**Przedsiębiorstwo Wodociągów i Kanalizacji „AQUA" Spółka z o.o.**
siedziba:12-100 Szczytno ul. Polska 38 , NIP 745-000-17-18, kapitał Spółki: 559400.-zł
Sąd Rejonowy w Olsztynie, VIII Wydział Gospodarczy Krajowego Rejestru Sądowego nr KRS: 0000000574
tel. 0 89 624 22 41

Szczytno, dnia 16.06.2026r.

**Rada Miasta Szczytno**
**Komisja Gospodarki Komunalnej,**
**Prawa i Bezpieczeństwa**

dotyczy: Informacji o stanie cyberbezpieczeństwa spółek komunalnych - ryzyka, zabezpieczenia, procedury awaryjne.

W Przedsiębiorstwie mogą występować ryzyka w zakresie przestrzeni cybernetycznej:

1. Nieautoryzowane logowania się do komunikacji danych telemetrycznych, w wyniku czego mogą następować zakłócenia prawidłowej pracy Stacji Uzdatniania Wody Lemany i ul. Polska 38.
2. Zakłócenia w pracy monitoringu wizyjnego terenu Stacji Uzdatniania Wody Lemany,
3. Nieautoryzowane logowanie się do wewnętrznej sieci Ethernet Przedsiębiorstwa.
4. Występujące w przestrzeni medialnej nieprawdziwe informacje o włamaniach oraz hakowaniu oprogramowania pracy Stacji Uzdatniania Wody.

W wyniku podjętych działań powyżej wymienione ryzyka zostały zabezpieczone lub wyeliminowane w następujący sposób:

1. Komunikacja przesyłania danych telemetrycznych pracy między Stacją Uzdatniania Wody Lemany i Stacją Uzdatniania Wody ul. Polska 38 jest realizowana za pomocą APN (unikalny identyfikator urządzenia). Łączenie jest wykonywane po transmisji 5G za pomocą kart SIM. Moduły komunikacyjne z kartami SIM są tylko i wyłączenie połączone między sobą na indywidualnych adresach IP. Dodatkowo trzeba znać bardzo dokładnie parametry kart i adres IP żeby móc się zalogować do modułów komunikacyjnych, jak też same parametry logowania. Kontrolę dostępu kart jak również parametrów tych kart i parametrów łącza kontroluje firma nadzorująca pracę modułów telemetrycznych na zlecenie PWiK AQUA Sp. z o.o. Parametry

te są ogólnie zastrzeżone i udostępniane tylko na polecenie Kierownika Oczyszczalni Ścieków i Utrzymania Ruchu PWiK AQUA Sp. z o.o. W związku, z tym możliwość włamania się do komunikacji między Stacją Uzdatniania Wody jest praktycznie niemożliwa.

Dodatkowo w celu ochrony obiektów i zabezpieczenia terenu Stacji Uzdatniania Wody Lemany wraz ze studniami głębinowymi w tym roku zamontowano 12 kamer monitoringu wizyjnego. Docelowo

ma być zamontowanych około 20 kamer. Obraz wizyjny przesyłany jest do siedziby Przedsiębiorstwa.

2. W celu wyeliminowania możliwości logowania się do monitoringu wizyjnego terenu Stacji Uzdatniania Wody Lemany utworzony został kanał radiowy o wysokiej transmisji danych przesyłanych za pomocą anten parabolicznych pomiędzy Stacją Lemany i siedzibą Przedsiębiorstwa wykorzystując maszt wieży ratuszowej Urzędu Miejskiego. Dzięki temu wydzielony kanał nie jest połączony z siecią internetową ogólnodostępną, co wyeliminowało jakąkolwiek możliwość logowania się z zewnątrz do sieci wewnętrznego monitoringu wizyjnego. Dodatkowo w przyszłości kanał transmisyjny zostanie wykorzystany do przesyłania dodatkowych danych telemetrycznych.
3. W siedzibie Przedsiębiorstwa zamontowany jest serwer do obsługi internetowej z danymi klientów na którym zainstalowane są najnowsze zabezpieczenia typu firewall oraz oprogramowanie antywirusowe. Oprogramowanie jest na bieżąco aktualizowane do bieżących wersji. Przedsiębiorstwo posiada licencję na użytkowanie wyżej wymienionego oprogramowania przedłużane corocznie.
4. W okresie ostatniego roku zanotowano liczne informacje medialne, szczególnie na stronach cyberdefense24.pl, dotyczące nieautoryzowanego logowania do stacji operatorskich Stacji Uzdatniania Wody Lemany i zmian parametrów pracy Stacji przez rosyjskich hakerów oraz zakłóceń w dostarczaniu wody mieszkańcom miasta. Na internetowych stronach rosyjskich hakerów zostały opublikowane nagrania pokazujące moment logowania i zmian tych parametrów.

   Pracownicy nadzorujący pracę Stacji Uzdatniania Wody Lemany nie odnotowali jakichkolwiek działań z zewnątrz. Pokazane na stronach rosyjskich wizualizacje technologiczne Stacji nie odpowiadają rzeczywistym wizualizacjom zainstalowanym i pracującym na Stacjach Uzdatniania Wody Lemany i ul. Polska 38. Trudno przeciwdziałać pojawianiu się takich

informacji. Przedsiębiorstwo w tym okresie dementowało te informacje przesyłając sprostowania dla służb mundurowych, jak też dla władz samorządowych i centralnych.

W wyniku zastosowania wyżej wymienionych zabezpieczeń wyeliminowano w znaczący sposób lub całkowicie możliwość nieautoryzowanych logowań i zakłóceń w pracy w Stacjach Uzdatniania Wody oraz w samej siedzibie Przedsiębiorstwa.

W przypadku odnotowania przez pracowników zakłóceń i nieautoryzowanych zmian parametrów w pracy Stacji Uzdatniania Wody Lemany obsługa obu Stacji szybko zauważyłaby takie zdarzenie i przeszłaby na sterowanie miejscowe bez komunikacji, do czasu znalezienia przyczyny takiego zdarzenia, sprawdzenia nieautoryzowanych działań i możliwości dodatkowego zabezpieczenia. Na korzyść działa również całodobowa kontrola i nadzór pracy przez pracowników Przedsiębiorstwa obu Stacji Uzdatniania Wody Lemany i ul. Polska 38, w wyniku czego reakcja na nieprawidłową pracę Stacji jest natychmiastowa, co przekłada się na zminimalizowanie przerw w zaopatrzenie miasta w wodę.

W przypadku utraty danych na serwerze w siedzibie, Przedsiębiorstwo ma możliwość odtworzenia danych z zewnętrznego źródła, na którym jest wykonywany zakodowany backup wszystkich danych.

PREZES ZARZĄDU

Arkadiusz Brzozowski

EKO SZCZYTNO
NON PROFIT SP. Z O.O.

ul. Krzysztofa Mrongowiusza 1D, 12-100 Szczytno
tel. 89 672 32 65
www.eko-szczytno.pl, E-Mail: biuro@eko-szczytno.pl
NIP 745-186-63-66 , REGON 543164126 , KRS 0001210692 , BDO 000698245

EKO - 245/2026.ES

Szczytno, dnia 17.06.2026 r.

**Komisji Gospodarki Komunalnej,**

**Prawa i Bezpieczeństwa Publicznego**

INFORMACJA O STANIE CYBERBEZPIECZEŃSTWA

EKO – SZCZYTNO NON PROFIT

SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ W SZCZYTNIE

(Ryzyka, Zabezpieczenia, Procedury)

**1. Charakterystyka informatyczna spółki.**

Infrastrukturą informatyczną w spółce zarządza podmiot zewnętrzny wyspecjalizowany w usługach IT na podstawie umowy.

**Sprzęt:** Komputery stacjonarne 3szt., tablety dla kierowców pojazdów 5szt..

**Systemy:** Wykorzystywane oprogramowanie księgowo-finansowe, kadrowo-płacowe, aplikacje biurowe, a także system monitoringu i realizacji zadaniowych przypisanym pojazdom specjalistycznym do odbioru odpadów komunalnych.

**Serwer:** Centralny serwer lokalny (ZKM), którego dyski funkcjonują w bezpiecznej konfiguracji (RAID 1).

**2. Zagrożenia cyberbezpieczeństwa.**

Głównymi zagrożeniami dla spółki są fałszywe maile typu phishing, złośliwe oprogramowania, błędy ludzkie czyli nieprzestrzeganie procedur oraz awarie sprzętu.

Spółka prowadzi regularne szkolenia pracowników z zakresu bezpieczeństwa oraz procedur zapobiegania błędów ludzkich.

**3. Środki ochrony.**

W spółce wdrażana jest **Polityka Ochrony Danych Osobowych,** pracownicy są szkoleni przez zewnętrznego **Inspektora Danych Osobowych.**

Wdrożono scentralizowany systemy ochrony takich jak **NORTON, ESET,** który jest zainstalowany na wszystkich stacjonarnych stacjach roboczych.

Dostęp do poszczególnych systemów, programów i aplikacji nadawany jest imiennie dla poszczególnych pracowników.

**4. Kopie zapasowe i odtwarzanie danych**

**Kopia lokalna**: kluczowe bazy danych i pliki utrzymywane na serwerze (Dell), dodatkowo są kopiowane na kolejny zapasowy dysk sieciowy.

**Kopie bezpieczeństwa** przechowywane są na oddzielnym serwerze, co ma na celu zabezpieczenie danych przed ich utratą.

**Procedura BCP** (ciągłości działania): W ramach umów serwisowych zewnętrzna firma IT gwarantuje, w przypadku uszkodzenia serwera lub krytycznej stacji roboczej, szybkie uruchomienie jednostki sprzętowej w celu wznowienia pracy biura.

**5. Procedury awaryjne**

Pracownicy zgodnie z instrukcją są zobligowani do bezzwłocznego zgłoszenia wykrytych incydentów dla przełożonych, zewnętrznego podmiotowi w ramach usług IT oraz zewnętrznemu Inspektorowi Danych Osobowych.

**6. Incydenty cyberbezpieczeństwa od 11.2025r do 05.2026r.**

Spółka w okresie funkcjonowania nie odnotowała żadnych incydentów.

**7. Plan działanie.**

Przeprowadzenie systematycznych szkoleń dla pracowników w zakresie cyberbezpieczeństwa i zagrożeń internetowych.

Cykliczna aktualizacja systemów i aplikacji.

Wdrożenie procedur RODO.

PREZES ZARZĄDU
inż. Daniel Zaborowski

Szczytno, dnia 17 czerwca 2026 r.

ZAKŁAD KOMUNIKACJI MIEJSKIEJ
SP Z O.O.
12-100 SZCZYTNO
ul. Mrongowiusza 1 D
tel./fax 89 624 33 -54
NIP 745-16-94-801

**Komisja Gospodarki Komunalnej,**
**Prawa i Bezpieczeństwa**

**INFORMACJA O STANIE CYBERBEZPIECZEŃSTWA**

**ZAKŁADU KOMUNIKACJI MIEJSKIEJ SPÓŁKA Z OGRANICZONA ODPOWIEDZIALNOŚCIĄ W SZCZYTNIE**

**– RYZYKA, ZABEZPIECZENIA, PROCEDURY**

**1. Charakterystyka środowiska informatycznego:**

- Infrastrukturą informatyczną Zakładu Komunikacji Miejskiej w Szczytnie opiekuje się i zarządza **zewnętrzna firma specjalizująca się w usługach IT.**
- Opieka nad danymi osobowymi **IDO** realizowana jest z podmiotem zewnętrznym.
- **Sprzęt:** w skład wykorzystywanego sprzętu wchodzą komputery stacjonarne, laptopy (będące do dyspozycji mechaników) oraz urządzenia peryferyjne wykorzystywane do obsługi administracyjnej i operacyjnej jednostki.
- **Serwer:** Centralny serwer lokalny, którego dyski funkcjonują w bezpiecznej konfiguracji (RAID 1).
- **Systemy:** Użytkowane są systemy i aplikacje niezbędne do realizacji zadań jednostki, w szczególności w zakresie administracji, księgowości, kadr i płac oraz bieżącej działalności operacyjnej Zakładu. Systemy i aplikacja do kontroli przejazdów autobusu zgodnie z rozkładami jazdy są zabezpieczone przez firmę zewnętrzną.

**2. Główne zagrożenia cyberbezpieczeństwa:**

- **Najistotniejsze zidentyfikowane ryzyka** obejmują ataki socjotechniczne (w tym phishing), złośliwe oprogramowanie, nieuprawniony dostęp do systemów i danych, błędy ludzkie oraz awarie sprzętu lub oprogramowania.
- **Przeciwdziałanie:** Spółka regularnie szkoli personel z zakresu bezpieczeństwa, aby zapobiegać błędom ludzkim. Dodatkowo, zespół zewnętrznej firmy IT pozostaje w stałej dyspozycji i interweniuje w przypadku zauważenia jakichkolwiek podejrzanych zdarzeń i działań.

**3. Stosowane środki ochrony:**

- W spółce formalnie wdrożone jest Polityka Ochrony Danych Osobowych
- Na stacjach roboczych i urządzeniach końcowych stosowane jest oprogramowanie antywirusowe oraz aktualne mechanizmy ochronne.
- Dostęp do systemów informatycznych nadawany jest wyłącznie upoważnionym pracownikom, zgodnie z zakresem obowiązków.

- Stosowane są hasła dostępu, ograniczenia uprawnień użytkowników oraz zasady „czystego biurka" i „czystego ekranu".
- Realizowane są okresowe przeglądy i aktualizacje zabezpieczeń środowiska informatycznego.

**4. Kopie zapasowe i odtwarzanie danych:**

- **Kopia lokalna:** kluczowe bazy danych i pliki utrzymywane na serwerze (Dell), dodatkowo są kopiowane na kolejny zapasowy dysk sieciowy.
- **Kopie bezpieczeństwa** przechowywane są na oddzielnym serwerze, co ma na celu zabezpieczenie danych przed ich utratą.
- **Procedura BCP** (ciągłości działania): W ramach umów serwisowych zewnętrzna firma IT gwarantuje, w przypadku uszkodzenia serwera lub krytycznej stacji roboczej, szybkie uruchomienie jednostki sprzętowej w celu wznowienia pracy biura.

**5. Procedury awaryjne i reagowanie na incydenty:**

- W ramach obsługi informatycznej zapewnione są działania serwisowe umożliwiające szybkie usunięcie awarii oraz przywrócenie sprawności sprzętu i oprogramowania.
- Pracownicy są zobowiązani do niezwłocznego zgłaszania wszelkich zauważonych incydentów, nieprawidłowości lub podejrzeń naruszenia bezpieczeństwa przełożonym oraz osobom odpowiedzialnym za obsługę IT.
- Każdy pracownik zobligowany jest przez wewnętrzne instrukcje do bezzwłocznego zgłaszania wykrytych incydentów lub podatności przełożonemu, zespołowi IT oraz Inspektorowi Ochrony Danych (IOD)
- Wszelkie incydenty i problemy związane z bezpieczeństwem są dokumentowane i analizowane.
- W przypadku stwierdzenia naruszenia ochrony danych osobowych podejmowane są działania zgodne z obowiązującymi przepisami prawa, w tym – jeśli zachodzi taka konieczność – zgłoszenie naruszenia do właściwego organu nadzorczego w ustawowym terminie.

**6. Incydenty cyberbezpieczeństwa w 2025 roku:**

- W 2025 roku w Zakładzie Komunikacji Miejskiej w Szczytnie **nie odnotowano żadnych incydentów** naruszających cyberbezpieczeństwa jednostki.

**7. Planowane działania:**

- Kontynuowanie i aktualizacja szkoleń pracowników w zakresie cyberbezpieczeństwa oraz zagrożeń związanych z korzystaniem z poczty elektronicznej i Internetu.
- Dalsze wzmacnianie zabezpieczeń technicznych i organizacyjnych.
- Stopniowa modernizacja sprzętu komputerowego oraz aktualizacja oprogramowania do wspieranych wersji.
- Doskonalenie procedur tworzenia kopii zapasowych oraz reagowania na incydenty bezpieczeństwa.

PREZES ZARZĄDU
inż. Daniel Zaborowski

Szczytno, dnia 16 czerwca 2026 r.

**Komisja Gospodarki Komunalnej,**
**Prawa i Bezpieczeństwa**

INFORMACJA O STANIE CYBERBEZPIECZEŃSTWA TOWARZYSTWA BUDOWNICTWA SPOŁECZNEGO SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ „JURAND" W SZCZYTNIE – RYZYKA, ZABEZPIECZENIA, PROCEDURY

1. **Charakterystyka środowiska informatycznego:**
   - Infrastrukturą informatyczną spółki opiekuje się i zarządza **zewnętrzna firma specjalizująca się w usługach IT.**
   - **Sprzęt:** Stacje robocze to komputery stacjonarne oraz jeden laptop (będący do dyspozycji dyrekcji).
   - **Serwer:** Centralny serwer lokalny, którego dyski funkcjonują w bezpiecznej konfiguracji RAID 1 (lustrzane odbicie zabezpieczające przed awarią dysku).
   - **Systemy:** Wykorzystywane jest dedykowane oprogramowanie finansowo-księgowe, kadrowo-płacowe oraz aplikacje biurowe.

2. **Główne zagrożenia cyberbezpieczeństwa:**
   - **Najistotniejsze identyfikowane ryzyka to:** ataki socjotechniczne (np. fałszywe maile typu phishing), złośliwe oprogramowanie (w tym ransomware szyfrujące pliki dla okupu), błędy ludzkie (nieprzestrzeganie procedur) oraz awarie sprzętu.
   - **Przeciwdziałanie:** Spółka regularnie szkoli personel z zakresu bezpieczeństwa, aby zapobiegać błędom ludzkim. Dodatkowo, zespół zewnętrznej firmy IT pozostaje w stałej dyspozycji i interweniuje w przypadku zauważenia jakichkolwiek podejrzanych zdarzeń i działań.

3. **Stosowane środki ochrony:**
   - W spółce formalnie wdrożona jest **Polityka Ochrony Danych Osobowych**, z którą pracownicy są zapoznawani.
   - Wdrożono scentralizowany system antywirusowy **ESET PROTECT Entry**, który jest zainstalowany i działa na każdej stacji roboczej w organizacji.
   - Dostęp do poszczególnych systemów i programów nadawany jest na podstawie sformalizowanych, imiennych upoważnień.

- Stosowane są rygorystyczne procedury ochrony fizycznej, takie jak obowiązek stosowania zasady "czystego biurka" i "czystego ekranu".
- Realizowane są cykliczne audyty skuteczności zabezpieczeń środowiska.

4. **Kopie zapasowe i odtwarzanie danych:**
   - **Kopia lokalna:** Kluczowe bazy danych i pliki utrzymywane na serwerze (działającym w RAID 1) są dodatkowo kopiowane na kolejny zapasowy dysk wbudowany w serwer.
   - **Duplikacja na nośnik zewnętrzny:** Kopie zapasowe są automatycznie duplikowane na niezależny dysk sieciowy (NAS), zlokalizowany w odrębnym pomieszczeniu w celu zabezpieczenia fizycznego (np. przed pożarem).
   - **Procedura BCP (ciągłości działania):** W ramach umów serwisowych zewnętrzna firma IT gwarantuje, w przypadku uszkodzenia serwera lub krytycznej stacji roboczej, szybkie dostarczenie i uruchomienie **tymczasowej jednostki sprzętowej** w celu wznowienia pracy biura.

5. **Procedury awaryjne i reagowanie na incydenty:**
   - Każdy pracownik zobligowany jest przez wewnętrzne instrukcje do bezzwłocznego zgłaszania wykrytych incydentów lub podatności przełożonemu, zespołowi IT oraz Inspektorowi Ochrony Danych (IOD).
   - Wszelkie naruszenia i problemy są na bieżąco dokumentowane i ewidencjonowane.
   - Procedury określają konieczność oceny skali incydentu i, w razie wysokiego ryzyka, zgłoszenia naruszenia do organu nadzorczego (UODO) w ustawowym terminie 72 godzin.

6. **Incydenty cyberbezpieczeństwa w 2025 roku:**
   - W 2025 roku w TBS Sp. z o.o. "JURAND" **nie odnotowano żadnych incydentów** naruszających cyberbezpieczeństwo spółki.

7. **Planowane działania:**
   - Przeprowadzenie aktualizacyjnych, dedykowanych szkoleń dla całego personelu pod kątem cyberbezpieczeństwa i uczulenia na najnowsze zagrożenia internetowe.
   - Stopniowe wycofywanie sprzętu i wyeliminowanie komputerów pracujących na starych, niewspieranych systemach operacyjnych (Windows 10).

PREZES ZARZĄDU
mgr Karolina Łukaszewska