dokumenty (ISO 9001/27001/22301, referencje sektorowe, sieć serwisowa, oświadczenie o własności kodu; potwierdzenie kompatybilności ze SCADA — referencja albo oświadczenie producenta z protokołem testów; wykaz dokumentów weryfikacyjnych): przeniesione do warunków udziału w Zapytaniu ofertowym (Rozdział V) oraz dokumentów składanych z ofertą — nie stanowią części OPZ.

B.6. Serwery wirtualizacyjne - 3 szt. – Klaster HA

Dostawa 3 (trzech) fabrycznie nowych serwerów do budowy klastra HA wraz z montażem, instalacją i konfiguracją oraz instalacją oprogramowania Proxmox VE (licencja na 2 CPU na każdy serwer min. Community) w ramach budowy farmy wirtualnej. Wraz z serwerami należy dostarczyć Microsoft Windows Server 2025 Standard w licencji pokrywającej wszystkie rdzenie fizyczne procesorów. Parametry minimalne:

1. Obudowa: Rack 19", maks. 1U, z zestawem szyn i możliwością instalacji ramienia do kabli; Serwer w chwili dostawy musi zapewniać możliwość instalacji z frontu min. 8 sztuk dysków 2,5” SATA/SAS Hot Swap.
2. Procesor: architektura x86, TDP maks. 190 W, min. 16 rdzeni, min. 3,2 GHz; SPECrate 2017 Integer nie niższy niż 388 pkt base w konfiguracji dwuprocesorowej (publikacja SPEC.org). Liczba procesorów: 2.
3. Pamięć: min. 256 GB RAM 6400 MHz w kościach min. 32 GB; min. 32 sloty; rozbudowa do 8 TB. Zabezpieczenie: memory mirroring, ECC, SDDC, ADDDC.
4. Dyski (w chwili dostawy): 2× SSD SATA RI min. 480 GB oraz 3× SSD SAS MU min. 3,2 TB (2,5", DWPD 5 lat); wewnętrzny slot Micro SD.
5. Kontroler dyskowy: sprzętowy 12 Gb, min. 8 dysków SATA/SAS, min. 4 GB cache, RAID 0/1/10/5/50/6/60 skonfigurowany do pracy w trybie HBA (IT Mode)
6. Zasilanie: min. 2 redundantne zasilacze min. 1300 W, certyfikat min. Titanium.

KRAJOWY PLAN ODBUDOWY | Rzeczpospolita Polska | Sfinansowane przez Unię Europejską NextGenerationEU | CENTRUM PROJEKTÓW POLSKA CYFROWA

7. Interfejsy sieciowe: min. 1 karta 4-portowa 10/25 Gb SFP28 z wkładkami (VXLAN, NVGRE, GENEVE, RoCEv2), nie zajmująca slotów PCIe; min. 1 karta 4-portowa 1 Gb BaseT; dedykowany port RJ-45 1 GbE karty zarządzającej.
8. Sloty I/O: min. 3× PCIe Gen5 x16 (w tym 1 pełnej wysokości), 2× OCP Gen5. Chłodzenie: Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1.
9. Zarządzanie: sprzętowy kontroler zdalnego zarządzania (IPMI v2.0, SNMP v3, DCMI v1.5, REST API, zdalna konsola, montowanie ISO); oprogramowanie zarządzające bez agenta, skalowalne do min. 1000 urządzeń, integracja z MS AD/SAML/SSO, REST API, PowerShell.
10. Bezpieczeństwo: czujnik otwarcia obudowy, hasło włączania i administratora, moduł RoT (TPM 2.0, PFR), bezpieczne kasowanie danych z dysków, automatyczne przywrócenie BIOS po nieautoryzowanej modyfikacji.
11. Oprogramowanie dołączone: Microsoft Windows Server 2025 Standard (na wszystkie rdzenie fizyczne) oraz Proxmox VE (2 CPU na serwer) licencja min. Community na 12 m-cy dla każdego serwera; wymagany montaż, instalacja i konfiguracja w ramach budowy klastra HA.
12. Gwarancja: 36 miesięcy producenta, okno serwisowe 24×7, czas reakcji NBD; uszkodzone nośniki danych pozostają własnością Zamawiającego.

B.7. Serwer kopii zapasowych (backup) — 1 szt.

Dostawa 1 (jednego) fabrycznie nowego serwera na repozytorium kopii zapasowych wraz z montażem, konfiguracją i optymalizacją oprogramowania. Parametry minimalne:

1. Obudowa: Rack 19", maks. 2U, z zestawem szyn; z frontu min. 8 dysków 2,5" SATA/SAS Hot Swap.
2. Procesor: x86, TDP maks. 150 W, min. 16 rdzeni, min. 2,3 GHz; SPECrate 2017 Integer nie niższy niż 373 pkt base w konfiguracji dwuprocesorowej (SPEC.org). Liczba procesorów: 1.
3. Pamięć: min. 128 GB RAM 6400 MHz w kościach min. 32 GB; min. 32 sloty; rozbudowa do 8 TB. Zabezpieczenie: memory mirroring, ECC, SDDC, ADDDC.
4. Dyski (w chwili dostawy): 2× SSD SATA RI min. 480 GB oraz 12× SSD SATA RI min. 1,92 TB (2,5"); wewnętrzny slot Micro SD.
5. Kontroler dyskowy: sprzętowy 12 Gb, min. 16 dysków SATA/SAS, min. 8 GB cache, RAID 0/1/10/5/50/6/60. Zasilanie: min. 2× min. 1300 W, min. Titanium.
6. Interfejsy: min. 1 karta 4-portowa 10/25 Gb SFP28 z wkładkami; min. 1 karta 4-portowa 1 Gb BaseT; dedykowany port zarządzania 1 GbE. Kontroler zdalnego zarządzania o funkcjonalności tożsamej z poz. B.6.
7. Bezpieczeństwo jak w poz. B.6 (RoT/TPM 2.0/PFR, bezpieczne kasowanie, przywrócenie BIOS). Wymagany montaż, konfiguracja i optymalizacja.
8. Gwarancja: 36 miesięcy producenta, okno serwisowe 24×7, czas reakcji NBD; uszkodzone nośniki pozostają własnością Zamawiającego.

B.8. Szafa RACK 19" 42U — 1 szt.

1. Szafa stojąca do zastosowań wewnętrznych, wysokość 42U; Wymiary: 800 × 1000 × 2055 mm (szer. × gł. × wys.)
2. Konstrukcja: min. 4 stopki z regulacją wysokości, min. 4 kółka jezdne, uziemienie: tak, organizacja kabli: min. 2 organizery pionowe w zestawie.
3. Drzwi przednie: przeszklone, wentylowane, z zamkiem, wykonane z blachy stalowej z wklejoną szybą hartowaną lub rozwiązanie równoważne o porównywalnych parametrach. Drzwi tylne: perforowane, wentylowane, z zamkiem. Panele boczne: stalowe, demontowane na zatrzaskach (system szybkiego montażu/demontażu).

4. Kolor: czarny, zbliżony do RAL9005 lub równoważny, masa: ok. 130–135 kg, obciążalność: min. 1000 kg, Stopień ochrony: min. IP20, zastosowanie: wewnętrzne.

B.9. Firewall UTM/NGFW FortiGate 120G (klaster HA) — 2 szt.

Dostawa 2 (dwóch) fabrycznie nowych urządzeń NGFW Fortinet FortiGate 120G (lub równoważnych) w klastrze wysokiej dostępności (HA) wraz z usługą FortiCare Premium Support (lub równoważną) na 12 miesięcy dla każdego urządzenia. Parametry minimalne:

1. Model referencyjny: Fortinet FortiGate 120G lub rozwiązanie równoważne; obudowa Rack 19", maks. 1U.
2. Porty: min. 16× GE RJ45, min. 2× RJ45 HA/Management, min. 8× SFP, min. 4× 10GE SFP+ FortiLink (lub równoważne), 1× Console RJ45, 1× USB.
3. Wyposażenie: moduł TPM; Bluetooth Low Energy (BLE); 2 wbudowane zasilacze AC (1+1). Certyfikaty: min. FCC, CE, RCM, VCCI, UL/cUL, CB, BSMI, IPv6/USGv6.
4. Wydajność — firewall: throughput (1518/512/64B) min. 39/39/28 Gbps; min. 140 000 nowych sesji/s; min. 3 000 000 sesji TCP; min. 10 000 polityk.
5. Wydajność — VPN: IPsec min. 35 Gbps; min. 2 000 tuneli site-to-site i 16 000 client-to-gateway; SSL-VPN min. 1,5 Gbps (min. 500 użytkowników); SSL inspection min. 3 Gbps.
6. Wydajność — ochrona: Application Control min. 6,7 Gbps; IPS min. 5,3 Gbps; NGFW min. 3,1 Gbps; Threat Protection min. 2,8 Gbps; CAPWAP min. 35 Gbps.
7. Funkcje (F.01–F.14): Stateful Firewall L3–L7; IPS; Application Control; SSL Deep Inspection; IPsec i SSL-VPN; Secure SD-WAN (bez odrębnej licencji); routing BGP/OSPF/RIP, NAT; VLAN 802.1Q i VRF; HA Active-Active i Active-Passive; MFA/2FA; GUI HTTPS i CLI; logowanie syslog/CEF/SNMP.
8. Wsparcie (W.01–W.06): FortiCare Premium 12 mies., 24×7×365, czas reakcji ≤ 1 h dla zgłoszeń krytycznych, NBD RMA (advanced replacement), dostęp do firmware/sygnatur, przypisanie do numeru seryjnego.
9. Model licencyjny (KK.01–KK.03): wszystkie funkcje w pakiecie podstawowym; cena obejmuje dostawę, akcesoria i 12-miesięczne wsparcie bez dodatkowych kosztów. Dostawa: elementy montażowe Rack 19", kable, datasheet, oświadczenie o autoryzowanym kanale na rynek RP, dane do rejestracji i aktywacji.

B.10. Napęd taśmowy LTO-7 z akcesoriami — zestaw

1. Typ: napęd taśmowy LTO-7 lub równoważny, w pełni kompatybilny z nośnikami Ultrium-7.
2. Pojemność: natywna min. 6 TB, skompresowana min. 15 TB; wydajność min. 300 MB/s (natywnie). Interfejs SAS lub FC; przewód 2 m Mini-SAS ↔ HD Mini-SAS 6 Gb/s.
3. Kompatybilność nośników: zapis/odczyt LTO-7, zapis/odczyt LTO-6, odczyt LTO-5.
4. Zestaw (kryteria odbioru): 1× napęd LTO-7; 14× nośnik LTO-7; 1× taśma czyszcząca (UCC); 1× przewód 2 m Mini-SAS↔HD Mini-SAS; 1× przewód zasilający 4 m Rack PDU C13/C14.
5. Napęd taśmowy musi być kompatybilny z serwerem z pkt. **B.7.** w sensie podłączenia i działania. Po stronie dostawcy podłączenie i wdrożenie napędu wraz z oprogramowaniem z pkt. **B.11.**
5. Gwarancja: 36 miesięcy producenta, czas reakcji NBD; weryfikacja po numerze seryjnym.

B.11. Oprogramowanie backupu i ochrony danych (klasa Enterprise) — licencja wieczysta

Dostawa oprogramowania backupu klasy Enterprise wraz z licencjami wieczystymi (perpetual) i wsparciem; model subskrypcyjny niedopuszczalny. Skala orientacyjna: 25 zabezpieczanych maszyn; wsparcie min. 12 miesięcy od odbioru. Parametry minimalne:

KRAJOWY PLAN ODBUDOWY | Rzeczpospolita Polska | Sfinansowane przez Unię Europejską NextGenerationEU | CENTRUM PROJEKTÓW POLSKA CYFROWA

1. Model licencyjny: licencja wieczysta (perpetual) wraz ze wsparciem; model subskrypcyjny niedopuszczalny.
2. Platformy wirtualizacji: VMware 7.x/8.x/9.0, Hyper-V 2016–2025, Nutanix 6.8–7.3, RHV 4.4 SP1, Oracle Linux Virtualization 4.5.5+, Proxmox VE 8.2/8.3/8.4/9.0.
3. Źródła: NAS (SMB/CIFS/NFS), pamięci obiektowe S3/Azure/AWS, serwery Windows i Linux; backup bezagentowy i spójny aplikacyjnie dla vSphere, Hyper-V, Nutanix AHV, Proxmox.
4. Repozytoria/niezmienność: obsługa immutability (ochrona przed ransomware), ReFS BlockClone i XFS, kopiowanie na taśmy LTO oraz IBM 3592, retencja GFS, archiwizacja S3 Glacier/Azure Archive.
5. Bezpieczeństwo: szyfrowanie plików i transmisji, natywne MFA konsoli, integracja SAML (Entra ID, Okta) i SIEM (Splunk, Palo Alto XSOAR/XSIAM, CrowdStrike, Microsoft Sentinel).
6. RPO/replikacja: śledzenie zmienionych plików, akceleracja WAN, replikacja asynchroniczna VM (ESXi↔ESXi, Hyper-V).
7. Pozostałe: portal samoobsługowy (odtwarzanie VM/baz, point-in-time), RBAC, integracja z urządzeniami deduplikacyjnymi (Dell DataDomain, HPE StoreOnce, ExaGrid i inne).

B.12. System monitoringu infrastruktury IT/OT — licencja na 12 miesięcy

Dostawa systemu klasy Infrastructure Monitoring (NMS). Skala orientacyjna: 250 monitorowanych hostów IT i OT; pełne pokrycie kosztów licencji i utrzymania w cenie oferty przez min. 36 miesięcy od odbioru. Dopuszczalne rozwiązania komercyjne i open source. Parametry minimalne:

1. Model licencyjny: komercyjny perpetual (per-host/metryka/NVPS/instancja) lub open source (licencja OSI); brak dodatkowych kosztów licencyjnych i utrzymaniowych przez min. 36 miesięcy od odbioru.
2. Skala/retencja: 250 hostów IT i OT; surowe wartości min. 30 dni, trendy/agregacje min. 6 miesięcy.
3. Architektura: serwer zarządzający, baza, konsola webowa, komponenty zbierające (agenci i/lub proxy); pojedyncza instancja z udokumentowaną rozbudową do HA bez wymiany platformy i bez dodatkowych licencji.
4. Zbieranie danych: agentowe (Windows, Server 2016+, Linux/Unix) i bezagentowe (SNMP v1/v2c/v3, IPMI 2.0, JMX, ODBC, ICMP, SSH, HTTP/HTTPS); proxy w lokalizacjach zdalnych z buforowaniem przy zerwaniu WAN.
5. Źródła: OS, urządzenia sieciowe (SNMP), serwery (IPMI), bazy danych, środowiska wirtualne, chmura, kontenery, UPS i klimatyzacja (SNMP), urządzenia OT/SCADA (SNMP lub Modbus TCP).
6. Automatyzacja: silnik triggerów z korelacją, min. 5 poziomów krytyczności, powiadomienia (SMTP/TLS, SMS, webhooki Teams/Slack, REST, SNMP trap), akcje i eskalacja, okna serwisowe, prognozowanie i wykrywanie anomalii.
7. Dostęp: konsola webowa HTML5; uwierzytelnianie lokalne, LDAP/LDAPS (AD), SSO SAML 2.0/OIDC, MFA (TOTP). Wizualizacja: dashboardy, mapy sieci/geomapy, raporty dostępności/SLA, RBAC.

B.13. System uwierzytelniania wieloskładnikowego (MFA) — licencja na 12 miesięcy

Dostawa systemu MFA dla użytkowników infrastruktury teleinformatycznej. Producent z siedzibą w UE, certyfikat ISO/IEC 27001:2023, min. 3 lata na rynku, wsparcie w języku polskim. Skala orientacyjna: do 100 użytkowników; licencja min. 12 miesięcy od odbioru. Parametry minimalne:

1. Producent: podmiot z siedzibą w UE, ISO/IEC 27001:2023 (lub równoważny), min. 3 lata na rynku, wsparcie techniczne w języku polskim.
2. Standardy: LDAP v3, LDAPS, RADIUS, SAML 2.0, TOTP (RFC 6238), FIDO2/WebAuthn, REST API.

KRAJOWY PLAN ODBUDOWY | Rzeczpospolita Polska | Sfinansowane przez Unię Europejską NextGenerationEU | CENTRUM PROJEKTÓW POLSKA CYFROWA

3. Konsola: webowa HTTPS/HTML5 chroniona MFA (czynnik odporny na phishing — FIDO2/U2F); role (administrator pełny, operator, audytor); polityki wg grupy/zasobu/lokalizacji/IP; interfejs w języku polskim; logowanie zdarzeń z eksportem.
4. Metody: Push, TOTP, SMS (kod i link), aplikacja mobilna z blokadą biometryczną, połączenie głosowe, FIDO2/U2F, karta RFID, tryb offline OTP.
5. Integracje: AD (LDAP/LDAPS), OpenLDAP, Entra ID; RADIUS (NPS, urządzenia sieciowe, VPN); MFA dla logowania Windows i RDP; OWA, RD Gateway/Web, AD FS; SSH (Linux); SDK (.NET, Java, PHP).

B.14. System zarządzania dostępem uprzywilejowanym (PAM) — wsparcie 12 miesięcy

Dostawa licencji, instalacja, konfiguracja i uruchomienie systemu klasy PAM wraz z 12-miesięcznym wsparciem. Skala: 3 konta administratorów, 100 zarządzanych zasobów (kont uprzywilejowanych). Parametry minimalne:

1. Architektura: instalacja na Windows Server 2019/2022/2025 lub Linux, środowisko fizyczne/wirtualne; baza wbudowana lub zewnętrzna (MS SQL 2016+); konsola wyłącznie webowa HTTPS/HTML5, TLS 1.2+; kopie zapasowe na SMB/NFS/SFTP; procedura odtworzenia klucza głównego.
2. Sejf haseł: repozytorium min. AES-256; import CSV; automatyczna rotacja haseł (konta Windows, Linux/Unix SSH, urządzenia sieciowe, bazy); check-out z rotacją po czasie; rejestracja każdej operacji (czas, użytkownik, IP).
3. Użytkownicy: min. 3 konta administratorów i nieograniczona liczba operatorów w ramach licencji; RBAC; integracja z AD/LDAP v3 (import, role wg grup AD, synchronizacja cykliczna).
4. Interoperacyjność: integracja z SIEM i ITSM (REST API lub syslog); SAML 2.0/OIDC; zarządzanie sesjami SSH/RDP/HTTPS.

B.15. System zarządzania podatnościami i łatami (VMP) — wsparcie 12 miesięcy

Dostawa licencji, instalacja, konfiguracja i uruchomienie systemu zarządzania podatnościami i łatami wraz z 12-miesięcznym wsparciem. Skala: 100 stacji roboczych, 45 serwerów Windows/Linux, 2 konta administratorów, 1 serwer typu gateway. Interfejs konsoli w języku polskim. Parametry minimalne:

1. Architektura: agentowa; dedykowany serwer typu gateway (min. 1, bez dodatkowych opłat) dla segmentów odseparowanych (DMZ/OT) z szyfrowaniem; obsługa środowisk z domeną AD i bez domeny; konsola webowa HTTPS/HTML5 w języku polskim; natywne MFA administratorów (TOTP, SAML 2.0); integracja LDAP v3/AD.
2. Standardy: CVE, CVSS v3.1/v4.0, OVAL, SCAP, syslog CEF/LEEF, SNMP v2c/v3, REST API, TLS 1.2+.
3. Zakres funkcjonalny: automatyczne wykrywanie podatności, pełny cykl dystrybucji i instalacji łat systemowych i aplikacyjnych, inwentaryzacja zasobów, raportowanie zgodności.
4. Interoperacyjność: integracja z SIEM i ITSM (REST API, webhooks lub syslog); chmurowi dostawcy tożsamości (Entra ID, Okta, Google Workspace) przez SAML 2.0.

B.16. System SIEM (klasy Lite) — licencja wieczysta ze wsparciem na 12 miesięcy, wdrożenie i szkolenie

Dostawa systemu SIEM zapewniającego monitorowanie, analizę i korelację zdarzeń bezpieczeństwa wraz z wdrożeniem przez producenta i szkoleniem. Wydajność min. 1000 EPS lub 20 GB danych dziennie, retencja min. 365 dni. Licencja wieczysta wraz ze wsparciem community producenta na 1 rok; licencja nie ogranicza liczby użytkowników ani źródeł logów. Parametry minimalne:

1. Wydajność/retencja: min. 1000 EPS lub 20 GB dziennie; retencja min. 365 dni; buforowanie danych min. 2 dni przy awarii komponentu.

KRAJOWY PLAN ODBUDOWY | Rzeczpospolita Polska | Sfinansowane przez Unię Europejską NextGenerationEU | CENTRUM PROJEKTÓW POLSKA CYFROWA

2. Architektura: baza NoSQL, Linux; rozdzielenie min. 3 ról (Agregacja, Prezentacja, Retencja); skalowanie przez dołączanie węzłów bez restartu; wysoka dostępność na poziomie Agregacji i Retencji.
3. Bezpieczeństwo/dostęp: TLS min. 1.2 między komponentami, min. 1.3 do przeglądarki; zgodność z OWASP TOP 10 i ASVS 4.0 (min. L1); integracja z AD/LDAP/RADIUS, SSO; pełny audyt; tryb multitenant.
4. Zbieranie/parsowanie: tryb agentowy i bezagentowy; Syslog, WEF, Event log, WMI, SNMP trap, XML, JSON, JDBC/ODBC, CSV; tworzenie parserów z GUI; zbieranie z chmury (AWS, Azure); prezentacja logu RAW.
5. Analityka: korelacja zdarzeń, modele prognostyczne (ML), szacowanie ryzyka, scenariusze obsługi incydentów, wizualizacja, eksport CSV/HTML, raporty ręczne i automatyczne.
6. Wdrożenie i szkolenie: wdrożenie realizowane przez producenta oprogramowania SIEM; szkolenie zdalne w języku polskim, prowadzone przez osoby z certyfikatem producenta oferowanego rozwiązania.

CZĘŚĆ C — ZAKRES USŁUGOWY (organizacyjny)

Poniżej opisano cztery zadania usługowe wraz z zakresem prac i wymaganymi dokumentami wynikowymi. Wszystkie dokumenty przekazywane są w języku polskim i podlegają odbiorom etapowym.

Zadanie 1: Opracowanie, wdrożenie, przegląd i aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

Zakres prac:

1. Analiza stanu wyjściowego
    1.1. Analiza dotychczasowego stanu bezpieczeństwa informacji w obszarach IT i OT
    1.2. Identyfikacja luk i obszarów wymagających wzmocnienia
    1.3. Analiza zgodności z wymaganiami ustawy o krajowym systemie cyberbezpieczeństwa (uoKSC)
    1.4. Przegląd infrastruktury IT oraz systemów OT/ICS/IIoT wykorzystywanych w procesach poboru, uzdatniania i dystrybucji wody
    1.5. Identyfikacja krytycznych systemów teleinformatycznych (STI)
2. Określenie zakresu SZBI
    2.1. Zdefiniowanie granic SZBI (procesy biznesowe, systemy IT, systemy OT)
    2.2. Określenie procesów objętych systemem zarządzania
    2.3. Identyfikacja interesariuszy i ich wymagań
    2.4. Wyznaczenie lokalizacji i zasobów objętych zakresem SZBI
3. Analiza ryzyka bezpieczeństwa informacji
    3.1. Identyfikacja zasobów informacyjnych (w tym danych procesowych systemów OT)
    3.2. Określenie wartości zasobów i ich klasyfikacja
    3.3. Identyfikacja zagrożeń i podatności
    3.4. Ocena prawdopodobieństwa i wpływu zagrożeń
    3.5. Oszacowanie poziomu ryzyka
    3.6. Opracowanie rejestru ryzyka
    3.7. Zaproponowanie działań (akceptacja, obniżenie, unikanie, transfer)
    3.8. Opracowanie Planu Postępowania z Ryzykiem (Risk Treatment Plan)
4. Opracowanie dokumentacji SZBI zgodnej z PN-EN ISO/IEC 27001:2023-08

KRAJOWY PLAN ODBUDOWY | Rzeczpospolita Polska | Sfinansowane przez Unię Europejską NextGenerationEU | CENTRUM PROJEKTÓW POLSKA CYFROWA

4.1. Polityka Bezpieczeństwa Informacji
4.2. Polityka zarządzania ryzykiem
4.3. Procedury operacyjne w zakresie zabezpieczeń z Załącznika A normy
4.4. Instrukcje dla użytkowników systemów IT i OT
4.5. Regulamin organizacyjny SZBI (role i odpowiedzialności)
4.6. Procedura zarządzania incydentami bezpieczeństwa informacji
4.7. Procedura zarządzania zmianą
4.8. Procedura kontroli dostępu (fizycznego i logicznego)
4.9. Procedura backup i odzyskiwania danych
4.10. Procedura zarządzania podatnościami
4.11. Procedura zarządzania aktualizacjami i poprawkami
4.12. Procedura monitorowania i przeglądu bezpieczeństwa
4.13. Procedura audytów wewnętrznych SZBI
4.14. Procedura przeglądu zarządczego
4.15. Statement of Applicability (SoA)
4.16. Rejestry wymagane normą (zasobów, incydentów, audytów itp.)
4.17. Plany testów i przeglądów

5. Wdrożenie SZBI
   5.1. Szkolenia dla kadry zarządzającej z zakresu SZBI
   5.2. Szkolenia dla pracowników IT i OT z procedur bezpieczeństwa
   5.3. Szkolenia podstawowe ze świadomości cyberzagrożeń dla wszystkich pracowników
   5.4. Wsparcie przy implementacji zabezpieczeń z SoA
   5.5. Nadzór nad procesem wdrożenia
   5.6. Weryfikacja skuteczności zabezpieczeń
6. Przegląd i aktualizacja dokumentacji SZBI
   6.1. Przegląd zarządczy SZBI
   6.2. Audyt wewnętrzny SZBI
   6.3. Aktualizacja dokumentacji w oparciu o wyniki
   6.4. Aktualizacja analizy ryzyka
   6.5. Działania korygujące i doskonalące

Dokumenty wynikowe:

1. Raport z analizy stanu wyjściowego
2. Dokument zakresu SZBI
3. Raport z analizy ryzyka wraz z rejestrem ryzyka
4. Plan Postępowania z Ryzykiem
5. Komplet dokumentacji SZBI (polityki, procedury, instrukcje, regulaminy)
6. Statement of Applicability (SoA)
7. Komplet rejestrów wymaganych normą ISO/IEC 27001:2023
8. Protokoły ze szkoleń (listy obecności, programy, materiały)
9. Raport z wdrożenia SZBI
10. Protokół z audytu wewnętrznego SZBI
11. Protokół z przeglądu zarządczego SZBI

KRAJOWY PLAN ODBUDOWY | Rzeczpospolita Polska | Sfinansowane przez Unię Europejską NextGenerationEU | CENTRUM PROJEKTÓW POLSKA CYFROWA

12. Zaktualizowana dokumentacja SZBI po przeglądzie

Zadanie 2: Audyt SZBI zgodnie z metodologią ISO 19011

Zakres prac:

1. Audyt zgodności SZBI z PN-EN ISO/IEC 27001:2023-08
    1.1. Przegląd dokumentacji SZBI pod kątem zgodności z normą
    1.2. Weryfikacja kompletności dokumentacji
    1.3. Ocena skuteczności zabezpieczeń z Załącznika A
    1.4. Weryfikacja poprawności analizy ryzyka
    1.5. Ocena funkcjonowania procesów zarządzania bezpieczeństwem informacji
2. Audyt zgodności z ustawą o KSC
    2.1. Weryfikacja spełnienia wymogów art. 8 uoKSC
    2.2. Ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI)
    2.3. Weryfikacja zgłoszeń incydentów do CSIRT MON, CSIRT NASK, CSIRT GOV
    2.4. Weryfikacja procedur zgłaszania incydentów poważnych
    2.5. Ocena zgodności z komunikatem Pełnomocnika Rządu ds. Cyberbezpieczeństwa w sprawie ataków na ICS/OT
3. Audyt techniczny zabezpieczeń IT i OT
    3.1. Weryfikacja konfiguracji zabezpieczeń IT
    3.2. Przegląd zabezpieczeń OT/ICS/IIoT (stacje uzdatniania, SCADA, PLC)
    3.3. Ocena segmentacji sieci IT i OT
    3.4. Weryfikacja mechanizmów kontroli dostępu
    3.5. Przegląd polityki haseł i MFA
    3.6. Weryfikacja procedur backup i odzyskiwania
    3.7. Ocena zabezpieczeń fizycznych infrastruktury krytycznej
4. Wywiady i inspekcje
    4.1. Wywiady z kluczowymi pracownikami (zarząd, kadra IT/OT, użytkownicy)
    4.2. Inspekcje na miejscu w lokalizacjach objętych SZBI
    4.3. Weryfikacja stosowania procedur w praktyce
    4.4. Ocena świadomości pracowników
5. Raportowanie i rekomendacje
    5.1. Szczegółowy raport z audytu
    5.2. Identyfikacja niezgodności i obszarów do poprawy
    5.3. Rekomendacje działań korygujących i doskonalących
    5.4. Priorytetyzacja wdrożenia zmian
    5.5. Prezentacja wyników dla zarządu

Dokumenty wynikowe:

1. Raport z audytu SZBI wg PN-EN ISO/IEC 27001:2023-08
2. Raport z audytu zgodności z uoKSC i KRI
3. Wykaz niezgodności (major/minor)
4. Rekomendacje działań naprawczych z priorytetami
5. Prezentacja wyników audytu dla zarządu

KRAJOWY PLAN ODBUDOWY | Rzeczpospolita Polska | Sfinansowane przez Unię Europejską NextGenerationEU | CENTRUM PROJEKTÓW POLSKA CYFROWA

Zadanie 3: Opracowanie planów ciągłości działania (BCP) i odtwarzania po awarii (DRP) STI

Zakres prac:

1. Analiza wpływu na działalność (BIA)
    1.1. Identyfikacja krytycznych procesów biznesowych
    1.2. Identyfikacja krytycznych STI wspierających procesy
    1.3. Analiza zależności procesy–systemy IT/OT
    1.4. Maksymalny tolerowany czas niedostępności (MTD)
    1.5. Cel czasu odzyskiwania (RTO)
    1.6. Cel punktu odzyskiwania (RPO)
    1.7. Oszacowanie skutków finansowych, operacyjnych i wizerunkowych
    1.8. Minimalne wymagania operacyjne dla kontynuacji działalności
2. Analiza ryzyka ciągłości działania
    2.1. Identyfikacja scenariuszy zakłóceń (klęski, awarie, cyberataki, błędy ludzkie)
    2.2. Ocena prawdopodobieństwa
    2.3. Ocena wpływu na działalność
    2.4. Oszacowanie poziomu ryzyka
    2.5. Priorytetyzacja scenariuszy
3. Strategia ciągłości działania
    3.1. Strategia zapewnienia ciągłości krytycznych procesów
    3.2. Alternatywne sposoby wykonywania procesów
    3.3. Wymagania dotyczące zasobów (personel, infrastruktura, systemy)
    3.4. Strategia backup i odzyskiwania danych
    3.5. Strategia redundancji systemów krytycznych
    3.6. Lokalizacje zapasowe lub procedury awaryjne
4. Plan Ciągłości Działania (BCP)
    4.1. Dokument strategiczny zatwierdzany przez zarząd
    4.2. Procedury reagowania na incydenty zakłócające ciągłość
    4.3. Procedury aktywacji planu
    4.4. Role i odpowiedzialności (zespół reagowania kryzysowego)
    4.5. Procedury komunikacji wewnętrznej i zewnętrznej
    4.6. Procedury bezpieczeństwa pracowników
    4.7. Procedury przywracania normalnej działalności
    4.8. Procedury obejścia (workarounds)
    4.9. Kontakty alarmowe i listy powiadamiania
    4.10. Procedury zarządzania kryzysowego
5. Plan Odtwarzania po Awarii (DRP)
    5.1. Procedury odzyskiwania systemów IT
    5.2. Procedury odzyskiwania systemów OT/ICS
    5.3. Przywracanie danych z kopii zapasowych
    5.4. Rekonfiguracja systemów i przywracanie usług
    5.5. Scenariusze odzyskiwania (awaria sprzętu, centrum danych, cyberatak, utrata danych)

KRAJOWY PLAN ODBUDOWY | Rzeczpospolita Polska | Sfinansowane przez Unię Europejską NextGenerationEU | CENTRUM PROJEKTÓW POLSKA CYFROWA

5.6. Testowanie kopii zapasowych
5.7. Przywracanie SCADA i PLC w stacjach uzdatniania wody
5.8. Kolejność przywracania (priorytetyzacja)
5.9. Walidacja przywróconych systemów
5.10. Diagramy i schematy infrastruktury IT/OT
5.11. Listy kontaktowe do dostawców i wsparcia

6. Integracja BCP i DRP z SZBI
   6.1. Spójność planów z dokumentacją SZBI
   6.2. Uwzględnienie wymagań bezpieczeństwa informacji
   6.3. Koordynacja z procedurami zarządzania incydentami
7. Testowanie planów
   7.1. Scenariusze testowe BCP i DRP
   7.2. Testy desktop (teoretyczne)
   7.3. Testy symulacyjne (ćwiczenia)
   7.4. Dokumentowanie wyników
   7.5. Identyfikacja obszarów do poprawy
   7.6. Aktualizacja planów po testach
8. Szkolenia
   8.1. Zespół reagowania kryzysowego (BCP)
   8.2. Administratorzy IT/OT (DRP)
   8.3. Kadra zarządzająca (zarządzanie kryzysowe)
   8.4. Wszyscy pracownicy (podstawowe procedury kryzysowe)

Dokumenty wynikowe:

1. Raport z analizy wpływu na działalność (BIA)
2. Raport z analizy ryzyka ciągłości
3. Plan Ciągłości Działania (BCP)
4. DRP — procedury operacyjne dla IT
5. DRP — procedury operacyjne dla OT/ICS
6. Scenariusze testowe BCP i DRP
7. Protokoły z testów planów
8. Zaktualizowane plany BCP i DRP po testach
9. Materiały szkoleniowe i protokoły ze szkoleń
10. Diagramy i schematy infrastruktury IT/OT
11. Listy kontaktowe i procedury komunikacji kryzysowej

Zadanie 4: Opracowanie, wdrożenie, przegląd i aktualizacja Systemu Zarządzania Ciągłością Działania (SZCD) STI

Zakres prac:

1. Analiza kontekstu organizacji i wymagań SZCD
   1.1. Kontekst organizacyjny SZCD
   1.2. Zainteresowane strony i ich wymagania
   1.3. Zakres SZCD (procesy, systemy, lokalizacje)
   1.4. Wymagania regulacyjne (uoKSC, NIS2, DORA — jeśli dotyczy)

KRAJOWY PLAN ODBUDOWY | Rzeczpospolita Polska | Sfinansowane przez Unię Europejską NextGenerationEU | CENTRUM PROJEKTÓW POLSKA CYFROWA

1.5. Przegląd wymogów PN-EN ISO 22301:2020-04

2. Polityka i cele SZCD
   - 2.1. Polityka Ciągłości Działania zatwierdzona przez kierownictwo
   - 2.2. Cele ciągłości działania
   - 2.3. Wskaźniki efektywności (KPI)
   - 2.4. Role i odpowiedzialności
3. Planowanie i zarządzanie ryzykiem ciągłości
   - 3.1. Analiza ryzyka ciągłości (jeśli nie w Zadaniu 3)
   - 3.2. Metodologia oceny ryzyka
   - 3.3. Kryteria akceptacji ryzyka
   - 3.4. Plan Postępowania z Ryzykiem Ciągłości
4. Dokumentacja SZCD zgodna z PN-EN ISO 22301:2020-04
   - 4.1. Polityka Zarządzania Ciągłością Działania
   - 4.2. Procedura analizy wpływu (BIA)
   - 4.3. Procedura analizy ryzyka ciągłości
   - 4.4. Procedura strategii ciągłości
   - 4.5. Procedura planów ciągłości (BCP)
   - 4.6. Procedura planów odtwarzania (DRP)
   - 4.7. Procedura reagowania na incydenty zakłócające ciągłość
   - 4.8. Procedura zarządzania kryzysowego
   - 4.9. Procedura komunikacji kryzysowej
   - 4.10. Procedura testowania i ćwiczeń
   - 4.11. Procedura audytów wewnętrznych
   - 4.12. Procedura przeglądu zarządczego
   - 4.13. Procedura zarządzania zmianą
   - 4.14. Procedura zarządzania dokumentacją i zapisami
   - 4.15. Procedura doskonalenia SZCD
   - 4.16. Rejestry wymagane normą (incydentów, testów, audytów, działań korygujących)
5. Wdrożenie SZCD
   - 5.1. Szkolenie kadry zarządzającej (SZCD, ISO 22301)
   - 5.2. Szkolenie zespołu reagowania kryzysowego
   - 5.3. Szkolenie administratorów IT/OT
   - 5.4. Szkolenia świadomości dla wszystkich pracowników
   - 5.5. Implementacja procedur SZCD
   - 5.6. Integracja SZCD z SZBI
   - 5.7. Nadzór nad wdrożeniem
   - 5.8. Weryfikacja skuteczności
6. Testy i ćwiczenia
   - 6.1. Program testów i ćwiczeń
   - 6.2. Testy desktop
   - 6.3. Ćwiczenia symulacyjne
   - 6.4. Dokumentowanie wyników

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU
CENTRUM PROJEKTÓW POLSKA CYFROWA

6.5. Analiza efektywności SZCD

7. Audyt wewnętrzny SZCD
   - 7.1. Audyt wg PN-EN ISO 22301:2020-04
   - 7.2. Weryfikacja zgodności z normą
   - 7.3. Ocena skuteczności
   - 7.4. Identyfikacja niezgodności
   - 7.5. Raport z audytu wewnętrznego
8. Przegląd zarządczy i aktualizacja SZCD
   - 8.1. Przegląd zarządczy
   - 8.2. Ocena osiągnięcia celów ciągłości
   - 8.3. Analiza wyników audytów, testów i incydentów
   - 8.4. Aktualizacja dokumentacji
   - 8.5. Działania korygujące i doskonalące
   - 8.6. Aktualizacja analizy ryzyka
9. Przygotowanie do certyfikacji SZCD (opcjonalnie)
   - 9.1. Analiza gotowości do certyfikacji ISO 22301
   - 9.2. Audyt pre-certyfikacyjny
   - 9.3. Wsparcie w procesie certyfikacji przez akredytowaną jednostkę

Dokumenty wynikowe:

1. Dokument kontekstu i zakresu SZCD
2. Polityka Zarządzania Ciągłością Działania
3. Komplet procedur SZCD wg PN-EN ISO 22301:2020-04
4. Komplet rejestrów wymaganych normą ISO 22301
5. Raport z analizy ryzyka ciągłości (jeśli nie w Zadaniu 3)
6. Plan Postępowania z Ryzykiem Ciągłości
7. Raport z wdrożenia SZCD
8. Program testów i ćwiczeń
9. Protokoły z testów i ćwiczeń
10. Protokół z audytu wewnętrznego SZCD
11. Protokół z przeglądu zarządczego SZCD
12. Zaktualizowana dokumentacja SZCD
13. Materiały szkoleniowe i protokoły ze szkoleń

CZĘŚĆ D — USŁUGI WDROŻENIOWE URZĄDZEŃ

D.1. Wdrożenie diody danych i integracja z SCADA

1. Dostawa urządzenia spełniającego wymagania OPZ (B.5).
2. Instalacja w lokalizacji wskazanej przez Zamawiającego.
3. Uruchomienie i konfiguracja w środowisku produkcyjnym.
4. Integracja z eksploatowanym SCADA (TelWin SCADA lub równoważnym).
5. Testy integracyjne potwierdzające współpracę ze SCADA.
6. Przeszkolenie pracowników z obsługi i administracji.
7. Dokumentacja techniczna i eksploatacyjna w języku polskim.

KRAJOWY PLAN ODBUDOWY | Rzeczpospolita Polska | Sfinansowane przez Unię Europejską NextGenerationEU | CENTRUM PROJEKTÓW POLSKA CYFROWA

8. Gwarancja i wsparcie na warunkach OPZ/umowy.

D.2. Wdrożenie i konfiguracja urządzeń brzegowych OT

Instalacja, konfiguracja i uruchomienie firewalli UTM OPNsense (HA), przełączników przemysłowych, routerów LTE i systemu IPS, konfiguracja oprogramowania do zarządzania, testy akceptacyjne (UAT) i dokumentacja powykonawcza.

D.3. Wdrożenie klastra FortiGate 120G (HA) wraz ze szkoleniem

Kompletny cykl wdrożenia 2 urządzeń FortiGate 120G w klastrze HA (poz. B.9): faza przygotowawcza (kick-off, RACI, plan projektu, kryteria odbioru), analiza przedwdrożeniowa, instalacja i konfiguracja klastra HA, testy odbiorcze i stabilizacja, szkolenie personelu (maks. 4 osoby, min. 8 godzin) oraz dokumentacja powykonawcza.

D.4. Wdrożenie platformy backupu (oprogramowanie z poz. B.11)

Start projektu i specyfikacja (zasoby, RPO/RTO, retencja, harmonogramy), projekt architektury (repozytorium niezmiennych kopii), wdrożenie i stabilizacja (instalacja, repozytorium immutable, integracja z wirtualizacją, agenci na serwerach fizycznych, testy funkcjonalne i przywracania, test nienaruszalności danych, stabilizacja 7 dni), dokumentacja powykonawcza i warsztaty (maks. 4 osoby).

D.5. Wdrożenie systemu monitoringu IT/OT (oprogramowanie z poz. B.12)

Uruchomienie projektu i specyfikacja, audyt i inwentaryzacja infrastruktury IT/OT we wszystkich lokalizacjach, projekt techniczny, instalacja i konfiguracja (w tym warstwa proxy w lokalizacjach zdalnych), wdrożenie szablonów, wyzwalaczy i dashboardów, testy, uruchomienie produkcyjne oraz dokumentacja powykonawcza i transfer wiedzy.

D.6. Wdrożenie systemu MFA (oprogramowanie z poz. B.13)

Analiza środowiska i projekt techniczny, instalacja i konfiguracja (integracja ze źródłami tożsamości AD/LDAP/Entra ID, RADIUS, scenariusze Windows/RDP/SSH/VPN), wdrożenie polityk i metod uwierzytelniania, stabilizacja, szkolenie oraz dokumentacja powykonawcza.

D.7. Wdrożenie systemu PAM (oprogramowanie z poz. B.14)

Analiza i projekt, instalacja i konfiguracja serwera oraz sejfu haseł, integracja z AD/LDAP, konfiguracja zarządzanych zasobów oraz polityk rotacji i check-out, testy, stabilizacja, szkolenie i dokumentacja powykonawcza.

D.8. Wdrożenie systemu VMP (oprogramowanie z poz. B.15)

Analiza i projekt, instalacja serwera centralnego i serwera typu gateway, dystrybucja agentów, konfiguracja skanowania podatności i polityk wdrażania łat, integracje (AD/LDAP, SIEM/ITSM), testy, stabilizacja, szkolenie i dokumentacja powykonawcza.

D.9. Wdrożenie i szkolenie systemu SIEM (oprogramowanie z poz. B.16)

Wdrożenie realizowane przez producenta oprogramowania: instalacja i konfiguracja komponentów (Agregacja, Prezentacja, Retencja), podłączenie źródeł logów, konfiguracja parserów i reguł korelacyjnych oraz dashboardów. Szkolenie zdalne w języku polskim, prowadzone przez osoby z certyfikatem producenta.

D.10. Usługa segmentacji i rekonfiguracji sieci OT/IT

Faza 1 (analiza i projekt): audyt infrastruktury OT/IT, projekt architektury z podziałem na strefy (OT, IT, DMZ, zarządzania), schemat adresacji i VLAN, polityki inter-VLAN i ACL, plan realizacji. Faza

2 (wdrożenie): kopie zapasowe konfiguracji i plan rollback, hardening, wdrożenie segmentacji (strefy, VLAN, polityki, ACL, NAT/PAT), testy akceptacyjne (UAT), uruchomienie produkcyjne w oknach serwisowych. Faza 3 (dokumentacja i transfer wiedzy): dokumentacja powykonawcza oraz szkolenie (maks. 3 osoby, min. 8 godzin). Zakres usługi dotyczy istniejących urządzeń w infrastrukturze Zamawiającego.

CZĘŚĆ E — ZBIORCZE ZESTAWIENIE POZYCJI DO WYCENY

Wykonawca wypełnia poniższe zbiorcze zestawienie obejmujące całość zamówienia (usługi organizacyjne, dostawy urządzeń oraz usługi wdrożeniowe). Ceny w PLN; wartość brutto = netto + VAT; suma wartości brutto stanowi cenę oferty. Zestawienie odpowiada formularzowi asortymentowo-cenowemu zawartemu w Załączniku nr 2 do Zapytania ofertowego i stanowi z nim całość.

Lp.	Opis pozycji	Odn.	Jedn.	Ilość	Wartość netto	Wartość brutto
1	Zadanie 1 — dokumentacja i wdrożenie SZBI (ISO/IEC 27001)	OPZ C	usługa	1		
2	Zadanie 2 — audyt SZBI (ISO 19011)	OPZ C	usługa	1		
3	Zadanie 3 — plany ciągłości działania (BCP) i odtwarzania po awarii (DRP)	OPZ C	usługa	1		
4	Zadanie 4 — System Zarządzania Ciągłością Działania (SZCD, ISO 22301)	OPZ C	usługa	1		
5	Firewall UTM „Next-Gen” OPNsense (HA) z 12-mies. wsparciem	B.1	szt.	2		
6	Przełącznik przemysłowy + oprogramowanie zarządzające (gwarancja 60 mies.)	B.2	szt.	5		
7	Router LTE (IEC 62443-4-2 SL1) + platforma zarządzania	B.3	szt.	17		
8	Przemysłowy system IPS z DPI	B.4	szt.	2		
9	Dioda danych OT→IT + oprogramowanie + wdrożenie/integracja SCADA	B.5 / D.1	szt.	1		
10	Serwer wirtualizacyjny (farma) + Windows Server 2025 Std + Proxmox	B.6	szt.	3		
11	Serwer kopii zapasowych (backup)	B.7	szt.	1		
12	Szafa RACK 19" 42U	B.8	szt.	1		
13	Firewall UTM/NGFW FortiGate 120G (HA) + FortiCare Premium 12 mies.	B.9	szt.	2		
14	Napęd taśmowy LTO-7 — zestaw (napęd, 14 nośników, taśma czyszcząca, okablowanie)	B.10	zestaw	1		
15	Oprogramowanie backupu klasy Enterprise — licencja wieczysta + wsparcie 12 mies.	B.11	kpl.	1		

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU
CENTRUM PROJEKTÓW POLSKA CYFROWA

Lp.	Opis pozycji	Odn.	Jedn.	Ilość	Wartość netto	Wartość brutto
16	System monitoringu IT/OT — licencja na min. 36 mies. (orient. 250 hostów)	B.12	kpl.	1		
17	System MFA — licencja na min. 36 mies. (do 100 użytkowników)	B.13	kpl.	1		
18	System PAM — licencja (3 administratorów, 100 zasobów) + wsparcie 12 mies.	B.14	kpl.	1		
19	System VMP — licencja (100 stacji, 45 serwerów, 1 gateway) + wsparcie 12 mies.	B.15	kpl.	1		
20	System SIEM (Lite) — licencja wieczysta + wsparcie 1 rok	B.16	kpl.	1		
21	Usługa wdrożenia klastra FortiGate 120G (HA) ze szkoleniem	D.3	usługa	1		
22	Usługa wdrożenia platformy backupu	D.4	usługa	1		
23	Usługa wdrożenia systemu monitoringu IT/OT	D.5	usługa	1		
24	Usługa wdrożenia systemu MFA	D.6	usługa	1		
25	Usługa wdrożenia systemu PAM	D.7	usługa	1		
26	Usługa wdrożenia systemu VMP	D.8	usługa	1		
27	Usługa wdrożenia i szkolenia systemu SIEM	D.9	usługa	1		
28	Usługa segmentacji i rekonfiguracji sieci OT/IT	D.10	usługa	1		
29	Usługa wdrożenia i konfiguracji urządzeń brzegowych OT	D.2	usługa	1		
	RAZEM (całość zamówienia)					

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU
CENTRUM PROJEKTÓW POLSKA CYFROWA