



Poznań, 16 września 2012 r.

**RAPORT Z PRZEPROWADZONEJ WIZJI LOKALNEJ,  
INWENTARYZACJI ELEKTRONICZNYCH SYSTEMÓW ZAPEZPIECZEŃ  
ORAZ ANALIZY PROCEDUR OCHRONY  
NA OBIEKTACH ZARZĄDZANYCH PRZEZ MZK Sp. z o.o. w Kostrzynie nad Odrą**

*Niniejsze opracowanie ma na celu przedstawienie wyników praktycznego sprawdzenia poziomu bezpieczeństwa elektronicznych systemów zabezpieczeń, związanych z tym procedur oraz czynności eksploatacyjno serwisowych, identyfikację słabych punktów, analizę potrzeb oraz określenie obszarów ochrony wymagających zmian.*

**1. Zbiornik Wody na Wzgórzu Grudzia**

*1.1. Charakterystyka obiektu*

*Teren o powierzchni około 46,8 [a], ogrodzony płotem, wyposażony w system alarmowy.*

*1.2. Ocena ryzyka i analiza zagrożeń-wnioski*

- Obiekt położony w terenie niezabudowanym,*
- Brak stałej obsługi i nadzoru,*
- Obiekt narażony na akty sabotażowe,*
- Obiekt narażony na akty wandalizmu i kradzieży.*

*1.3. Wyposażenie obiektu w elektroniczne systemy zabezpieczeń – stan istniejący*

- Teren zewnętrzny zabezpieczony jest barierami mikrofalowymi podłączonymi do centrali alarmowej,*
- Pomieszczenie techniczne zabezpieczone za pomocą czujki pasywnej podczerwieni,*
- Sygnał transmitowany za pomocą toru bezprzewodowego do stacji monitorowania alarmów [SMA] zlokalizowanej w Bazie MZK przy ul Kopernika 4a.*

#### 1.4. Określenie poziomu dostępu do obiektu

W ramach reorganizacji systemu ochrony i wdrażania procedur wspomagających funkcjonowanie systemu zarządzania bezpieczeństwem należy jednoznacznie określić poziom dostępu do obiektu oraz :

- należy wyznaczyć osobę odpowiedzialną za obiekt;

- należy określić osoby, które mają dostęp do obiektu;
- należy określić indywidualne kody dostępu do systemu alarmowego oraz hasła odwoławcze do komunikacji z agencją ochrony.

#### 1.5. Procedury postępowania w przypadku alarmu oraz dozoru

Do obowiązków służb ochrony należy kontrola stanu toru transmisyjnego pomiędzy [SMA] a obiektem, kontrolowanie stanu uzbrojenia/ rozbrojenia systemu, weryfikacja alarmu, wysłanie patrolu, adnotacje o alarmach prowadzone w książce obiektu,

#### DOSTĘP DO OBIEKTU

- a. osoba uprawniona uruchamia pilotem odliczanie czasu na wejście do obiektu,
- b. w trakcie odliczania przez centralę alarmową czasu na wejście, osoba uprawniona wchodzi na teren i indywidualnym kodem rozbraja system alarmowy,
- c. po rozbrojeniu systemu alarmowego należy niezwłocznie, telefonicznie, poinformować operatora stacji monitorującej o wejściu na teren obiektu chronionego oraz określić szacunkowy czas przebywania na terenie chronionym, operator weryfikuje osobę uprawnioną do wejścia na teren poprzez indywidualne hasło odwoławcze użytkownika,
- d. informacja o rozbrojeniu systemu alarmowego jest przekazywana automatycznie przez centralę alarmową do SMA i jeśli operator w czasie 5 minut nie otrzyma telefonicznego potwierdzenia od osoby dokonującej rozbrojenia, traktuje zdarzenie, jako alarmowe – alarm napadowy,
- e. jeśli czas przebywania na obiekcie podany przez użytkownika, operatorowi SMA zostanie przekroczony, operator weryfikuje telefonicznie (lub poprzez system CCTV) czy użytkownik przebywa nadal na obiekcie, brak potwierdzenia traktowany jest, jako zdarzenie alarmowe – alarm napadowy,
- f. przed opuszczeniem obiektu użytkownik uzbraja system alarmowy indywidualnym kodem. Informacja o uzbrojeniu alarmu zostaje automatycznie przekazana przez centralę alarmową do SMA.

#### DOSTĘP DO OBIEKTU – WEJŚCIE POD PRZYMUSEM

- a. osoba uprawniona uruchamia pilotem odliczanie czasu na wejście do obiektu pod przymusem osoby niepowołanej,

- b. w trakcie odliczania przez centralę alarmową czasu na wejście, osoba uprawniona wchodzi na teren i kodem przymusu rozbraja system alarmowy pod przymusem osoby niepowołanej,*
- c. przed wejściem na teren obiektu należy telefonicznie poinformować operatora stacji monitorującej o konieczności wejścia na teren obiektu chronionego oraz określić szacunkowy czas przebywania na terenie chronionym, operator weryfikuje osobę uprawnioną do wejścia na teren poprzez indywidualne hasło odwoławcze użytkownika. Użytkownik pod przymusem podaje hasło identyfikowane przez operatora, jako hasło przymusowego rozbrojenia alarmu, kolejna działania operator wykonuje zgodnie ze schematem alarmu napadowego.*

#### ALARM WŁAMANIOWY

- a. otrzymanie alarmu włamaniowego,*
- b. weryfikacja – sprawdzenie obrazów bieżących z kamer,*
- c. wysłanie patrolu,*
- d. ocena sytuacji – postępowanie służb w przypadku włamania lub alarmu fałszywego określone odrębnymi procedurami,*
- e. powiadomienie osób odpowiedzialnych,*
- f. reset sygnału,*
- g. uzbrojenie systemu,*
- h. powrót patrolu i dokonanie adnotacji w książce obiektu,*

#### ALARM NAPADOWY

- a. otrzymanie alarmu napadowego,*
- b. wysłanie patrolu,*
- c. ocena sytuacji – postępowanie służb w przypadku napadu określone odrębnymi procedurami,*
- d. powiadomienie osób odpowiedzialnych,*
- e. reset sygnału,*
- f. uzbrojenie systemu,*
- g. powrót patrolu i dokonanie adnotacji w książce obiektu,*

#### UTRATA ŁĄCZNOŚCI Z OBIEKTEM

- a. otrzymanie informacji o awarii,*
- b. wysłanie patrolu,*
- c. ocena sytuacji,*
- d. powiadomienie osób odpowiedzialnych za dozór i serwis,*
- e. uzbrojenie systemu,*
- f. powrót patrolu i dokonanie adnotacji w książce obiektu,*
- g. wzmożone patrole ochrony fizycznej do czasu usunięcia usterki,*

#### 1.6. Określenie standaryzacji rozbudowy elektronicznych systemów zabezpieczeń

- *Istniejący system należy sprawdzić/rozbudować w oparciu o urządzenia elektronicznych systemów zabezpieczeń w klasie co najmniej C – urządzenia profesjonalne,*
- *Centrala alarmowa musi być zabezpieczona stykiem antysabotażowym ,*
- *Zasilanie centrali musi być wykonane z odrębnego obwodu rozdzielnic elektrycznej z odpowiednio dobranym zabezpieczeniem przeciążeniowo – zwarciovym,*
- *Centrala musi posiadać zasilanie rezerwowe – akumulator z czasem podtrzymania co najmniej 72 h w dozorze, 0,5 h w alarmie,*
- *Styk antysabotażowy klawiatury/manipulatora centrali musi być podłączony do centrali alarmowej,*
- *Okablowanie magistralowe oraz linii dozorowych musi być zabezpieczone przed uszkodzeniami mechanicznymi (wewnątrz instalację prowadzić w rurkach RL natomiast na zewnątrz w rurach osłonowych np. AROT),*
- *Wszystkie linie dozorowe muszą być parametryzowane w konfiguracji 2EOL (wartości rezystancji zgodne z typem centrali),*
- *Wszystkie puszk połączeniowe muszą być wyposażone w styki antysabotażowe włączone w obwody dozorowe,*
- *Drzwi do pomieszczenia technicznego zabezpieczyć kontaktronem, co najmniej w klasie C,*
- *Pomieszczenie techniczne zabezpieczyć czujką dualną co najmniej w klasie C,*
- *Pomieszczenie techniczne zabezpieczyć przyciskiem antynapadowym, co najmniej w klasie C,*
- *Sygnalizator optyczno-akustyczny zlokalizować na zewnątrz na wysokości, co najmniej 2,5m, styk antysabotażowy sygnalizatora podłączyć do centrali,*
- *Wszystkie połączenia przewodów, rezystorów należy wykonać, jako lutowane,*
- *Włazy studni zabezpieczyć przed otwarciem przy pomocy kontaktronu – klasa, co najmniej C, kontaktron do zastosowań zewnętrznych,*
- *Teren zewnętrzny dozorować dodatkowo przy pomocy systemu nadzoru wizyjnego - 2 kamery dualne - sygnał transmitowany za pomocą toru bezprzewodowego do stacji monitorowania alarmów [SMA] zlokalizowanej w Bazie MZK przy ul Kopernika 4a,*
- *Kody do rozbrojenia/uzbrojenia systemu mogą być znane tylko osobom wyznaczonym przez właściciela do czynności eksploatacyjnych, serwisowych i dozorowych. Po nadaniu uprawnień do znajomości kodu (oraz posiadania pilota) każdy pracownik musi złożyć podpis potwierdzający zapoznanie oraz bezwzględne przestrzeganie tajemnicy,*
- *Każdorazowo po rezygnacji bądź zwolnieniu z pracy pracownika posiadającego wcześniej dostęp do obiektu należy bezzwłocznie zmienić kod dostępu oraz poinformować odpowiedzialnych pracowników – zmiany odnotować w książce kodów. Po zmianie kodu każdy pracownik musi złożyć podpis potwierdzający zapoznanie oraz bezwzględne przestrzeganie tajemnicy,*

### *1.7. Podział na strefy dozorowe*

- *Strefa I – teren zewnętrzny dozorowany barierami mikrofalowymi – rozbrajanie dualne (pilot radiolinii rozpoczynający procedurę rozbrajania z czasem na wejście + kod wprowadzony na manipulatorze),*
- *Strefa II – pomieszczenie techniczne (kod wprowadzony na manipulatorze),*
- *Strefa III – włązy studni (kod wprowadzony na manipulatorze),*

### *1.8. Przeglądy techniczne systemów*

- *Co najmniej raz na kwartał należy przeprowadzić czynności konserwacyjne polegające na sprawdzeniu parametrów wszystkich urządzeń peryferyjnych,*
- *Należy przeprowadzić test transmisji sygnału alarmowego,*
- *Należy odkurzyć, wyczyścić detektory, kamery, itp.,*
- *Należy sprawdzić stan akumulatora zasilania rezerwowego,*
- *W celu eliminacji fałszywych alarmów należy kosić trawę oraz dbać o odśnieżanie w obszarze działania barier mikrofalowych – wyznaczyć osobę odpowiedzialną.*

### *1.9. Uwagi*

- *Niniejsze opracowanie nie dotyczy procedur związanych z doborem zabezpieczeń mechanicznych,*
- *Niniejsze opracowanie nie dotyczy procedur związanych z przechowywaniem, dysponowaniem, zarządzaniem kluczami – zarządzanie kluczami powinno się odbywać poprzez firmę świadczącą usługi ochrony fizycznej (bazując na odrębnych procedurach opracowanych przez firmę świadczącą usługi ochrony fizycznej i zaakceptowanych przez MZK Sp. z o.o.).*
- *Na prace związane z modernizacją elektronicznych systemów zabezpieczeń należy opracować dokumentację projektową sporządzoną przez osobę uprawnioną. Prace należy prowadzić pod nadzorem projektanta/inspektora.*

## **2. Ujęcie wody przy ul. Prostej**

### *2.1. Charakterystyka obiektu.*

*Obiekt budowlany w skład, którego wchodzi budynek gospodarczy, warsztat, budynek stacji pomp, budynek rozdzielni elektrycznej, studnie głębinowe-20 szt., teren o powierzchni około 513,32 [a], ogrodzony płotem, wyposażony w system alarmowy oraz kamery obrotowe.*

### *2.2. Ocena ryzyka i analiza zagrożeń-wnioski*

- Obiekt położony w terenie niezabudowanym,*
- Brak stałej obsługi i nadzoru,*
- Obiekt narażony na akty sabotażowe,*
- Obiekt narażony na akty wandalizmu i kradzieży.*

### *2.3. Wyposażenie obiektu w elektroniczne systemy zabezpieczeń – stan istniejący*

- Teren zewnętrzny zabezpieczony jest barierami mikrofalowymi podłączonymi do centrali alarmowej,*
- Pomieszczenie techniczne zabezpieczone za pomocą czujki pasywnej podczerwieni,*
- Sygnał alarmowy transmitowany za pomocą toru bezprzewodowego do stacji monitorowania alarmów [SMA] zlokalizowanej w Bazie MZK przy ul Kopernika 4a,*
- Sygnały wizyjne transmitowane za pomocą toru bezprzewodowego do stacji monitorowania alarmów [SMA] zlokalizowanej w Bazie MZK przy ul Kopernika 4a,*

### *2.4. Określenie poziomu dostępu do obiektu*

*W ramach reorganizacji systemu ochrony i wdrażania procedur wspomagających funkcjonowanie systemu zarządzania bezpieczeństwem należy jednoznacznie określić poziom dostępu do obiektu oraz • należy wyznaczyć osobę odpowiedzialną za obiekt,*

- należy określić osoby, które mają dostęp do obiektu,*
- należy określić indywidualne kody dostępu do systemu alarmowego oraz hasła odwoławcze do komunikacji z agencją ochrony.*

### *2.5. Procedury postępowania w przypadku alarmu oraz dozoru*

*Do obowiązków służb ochrony należy kontrola stanu toru transmisyjnego pomiędzy [SMA] a obiektem, kontrolowanie stanu uzbrojenia/ rozbrojenia systemu, weryfikacja alarmu, wysłanie patrolu, adnotacje o alarmach prowadzone w książce obiektu,*

### DOSTĘP DO OBIEKTU

- a. osoba uprawniona uruchamia pilotem odliczanie czasu na wejście do obiektu
- b. w trakcie odliczania przez centralę alarmową czasu na wejście, osoba uprawniona wchodzi na teren i indywidualnym kodem rozbraja system alarmowy
- c. po rozbrojeniu systemu alarmowego należy niezwłocznie, telefonicznie, poinformować operatora stacji monitorującej o wejściu na teren obiektu chronionego oraz określić szacunkowy czas przebywania na terenie chronionym, operator weryfikuje osobę uprawnioną do wejścia na teren poprzez indywidualne hasło odwoławcze użytkownika
- d. informacja o rozbrojeniu systemu alarmowego jest przekazywana automatycznie przez centralę alarmową do SMA i jeśli operator w czasie 5 minut nie otrzyma telefonicznego potwierdzenia od osoby dokonującej rozbrojenia, traktuje zdarzenie, jako alarmowe – alarm napadowy
- e. jeśli czas przebywania na obiekcie podany przez użytkownika, operatorowi SMA zostanie przekroczony, operator weryfikuje telefonicznie (lub poprzez system CCTV) czy użytkownik przebywa nadal na obiekcie, brak potwierdzenia traktowany jest jako zdarzenie alarmowe – alarm napadowy
- f. przed opuszczeniem obiektu użytkownik uzbraja system alarmowy indywidualnym kodem. Informacja o uzbrojeniu alarmu zostaje automatycznie przekazana przez centralę alarmową do SMA

### DOSTĘP DO OBIEKTU – WEJŚCIE POD PRZYMUSEM

- a. osoba uprawniona uruchamia pilotem odliczanie czasu na wejście do obiektu pod przymusem osoby niepowołanej,
- b. w trakcie odliczania przez centralę alarmową czasu na wejście, osoba uprawniona wchodzi na teren i kodem przymusu rozbraja system alarmowy pod przymusem osoby niepowołanej,
- c. przed wejściem na teren obiektu należy telefonicznie poinformować operatora stacji monitorującej o konieczności wejścia na teren obiektu chronionego oraz określić szacunkowy czas przebywania na terenie chronionym, operator weryfikuje osobę uprawnioną do wejścia na teren poprzez indywidualne hasło odwoławcze użytkownika. Użytkownik pod przymusem podaje hasło identyfikowane przez operatora, jako hasło przymusowego rozbrojenia alarmu, kolejna działania operator wykonuje zgodnie ze schematem alarmu napadowego.

### ALARM WŁAMANIOWY

- a. otrzymanie alarmu włamaniowego,
- b. weryfikacja – sprawdzenie obrazów bieżących z kamer,
- c. wysłanie patrolu,
- d. ocena sytuacji – postępowanie służb w przypadku włamania lub alarmu fałszywego określone odrębnymi procedurami,
- e. powiadomienie osób odpowiedzialnych,

- f. reset sygnału,
- g. uzbrojenie systemu,
- h. powrót patrolu i dokonanie adnotacji w książce obiektu,

#### ALARM NAPADOWY

- a. otrzymanie alarmu napadowego,
- b. wysłanie patrolu,
- c. ocena sytuacji – postępowanie służb w przypadku napadu określone odrębnymi procedurami,
- d. powiadomienie osób odpowiedzialnych,
- e. reset sygnału,
- f. uzbrojenie systemu,
- g. powrót patrolu i dokonanie adnotacji w książce obiektu,

#### UTRATA ŁĄCZNOŚCI Z OBIEKTEM

- a. otrzymanie informacji o awarii,
- b. wysłanie patrolu,
- c. ocena sytuacji,
- d. powiadomienie osób odpowiedzialnych za dozór i serwis,
- e. uzbrojenie systemu,
- f. powrót patrolu i dokonanie adnotacji w książce obiektu,
- g. wzmożone patrole ochrony fizycznej do czasu usunięcia usterki,

### 2.6. Określenie standaryzacji rozbudowy elektronicznych systemów zabezpieczeń

- Istniejący system należy sprawdzić/rozbudować w oparciu o urządzenia elektronicznych systemów zabezpieczeń w klasie co najmniej C – urządzenia profesjonalne,
- Centrala alarmowa musi być zabezpieczona stykiem antysabotażowym ,
- Zasilanie centrali musi być wykonane z odrębnego obwodu rozdzielnic elektrycznej z odpowiednio dobranym zabezpieczeniem przeciążeniowo – zwarciovym,
- Centrala musi posiadać zasilanie rezerwowe – akumulator z czasem podtrzymania co najmniej 72 h w dozorze, 0,5 h w alarmie,
- Styk antysabotażowy klawiatury/manipulatora centrali musi być podłączony do centrali alarmowej,
- Okablowanie magistralowe oraz linii dozorowych musi być zabezpieczone przed uszkodzeniami mechanicznymi (wewnątrz instalację prowadzić w rurkach RL natomiast na zewnątrz w rurach osłonowych np. AROT),
- Wszystkie linie dozorowe muszą być parametryzowane w konfiguracji 2EOL (wartości rezystancji zgodne z typem centrali),



- *Wszystkie puszki połączeniowe muszą być wyposażone w styki antysabotażowe włączone w obwody dozorowe,*
- *Drzwi do pomieszczenia technicznego zabezpieczyć kontaktronem co najmniej w klasie C,*
- *Pomieszczenie techniczne zabezpieczyć czujką dualną co najmniej w klasie C,*
- *Pomieszczenie techniczne zabezpieczyć przyciskiem antynapadowym co najmniej w klasie C,*
- *Sygnalizator optyczno-akustyczny zlokalizować na zewnątrz na wysokości co najmniej 2,5m, styk antysabotażowy sygnalizatora podłączyć do centrali,*
- *Wszystkie połączenia przewodów, rezystorów należy wykonać jako lutowane,*
- *Włazy studni zabezpieczyć przed otwarciem przy pomocy kontaktronu – klasa co najmniej C, kontaktron do zastosowań zewnętrznych,*
- *Teren zewnętrzny dozorować dodatkowo przy pomocy systemu nadzoru wizyjnego - kamery obrotowe - sygnały transmitowane za pomocą toru bezprzewodowego do stacji monitorowania alarmów [SMA] zlokalizowanej w Bazie MZK przy ul Kopernika 4a,*
- *Kody do rozbrojenia/uzbrojenia systemu mogą być znane tylko osobom wyznaczonym przez właściciela do czynności eksploatacyjnych, serwisowych i dozorowych. Po nadaniu uprawnień do znajomości kodu (oraz posiadania pilota) każdy pracownik musi złożyć podpis potwierdzający zapoznanie oraz bezwzględne przestrzeganie tajemnicy,*
- *Każdorazowo po rezygnacji bądź zwolnieniu z pracy pracownika posiadającego wcześniej dostęp do obiektu należy bezzwłocznie zmienić kod dostępu oraz poinformować odpowiedzialnych pracowników – zmiany odnotować w książce kodów. Po zmianie kodu każdy pracownik musi złożyć podpis potwierdzający zapoznanie oraz bezwzględne przestrzeganie tajemnicy,*

## *2.7. Podział na strefy dozorowe*

- *Strefa I – teren zewnętrzny dozorowany barierami mikrofalowymi (linia bramy wjazdowej) – rozbrajanie dualne (pilot radiolinii rozpoczynający procedurę rozbrajania z czasem na wejście + kod wprowadzony na manipulatorze),*
- *Strefa II – teren zewnętrzny dozorowany barierami mikrofalowymi (pozostałe linie) –(kod wprowadzony na manipulatorze),*
- *Strefa III – budynek stacji pomp (kod wprowadzony na manipulatorze),*
- *Strefa IV – włazy/kopułki studni (kod wprowadzony na manipulatorze),*

## *2.8. Przeglądy techniczne systemów.*

- *Co najmniej raz na kwartał należy przeprowadzić czynności konserwacyjne polegające na sprawdzeniu parametrów wszystkich urządzeń peryferyjnych,*
- *Należy przeprowadzić test transmisji sygnału alarmowego,*
- *Należy odkurzyć, wyczyścić detektory, kamery, itp.,*

- *Należy sprawdzić stan akumulatora zasilania rezerwowego,*
- *W celu eliminacji fałszywych alarmów należy kosić trawę oraz dbać o odśnieżanie w obszarze działania barier mikrofalowych – wyznaczyć osobę odpowiedzialną.*

### *2.9. Uwagi*

- *Niniejsze opracowanie nie dotyczy procedur związanych z doborem zabezpieczeń mechanicznych,*
- *Niniejsze opracowanie nie dotyczy procedur związanych z przechowywaniem, dysponowaniem, zarządzaniem kluczami – zarządzanie kluczami powinno się odbywać poprzez firmę świadczącą usługi ochrony fizycznej (bazując na odrębnych procedurach opracowanych przez firmę świadczącą usługi ochrony fizycznej i zaakceptowanych przez MZK Sp. z o.o.).*
- *Na prace związane z modernizacją elektronicznych systemów zabezpieczeń należy opracować dokumentację projektową sporządzoną przez osobę uprawnioną. Prace należy prowadzić pod nadzorem projektanta/inspektora.*

## **3. Ujęcie wody przy ul. Granicznej**

### *3.1. Charakterystyka obiektu.*

*Obiekt budowlany w skład, którego wchodzi budynek stacji uzdatniania wody, zbiorniki-2 szt., studnie głębinowe-3 szt., teren o powierzchni około 92,88 [a], ogrodzony płotem, personel przebywający całą dobę.*

### 3.2. Ocena ryzyka i analiza zagrożeń-wnioski

- Obiekt położony w terenie niezabudowanym,
- Stała obsługa i nadzór nad procesem technologicznym,
- Obiekt narażony na akty sabotażowe,
- Obiekt narażony na akty wandalizmu i kradzieży.

### 3.3. Wyposażenie obiektu w elektroniczne systemy zabezpieczeń – stan istniejący.

- Teren zewnętrzny – brak elektronicznego systemu zabezpieczeń,
- Zbiorniki - brak elektronicznego systemu zabezpieczeń,
- Studnie - brak elektronicznego systemu zabezpieczeń,

### 3.4. Określenie poziomu dostępu do obiektu.

W ramach reorganizacji systemu ochrony i wdrażania procedur wspomagających funkcjonowanie systemu zarządzania bezpieczeństwem należy jednoznacznie określić poziom dostępu do obiektu oraz • należy wyznaczyć osobę odpowiedzialną za obiekt,

- należy określić osoby, które mają dostęp do obiektu,
- należy określić indywidualne kody dostępu do systemu alarmowego oraz hasła odwoławcze do komunikacji z agencją ochrony.

### 3.5. Procedury postępowania w przypadku alarmu oraz dozoru – po zaprojektowaniu i wyposażeniu obiektu w elektroniczne systemy zabezpieczeń.

Do obowiązków służb ochrony należy kontrola stanu toru transmisyjnego pomiędzy [SMA] a obiektem, kontrolowanie stanu uzbrojenia/ rozbrojenia systemu, weryfikacja alarmu, wysłanie patrolu, adnotacje o alarmach prowadzone w książce obiektu,

#### DOSTĘP DO STREFY CHRONIONEJ

- a. osoba uprawniona indywidualnym kodem rozbraja system alarmowy,
- b. po rozbrojeniu systemu alarmowego należy niezwłocznie, telefonicznie, poinformować operatora stacji monitorującej o wejściu na teren strefy chronionej oraz określić szacunkowy czas przebywania w strefie chronionej, operator weryfikuje osobę uprawnioną do wejścia na teren poprzez indywidualne hasło odwoławcze użytkownika,
- c. informacja o rozbrojeniu systemu alarmowego jest przekazywana automatycznie przez centralę alarmową do SMA i jeśli operator w czasie 5 minut nie otrzyma telefonicznego potwierdzenia od osoby dokonującej rozbrojenia, traktuje zdarzenie, jako alarmowe – alarm napadowy,
- d. jeśli czas przebywania na obiekcie podany przez użytkownika, operatorowi SMA zostanie przekroczony, operator weryfikuje telefonicznie (lub poprzez system CCTV) czy użytkownik przebywa nadal w strefie chronionej, brak potwierdzenia traktowany jest, jako zdarzenie alarmowe – alarm napadowy,

- e. po opuszczeniu strefy chronionej użytkownik uzbraja system alarmowy indywidualnym kodem. Informacja o uzbrojeniu alarmu zostaje automatycznie przekazana przez centralę alarmową do SMA.

#### DOSTĘP DO OBIEKTU – WEJŚCIE POD PRZYMUSEM

- a. osoba uprawniona indywidualnym kodem rozbraja system alarmowy pod przymusem osoby niepowołanej,
- b. osoba uprawniona kodem przymusu rozbraja system alarmowy pod przymusem osoby niepowołanej,
- c. przed wejściem do strefy chronionej należy telefonicznie poinformować operatora stacji monitorującej o konieczności wejścia na teren strefy chronionej oraz określić szacunkowy czas przebywania na terenie chronionym, operator weryfikuje osobę uprawnioną do wejścia na teren poprzez indywidualne hasło odwoławcze użytkownika. Użytkownik pod przymusem podaje hasło identyfikowane przez operatora, jako hasło przymusowego rozbrojenia alarmu, kolejne działania operator wykonuje zgodnie ze schematem alarmu napadowego.

#### ALARM WŁAMANIOWY

- a. otrzymanie alarmu włamaniowego,
- b. weryfikacja – sprawdzenie obrazów bieżących z kamer,
- c. wysłanie patrolu,
- d. ocena sytuacji – postępowanie służb w przypadku włamania lub alarmu fałszywego określone odrębnymi procedurami,
- e. powiadomienie osób odpowiedzialnych,
- f. reset sygnału,
- g. uzbrojenie systemu,
- h. powrót patrolu i dokonanie adnotacji w książce obiektu,

#### ALARM NAPADOWY

- a. otrzymanie alarmu napadowego,
- b. wysłanie patrolu,
- c. ocena sytuacji – postępowanie służb w przypadku napadu określone odrębnymi procedurami,
- d. powiadomienie osób odpowiedzialnych,
- e. reset sygnału,
- f. uzbrojenie systemu,
- g. powrót patrolu i dokonanie adnotacji w książce obiektu,

#### UTRATA ŁĄCZNOŚCI Z OBIEKTEM

- a. otrzymanie informacji o awarii,
- b. wysłanie patrolu,
- c. ocena sytuacji,
- d. powiadomienie osób odpowiedzialnych za dozór i serwis,
- e. uzbrojenie systemu,
- f. powrót patrolu i dokonanie adnotacji w książce obiektu,

g. wzmożone patrole ochrony fizycznej do czasu usunięcia usterki,

### 3.6. Określenie standaryzacji projektu i realizacji elektronicznych systemów zabezpieczeń

- Nowoprojektowany system należy wykonać w oparciu o urządzenia elektronicznych systemów zabezpieczeń w klasie co najmniej C – urządzenia profesjonalne,
- Centrala alarmowa musi być zabezpieczona stykiem antysabotażowym ,
- Zasilanie centrali musi być wykonane z odrębnego obwodu rozdzielnic elektrycznej z odpowiednio dobranym zabezpieczeniem przeciążeniowo – zwarciovym,
- Centrala musi posiadać zasilanie rezerwowe – akumulator z czasem podtrzymania co najmniej 72 h w dozorze, 0,5 h w alarmie,
- Styk antysabotażowy klawiatury/manipulatora centrali musi być podłączony do centrali alarmowej,
- Okablowanie magistralowe oraz linii dozorowych musi być zabezpieczone przed uszkodzeniami mechanicznymi (wewnątrz instalację prowadzić w rurkach RL natomiast na zewnątrz w rurach osłonowych np. AROT),
- Wszystkie linie dozorowe muszą być parametryzowane w konfiguracji 2EOL (wartości rezystancji zgodne z typem centrali),
- Wszystkie puszki połączeniowe muszą być wyposażone w styki antysabotażowe włączone w obwody dozorowe,
- Drzwi do pomieszczeń technologicznych technicznego zabezpieczyć kontaktronem co najmniej w klasie C,
- Pomieszczenia techniczne zabezpieczyć czujką dualną co najmniej w klasie C,
- Pomieszczenie stałej obsługi zabezpieczyć przyciskiem antynapadowym co najmniej w klasie C,
- Sygnalizator optyczno-akustyczny zlokalizować na zewnątrz na wysokości, co najmniej 2,5m, styk antysabotażowy sygnalizatora podłączyć do centrali,
- Wszystkie połączenia przewodów, rezystorów należy wykonać jako lutowane,
- Włazy studni zabezpieczyć przed otwarciem przy pomocy kontaktronu – klasa co najmniej C, kontaktron do zastosowań zewnętrznych,
- Teren zewnętrzny dozorować dodatkowo przy pomocy systemu nadzoru wizyjnego - kamery obrotowe - sygnały transmitowane za pomocą toru bezprzewodowego do stacji monitorowania alarmów [SMA] zlokalizowanej w Bazie MZK przy ul Kopernika 4a,
- Zrealizować podgląd lokalny dla służb dozoru technologicznego,
- Kody do rozbrojenia/uzbrojenia systemu mogą być znane tylko osobom wyznaczonym przez właściciela do czynności eksploatacyjnych, serwisowych i dozorowych. Po nadaniu uprawnień do znajomości kodu (oraz posiadania pilota) każdy pracownik musi złożyć podpis potwierdzający zapoznanie oraz bezzwłędne przestrzeganie tajemnicy,
- Każdorazowo po rezygnacji bądź zwolnieniu z pracy pracownika posiadającego wcześniej dostęp do obiektu należy bezzwłocznie zmienić kod dostępu oraz

*poinformować odpowiedzialnych pracowników – zmiany odnotować w książce kodów. Po zmianie kodu każdy pracownik musi złożyć podpis potwierdzający zapoznanie oraz bezwzględne przestrzeganie tajemnicy,*

### *3.7. Podział na strefy dozorowe.*

- Strefa I – teren zewnętrzny dozorowany barierami mikrofalowymi (linia bramy wjazdowej) – rozbrajanie dualne (pilot radiolinii rozpoczynający procedurę rozbrajania z czasem na wejście + kod wprowadzony na manipulatorze),*
- Strefa II – teren zewnętrzny dozorowany barierami mikrofalowymi (pozostałe linie) –(kod wprowadzony na manipulatorze),*
- Strefa III – budynek główny (kod wprowadzony na manipulatorze),*
- Strefa IV – włązy/kopułki studni (kod wprowadzony na manipulatorze),*

### *3.8. Przeglądy techniczne systemów.*

- Co najmniej raz na kwartał należy przeprowadzić czynności konserwacyjne polegające na sprawdzeniu parametrów wszystkich urządzeń peryferyjnych,*
- Należy przeprowadzić test transmisji sygnału alarmowego,*
- Należy odkurzyć, wyczyścić detektory, kamery, itp.,*
- Należy sprawdzić stan akumulatora zasilania rezerwowego,*
- W celu eliminacji fałszywych alarmów należy kosić trawę oraz dbać o odśnieżanie w obszarze działania barier mikrofalowych – wyznaczyć osobę odpowiedzialną.*

### *3.9. Uwagi*

- Niniejsze opracowanie nie dotyczy procedur związanych z doborem zabezpieczeń mechanicznych,*
- Niniejsze opracowanie nie dotyczy procedur związanych z przechowywaniem, dysponowaniem, zarządzaniem kluczami – zarządzanie kluczami powinno się odbywać poprzez firmę świadczącą usługi ochrony fizycznej (bazując na odrębnych procedurach opracowanych przez firmę świadczącą usługi ochrony fizycznej i zaakceptowanych przez MZK Sp. z o.o.).*
- Na prace związane z modernizacją elektronicznych systemów zabezpieczeń należy opracować dokumentację projektową sporządzoną przez osobę uprawnioną. Prace należy prowadzić pod nadzorem projektanta/inspektora.*

## **4. Przepompownia Ścieków ul. Asfaltowa**

### *4.1. Charakterystyka obiektu.*

*Budynek przepompowni zlokalizowany jest na działce o powierzchni około 19,95 [a] ogrodzony, monitorowany poprzez dwie kamery, obraz przesłany do pracowników obsługi oczyszczalni ścieków*

#### 4.2. Ocena ryzyka i analiza zagrożeń-wnioski

- *Obiekt położony w terenie niezabudowanym,*
- *Stąła obsługa i nadzór nad procesem technologicznym,*
- *Obiekt narażony na akty sabotażowe,*
- *Obiekt narażony na akty wandalizmu i kradzieży.*

#### 4.3. Wyposażenie obiektu w elektroniczne systemy zabezpieczeń – stan istniejący

- *Teren zewnętrzny – monitorowany poprzez dwie kamery sytemu telewizji przemysłowej,*
- *Budynki - brak elektronicznego systemu zabezpieczeń.*

#### 4.4. Określenie poziomu dostępu do obiektu

*W ramach reorganizacji systemu ochrony i wdrażania procedur wspomagających funkcjonowanie systemu zarządzania bezpieczeństwem należy jednoznacznie określić poziom dostępu do obiektu oraz • należy wyznaczyć osobę odpowiedzialną za obiekt,*

- *należy określić osoby, które mają dostęp do obiektu,*
- *należy określić indywidualne kody dostępu do systemu alarmowego oraz hasła odwoławcze do komunikacji z agencją ochrony.*
- *należy umożliwić agencji ochrony w Bazie MZK podgląd obrazu z kamer istniejących i ewentualnie nowo zaprojektowanych*

#### 4.5. Procedury postępowania w przypadku alarmu oraz dozoru – po zaprojektowaniu i wyposażeniu obiektu w elektroniczne systemy zabezpieczeń

*Do obowiązków służb ochrony należy kontrola stanu toru transmisyjnego pomiędzy [SMA] a obiektem, kontrolowanie stanu uzbrojenia/ rozbrojenia systemu, weryfikacja alarmu, wysłanie patrolu, adnotacje o alarmach prowadzone w książce obiektu, obiekt zostanie podłączony do projektowanej centrali alarmowej w budynku Miejskiej Oczyszczalni Ścieków, jako odrębna strefa dozorowa.*

#### DOSTĘP DO STREFY CHRONIONEJ

- osoba uprawniona indywidualnym kodem rozbraja system alarmowy,*
- po rozbrojeniu systemu alarmowego należy niezwłocznie, telefonicznie, poinformować operatora stacji monitorującej o wejściu na teren strefy chronionej oraz określić szacunkowy czas przebywania w strefie chronionej, operator weryfikuje osobę uprawnioną do wejścia na teren poprzez indywidualne hasło odwoławcze użytkownika,*



- c. informacja o rozbrojeniu systemu alarmowego jest przekazywana automatycznie przez centralę alarmową do SMA i jeśli operator w czasie 5 minut nie otrzyma telefonicznego potwierdzenia od osoby dokonującej rozbrojenia, traktuje zdarzenie, jako alarmowe – alarm napadowy,
- d. jeśli czas przebywania na obiekcie podany przez użytkownika, operatorowi SMA zostanie przekroczony, operator weryfikuje telefonicznie (lub poprzez system CCTV) czy użytkownik przebywa nadal w strefie chronionej, brak potwierdzenia traktowany jest, jako zdarzenie alarmowe – alarm napadowy,
- e. po opuszczeniu strefy chronionej użytkownik uzbraja system alarmowy indywidualnym kodem. Informacja o uzbrojeniu alarmu zostaje automatycznie przekazana przez centralę alarmową do SMA.

#### DOSTĘP DO OBIEKTU – WEJŚCIE POD PRZYMUSEM

- a. osoba uprawniona indywidualnym kodem rozbraja system alarmowy pod przymusem osoby niepowołanej,
- b. osoba uprawniona kodem przymusu rozbraja system alarmowy pod przymusem osoby niepowołanej,
- c. przed wejściem do strefy chronionej należy telefonicznie poinformować operatora stacji monitorującej o konieczności wejścia na teren strefy chronionej oraz określić szacunkowy czas przebywania na terenie chronionym, operator weryfikuje osobę uprawnioną do wejścia na teren poprzez indywidualne hasło odwoławcze użytkownika. Użytkownik pod przymusem podaje hasło identyfikowane przez operatora, jako hasło przymusowego rozbrojenia alarmu, kolejne działania operator wykonuje zgodnie ze schematem alarmu napadowego.

#### ALARM WŁAMANIOWY

- a. otrzymanie alarmu włamaniowego,
- b. weryfikacja – sprawdzenie obrazów bieżących z kamer,
- c. wysłanie patrolu,
- d. ocena sytuacji – postępowanie służb w przypadku włamania lub alarmu fałszywego określone odrębnymi procedurami,
- e. powiadomienie osób odpowiedzialnych,
- f. reset sygnału,
- g. uzbrojenie systemu,
- h. powrót patrolu i dokonanie adnotacji w książce obiektu,

#### ALARM NAPADOWY

- a. otrzymanie alarmu napadowego,
- b. wysłanie patrolu,
- c. ocena sytuacji – postępowanie służb w przypadku napadu określone odrębnymi procedurami,
- d. powiadomienie osób odpowiedzialnych,
- e. reset sygnału,
- f. uzbrojenie systemu,



*g. powrót patrolu i dokonanie adnotacji w książce obiektu,*

#### *UTRATA ŁACZNOŚCI Z OBIEKTEM*

- a. otrzymanie informacji o awarii,*
- b. wysłanie patrolu,*
- c. ocena sytuacji,*
- d. powiadomienie osób odpowiedzialnych za dozór i serwis,*
- e. uzbrojenie systemu,*
- f. powrót patrolu i dokonanie adnotacji w książce obiektu,*
- g. wzmożone patrole ochrony fizycznej do czasu usunięcia usterki,*

#### *4.6. Określenie standaryzacji projektu i realizacji elektronicznych systemów zabezpieczeń*

- Nowoprojektowany system należy wykonać w oparciu o urządzenia elektronicznych systemów zabezpieczeń w klasie co najmniej C – urządzenia profesjonalne,*
- Centrala alarmowa musi być zabezpieczona stykiem antysabotażowym ,*
- Zasilanie centrali musi być wykonane z odrębnego obwodu rozdzielnic elektrycznej z odpowiednio dobranym zabezpieczeniem przeciążeniowo – zwarciovym,*
- Centrala musi posiadać zasilanie rezerwowe – akumulator z czasem podtrzymania co najmniej 72 h w dozorze, 0,5 h w alarmie,*
- Styk antysabotażowy klawiatury/manipulatora centrali musi być podłączony do centrali alarmowej,*
- Okablowanie magistralowe oraz linii dozorowych musi być zabezpieczone przed uszkodzeniami mechanicznymi (wewnątrz instalację prowadzić w rurkach RL natomiast na zewnątrz w rurach osłonowych np. AROT),*
- Wszystkie linie dozorowe muszą być parametryzowane w konfiguracji 2EOL (wartości rezystancji zgodne z typem centrali),*
- Wszystkie puszkę połączeniowe muszą być wyposażone w styki antysabotażowe włączone w obwody dozorowe,*
- Drzwi do pomieszczeń technicznych technicznego zabezpieczyć kontaktronem co najmniej w klasie C,*
- Pomieszczenia techniczne zabezpieczyć czujką dualną co najmniej w klasie C,*

- *Pomieszczenie stałej obsługi zabezpieczyć przyciskiem antynapadowym co najmniej w klasie C,*
- *Sygnalizator optyczno-akustyczny zlokalizować na zewnątrz na wysokości, co najmniej 2,5m, styk antysabotażowy sygnalizatora podłączyć do centrali,*
- *Wszystkie połączenia przewodów, rezystorów należy wykonać jako lutowane,*
- *Włazy studni zabezpieczyć przed otwarciem przy pomocy kontaktronu – klasa co najmniej C, kontaktron do zastosowań zewnętrznych,*
- *Teren zewnętrzny dozorować dodatkowo przy pomocy systemu nadzoru wizyjnego - kamery obrotowe - sygnały transmitowane za pomocą toru bezprzewodowego do stacji monitorowania alarmów [SMA] zlokalizowanej w Bazie MZK przy ul Kopernika 4a,*
- *Zrealizować podgląd lokalny dla służb dozoru technologicznego,*
- *Kody do rozbrojenia/uzbrojenia systemu mogą być znane tylko osobom wyznaczonym przez właściciela do czynności eksploatacyjnych, serwisowych i dozorowych. Po nadaniu uprawnień do znajomości kodu (oraz posiadania pilota) każdy pracownik musi złożyć podpis potwierdzający zapoznanie oraz bezwzględne przestrzeganie tajemnicy,*
- *Każdorazowo po rezygnacji bądź zwolnieniu z pracy pracownika posiadającego wcześniej dostęp do obiektu należy bezzwłocznie zmienić kod dostępu oraz poinformować odpowiedzialnych pracowników – zmiany odnotować w książce kodów. Po zmianie kodu każdy pracownik musi złożyć podpis potwierdzający zapoznanie oraz bezwzględne przestrzeganie tajemnicy,*

#### 4.7. Podział na strefy dozorowe

- *Strefa I – alarm napadowy na terenie Miejskiej Oczyszczalni Ścieków,*
- *Strefa II – Przepompownia ul. Asfaltowa(kod wprowadzony na manipulatorze)*
- *Strefa III – Przepompownia ul. Niepodległości(kod wprowadzony na manipulatorze)*

#### 4.8. Przeglądy techniczne systemów

- *Co najmniej raz na kwartał należy przeprowadzić czynności konserwacyjne polegające na sprawdzeniu parametrów wszystkich urządzeń peryferyjnych,*
- *Należy przeprowadzić test transmisji sygnału alarmowego,*
- *Należy odkurzyć, wyczyścić detektory, kamery, itp.,*
- *Należy sprawdzić stan akumulatora zasilania rezerwowego,*
- *W celu eliminacji fałszywych alarmów należy kosić trawę oraz dbać o odsnieżanie w obszarze działania czujników zewnętrznych – wyznaczyć osobę odpowiedzialną.*

#### 4.9. Uwagi

- Niniejsze opracowanie nie dotyczy procedur związanych z doborem zabezpieczeń mechanicznych,
- Niniejsze opracowanie nie dotyczy procedur związanych z przechowywaniem, dysponowaniem, zarządzaniem kluczami – zarządzanie kluczami powinno się odbywać poprzez firmę świadczącą usługi ochrony fizycznej (bazując na odrębnych procedurach opracowanych przez firmę świadczącą usługi ochrony fizycznej i zaakceptowanych przez MZK Sp. z o.o.).
- Na prace związane z modernizacją elektronicznych systemów zabezpieczeń należy opracować dokumentację projektową sporządzoną przez osobę uprawnioną. Prace należy prowadzić pod nadzorem projektanta/inspektora.

### 5. Przepompownia Ścieków ul. Niepodległości

#### 5.1. Charakterystyka obiektu.

*Budynek przepompowni zlokalizowany jest na działce o powierzchni około 10,28 [a] ogrodzony, monitorowany poprzez dwie kamery, obraz przesłany do pracowników obsługi oczyszczalni ścieków*

#### 5.2. Ocena ryzyka i analiza zagrożeń-wnioski

- Obiekt położony w terenie niezabudowanym,
- Stała obsługa i nadzór nad procesem technologicznym,
- Obiekt narażony na akty sabotażowe,
- Obiekt narażony na akty wandalizmu i kradzieży.

#### 5.3. Wyposażenie obiektu w elektroniczne systemy zabezpieczeń – stan istniejący

- Teren zewnętrzny – monitorowany poprzez dwie kamery systemu telewizji przemysłowej
- Budynek - brak elektronicznego systemu sygnalizacji włamania i napadu

#### 5.4. Określenie poziomu dostępu do obiektu

*W ramach reorganizacji systemu ochrony i wdrażania procedur wspomagających funkcjonowanie systemu zarządzania bezpieczeństwem należy jednoznacznie określić poziom dostępu do obiektu oraz • należy wyznaczyć osobę odpowiedzialną za obiekt,*

- należy określić osoby, które mają dostęp do obiektu,
- należy określić indywidualne kody dostępu do systemu alarmowego oraz hasła odwoławcze do komunikacji z agencją ochrony,

należy umożliwić agencji ochrony w Bazie MZK podgląd obrazu z kamer istniejących i ewentualnie nowo zaprojektowanych.

#### *5.5. Procedury postępowania w przypadku alarmu oraz dozoru – po zaprojektowaniu i wyposażeniu obiektu w elektroniczne systemy zabezpieczeń*

*Do obowiązków służb ochrony należy kontrola stanu toru transmisyjnego pomiędzy [SMA] a obiektem, kontrolowanie stanu uzbrojenia/ rozbrojenia systemu, weryfikacja alarmu, wysłanie patrolu, adnotacje o alarmach prowadzone w książce obiektu, obiekt zostanie podłączony do projektowanej centrali alarmowej w budynku Miejskiej Oczyszczalni Ścieków, jako odrębna strefa dozorowa.*

#### *DOSTĘP DO STREFY CHRONIONEJ*

- a. osoba uprawniona indywidualnym kodem rozbraja system alarmowy,*
- b. po rozbrojeniu systemu alarmowego należy niezwłocznie, telefonicznie, poinformować operatora stacji monitorującej o wejściu na teren strefy chronionej oraz określić szacunkowy czas przebywania w strefie chronionej, operator weryfikuje osobę uprawnioną do wejścia na teren poprzez indywidualne hasło odwoławcze użytkownika,*
- c. informacja o rozbrojeniu systemu alarmowego jest przekazywana automatycznie przez centralę alarmową do SMA i jeśli operator w czasie 5 minut nie otrzyma telefonicznego potwierdzenia od osoby dokonującej rozbrojenia, traktuje zdarzenie, jako alarmowe – alarm napadowy,*
- d. jeśli czas przebywania na obiekcie podany przez użytkownika, operatorowi SMA zostanie przekroczony, operator weryfikuje telefonicznie (lub poprzez system CCTV) czy użytkownik przebywa nadal w strefie chronionej, brak potwierdzenia traktowany jest, jako zdarzenie alarmowe – alarm napadowy,*
- e. po opuszczeniu strefy chronionej użytkownik uzbraja system alarmowy indywidualnym kodem. Informacja o uzbrojeniu alarmu zostaje automatycznie przekazana przez centralę alarmową do SMA.*

#### *DOSTĘP DO OBIEKTU – WEJŚCIE POD PRZYMUSEM*

- a. osoba uprawniona indywidualnym kodem rozbraja system alarmowy pod przymusem osoby niepowołanej,*
- b. osoba uprawniona kodem przymusu rozbraja system alarmowy pod przymusem osoby niepowołanej,*
- c. przed wejściem do strefy chronionej należy telefonicznie poinformować operatora stacji monitorującej o konieczności wejścia na teren strefy chronionej oraz określić szacunkowy czas przebywania na terenie chronionym, operator weryfikuje osobę uprawnioną do wejścia na teren poprzez indywidualne hasło odwoławcze użytkownika. Użytkownik pod przymusem podaje hasło identyfikowane przez operatora, jako hasło przymusowego rozbrojenia alarmu, kolejne działania operator wykonuje zgodnie ze schematem alarmu napadowego.*

## ALARM WŁAMANIOWY

- a. otrzymanie alarmu włamaniowego,
- b. weryfikacja – sprawdzenie obrazów bieżących z kamer,
- c. wysłanie patrolu,
- d. ocena sytuacji – postępowanie służb w przypadku włamania lub alarmu fałszywego określone odrębnymi procedurami,
- e. powiadomienie osób odpowiedzialnych,
- f. reset sygnału,
- g. uzbrojenie systemu,
- h. powrót patrolu i dokonanie adnotacji w książce obiektu,

## ALARM NAPADOWY

- a. otrzymanie alarmu napadowego,
- b. wysłanie patrolu,
- c. ocena sytuacji – postępowanie służb w przypadku napadu określone odrębnymi procedurami,
- d. powiadomienie osób odpowiedzialnych,
- e. reset sygnału,
- f. uzbrojenie systemu,
- g. powrót patrolu i dokonanie adnotacji w książce obiektu,

## UTRATA ŁĄCZNOŚCI Z OBIEKTEM

- a. otrzymanie informacji o awarii,
- b. wysłanie patrolu,
- c. ocena sytuacji,
- d. powiadomienie osób odpowiedzialnych za dozór i serwis,
- e. uzbrojenie systemu,
- f. powrót patrolu i dokonanie adnotacji w książce obiektu,
- g. wzmożone patrole ochrony fizycznej do czasu usunięcia usterki,

### 5.6. Określenie standaryzacji projektu i realizacji elektronicznych systemów zabezpieczeń

- Nowoprojektowany system należy wykonać w oparciu o urządzenia elektronicznych systemów zabezpieczeń w klasie co najmniej C – urządzenia profesjonalne,
- Centrala alarmowa musi być zabezpieczona stykiem antysabotażowym ,
- Zasilanie centrali musi być wykonane z odrębnego obwodu rozdzielnic elektrycznej z odpowiednio dobranym zabezpieczeniem przeciążeniowo – zwarciovym,

- 
- *Centrala musi posiadać zasilanie rezerwowe – akumulator z czasem podtrzymania co najmniej 72 h w dozorze, 0,5 h w alarmie,*
- *Styk antysabotażowy klawiatury/manipulatora centrali musi być podłączony do centrali alarmowej,*
- *Okablowanie magistralowe oraz linii dozorowych musi być zabezpieczone przed uszkodzeniami mechanicznymi (wewnątrz instalację prowadzić w rurkach RL natomiast na zewnątrz w rurach osłonowych np. AROT),*
- *Wszystkie linie dozorowe muszą być parametryzowane w konfiguracji 2EOL (wartości rezystancji zgodne z typem centrali),*
- *Wszystkie puszkę połączeniowe muszą być wyposażone w styki antysabotażowe włączone w obwody dozorowe,*
- *Drzwi do pomieszczeń technicznych technicznego zabezpieczyć kontaktronem, co najmniej w klasie C,*
- *Pomieszczenia techniczne zabezpieczyć czujką dualną co najmniej w klasie C,*
- *Pomieszczenie stałej obsługi zabezpieczyć przyciskiem antynapadowym, co najmniej w klasie C,*
- *Sygnalizator optyczno-akustyczny zlokalizować na zewnątrz na wysokości, co najmniej 2,5m, styk antysabotażowy sygnalizatora podłączyć do centrali,*
- *Wszystkie połączenia przewodów, rezystorów należy wykonać jako lutowane,*
- *Włazy studni zabezpieczyć przed otwarciem przy pomocy kontaktronu – klasa, co najmniej C, kontaktron do zastosowań zewnętrznych,*
- *Teren zewnętrzny dozorować dodatkowo przy pomocy systemu nadzoru wizyjnego - kamery obrotowe - sygnały transmitowane za pomocą toru bezprzewodowego do stacji monitorowania alarmów [SMA] zlokalizowanej w Bazie MZK przy ul Kopernika 4a,*
- *Zrealizować podgląd lokalny dla służb dozoru technicznego,*
- *Kody do rozbrojenia/uzbrojenia systemu mogą być znane tylko osobom wyznaczonym przez właściciela do czynności eksploatacyjnych, serwisowych i dozorowych. Po nadaniu uprawnień do znajomości kodu (oraz posiadania pilota) każdy pracownik musi złożyć podpis potwierdzający zapoznanie oraz bezwzględne przestrzeganie tajemnicy,*
- *Każdorazowo po rezygnacji bądź zwolnieniu z pracy pracownika posiadającego wcześniej dostęp do obiektu należy bezzwłocznie zmienić kod dostępu oraz poinformować odpowiedzialnych pracowników – zmiany odnotować w książce kodów. Po zmianie kodu każdy pracownik musi złożyć podpis potwierdzający zapoznanie oraz bezwzględne przestrzeganie tajemnicy,*

#### 5.7. Podział na strefy dozorowe

- *Strefa I – alarm napadowy na terenie Miejskiej Oczyszczalni Ścieków,*
- *Strefa II – Przepompownia ul. Asfaltowa(kod wprowadzony na manipulatorze)*
- *Strefa III – Przepompownia ul. Niepodległości(kod wprowadzony na manipulatorze)*



### 5.8. Przeglądy techniczne systemów.

- *Co najmniej raz na kwartał należy przeprowadzić czynności konserwacyjne polegające na sprawdzeniu parametrów wszystkich urządzeń peryferyjnych,*
- *Należy przeprowadzić test transmisji sygnału alarmowego,*
- *Należy odkurzyć, wyczyścić detektory, kamery, itp.,*
- *Należy sprawdzić stan akumulatora zasilania rezerwowego,*
- *W celu eliminacji fałszywych alarmów należy kosić trawę oraz dbać o odśnieżanie w obszarze działania czujników zewnętrznych – wyznaczyć osobę odpowiedzialną.*

### 5.9. Uwagi

- *Niniejsze opracowanie nie dotyczy procedur związanych z doбором zabezpieczeń mechanicznych,*
- *Niniejsze opracowanie nie dotyczy procedur związanych z przechowywaniem, dysponowaniem, zarządzaniem kluczami – zarządzanie kluczami powinno się odbywać poprzez firmę świadczącą usługi ochrony fizycznej (bazując na odrębnych procedurach opracowanych przez firmę świadczącą usługi ochrony fizycznej i zaakceptowanych przez MZK Sp. z o.o.).*
- *Na prace związane z modernizacją elektronicznych systemów zabezpieczeń należy opracować dokumentację projektową sporządzoną przez osobę uprawnioną. Prace należy prowadzić pod nadzorem projektanta/inspektora.*

## 6. **Miejska Oczyszczalnia Ścieków**

### 6.1. Charakterystyka obiektu.

*Obiekt budowlany w skład, którego wchodzi budynek sił, budynek pras, budynek gospodarczy, zbiornik retencyjny, blok biologicznego oczyszczania, grawitacyjny zagęszczacz osadu, piaskownik, osadnik wtórny, zbiornik wód deszczowych, teren o powierzchni około 283,8 [a], ogrodzony płotem, personel przebywający całą dobę.*

### 6.2. Ocena ryzyka i analiza zagrożeń-wnioski.

- *Obiekt położony w terenie niezabudowanym,*
- *Stała obsługa i nadzór nad procesem technologicznym,*
- *Obiekt narażony na akty sabotażowe,*
- *Obiekt narażony na akty wandalizmu i kradzieży.*

### 6.3. Wyposażenie obiektu w elektroniczne systemy zabezpieczeń – stan istniejący

- Teren zewnętrzny – brak elektronicznego systemu zabezpieczeń,  
Budynki - brak elektronicznego systemu zabezpieczeń,

#### 6.4. Określenie poziomu dostępu do obiektu.

W ramach reorganizacji systemu ochrony i wdrażania procedur wspomagających funkcjonowanie systemu zarządzania bezpieczeństwem należy jednoznacznie określić poziom dostępu do obiektu oraz • należy wyznaczyć osobę odpowiedzialną za obiekt,

- należy określić osoby, które mają dostęp do obiektu,
- należy określić indywidualne kody dostępu do systemu alarmowego oraz hasła odwoławcze do komunikacji z agencją ochrony.
- należy umożliwić agencji ochrony w Bazie MZK podgląd obrazu z kamer istniejących i ewentualnie nowo zaprojektowanych

#### 6.5. Procedury postępowania w przypadku alarmu oraz dozoru – po zaprojektowaniu i wyposażeniu obiektu w elektroniczne systemy zabezpieczeń.

Do obowiązków służb ochrony należy kontrola stanu toru transmisyjnego pomiędzy [SMA] a obiektem, kontrolowanie stanu uzbrojenia/ rozbrojenia systemu, weryfikacja alarmu, wysłanie patrolu, adnotacje o alarmach prowadzone w książce obiektu,

#### ALARM NAPADOWY

- otrzymanie alarmu napadowego,
- wysłanie patrolu,
- ocena sytuacji – postępowanie służb w przypadku napadu określone odrębnymi procedurami,
- powiadomienie osób odpowiedzialnych,
- reset sygnału,
- uzbrojenie systemu,
- powrót patrolu i dokonanie adnotacji w książce obiektu,

#### UTRATA ŁĄCZNOŚCI Z OBIEKTEM

- otrzymanie informacji o awarii,
- wysłanie patrolu,
- ocena sytuacji,
- powiadomienie osób odpowiedzialnych za dozór i serwis,
- uzbrojenie systemu,
- powrót patrolu i dokonanie adnotacji w książce obiektu,
- wzmoczone patrole ochrony fizycznej do czasu usunięcia usterki,



#### 6.6. Określenie standaryzacji projektu i realizacji elektronicznych systemów zabezpieczeń

- Nowoprojektowany system należy wykonać w oparciu o urządzenia elektronicznych systemów zabezpieczeń w klasie co najmniej C – urządzenia profesjonalne,
- Centrala alarmowa musi być zabezpieczona stykiem antysabotażowym ,
- Zasilanie centrali musi być wykonane z odrębnego obwodu rozdzielnic elektrycznej z odpowiednio dobranym zabezpieczeniem przeciążeniowo – zwarciovym,
- Centrala musi posiadać zasilanie rezerwowe – akumulator z czasem podtrzymania co najmniej 72 h w dozorze, 0,5 h w alarmie,
- Styk antysabotażowy klawiatury/manipulatora centrali musi być podłączony do centrali alarmowej,
- Okablowanie magistralowe oraz linii dozorowych musi być zabezpieczone przed uszkodzeniami mechanicznymi (wewnątrz instalację prowadzić w rurkach RL natomiast na zewnątrz w rurach osłonowych np. AROT),
- Wszystkie linie dozorowe muszą być parametryzowane w konfiguracji 2EOL (wartości rezystancji zgodne z typem centrali),
- Wszystkie puszk połączeniowe muszą być wyposażone w styki antysabotażowe włączone w obwody dozorowe,
- Drzwi do pomieszczeń technologicznych technicznego zabezpieczyć kontaktronem co najmniej w klasie C,
- Pomieszczenia techniczne zabezpieczyć czujką dualną co najmniej w klasie C,
- Pomieszczenie stałej obsługi zabezpieczyć przyciskiem antynapadowym co najmniej w klasie C,
- Sygnalizator optyczno-akustyczny zlokalizować na zewnątrz na wysokości, co najmniej 2,5m, styk antysabotażowy sygnalizatora podłączyć do centrali,
- Wszystkie połączenia przewodów, rezystorów należy wykonać jako lutowane,
- Włazy studni zabezpieczyć przed otwarciem przy pomocy kontaktronu – klasa co najmniej C, kontaktron do zastosowań zewnętrznych,
- Teren zewnętrzny dozorować dodatkowo przy pomocy systemu nadzoru wizyjnego - kamery obrotowe - sygnały transmitowane za pomocą toru bezprzewodowego do stacji monitorowania alarmów [SMA] zlokalizowanej w Bazie MZK przy ul Kopernika 4a,
- Zrealizować podgląd lokalny dla służb dozoru technologicznego,
- Kody do rozbrojenia/uzbrojenia systemu mogą być znane tylko osobom wyznaczonym przez właściciela do czynności eksploatacyjnych, serwisowych i dozorowych. Po nadaniu uprawnień do znajomości kodu (oraz posiadania pilota) każdy pracownik musi złożyć podpis potwierdzający zapoznanie oraz bezwzględne przestrzeganie tajemnicy,

- *Każdorazowo po rezygnacji bądź zwolnieniu z pracy pracownika posiadającego wcześniej dostęp do obiektu należy bezzwłocznie zmienić kod dostępu oraz poinformować odpowiedzialnych pracowników – zmiany odnotować w książce kodów. Po zmianie kodu każdy pracownik musi złożyć podpis potwierdzający zapoznanie oraz bezwzględne przestrzeganie tajemnicy,*

#### 6.7. Podział na strefy dozorowe

- Strefa I – alarm napadowy na terenie Miejskiej Oczyszczalni Ścieków,
- Strefa II – Przepompownia ul. Asfaltowa(kod wprowadzony na manipulatorze)
- Strefa III – Przepompownia ul. Niepodległości(kod wprowadzony na manipulatorze)

#### 6.8. Przeglądy techniczne systemów

- Co najmniej raz na kwartał należy przeprowadzić czynności konserwacyjne polegające na sprawdzeniu parametrów wszystkich urządzeń peryferyjnych,
- Należy przeprowadzić test transmisji sygnału alarmowego,
- Należy odkurzyć, wyczyścić detektory, kamery, itp.,
- Należy sprawdzić stan akumulatora zasilania rezerwowego,
- W celu eliminacji fałszywych alarmów należy kosić trawę oraz dbać o odsnieżanie w obszarze działania czujników zewnętrznych – wyznaczyć osobę odpowiedzialną.

#### 6.9. Uwagi

- Niniejsze opracowanie nie dotyczy procedur związanych z doborem zabezpieczeń mechanicznych,
- Niniejsze opracowanie nie dotyczy procedur związanych z przechowywaniem, dysponowaniem, zarządzaniem kluczami – zarządzanie kluczami powinno się odbywać poprzez firmę świadczącą usługi ochrony fizycznej (bazując na odrębnych procedurach opracowanych przez firmę świadczącą usługi ochrony fizycznej i zaakceptowanych przez MZK Sp. z o.o.).
- Na prace związane z modernizacją elektronicznych systemów zabezpieczeń należy opracować dokumentację projektową sporządzoną przez osobę uprawnioną. Prace należy prowadzić pod nadzorem projektanta/inspektora.

### 7. Oczyszczalnia ścieków Stary Kostrzyn (Kontenerowa) przy ul. Sikorskiego

#### 7.1. Charakterystyka obiektu.

Obiekt podziemny, teren o powierzchni około 9,30 [a], teren ogrodzony

#### 7.2. Ocena ryzyka i analiza zagrożeń-wnioski.

- Obiekt położony w terenie niezabudowanym,
- Brak stałej obsługi i nadzoru,
- Obiekt narażony na akty sabotażowe,

- *Obiekt narażony na akty wandalizmu i kradzieży.*

### *7.3. Wyposażenie obiektu w elektroniczne systemy zabezpieczeń – stan istniejący.*

- *Teren zewnętrzny – brak elektronicznego systemu zabezpieczeń,*
- *Budynek sterowni- brak elektronicznego systemu zabezpieczeń,*
- *Kontenery technologiczne - brak elektronicznego systemu zabezpieczeń,*

### *7.4. Określenie poziomu dostępu do obiektu*

*W ramach reorganizacji systemu ochrony i wdrażania procedur wspomagających funkcjonowanie systemu zarządzania bezpieczeństwem należy jednoznacznie określić poziom dostępu do obiektu oraz • należy wyznaczyć osobę odpowiedzialną za obiekt,*

- *należy określić osoby, które mają dostęp do obiektu,*
- *należy określić indywidualne kody dostępu do systemu alarmowego oraz hasła odwoławcze do komunikacji z agencją ochrony.*

### *7.5. Procedury postępowania w przypadku alarmu oraz dozoru – po zaprojektowaniu i wyposażeniu obiektu w elektroniczne systemy zabezpieczeń.*

*Do obowiązków służb ochrony należy kontrola stanu toru transmisyjnego pomiędzy [SMA] a obiektem, kontrolowanie stanu uzbrojenia/ rozbrojenia systemu, weryfikacja alarmu, wysłanie patrolu, adnotacje o alarmach prowadzone w księżce obiektu,*

### *DOSTĘP DO STREFY CHRONIONEJ*

- a. osoba uprawniona indywidualnym kodem rozbraja system alarmowy,*
- b. po rozbrojeniu systemu alarmowego należy niezwłocznie, telefonicznie, poinformować operatora stacji monitorującej o wejściu na teren strefy chronionej oraz określić szacunkowy czas przebywania w strefie chronionej, operator weryfikuje osobę uprawnioną do wejścia na teren poprzez indywidualne hasło odwoławcze użytkownika,*
- c. informacja o rozbrojeniu systemu alarmowego jest przekazywana automatycznie przez centralę alarmową do SMA i jeśli operator w czasie 5 minut nie otrzyma telefonicznego potwierdzenia od osoby dokonującej rozbrojenia, traktuje zdarzenie, jako alarmowe – alarm napadowy,*
- d. jeśli czas przebywania na obiekcie podany przez użytkownika, operatorowi SMA zostanie przekroczony, operator weryfikuje telefonicznie (lub poprzez system CCTV) czy użytkownik przebywa nadal w strefie chronionej, brak potwierdzenia traktowany jest, jako zdarzenie alarmowe – alarm napadowy,*
- e. po opuszczeniu strefy chronionej użytkownik uzbraja system alarmowy indywidualnym kodem. Informacja o uzbrojeniu alarmu zostaje automatycznie przekazana przez centralę alarmową do SMA.*

### DOSTĘP DO OBIEKTU – WEJŚCIE POD PRYMUSEM

- a. osoba uprawniona indywidualnym kodem rozbraja system alarmowy pod przymusem osoby niepowołanej,
- b. osoba uprawniona kodem przymusu rozbraja system alarmowy pod przymusem osoby niepowołanej,
- c. przed wejściem do strefy chronionej należy telefonicznie poinformować operatora stacji monitorującej o konieczności wejścia na teren strefy chronionej oraz określić szacunkowy czas przebywania na terenie chronionym, operator weryfikuje osobę uprawnioną do wejścia na teren poprzez indywidualne hasło odwoławcze użytkownika. Użytkownik pod przymusem podaje hasło identyfikowane przez operatora, jako hasło przymusowego rozbrojenia alarmu, kolejne działania operator wykonuje zgodnie ze schematem alarmu napadowego.

### ALARM WŁAMANIOWY

- a. otrzymanie alarmu włamaniowego,
- b. weryfikacja – sprawdzenie obrazów bieżących z kamer,
- c. wysłanie patrolu,
- d. ocena sytuacji – postępowanie służb w przypadku włamania lub alarmu fałszywego określone odrębnymi procedurami,
- e. powiadomienie osób odpowiedzialnych,
- f. reset sygnału,
- g. uzbrojenie systemu,
- h. powrót patrolu i dokonanie adnotacji w książce obiektu,

### ALARM NAPADOWY

- a. otrzymanie alarmu napadowego,
- b. wysłanie patrolu,
- c. ocena sytuacji – postępowanie służb w przypadku napadu określone odrębnymi procedurami,
- d. powiadomienie osób odpowiedzialnych,
- e. reset sygnału,
- f. uzbrojenie systemu,
- g. powrót patrolu i dokonanie adnotacji w książce obiektu,

### UTRATA ŁĄCZNOŚCI Z OBIEKTEM

- a. otrzymanie informacji o awarii,
- b. wysłanie patrolu,
- c. ocena sytuacji,
- d. powiadomienie osób odpowiedzialnych za dozór i serwis,

- e. uzbrojenie systemu,
- f. powrót patrolu i dokonanie adnotacji w książce obiektu,
- g. wzmożone patrole ochrony fizycznej do czasu usunięcia usterki,

#### 7.6. Określenie standaryzacji projektu i realizacji elektronicznych systemów zabezpieczeń

- Nowoprojektowany system należy wykonać w oparciu o urządzenia elektronicznych systemów zabezpieczeń w klasie co najmniej C – urządzenia profesjonalne,
- Centrala alarmowa musi być zabezpieczona stykiem antysabotażowym ,
- Zasilanie centrali musi być wykonane z odrębnego obwodu rozdzielnic elektrycznej z odpowiednio dobranym zabezpieczeniem przeciążeniowo – zwarciovym,
- Centrala musi posiadać zasilanie rezerwowe – akumulator z czasem podtrzymania co najmniej 72 h w dozorze, 0,5 h w alarmie,
- Styk antysabotażowy klawiatury/manipulatora centrali musi być podłączony do centrali alarmowej,
- Okablowanie magistralowe oraz linii dozorowych musi być zabezpieczone przed uszkodzeniami mechanicznymi (wewnątrz instalację prowadzić w rurkach RL natomiast na zewnątrz w rurach osłonowych np. AROT),
- Wszystkie linie dozorowe muszą być parametryzowane w konfiguracji 2EOL (wartości rezystancji zgodne z typem centrali),
- Wszystkie puszkę połączeniowe muszą być wyposażone w styki antysabotażowe włączone w obwody dozorowe,
- Drzwi do pomieszczenia technicznego sterowni zabezpieczyć kontaktronem co najmniej w klasie C,
- Sygnalizator optyczno-akustyczny zlokalizować na zewnątrz budynku sterowni, styk antysabotażowy sygnalizatora podłączyć do centrali,
- Wszystkie połączenia przewodów, rezystorów należy wykonać jako lutowane,
- Włazy studni zabezpieczyć przed otwarciem przy pomocy kontaktronu – klasa co najmniej C, kontaktron do zastosowań zewnętrznych,
- Teren zewnętrzny dozorować dodatkowo przy pomocy systemu nadzoru wizyjnego - kamery stacjonarne- sygnały transmitowane za pomocą toru bezprzewodowego do stacji monitorowania alarmów [SMA] zlokalizowanej w Bazie MZK przy ul Kopernika 4a,
- Kody do rozbrojenia/uzbrojenia systemu mogą być znane tylko osobom wyznaczonym przez właściciela do czynności eksploatacyjnych, serwisowych i dozorowych. Po nadaniu uprawnień do znajomości kodu (oraz posiadania pilota) każdy pracownik musi złożyć podpis potwierdzający zapoznanie oraz bezwzględne przestrzeganie tajemnicy,
- Każdorazowo po rezygnacji bądź zwolnieniu z pracy pracownika posiadającego wcześniej dostęp do obiektu należy niezwłocznie zmienić kod dostępu oraz poinformować odpowiedzialnych pracowników – zmiany odnotować w książce

*kodów. Po zmianie kodu każdy pracownik musi złożyć podpis potwierdzający zapoznanie oraz bezwzględne przestrzeganie tajemnicy,*

#### *7.7. Podział na strefy dozorowe.*

- Strefa I – teren zewnętrzny dozorowany barierami mikrofalowymi (linia bramy wjazdowej) – rozbrajanie dualne (pilot radiolinii rozpoczynający procedurę rozbrajania z czasem na wejście + kod wprowadzony na manipulatorze),*
- Strefa II – teren zewnętrzny dozorowany barierami mikrofalowymi (pozostałe linie) –(kod wprowadzony na manipulatorze),*
- Strefa III – budynek sterowni (kod wprowadzony na manipulatorze),*

#### *7.8. Przeglądy techniczne systemów.*

- Co najmniej raz na kwartał należy przeprowadzić czynności konserwacyjne polegające na sprawdzeniu parametrów wszystkich urządzeń peryferyjnych,*
- Należy przeprowadzić test transmisji sygnału alarmowego,*
- Należy odkurzyć, wyczyścić detektory, kamery, itp.,*
- Należy sprawdzić stan akumulatora zasilania rezerwowego,*
- W celu eliminacji fałszywych alarmów należy kosić trawę oraz dbać o odśnieżanie w obszarze działania barier mikrofalowych – wyznaczyć osobę odpowiedzialną.*

#### *7.9. Uwagi*

- Niniejsze opracowanie nie dotyczy procedur związanych z doborem zabezpieczeń mechanicznych,*
- Niniejsze opracowanie nie dotyczy procedur związanych z przechowywaniem, dysponowaniem, zarządzaniem kluczami – zarządzanie kluczami powinno się odbywać poprzez firmę świadczącą usługi ochrony fizycznej (bazując na odrębnych procedurach opracowanych przez firmę świadczącą usługi ochrony fizycznej i zaakceptowanych przez MZK Sp. z o.o.).*
- Na prace związane z modernizacją elektronicznych systemów zabezpieczeń należy opracować dokumentację projektową sporządzoną przez osobę uprawnioną. Prace należy prowadzić pod nadzorem projektanta/inspektora.*

## **8. Przyszła baza transportowo-magazynowa ZOŚ przy ul. Sportowej**

### *8.1. Charakterystyka obiektu.*

*Teren o powierzchni około 77,32 [a], teren ogrodzony*

#### *8.2. Ocena ryzyka i analiza zagrożeń-wnioski.*

- *Obiekt położony w terenie niezabudowanym,*
- *Brak stałej obsługi i nadzoru,*
- *Obiekt narażony na akty sabotażowe,*
- *Obiekt narażony na akty wandalizmu i kradzieży.*

#### *8.3. Wyposażenie obiektu w elektroniczne systemy zabezpieczeń – stan istniejący*

- *Teren zewnętrzny – brak elektronicznego systemu zabezpieczeń,*
- *Monitorowane przewodowanie na ogrodzeniu (zabezpieczenie siatki przed kradzieżą)– rozwiązanie niecertyfikowane,*

#### *8.4. Określenie poziomu dostępu do obiektu.*

*W ramach reorganizacji systemu ochrony i wdrażania procedur wspomagających funkcjonowanie systemu zarządzania bezpieczeństwem należy jednoznacznie określić poziom dostępu do obiektu oraz • należy wyznaczyć osobę odpowiedzialną za obiekt,*

- *należy określić osoby, które mają dostęp do obiektu,*

#### *8.5. Procedury postępowania w przypadku alarmu oraz dozoru – po zaprojektowaniu i wyposażeniu obiektu w elektroniczne systemy zabezpieczeń.*

*Do obowiązków służb ochrony należy kontrola stanu toru transmisyjnego pomiędzy [SMA] a obiektem, kontrolowanie stanu zamknięcia bramy systemu (weryfikacja alarmu, wysłanie patrolu, adnotacje o alarmach prowadzone w książce obiektu,*

#### *SPOSÓB OCHRONY*

- a. *Sugeruje się 24 h dozór tylko stanu otwarcia/zamknięcia bramy wspomagany systemem dozoru wizyjnego,*

#### *UTRATA ŁĄCZNOŚCI Z OBIEKTEM*

- a. *otrzymanie informacji o awarii,*
- b. *wysłanie patrolu,*
- c. *ocena sytuacji,*



- d. powiadomienie osób odpowiedzialnych za dozór i serwis,
- e. uzbrojenie systemu,
- f. powrót patrolu i dokonanie adnotacji w książce obiektu,
- g. wzmożone patrole ochrony fizycznej do czasu usunięcia usterki,

#### 8.6. Określenie standaryzacji projektu i realizacji elektronicznych systemów zabezpieczeń

- Nowoprojektowany system należy wykonać w oparciu o urządzenia elektronicznych systemów zabezpieczeń w klasie co najmniej C – urządzenia profesjonalne,
- Centrala alarmowa musi być zabezpieczona stykiem antysabotażowym ,
- Zasilanie centrali musi być wykonane z odrębnego obwodu rozdzielnic elektrycznej z odpowiednio dobranym zabezpieczeniem przeciążeniowo – zwarciovym,
- Centrala musi posiadać zasilanie rezerwowe – akumulator z czasem podtrzymania co najmniej 72 h w dozorze, 0,5 h w alarmie,
- Styk antysabotażowy klawiatury/manipulatora centrali musi być podłączony do centrali alarmowej,
- Okablowanie magistralowe oraz linii dozorowych musi być zabezpieczone przed uszkodzeniami mechanicznymi (wewnątrz instalację prowadzić w rurkach RL natomiast na zewnątrz w rurach osłonowych np. AROT),
- Wszystkie linie dozorowe muszą być parametryzowane w konfiguracji 2EOL (wartości rezystancji zgodne z typem centrali),
- Wszystkie puszkę połączeniowe muszą być wyposażone w styki antysabotażowe włączone w obwody dozorowe,
- Sygnalizator optyczno-akustyczny zlokalizować na zewnątrz budynku sterowni, styk antysabotażowy sygnalizatora podłączyć do centrali,
- Wszystkie połączenia przewodów, rezystorów należy wykonać jako lutowane,
- Teren zewnętrzny dozorować dodatkowo przy pomocy systemu nadzoru wizyjnego - kamery stacjonarne- sygnały transmitowane za pomocą toru bezprzewodowego do stacji monitorowania alarmów [SMA] zlokalizowanej w Bazie MZK przy ul Kopernika 4a,
- Kody do rozbrojenia/uzbrojenia systemu mogą być znane tylko osobom wyznaczonym przez właściciela do czynności eksploatacyjnych, serwisowych i dozorowych. Po nadaniu uprawnień do znajomości kodu (oraz posiadania pilota) każdy pracownik musi złożyć podpis potwierdzający zapoznanie oraz bezwzględne przestrzeganie tajemnicy,
- Każdorazowo po rezygnacji bądź zwolnieniu z pracy pracownika posiadającego wcześniej dostęp do obiektu należy bezzwłocznie zmienić kod dostępu oraz poinformować odpowiedzialnych pracowników – zmiany odnotować w książce kodów. Po zmianie kodu każdy pracownik musi złożyć podpis potwierdzający zapoznanie oraz bezwzględne przestrzeganie tajemnicy,

#### 8.7. Podział na strefy dozorowe.

- *Strefa I – kontrola stanu otwarcia/zamknięcia bramy wjazdowej,*
- *Strefa II – jako uzupełnienie zabezpieczenie siatki opłotowania przed kradzieżą – rozwiązanie istniejące.*

#### *8.8. Przeglądy techniczne systemów.*

- *Co najmniej raz na kwartał należy przeprowadzić czynności konserwacyjne polegające na sprawdzeniu parametrów wszystkich urządzeń peryferyjnych,*
- *Należy przeprowadzić test transmisji sygnału alarmowego,*
- *Należy odkurzyć, wyczyścić kamery, itp.,*
- *Należy sprawdzić stan akumulatora zasilania rezerwowego,*

#### *8.9. Uwagi.*

- *Niniejsze opracowanie nie dotyczy procedur związanych z doborem zabezpieczeń mechanicznych,*
- *Niniejsze opracowanie nie dotyczy procedur związanych z przechowywaniem, dysponowaniem, zarządzaniem kluczami – zarządzanie kluczami powinno się odbywać poprzez firmę świadczącą usługi ochrony fizycznej (bazując na odrębnych procedurach opracowanych przez firmę świadczącą usługi ochrony fizycznej i zaakceptowanych przez MZK Sp. z o.o.).*
- *Na prace związane z modernizacją elektronicznych systemów zabezpieczeń należy opracować dokumentację projektową sporządzoną przez osobę uprawnioną. Prace należy prowadzić pod nadzorem projektanta/inspektora.*
- *W miarę rozwoju obiektu należy w przyszłości wziąć pod uwagę rozbudowę elektronicznych systemów zabezpieczeń,*
- *Na obiekcie należy rozważyć montaż bramy przesuwnej z napędem elektrycznym uruchamianym za pomocą pilotów przez kierowców.*

### **9. Kotłownia ZEC Osiedle Leśne**

#### *9.1. Charakterystyka obiektu.*

*Budynek zlokalizowany na terenie o powierzchni około 12,25 [a], ogrodzony płotem.*

#### *9.2. Ocena ryzyka i analiza zagrożeń-wnioski.*

- *Obiekt położony w terenie niezabudowanym,*
- *Brak stałej obsługi i nadzoru,*
- *Obiekt narażony na akty sabotażowe,*
- *Obiekt narażony na akty wandalizmu i kradzieży.*

#### *9.3. Wyposażenie obiektu w elektroniczne systemy zabezpieczeń – stan istniejący.*

- *Teren zewnętrzny – brak elektronicznego systemu zabezpieczeń,*
- *Budynek kotłowni - brak elektronicznego systemu zabezpieczeń,*

#### 9.4. Określenie poziomu dostępu do obiektu.

*W ramach reorganizacji systemu ochrony i wdrażania procedur wspomagających funkcjonowanie systemu zarządzania bezpieczeństwem należy jednoznacznie określić poziom dostępu do obiektu oraz*

- należy wyznaczyć osobę odpowiedzialną za obiekt,*
- należy określić osoby, które mają dostęp do obiektu,*
- należy określić indywidualne kody dostępu do systemu alarmowego oraz hasła odwoławcze do komunikacji z agencją ochrony.*

#### 9.5. Procedury postępowania w przypadku alarmu oraz dozoru.

*Do obowiązków służb ochrony należy kontrola stanu toru transmisyjnego pomiędzy [SMA] a obiektem, kontrolowanie stanu uzbrojenia/ rozbrojenia systemu, weryfikacja alarmu, wysłanie patrolu, adnotacje o alarmach prowadzone w książce obiektu,*

##### DOSTĘP DO OBIEKTU

- a. osoba uprawniona wchodzi na teren i indywidualnym kodem rozbraja system alarmowy,*
- b. po rozbrojeniu systemu alarmowego należy niezwłocznie, telefonicznie, poinformować operatora stacji monitorującej o wejściu na teren obiektu chronionego oraz określić szacunkowy czas przebywania na terenie chronionym, operator weryfikuje osobę uprawnioną do wejścia na teren poprzez indywidualne hasło odwoławcze użytkownika,*
- c. informacja o rozbrojeniu systemu alarmowego jest przekazywana automatycznie przez centralę alarmową do SMA i jeśli operator w czasie 5 minut nie otrzyma telefonicznego potwierdzenia od osoby dokonującej rozbrojenia, traktuje zdarzenie, jako alarmowe – alarm napadowy,*
- d. jeśli czas przebywania na obiekcie podany przez użytkownika, operatorowi SMA zostanie przekroczony, operator weryfikuje telefonicznie (lub poprzez system CCTV) czy użytkownik przebywa nadal na obiekcie, brak potwierdzenia traktowany jest, jako zdarzenie alarmowe – alarm napadowy,*
- e. przed opuszczeniem obiektu użytkownik uzbraja system alarmowy indywidualnym kodem. Informacja o uzbrojeniu alarmu zostaje automatycznie przekazana przez centralę alarmową do SMA.*

##### DOSTĘP DO OBIEKTU – WEJŚCIE POD PRZYMUSEM

- a. osoba uprawniona wchodzi na teren i kodem przymusu rozbraja system alarmowy pod przymusem osoby niepowołanej,*
- b. przed wejściem na teren obiektu należy telefonicznie poinformować operatora stacji monitorującej o konieczności wejścia na teren obiektu chronionego oraz określić szacunkowy czas przebywania na terenie chronionym, operator weryfikuje osobę uprawnioną do wejścia na teren poprzez indywidualne hasło*

odwoławcze użytkownika. Użytkownik pod przymusem podaje hasło identyfikowane przez operatora, jako hasło przymusowego rozbrojenia alarmu, kolejna działania operator wykonuje zgodnie ze schematem alarmu napadowego.

#### ALARM WŁAMANIOWY

- a. otrzymanie alarmu włamaniowego,
- b. weryfikacja – sprawdzenie obrazów bieżących z kamer,
- c. wysłanie patrolu,
- d. ocena sytuacji – postępowanie służb w przypadku włamania lub alarmu fałszywego określone odrębnymi procedurami,
- e. powiadomienie osób odpowiedzialnych,
- f. reset sygnału,
- g. uzbrojenie systemu,
- h. powrót patrolu i dokonanie adnotacji w książce obiektu,

#### ALARM NAPADOWY

- a. otrzymanie alarmu napadowego,
- b. wysłanie patrolu,
- c. ocena sytuacji – postępowanie służb w przypadku napadu określone odrębnymi procedurami,
- d. powiadomienie osób odpowiedzialnych,
- e. reset sygnału,
- f. uzbrojenie systemu,
- g. powrót patrolu i dokonanie adnotacji w książce obiektu,

#### UTRATA ŁACZNOŚCI Z OBIEKTEM

- a. otrzymanie informacji o awarii,
- b. wysłanie patrolu,
- c. ocena sytuacji,
- d. powiadomienie osób odpowiedzialnych za dozór i serwis,
- e. uzbrojenie systemu,
- f. powrót patrolu i dokonanie adnotacji w książce obiektu,
- g. wzmożone patrole ochrony fizycznej do czasu usunięcia usterki,

#### 9.6. Określenie standaryzacji rozbudowy elektronicznych systemów zabezpieczeń.

- Nowoprojektowany system należy wykonać w oparciu o urządzenia elektronicznych systemów zabezpieczeń w klasie co najmniej C – urządzenia profesjonalne,
- Centrala alarmowa musi być zabezpieczona stykiem antysabotażowym ,

- Zasilanie centrali musi być wykonane z odrębnego obwodu rozdzielnicy elektrycznej z odpowiednio dobranym zabezpieczeniem przeciążeniowo – zwarciovym,
- Centrala musi posiadać zasilanie rezerwowe – akumulator z czasem podtrzymania co najmniej 72 h w dozorze, 0,5 h w alarmie,
- Styk antysabotażowy klawiatury/manipulatora centrali musi być podłączony do centrali alarmowej,
- Okablowanie magistralowe oraz linii dozorowych musi być zabezpieczone przed uszkodzeniami mechanicznymi (wewnątrz instalację prowadzić w rurkach RL natomiast na zewnątrz w rurach osłonowych np. AROT),
- Wszystkie linie dozorowe muszą być parametryzowane w konfiguracji 2EOL (wartości rezystancji zgodne z typem centrali),
- Wszystkie puszkę połączeniowe muszą być wyposażone w styki antysabotażowe włączone w obwody dozorowe,
- Sygnalizator optyczno-akustyczny zlokalizować na zewnątrz budynku sterowni, styk antysabotażowy sygnalizatora podłączyć do centrali,
- Wszystkie połączenia przewodów, rezystorów należy wykonać jako lutowane,
- Teren zewnętrzny dozorować dodatkowo przy pomocy systemu nadzoru wizyjnego - kamery stacjonarne- sygnały transmitowane za pomocą toru bezprzewodowego do stacji monitorowania alarmów [SMA] zlokalizowanej w Bazie MZK przy ul Kopernika 4a,
- Kody do rozbrojenia/uzbrojenia systemu mogą być znane tylko osobom wyznaczonym przez właściciela do czynności eksploatacyjnych, serwisowych i dozorowych. Po nadaniu uprawnień do znajomości kodu (oraz posiadania pilota) każdy pracownik musi złożyć podpis potwierdzający zapoznanie oraz bezwzględne przestrzeganie tajemnicy,
- Każdorazowo po rezygnacji bądź zwolnieniu z pracy pracownika posiadającego wcześniej dostęp do obiektu należy bezzwłocznie zmienić kod dostępu oraz poinformować odpowiedzialnych pracowników – zmiany odnotować w książce kodów. Po zmianie kodu każdy pracownik musi złożyć podpis potwierdzający zapoznanie oraz bezwzględne przestrzeganie tajemnicy,

#### 9.7. Podział na strefy dozorowe.

- Strefa I – Budynek kotłowni (kod wprowadzony na manipulatorze)

#### 9.8. Przeglądy techniczne systemów.

- Co najmniej raz na kwartał należy przeprowadzić czynności konserwacyjne polegające na sprawdzeniu parametrów wszystkich urządzeń peryferyjnych,
- Należy przeprowadzić test transmisji sygnału alarmowego,
- Należy odkurzyć, wyczyścić detektory, kamery, itp.,
- Należy sprawdzić stan akumulatora zasilania rezerwowego,

#### 9.9. Uwagi.

- *Niniejsze opracowanie nie dotyczy procedur związanych z doborem zabezpieczeń mechanicznych,*
- *Niniejsze opracowanie nie dotyczy procedur związanych z przechowywaniem, dysponowaniem, zarządzaniem kluczami – zarządzanie kluczami powinno się odbywać poprzez firmę świadczącą usługi ochrony fizycznej (bazując na odrębnych procedurach opracowanych przez firmę świadczącą usługi ochrony fizycznej i zaakceptowanych przez MZK Sp. z o.o.).*
- *Na prace związane z modernizacją elektronicznych systemów zabezpieczeń należy opracować dokumentację projektową sporządzoną przez osobę uprawnioną. Prace należy prowadzić pod nadzorem projektanta/inspektora.*

## **10. Baza MZK (biurowce i garaże) przy ul. Kopernika 4a**

### *10.1. Charakterystyka obiektu.*

*Teren o pow. około 181,70 [a] ogrodzony, obiekty i teren są zabezpieczone systemem alarmowym, na terenie bazy znajduje się całodobowe stanowisko agencji ochrony.*

### *10.1. Ocena ryzyka i analiza zagrożeń-wnioski.*

- *Obiekt położony w terenie zabudowanym,*
- *Na terenie obiektu funkcjonują podmioty niezwiązane z MZK Sp. z o.o.*
- *Obiekt biurowy ogólnodostępny w godzinach pracy MZK Sp. z o.o.*
- *Całodobowy nadzór agencji ochrony,*
- *Obiekt narażony na akty wandalizmu, kradzieży, próby napad.*
- *Ochrona danych osobowych*

### *10.2. Wyposażenie obiektu w elektroniczne systemy zabezpieczeń – stan istniejący.*

- *Teren zewnętrzny zabezpieczony jest czujnikami pasywnej podczerwieni oraz barierą podczerwieni (linia parkingu) podłączonymi do centrali alarmowej,*
- *Pomieszczenia Biurowe MZK oraz Warsztat, Magazyn, Sklep, Zakład Energetyki Ciepłej znajdujące się na parterze oraz serwerownia, biura na piętrze są zabezpieczone czujnikami pasywnej podczerwieni*
- *System alarmowy jest obsługiwany za pomocą klawiatur LCD znajdujących się przy wejściu do biurowca i pomieszczeniu ochrony*
- *Sygnaly alarmowe są wyświetlane na klawiaturze LCD w pomieszczeniu ochrony*

### *10.3. Określenie poziomu dostępu do obiektu*

*W ramach reorganizacji systemu ochrony i wdrażania procedur wspomagających funkcjonowanie systemu zarządzania bezpieczeństwem należy*



*jednoznacznie określić poziomu dostępu do obiektu oraz poszczególnych stref dozorowych:*

- należy wyznaczyć osobę odpowiedzialną za obiekt oraz strefy dozorowe*
- należy określić osoby, które mają dostęp do obiektu oraz do poszczególnych stref dozorowych*
- należy określić indywidualne kody dostępu do systemu alarmowego w poszczególnych strefach dozorowych*

#### *10.4. Procedury postępowania w przypadku alarmu oraz dozoru*

*Do obowiązków służb ochrony należy kontrola stanu systemu alarmowego, kontrolowanie stanu uzbrojenia/ rozbrojenia systemu, weryfikacja alarmu, wysłanie patrolu, adnotacje o alarmach prowadzone w książce obiektu,*

##### *DOSTĘP DO OBIEKTU*

- a. osoba uprawniona wchodzi na teren i indywidualnym kodem na klawiaturze LCD w pomieszczeniu ochrony rozbraja system alarmowy*
- b. przed opuszczeniem obiektu użytkownik uzbraja system alarmowy indywidualnym kodem na klawiaturze LCD w pomieszczeniu ochrony. Informacja o uzbrojeniu alarmu zostaje automatycznie wyświetlona na klawiaturze LCD.*

##### *ALARM WŁAMANIOWY*

- a. otrzymanie alarmu włamaniowego,*
- b. weryfikacja – sprawdzenie obrazów bieżących z kamer,*
- c. wysłanie patrolu lokalnego oraz wezwanie grupy interwencyjnej*
- d. ocena sytuacji – postępowanie służb w przypadku włamania lub alarmu fałszywego określone odrębnymi procedurami,*
- e. powiadomienie osób odpowiedzialnych,*
- f. reset sygnału,*
- g. uzbrojenie systemu,*
- h. powrót patrolu i dokonanie adnotacji w książce obiektu,*

##### *ALARM NAPADOWY*

- a. otrzymanie alarmu napadowego dziennego z przycisku w KASIE lub nocnego pracownik ochrony*
- b. wysłanie patrolu lokalnego oraz wezwanie grupy interwencyjnej*
- c. ocena sytuacji – postępowanie służb w przypadku napadu określone odrębnymi procedurami,*
- d. powiadomienie osób odpowiedzialnych,*
- e. reset sygnału,*
- f. uzbrojenie systemu,*
- g. powrót patrolu i dokonanie adnotacji w książce obiektu,*



## UTRATA ŁACZNOŚCI Z OBIEKTEM, AWARIA SYSTEMU ALARMOWEGO

- a. otrzymanie informacji o awarii,
- b. wysłanie patrolu lokalnego
- c. ocena sytuacji,
- d. powiadomienie osób odpowiedzialnych za dozór i serwis,
- e. uzbrojenie systemu,
- f. powrót patrolu i dokonanie adnotacji w książce obiektu,
- g. wzmożone patrole ochrony fizycznej do czasu usunięcia usterki,

### 10.5. Określenie standaryzacji rozbudowy elektronicznych systemów zabezpieczeń.

- Istniejący system należy sprawdzić/rozbudować w oparciu o urządzenia elektronicznych systemów zabezpieczeń w klasie co najmniej C – urządzenia profesjonalne,
- Centrala alarmowa musi być zabezpieczona stykiem antysabotażowym ,
- Zasilanie centrali musi być wykonane z odrębnego obwodu rozdzielnic elektrycznej z odpowiednio dobranym zabezpieczeniem przeciążeniowo – zwarciovym,
- Centrala musi posiadać zasilanie rezerwowe – akumulator z czasem podtrzymania co najmniej 72 h w dozorze, 0,5 h w alarmie,
- Styk antysabotażowy klawiatury/manipulatora centrali musi być podłączony do centrali alarmowej,
- Okablowanie magistralowe oraz linii dozorowych musi być zabezpieczone przed uszkodzeniami mechanicznymi (wewnątrz instalację prowadzić w rurkach RL natomiast na zewnątrz w rurach osłonowych np. AROT),
- Wszystkie linie dozorowe muszą być parametryzowane w konfiguracji 2EOL (wartości rezystancji zgodne z typem centrali),
- Wszystkie puszkę połączeniowe muszą być wyposażone w styki antysabotażowe włączone w obwody dozorowe,
- Drzwi do pomieszczenia technicznego zabezpieczyć kontaktronem co najmniej w klasie C,
- Pomieszczenie techniczne zabezpieczyć czujką dualną co najmniej w klasie C,
- Pomieszczenie techniczne zabezpieczyć przyciskiem antynapadowym co najmniej w klasie C,
- Sygnalizator optyczno-akustyczny zlokalizować na zewnątrz na wysokości co najmniej 2,5m, styk antysabotażowy sygnalizatora podłączyć do centrali,
- Wszystkie połączenia przewodów, rezystorów należy wykonać jako lutowane,
- Włazy studni zabezpieczyć przed otwarciem przy pomocy kontaktronu – klasa co najmniej C, kontaktron do zastosowań zewnętrznych,
- Teren zewnętrzny dozorować dodatkowo przy pomocy systemu nadzoru wizyjnego - 2 kamery dualne - sygnał transmitowany za pomocą toru

*bezprzewodowego do stacji monitorowania alarmów [SMA] zlokalizowanej w Bazie MZK przy ul Kopernika 4a,*

- Kody do rozbrojenia/uzbrojenia systemu mogą być znane tylko osobom wyznaczonym przez właściciela do czynności eksploatacyjnych, serwisowych i dozorowych. Po nadaniu uprawnień do znajomości kodu (oraz posiadania pilota) każdy pracownik musi złożyć podpis potwierdzający zapoznanie oraz bezwzględne przestrzeganie tajemnicy,*
- Każdorazowo po rezygnacji bądź zwolnieniu z pracy pracownika posiadającego wcześniej dostęp do obiektu należy bezzwłocznie zmienić kod dostępu oraz poinformować odpowiedzialnych pracowników – zmiany odnotować w książce kodów. Po zmianie kodu każdy pracownik musi złożyć podpis potwierdzający zapoznanie oraz bezwzględne przestrzeganie tajemnicy,*

#### *10.6. Podział na strefy dozorowe*

##### *10.6.1. Istniejący :*

- Strefa I – teren zewnętrzny dozorowany czujnikami podczerwieni i barierą podczerwieni (kod wprowadzony na manipulatorze),*
- Strefa II – ZOŚ(kod wprowadzony na manipulatorze),*
- Strefa III – Biurowiec Mały(kod wprowadzony na manipulatorze),*
- Strefa IV – Serwerownia (kod wprowadzany na manipulatorze)*
- Strefa V – Kasa (kod wprowadzany na manipulatorze)*
- Strefa VI – Sklep (kod wprowadzany na manipulatorze)*
- Strefa VII – Biurowiec (kod wprowadzany na manipulatorze)*

##### *10.6.2. Proponowany :*

- Strefa I – teren zewnętrzny dozorowany czujnikami podczerwieni i barierą podczerwieni (kod wprowadzony na manipulatorze),*
- Strefa II – ZOŚ(kod wprowadzony na manipulatorze),*
- Strefa III – Biurowiec Mały(kod wprowadzony na manipulatorze),*
- Strefa IV – Serwerownia (kod wprowadzany na manipulatorze)*
- Strefa V – Kasa (kod wprowadzany na manipulatorze)*
- Strefa VI – Sklep (kod wprowadzany na manipulatorze)*
- Strefa VII – Warsztat (kod wprowadzany na manipulatorze)*
- Strefa VIII – Magazyn (kod wprowadzany na manipulatorze)*
- Strefa IX – ZEC (kod wprowadzany na manipulatorze)*
- Strefa X – BOK (kod wprowadzany na manipulatorze)*
- Strefa XI – Warsztat (kod wprowadzany na manipulatorze)*
- Strefa XII – Biura Piętra (kod wprowadzany na manipulatorze)*

#### *10.7. Przeglądy techniczne systemów.*

- Co najmniej raz na kwartał należy przeprowadzić czynności konserwacyjne polegające na sprawdzeniu parametrów wszystkich urządzeń peryferyjnych,*

- Należy przeprowadzić test transmisji sygnału alarmowego,
- Należy odkurzyć, wyczyścić detektory, kamery, itp.,
- Należy sprawdzić stan akumulatora zasilania rezerwowego,

#### 10.8. Uwagi.

- Niniejsze opracowanie nie dotyczy procedur związanych z doбором zabezpieczeń mechanicznych,
- Niniejsze opracowanie nie dotyczy procedur związanych z przechowywaniem, dysponowaniem, zarządzaniem kluczami – zarządzanie kluczami powinno się odbywać poprzez firmę świadczącą usługi ochrony fizycznej (bazując na odrębnych procedurach opracowanych przez firmę świadczącą usługi ochrony fizycznej i zaakceptowanych przez MZK Sp. z o.o.).
- Na prace związane z modernizacją elektronicznych systemów zabezpieczeń należy opracować dokumentację projektową sporządzoną przez osobę uprawnioną. Prace należy prowadzić pod nadzorem projektanta/inspektora.

#### 11. Zalecenia dotyczące organizacji „Stanowiska Agencji Ochrony” znajdującego się na terenie Bazy Miejskiego Zakładu Komunalnego Sp. z o.o.

- a. Stanowisko ochrony powinno funkcjonować całodobowo,
- b. Aby zapewnić poprawne funkcjonowanie obiektu, przy zachowaniu wysokiego poziomu bezpieczeństwa, całodobowa obsługa powinna się składać z dwóch osób,
- c. W pomieszczeniu ochrony należy zorganizować szafę na klucze do pomieszczeń biurowych w MZK Sp. z o.o. oraz wszystkich obiektów bez obsługi całodobowej należących do MZK Sp. z o.o.,
- d. W zależności od przyjętego rozwiązania wydawanie kluczy może odbywać się w następujący sposób:
  - automatycznie (poprzez system elektronicznego wydawania kluczy),
  - półautomatycznie (użytkownik identyfikuje się kartą w systemie i do niego zostaje przypisany wydany ręcznie przez agenta ochrony klucz),
  - ręcznie (agent ochrony wydaje klucz i zapisuje dane osoby w książce wydań kluczy),
- e. Zgodnie z wcześniejszymi zaleceniami, system alarmowy w budynku biurowym należy podzielić na większą ilość stref dozorowych, osoby odpowiedzialne za daną strefę pobierając lub zdając klucz w pomieszczeniu ochrony indywidualnym kodem rozbrajają lub uzbrajają system alarmowy w danej strefie,
- f. Pobieranie kluczy do obiektów znajdujących się na terenie miasta w pomieszczeniu agencji ochrony, uprzedzi również fakt rozbrojenia systemu alarmowego na danym obiekcie i dodatkowo uszczelni system ochrony,
- g. Pracowników agencji ochrony należy wyposażyć w system automatycznej kontroli wartowników, cyklicznie (w odstępach np. 30 minutowych) jeden z agentów będzie pobierał urządzenie „PATROL” z pomieszczenia ochrony i dokonywał obchodu zgodnie z rozmieszczeniem punktów kontroli wartowników na terenie obiektu. Punkty kontroli wartowników są urządzeniami pasywnymi, niewymagającymi zasilania, trwale umocowanymi do podłoża. Urządzenie

- „PATROL” posiada wbudowany bufor pamięci i w przypadku niepokojących wydarzeń lub wrywkowej kontroli zdarzenia można zaimportować do komputera i wydrukować raport patrolowania terenu,
- h. Pracownika ochrony dokonującego obchodu należy wyposażyć w urządzenie antynapadowe (pilota), którego sygnał w przypadku zagrożenia zostanie przekazany do drugiego pracownika ochrony,
  - i. W trakcie trwania obchodu drugi pracownik ochrony sprawuje nadzór nad stacją monitorującą pozostałe obiekty MZK Sp. z o.o.,
  - j. Stanowisko ochrony należy wyposażyć w stację monitorowania alarmów. Stacja powinna pracować w standardzie TCP/IP z wykorzystaniem istniejącej sieci ethernetowej.

**Wykaz przykładowych urządzeń i standardów technicznych przeznaczonych do rozbudowy/budowy elektronicznych systemów zabezpieczeń**

- |  |                         |
|--|-------------------------|
| • Stacja monitorowania alarmów [SMA] -       | Satel STAM-2            |
| • System wizualizacji alarmów-               | INT-PTSA                |
| • System rejestracji i dozoru wizyjnego-     | SeeTec Enterprise       |
| • KameraD/N -                                | Sanyo VCC-HD2500        |
| • Centrala alarmowa-                         | SATEL Integra           |
| • Czujka dualna-                             | ARITECH DD-100          |
| • Czujka kontaktronowa-                      | ARITECH DC-108, DC-102, |
| • Sygnalizator zewnętrzny-                   | ARITECH AS 510          |
| • Przycisk napadowy-                         | ARITECH HB191           |
| • Radiolinia-                                | ELMES AN-200H           |
| • Urządzenia transmisji sygnałów alarmowych- | UBIQUITI 5Ghz ETHM      |
| • Urządzenia transmisji sygnałów wizyjnych-  | UBIQUITI 5Ghz           |

Opracował:

mgr inż. Wojciech LEŚNY

Elprotech-Systemy Sp. z o.o.

Tel. 661-771-804