

Polityka bezpieczeństwa informacji

w Przedsiębiorstwie Wodociągów i Kanalizacji

Sp. z o.o. Olsztyn

Obowiązuje od dnia:

1.06.2021 r.



Wycofano dnia: *)

ver 2.0

ORYGINAŁ



**EGZEMPLARZ ROBOCZY
PODLEGA AKTUALIZACJI**

Opracował:	Inspektor Ochrony Danych Anita Chudzińska	Data/podpis 1.06.2021 <i>Anita Chudzińska</i>
Zatwierdził:	Wiesław Pancer – Prezes Zarządu Jarosław Słoma – Wiceprezes Zarządu	Data/podpis <i>Wiceprezes Zarządu</i> <i>Prezes Zarządu</i> <i>Jarosław Słoma</i> <i>Wiesław Pancer</i>

	Instrukcja ZSZ	Nr	I-3/03	
	Polityka bezpieczeństwa informacji w PWiK Sp. z o.o. Olsztyn	Strona: 2	Stron: 27	

Spis treści

Wstęp.....	3
Świadomość organizacji.....	4
Zasady przetwarzania danych w PWiK	5
Rodzaj przetwarzanych danych osobowych w systemie informatycznym	11
Kontrola nad wprowadzaniem, przetwarzaniem i udostępnianiem danych osobowych.....	12
Inwentaryzacja zasobów w kontekście podsystemów, w których przetwarzane są dane osobowe.....	13
Wykaz komórek organizacyjnych w PWiK.....	15
Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności.....	16
Wykaz budynków oraz pomieszczeń gdzie przetwarzane są dane osobowe	18
Lokalizacja budynków	23
Wykaz zbiorów i opis struktury danych.....	28
Struktura tabel w poszczególnych modułach systemu.....	30
Moduł RPG - wspólna kartoteka kontrahentów	32
Moduł Finanse-Księgowość.....	35
Moduł Sprzedaż Pozostała	40
Schemat przepływu danych pomiędzy podsystemami.....	44
Wykaz, struktura oraz połączenia pomiędzy polami zawierającymi dane osobowe w podsystemach.....	45
Przykładowy kontekst informacji Rejestru odbiorców.....	98
Przykładowy kontekst informacji Rejestru pracowników	100
Analiza ryzyka bezpieczeństwa informacji w PWiK Sp. z o.o. Olsztyn	106

	Instrukcja ZSZ	Nr	I-3/03	
	Polityka bezpieczeństwa informacji w PWiK Sp. z o.o. Olsztyn	Strona: 3	Stron: 27	



Wstęp

Opracowana Polityka Bezpieczeństwa Informacji w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn (zwana dalej „Polityką Bezpieczeństwa”) jest wyrażeniem woli Administratora Danych, który deklaruje zaangażowanie kierownictwa oraz pracowników w ochronę danych osobowych i innych informacji przetwarzanych w przedsiębiorstwie.

W celu realizacji zasad bezpiecznego przetwarzania informacji Administrator Danych opublikował oraz wdrożył w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn (zwanym dalej „PWiK”) procedury określone w: Polityce Bezpieczeństwa, Instrukcji zarządzania systemami informatycznymi oraz danymi przetwarzanymi w PWiK Sp. z o.o. Olsztyn (zwanymi dalej „Dokumentacją Bezpieczeństwa”). Nadrzędnym celem zasad opisanych w Dokumentacji Bezpieczeństwa jest organizacyjne, fizyczne i logiczne zabezpieczenie posiadanych przez PWiK danych osobowych oraz innych danych istotnych z punktu widzenia efektywności, racjonalizacji kosztów i tajemnicy przedsiębiorstwa tj. nieujawnionych do wiadomości publicznej informacji technicznych, technologicznych, organizacyjnych przedsiębiorstwa lub innych informacji posiadających wartość gospodarczą, w tym chronionych na mocy obowiązującego prawa.



Administrator Danych zapewnia, że poprzez wdrożenie w PWiK zasad zawartych w Dokumentacji Bezpieczeństwa nastąpi ujednolicenie stosowanych norm bezpieczeństwa, co zwiększy efektywność i jakość zarządzania informacjami niezależnie od źródeł ich powstawania i zastosowanych metod ich przetwarzania. Odpowiedzialność za przestrzeganie procedur, wytycznych oraz rekomendacji związanych z ochroną danych, ponoszą wszyscy pracownicy oraz współpracownicy PWiK.

Ze względu na konieczność rozdzielenia treści zawartych w Dokumentacji Bezpieczeństwa przyjęto, że dokumentem ogólnodostępnym dla pracowników oraz współpracowników PWiK - w którym określono zasady, i procedury przetwarzania - będzie Instrukcja Zarządzania Systemami Informatycznymi oraz Danymi Przetwarzanymi w PWiK Sp. z o.o. Olsztyn (zwana dalej Instrukcją), natomiast Polityka Bezpieczeństwa Informacji zawierająca informacje, których ujawnienie mogłoby obniżyć stopień bezpieczeństwa informacji będzie dokumentem jawnym wyłącznie do strony 17.

	Instrukcja ZSZ	Nr	I-3/03	
	Polityka bezpieczeństwa informacji w PWiK Sp. z o.o. Olsztyn	Strona: 4	Stron: 27	

Świadomość organizacji



1. Administrator Danych jest świadom zagrożeń związanych z przetwarzaniem przez organizację informacji, w tym w szczególności: danych osobowych, informacji stanowiących tajemnicę przedsiębiorstwa, innych informacji prawnie chronionych oraz wynikających z tego zagrożeń związanych z rozwojem metod i technik przetwarzania tych danych w systemach informatycznych. Wobec powyższego Administrator Danych deklaruje zamiar:
 - a) monitoringu oraz doskonalenia systemu zarządzania bezpieczeństwem informacji w celu zapewnienia poufności, dostępności i integralności informacji;
 - b) wdrażania wyłącznie sprawdzonych technik informatycznych, technicznych i organizacyjnych zapewniających wymaganą ochronę przetwarzanych informacji przed:
 - udostępnieniem ich osobom nieupoważnionym;
 - przetwarzaniem z naruszeniem przepisów prawa;
 - nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem;
 - c) podejmowania wszystkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów przedsiębiorstwa związanych z bezpieczeństwem informacji, w tym zapewnienia aby dane te były:
 - przetwarzane zgodnie z prawem;
 - przetwarzane wyłącznie w celu realizacji nałożonych na przedsiębiorstwo zadań;
 - merytorycznie poprawne i adekwatne w odniesieniu do celów, w jakich są przetwarzane;
 - przechowywane w sposób umożliwiający identyfikację osób, nie dłużej niż jest to niezbędne do realizacji celu przetwarzania;
 - d) stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających informacje w PWiK w zakresie zapewnienia bezpieczeństwa informacji;
 - e) egzekwowania przyjętych przez organizację wytycznych w zakresie bezpieczeństwa informacji przez zatrudnione w organizacji osoby;
 - f) doskonalenia i rozwijania organizacyjnych, technicznych oraz informatycznych środków ochrony informacji w celu zapobieżenia zagrożeniom związanym z:
 - infekcjami malware i innego niebezpiecznego oprogramowania mogącego przyczynić się do niekontrolowanego przejęcia zasobów komputera lub przetwarzanych danych;

	Instrukcja ZSZ	Nr	I-3/03	
	Polityka bezpieczeństwa informacji w PWiK Sp. z o.o. Olsztyn	Strona: 5	Stron: 27	

- spamem oraz atakami destabilizującymi wydajność systemów informatycznych;
 - dostępem do zasobów Internetu, w innym celu niż niezbędny na danym stanowisku pracy;
 - oprogramowaniem pochodzącym z nielegalnego źródła;
 - oprogramowaniem pozwalającym wykraść zasoby komputera – zarówno dane, jak i np.: moc obliczeniową, przestrzeń dyskową;
 - lekceważeniem zasad ochrony danych określonych w Dokumentacji Bezpieczeństwa;
 - atakami z sieci WAN oraz LAN mającymi na celu uniemożliwienie dostępu do danych;
 - innymi działaniami mogącymi mieć wpływ na integralność, poufność, dostępność oraz rozliczalność danych, kradzieżą sprzętu lub nośników z danymi;
 - niewłaściwą kontrolą nad infrastrukturą informatyczną;
 - innymi zagrożeniami mogącym wystąpić w przyszłości w związku z rozwojem technik, środków oraz metod przetwarzania danych.
2. W celu identyfikacji zagrożeń oraz im przeciwdziałaniu Administrator Danych zobowiązuje się do przeprowadzania analizy ryzyka w zakresie zagrożeń mogących spowodować naruszenie wszelkich zasad bezpieczeństwa informacji, w konsekwencji mogące doprowadzić do: **zniszczenia, utraty, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu** do danych przetwarzanych w PWiK. Dokumentacja przeprowadzonej Analizy ryzyka zawarta jest w Załączniku nr 1 do Polityki Bezpieczeństwa.
3. W celu zapewnienia bezpieczeństwa informacji w PWiK Administrator Danych zastrzega sobie prawo do monitorowania czynności podejmowanych przez pracowników przy przetwarzaniu danych, w szczególności w zakresie: dostępu do stron internetowych, użytkowanych programów, rodzaju danych przechowywanych na sprzęcie teleinformatycznym należącym do PWiK oraz danych przesyłanych ze służbowych kont pocztowych.



Zasady przetwarzania danych w PWiK

1. Oprócz danych dotyczących pracowników obecnie zatrudnionych oraz byłych, i członków ich rodzin w zakresie niezbędnym do obsługi świadczeń socjalnych, w PWiK przetwarzane są dane niezbędne do realizacji zadań nałożonych na przedsiębiorstwo przepisami prawa - w tym Ustawy o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzeniu ścieków - oraz dane niezbędne



	Instrukcja ZSZ	Nr	I-3/03	
	Polityka bezpieczeństwa informacji w PWiK Sp. z o.o. Olsztyn	Strona: 6	Stron: 27	

do rozliczenia się z odbiorcami za świadczone na ich rzecz usługi. Dane te są przetwarzane i składowane zarówno w postaci tradycyjnej (papierowej) jak i w formie elektronicznej.



2. Administratorem ww. danych jest Przedsiębiorstwo Wodociągów i Kanalizacji Sp. z o.o. w Olsztynie, ul. Oficerska 16a, kod pocztowy 10-218.
3. Administrator odpowiada za przetwarzanie danych oraz dobór środków niezbędnych do ich przetwarzania zgodnie z obowiązującymi przepisami, w szczególności przepisami z zakresu ochrony danych osobowych tj. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE - zwanego dalej RODO; Ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. - zwana dalej UODO.
4. Administrator Danych wdraża Dokumentację Bezpieczeństwa w celu realizacji zasad bezpiecznego przetwarzania informacji oraz danych w PWiK.
5. Dokumentacja Bezpieczeństwa obowiązująca w PWiK ma zapewnić przestrzeganie następujących zasad:
 - poufności - poprzez zapewnienie dostępu do informacji wyłącznie osobom upoważnionym;
 - integralności – poprzez zapewnienie autoryzowanych zmian danych w systemach przetwarzających dane osobowe;
 - dostępności informacji – poprzez zapewnienie, że osoby upoważnione mają niezakłócony dostęp do informacji tylko wtedy, gdy zachodzi taka potrzeba;
 - rozliczalności – poprzez zapewnienie przechowywania historii dostępu do danych wraz z informacją kto taki dostęp posiada lub posiadał.
6. Cele, o których mowa w pkt 5 realizowane są m.in. w oparciu o zasady:
 - minimalizacji uprawnień dostępowych, tzn. każdy pracownik/współpracownik posiada tylko takie uprawnienia, jakie są wymagane do realizacji zadań przetwarzania danych;
 - wielowarstwowych zabezpieczeń, tzn. system informatyczny podlega ochronie na wielu płaszczyznach fizycznych oraz technicznych.
7. Dokumentacja Bezpieczeństwa ma zastosowanie do wszystkich danych przetwarzanych w PWiK i obejmuje:

	Instrukcja ZSZ	Nr	I-3/03	
	Polityka bezpieczeństwa informacji w PWiK Sp. z o.o. Olsztyn	Strona: 7	Stron: 27	

- istniejące, wdrażane obecnie lub w przyszłości systemy informatyczne oraz informacje przetwarzane w sposób tradycyjny (papierowy);
 - informacje będące własnością PWiK oraz informacje będące własnością kontrahentów/osób fizycznych, którymi dysponuje PWiK;
 - wszystkie typy nośników informacji, na których są lub będą znajdować się informacje;
 - wszystkie lokalizacje PWiK, budynki i pomieszczenia, w których są lub będą przetwarzane informacje;
 - wszystkich pracowników PWiK, współpracowników oraz innych osób mających dostęp do informacji podczas zadań realizowanych na rzecz PWiK.
8. W celu nadzoru nad bezpieczeństwem danych osobowych, Zarząd PWiK powołał Zarządzeniem Nr 8/18 z dnia 19.02.2018 r. Zespół ds. Ochrony Danych Osobowych w składzie:
- Anita Chudzińska – Inspektor Ochrony Danych;
 - Adam Szymański – monitoring oraz wdrażanie metod zabezpieczeń informatycznych systemów przetwarzania danych;
 - Bogusława Rurka - monitoring oraz wdrażanie metod zabezpieczeń zbiorów danych osobowych pracowników/współpracowników PWiK;
 - Cezary Kowalewski - monitoring oraz wdrażanie metod zabezpieczeń zbiorów danych osobowych klientów zewnętrznych;
 - Adam Królak - nadzór nad dokumentacją przetwarzania danych.
9. Zespół ds. Ochrony Danych Osobowych jest odpowiedzialny za wdrożenie wymogów określonych w RODO, UODO oraz zapewnienie ich przestrzegania na stanowiskach pracy w PWiK.
10. Za bezpieczeństwo informacji odpowiedzialny jest każdy pracownik oraz współpracownik PWiK.
11. Proces zarządzania bezpieczeństwem informacji jest działaniem ciągłym, podlegającym monitorowaniu oraz doskonaleniu przy użyciu środków technicznych i organizacyjnych adekwatnych do skali zagrożeń.
12. Pracownicy oraz współpracownicy w trakcie trwania zatrudnienia w PWiK oraz po jego wygaśnięciu zobowiązani są do przestrzegania zasad określonych w Dokumentacji Bezpieczeństwa.



	Instrukcja ZSZ	Nr	I-3/03	
	Polityka bezpieczeństwa informacji w PWiK Sp. z o.o. Olsztyn	Strona: 8	Stron: 27	

13. Pracownicy oraz współpracownicy zobowiązani są do niezwłocznego informowania Inspektora Ochrony Danych, członków Zespołu ds. Ochrony Danych Osobowych lub Zarządu PWiK o zaobserwowanych nieprawidłowościach przy przetwarzaniu danych.
14. Pracownicy oraz współpracownicy PWiK zobowiązani są do zachowania w tajemnicy wszystkich danych przetwarzanych przez przedsiębiorstwo zarówno w trakcie zatrudnienia jak i po jego ustaniu.
15. Dokumentacja Bezpieczeństwa będzie na bieżąco weryfikowana i dostosowywana do zmian w technologii informatycznej oraz zmian obowiązujących przepisów.
16. Do przetwarzania danych osobowych dopuszczone są wyłącznie osoby posiadające stosowne upoważnienie Administratora Danych.
17. Upoważnienie, o którym mowa w pkt. 16 podlega rejestracji w Dziale Spraw Pracowniczych. Wzór upoważnienia stanowi Załącznik nr 4 Instrukcji zarządzania systemami informatycznymi oraz danymi przetwarzanymi w PWiK Sp. z o.o. Olsztyn (jego odwołanie Załącznik nr 5 do ww. Instrukcji).
18. Nadawanie\usunięcie uprawnień do systemów informatycznych eksploatowanych w PWiK odbywa się na zasadach określonych w Instrukcji – na podstawie wzoru druku stanowiącego Załącznik nr 1 oraz 2 do Instrukcji.
19. Informacje gromadzone i przetwarzane w PWiK podlegają bieżącej inwentaryzacji prowadzonej przez jednostki organizacyjne Spółki.
20. Zbiory danych zlokalizowane są w formie papierowej oraz w bazach danych umieszczonych na serwerach bazodanowych i przetwarzane w programach dostosowanych do merytorycznych potrzeb jednostek organizacyjnych PWiK.
21. Zawartość pól informacyjnych w programach, o których mowa w pkt. 19 winna być zgodna z przepisami prawa określonymi w RODO oraz UODO.
22. PWiK współpracuje z kontrahentami, którzy zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi poufności danych oraz chroniło prawa osób fizycznych.
23. Pomieszczenia, w których znajdują się serwery przetwarzające zasoby informacyjne pozostają pod stałym nadzorem pracowników Działu Informatyki, systemu alarmowego oraz są zabezpieczone fizycznie.
24. Dostęp do urządzeń IT przez pracowników zewnętrznego serwisu technicznego jest nadzorowany przez pracowników Działu Informatyki.
25. Każde nowe urządzenie wykorzystywane do przetwarzania informacji, bądź mogące w jakikolwiek sposób wpływać na bezpieczeństwo informacji, podlega weryfikacji w zakresie zgodności z wymaganiami

	Instrukcja ZSZ	Nr	I-3/03	
	Polityka bezpieczeństwa informacji w PWiK Sp. z o.o. Olsztyn	Strona: 9	Stron: 27	



stawianymi w PWiK odnośnie m.in. luk bezpieczeństwa, stwierdzonych podatności pozwalających na nieautoryzowane jego przejęcie, zmianę konfiguracji, podgląd/modyfikację danych.

26. Dostęp do sieci LAN/WAN oraz do zasobów danych odbywa się wyłącznie na sprzęcie, którego dysponentem jest PWiK. Dostęp za pośrednictwem innych urządzeń wymaga każdorazowo pisemnej zgody Administratora Danych bądź Kierownika Działu Informatyki.
27. Dostęp do zasobów informacji w systemach informatycznych odbywa się po pomyślnym uwierzytelnieniu/autoryzacji użytkownika.
28. Systemy o znaczeniu krytycznym dla prawidłowego funkcjonowania PWiK zainstalowane są na serwerach wyposażonych w mechanizmy redundancji dysków oraz przystosowane do pracy ciągłej.
29. Systemy operacyjne, bazy danych oraz programy wykorzystywane do przetwarzania danych osobowych lub danych stanowiących tajemnicę przedsiębiorstwa obsługują mechanizmy uwierzytelniania, autoryzacji.
30. Dostęp zdalny do systemów eksploatowanych przez PWiK możliwy jest wyłącznie za pośrednictwem kanałów szyfrowanych tzw. tuneli VPN.
31. Wdrażanie bezprzewodowych sieci dostępowych wymaga uzasadnionego celu i odbywa się wyłącznie na podstawie pisemnej decyzji Administratora Danych, po uprzednim wydaniu opinii przez Kierownika Działu Informatyki odnośnie zasadności oraz możliwości bezpiecznej eksploatacji ww. sieci.
32. Dział Informatyki, w celu ochrony informacji wykorzystywanej przy użyciu infrastruktury informatycznej dokonuje monitoringu wykorzystania sprzętu IT przez pracowników/współpracowników.
33. Monitoring, o którym mowa w pkt 31 polega w szczególności na:
 - analizie oprogramowania zainstalowanego na stacjach roboczych;
 - analizie stacji roboczych pod względem wykorzystania nielegalnego oprogramowania i plików multimedialnych oraz innych elementów naruszających Prawo Autorskie;
 - analizie odwiedzanych stron www oraz innych usług dostępnych w sieci WEB oraz intranetowej;
 - analizie czasu pracy na stanowiskach komputerowych;
 - analizie wszelkich dostępow oraz ich prób do systemów IT;
 - analizie ruchu sieciowego pod względem wystąpienia komunikacji, szkodliwej dla bezpieczeństwa danych przetwarzanych w PWiK.
34. PWiK, w procesie zarządzania ciągłością działania systemów informatycznych, dba o zapewnienie odpowiedniej jakości usług związanych z przetwarzaniem informacji, poprzez przewidywanie możliwości wystąpienia krytycznych zdarzeń i przeciwdziałanie awariom oraz przerwom w działaniu systemów i urządzeń.
35. Pracownicy PWiK odpowiedzialni za zapewnienie bezpieczeństwa systemów informatycznych podlegają sukcesywnym szkoleniom z zakresu bezpieczeństwa informacji. Pracownicy, w zależności od zajmowanego

	Instrukcja ZSZ	Nr	I-3/03	
	Polityka bezpieczeństwa informacji w PWiK Sp. z o.o. Olsztyn	Strona: 10	Stron: 27	

stanowiska, będą uczestniczyć w szkoleniach z zakresu ochrony danych osobowych i szczegółowych - technicznych aspektów bezpieczeństwa.

36. Pracownicy PWiK zobowiązani są do ochrony swoich danych oraz innych środków dostępowych do systemów informatycznych.
37. W przypadku rozwiązania umowy o pracę z pracownikiem\współpracownikiem, dezaktywowane są wszystkie jego dostępy w systemach IT.
38. Każde naruszenie\incydent bezpieczeństwa jest odnotowywany na zasadach określonych w Instrukcji - wg Procedury zgłaszania naruszenia\incydentu bezpieczeństwa teleinformatycznego.
39. Opisy struktur zbiorów danych wskazujące zawartość i wzajemne powiązania poszczególnych pól informacyjnych zawarte są w części niejawnej Polityki Bezpieczeństwa.
40. Opisy, o których mowa w pkt. 37 wykonywane są w postaci wydruków, zrzutów ekranowych lub struktur tabel bazy.
41. Schemat powiązania poszczególnych systemów informatycznych przetwarzających dane w zakresie przepływu\wymiany informacji, zawarty jest w części niejawnej Polityki Bezpieczeństwa.
42. Każde istotne dane są archiwizowane na wypadek awarii w infrastrukturze IT wg zasad określonych w Instrukcji (Procedura archiwizacji danych, danych kluczowych dla prawidłowego funkcjonowania przedsiębiorstwa oraz programów i narzędzi programowych, w których są przetwarzane dane osobowe).
43. Nośniki z kopiami zapasowymi są przechowywane w miejscu uniemożliwiającym dostęp osobom nieupoważnionym.
44. W PWiK dokonywana jest okresowa ocena ryzyka bezpieczeństwa informacji dla poszczególnych systemów oraz danych osobowych.
45. Analiza ryzyka zawiera:
 - identyfikację występujących zagrożeń dla systemów, zbiorów i baz danych;
 - ocenę dotychczas stosowanej ochrony przetwarzania danych osobowych;
 - określenie stopnia ryzyka, tj. wystąpienia prawdopodobieństwa określonego zagrożenia;
 - identyfikacji obszarów wymagających szczególnych zabezpieczeń.
46. Opisana w pkt 43 analiza jest udokumentowaną podstawą zastosowania odpowiednich środków technicznych i organizacyjnych w celu zapewnienia właściwej ochrony przetwarzania danych w poszczególnych obszarach.

	Instrukcja ZSZ	Nr	I-3/03	
	Polityka bezpieczeństwa informacji w PWiK Sp. z o.o. Olsztyn	Strona: 11	Stron: 27	

Rodzaj przetwarzanych danych osobowych w systemie informatycznym

System informatyczny zainstalowany w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn, jest oprogramowaniem wykonanym w bezpiecznej technologii bazy danych obsługującej mechanizmy zapewniające spójność logiczną modyfikowanych danych - transakcyjności, relacyjności, zaawansowane uwierzytelnianie użytkowników z autoryzacją tj. możliwością przydzielania praw dostępu do poszczególnych opcji programu.

Aplikacje przetwarzające dane osobowe wchodzi w skład Zintegrowanego Systemu Informatycznego (ZSI). Całość oprogramowania wchodzącego w skład ZSI jest zainstalowana na serwerach oraz macierzach dyskowych przystosowanych do pracy ciągłej oraz wyposażonych w mechanizmy redundancji dysków, zasilaczy, kart sieciowych.



Dostęp do zasobów serwerów odbywa się po pomyślnej autoryzacji użytkownika w dedykowanej domenie PWiK – wg ustalonego formatu logowania określonego w Instrukcji - Procedura nadania uprawnień do systemu przetwarzającego dane osobowe oraz do pozostałych usług informatycznych obsługujących metody uwierzytelniania.

Dane osobowe agregowane w systemie informatycznym służą do rozliczenia pracowników w kontekście ich obowiązków oraz uprawnień wynikających z świadczenia pracy na rzecz PWiK oraz prowadzenia rozrachunków zarówno z dostawcami, jak i odbiorcami za wykonane usługi. Stanowią też źródło informacji o kliencie - przetwarzanej wyłącznie w celu realizacji procesu świadczenia usług oraz właściwego rozliczenia należności wobec PWiK. Pozostałe dane przetwarzane przez PWiK dotyczą obsługi procesów technologicznych związanych z dostarczaniem wody oraz odprowadzaniem i oczyszczaniem ścieków.

Szczegółowy wykaz przetwarzanych danych osobowych w PWiK zawarty jest w Rejestrze Czynności Przetwarzania stanowiącym Załącznik nr 2 do Polityki Bezpieczeństwa .

Kontrola nad wprowadzaniem, przetwarzaniem i udostępnianiem danych osobowych



W bezpieczeństwie systemów informatycznych eksploatowanych przez PWiK nadrzędną rolę pełni funkcja rozliczalności. Jest ona realizowana najczęściej za pomocą różnych technik rejestrowania zdarzeń, w dziennikach baz danych zabezpieczonych przed dostępem użytkowników. Rozliczalność danych w połączeniu z ochroną ich integralności, niezaprzeczalności oraz autentyczności zapisów daje pełen obraz modyfikacji prowadzonych przez poszczególnych pracowników odpowiedzialnych za przetwarzanie informacji w PWiK. Dzienniki podlegają cyklicznej archiwizacji i traktowane są jako rejestry modyfikacji danych.

	Instrukcja ZSZ	Nr	I-3/03	
	Polityka bezpieczeństwa informacji w PWiK Sp. z o.o. Olsztyn	Strona: 12	Stron: 27	

Przyjęte przez PWiK procedury nadania uprawnień do systemów informatycznych, zapewniają dostęp do danych wyłącznie w stopniu adekwatnym do celu ich przetwarzania określonego i przypisanego do danego stanowiska pracy.



System informatyczny Administratora Danych umożliwia automatycznie:

- przypisanie wprowadzanych danych użytkownikowi (identyfikatorowi użytkownika), który te dane wprowadza do systemu,
- sporządzenie i wydrukowanie w ramach potrzeb dla każdego użytkownika raportu zawierającego:
 - datę pierwszego wprowadzenia danych do systemu Administratora Danych,
 - identyfikator użytkownika wprowadzającego określone dane,
 - źródła danych - w przypadku zbierania danych nie od osoby, której dane dotyczą,
 - datę kolejnych modyfikacji rekordu.
- informacje o odbiorcach danych, którym dane osobowe zostały udostępnione.

	Instrukcja ZSZ	Nr	I-3/03	
	Polityka bezpieczeństwa informacji w PWiK Sp. z o.o. Olsztyn	Strona: 13	Stron: 27	

Inwentaryzacja zasobów w kontekście podsystemów, w których przetwarzane są dane osobowe

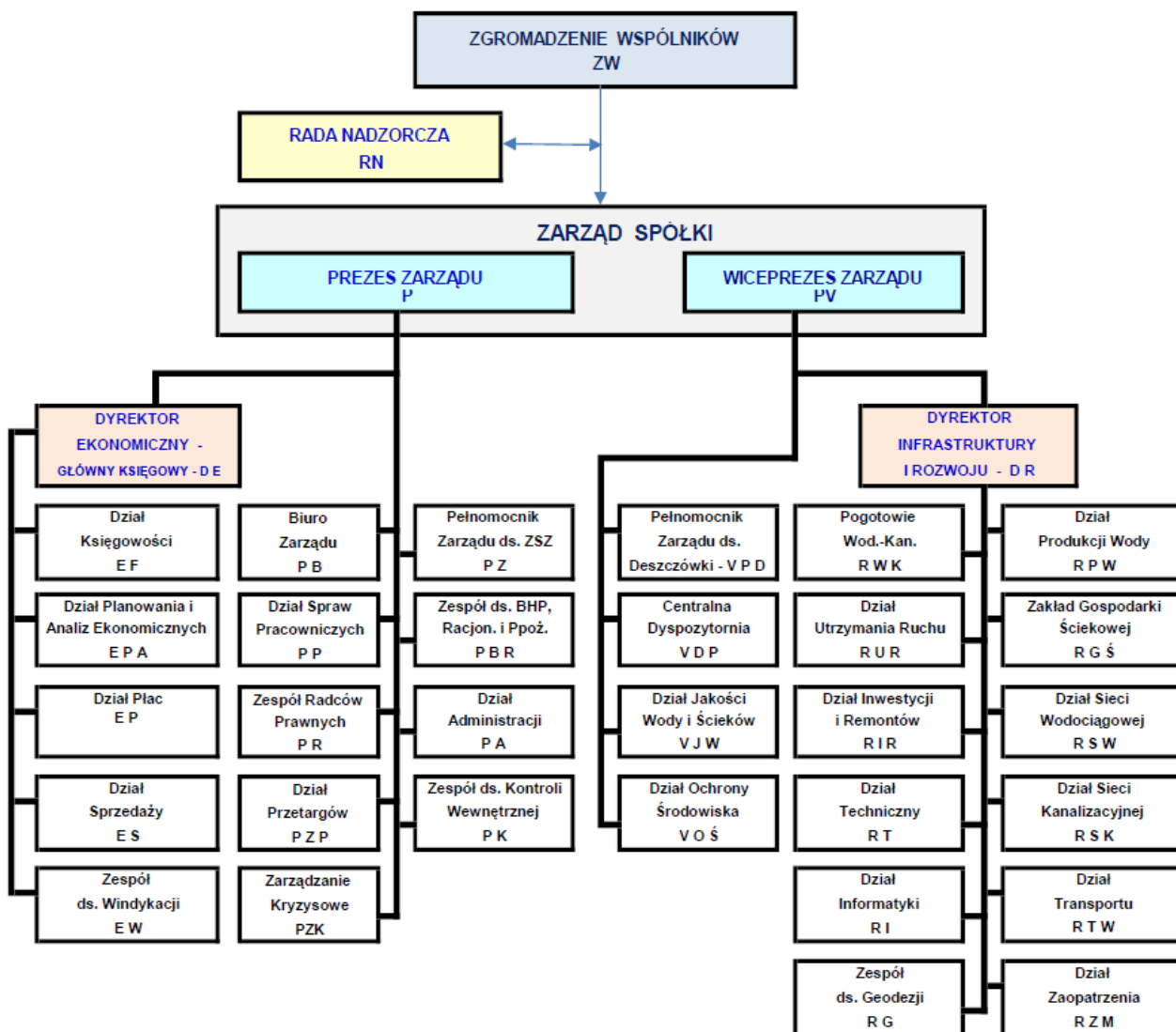
Lp.	Nazwa podsystemu/modułu	Rodzaj przetwarzanych danych osobowych
1.	Kartoteka podmiotów	Centralna kartoteka danych osobowych klientów firmy, udostępniająca dane pozostałym podsystemom w celu wystawienia faktury oraz do prowadzenia identyfikacji podmiotów.
2.	Finanse-Księgowość	Dane identyfikujące podmiot w celu prawidłowego prowadzenia rozrachunków.
3.	Gospodarka Materiałowa/Zarządzanie Zapasami	Dane identyfikujące podmiot w celu rejestracji dostawców i odbiorców asortymentu.
4.	Windykacja	Nadzór nad wierzytelnościami.
5.	Fakturowanie	Dane identyfikujące podmiot w celu wystawienia faktury.
6.	Kasa	Dane identyfikujące podmiot w celu przyjęcia wpłaty bądź dokonania wypłaty należności.
7.	Środki trwałe	Dane identyfikujące podmiot w celu rejestracji źródła nabycia majątku przedsiębiorstwa oraz dane identyfikujące osobę materialnie odpowiedzialną za powierzone mienie.
8.	Kadry-Płace/AxPeople	Dane osobowe każdego pracownika PWiK Olsztyn niezbędne do prowadzenia obsługi kadrowo-płacowej oraz obsługi należnych mu świadczeń.
9.	KOM-MEDIA	Dane identyfikujące podmiot w celu wystawiania faktur za dostawę wody i odbiór ścieków oraz

	Instrukcja ZSZ		Nr	I-3/03	
	Polityka bezpieczeństwa informacji w PWiK Sp. z o.o. Olsztyn		Strona: 14	Stron: 27	

		dane niezbędne do zawarcia umowy na świadczenie usług.
10.	KOM-BOK	Dane identyfikujące podmiot w celu rejestracji obiegu spraw dotyczących klienta.
11.	1 KOM-NET	Dane identyfikujące podmiot w celu rejestracji własności i atrybutów przyłączy wod-kan.
12.	TRANSPORT	Dane identyfikujące podmioty realizujące prace zlecone w zakresie transportu, dane pracowników w zakresie prowadzenia ewidencji i rozliczania pracy oraz wykorzystania zasobów transportowych PWiK.
13.	NND Integrum	Dane osobowe podane w pismach od klientów oraz pracowników PWiK.
14.	Zapotrzebowania i zamówienia zakupu/Rozrachunki z dostawcami - odbiorcami	Dane identyfikujące podmioty w zakresie zamówienia usług i produktów.
15.	BHP wypadki	Dane osobowe pracowników w zakresie rejestrowania i zgłoszeń wypadków w drodze i przy pracy.
16.	HOME-BANKING SANTANDER	Dane osobowe klientów, nr kont bankowych.
17.	Płatnik	Dane rozliczeniowe pracowników z ZUS.
18.	GIS	Dane klientów w zakresie integracji z podsystemem KOM-MEDIA, KOM-NET, KOM-BOK



Wykaz komórek organizacyjnych w PWiK

GRAFICZNY OBRAZ OSÓB FUNKCYJNYCH
DLA DWUOSOBOWEGO ZARZĄDU, JEDNOSTEK ORGANIZACYJNYCH I ZAKŁADÓW SPÓŁKI



Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności

Metody realizacji zasad bezpieczeństwa przy przetwarzaniu danych osobowych przyjęte przez organizację zawarto w ogólnodostępnej Instrukcji Zarządzania Systemem Informatycznym



	Instrukcja ZSZ	Nr	I-3/03	
	Polityka bezpieczeństwa informacji w PWiK Sp. z o.o. Olsztyn	Strona: 16	Stron: 27	

w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn w sekcjach: część organizacyjno-prawna, część techniczna.



Wykaz procedur oraz wniosków zawartych w Instrukcji zarządzania systemami informatycznymi oraz danymi przetwarzanymi w PWiK Sp. z o.o. Olsztyn

W celu realizacji Polityki Bezpieczeństwa Informacji wdrożono następujące procedury oraz wnioski:

- Procedura archiwizacji danych - str. 18
- Sposób, miejsce i okres przechowywania elektronicznych nośników informacji - str. 20
- Procedura nadania uprawnień - str. 21
- Procedura wykonywania przeglądów i konserwacji systemów oraz nośników - str. 23
- Procedura rozpoczęcia, zawieszenia i zakończenia pracy na stanowiskach - str. 24
- Procedura zgłaszania naruszenia/incydentu bezpieczeństwa teleinformatycznego - str. 25
- Sposób gromadzenia informacji o udostępnieniu, źródle oraz historii podmiotu - str. 27
- Wniosek o nadanie uprawnień do ZSI - str. 30
- Wniosek o usunięcie uprawnień do ZSI - str. 31
- Schemat zatwierdzeń wniosków o nadanie i usunięcie uprawnień do ZSI - str. 32
- Raport z incydentu bezpieczeństwa informacji - str. 33
- Raport z naruszenia ochrony danych osobowych - str. 34
- Upoważnienie do przetwarzania danych osobowych - str. 35
- Odwołanie upoważnienia do przetwarzania danych osobowych - str. 36
- Upoważnienie do dostępu do danych przetwarzanych w PWiK - str. 37
- Odwołanie upoważnienia do przetwarzania danych osobowych - str. 38
- Druk zgłoszenia danych do archiwizacji - str. 39
- Wniosek o odtworzenie danych z archiwum - str. 40
- Wniosek o wyrażenie zgody na wykorzystywanie pamięci przenośnej - str. 41

	Instrukcja ZSZ	Nr	I-3/03	
	Polityka bezpieczeństwa informacji w PWiK Sp. z o.o. Olsztyn	Strona: 17	Stron: 27	



- Informacja o planowanym utworzeniu nowego zbioru danych osobowych - str. 42
- Wzór umowy powierzenia przetwarzania danych osobowych - str. 43
- Potwierdzenie usunięcia danych z nośnika informatycznego - str. 47
- Wykaz niszczonek zainstalowanych w PWiK - str. 48
- Zasada czystego biurka - str. 49

	Instrukcja ZSZ	Nr	I-3/03	
	Polityka bezpieczeństwa informacji w PWiK Sp. z o.o. Olsztyn	Strona: 18	Stron: 27	

Wykaz budynków oraz pomieszczeń gdzie przetwarzane są dane osobowe

- Siedziba firmy przy ul Oficerskiej 16a Budynek A

Nazwa komórki organizacyjnej	Podsystem/Zbiory w których przetwarzane są dane osobowe	Zakres uprawnień	Nr/opis pomieszczenia
Zarząd i Dyrekcja	Dane przetwarzane poza ZSI w postaci dokumentów elektronicznych składowanych na komputerach lokalnych, kartoteki i aplikacje w formie papierowej, poczta e-mail	Odczyt-zapis danych osobowych pracowników firmy, klientów oraz osób aplikujących	104,105,106
Dział Spraw Pracowniczych	Kadry-Płace, AxPeople, kartoteki i aplikacje w formie papierowej, poczta e-mail, Zapotrzebowania i zamówienia	Odczyt-zapis danych osobowych pracowników/byłych pracowników firmy oraz osób aplikujących	204, 205, 206
Dział Płac	Kadry-Płace, AxPeople, kartoteki i aplikacje w formie papierowej, Zapotrzebowania i zamówienia	Odczyt-zapis danych osobowych pracowników/byłych pracowników firmy	201,202
Dział Księgowości	Finanse-Księgowość, RPG, Kasa, Kadry-Płace, AxPeople, Windykacja, Gospodarka Materiałowa/Zarządzane Zapasami, Środki Trwałe, kartoteki i aplikacje w formie papierowej, Home Banking, poczta e-mail, Zapotrzebowania i zamówienia	Odczyt-zapis danych osobowych klientów oraz pracowników firmy	Kasa,303,304, 305,306,309
Biuro Zarządu Spółki Punkt Obsługi Klienta	Kom-Bok, Kom-Net, Kom-Media, Zapotrzebowania i zamówienia, kartoteki i aplikacje w formie papierowej, poczta e-mail, NND Integrum	Odczyt-zapis danych osobowych klientów oraz pracowników firmy	101,102, Sekretariat Biuro Obsługi Klienta
Zespół Radców Prawnych	Dane przetwarzane poza ZSI w postaci dokumentów elektronicznych składowanych na komputerach lokalnych, kartoteki i aplikacje w formie papierowej, poczta e-mail	Odczyt-zapis danych osobowych klientów oraz pracowników firmy	5
Dział Planowania i Analiz Ekonomicznych	Kom-Bok, Kom-Net, Kom-Media	Odczyt danych osobowych klientów firmy, pracowników działów: Sieci Wodociągowej, Sieci Kanalizacyjnej, Utrzymania Ruchu	301,302

	Instrukcja ZSZ	Nr	I-3/03	
	Polityka bezpieczeństwa informacji w PWiK Sp. z o.o. Olsztyn	Strona: 19	Stron: 27	

- Siedziba firmy przy ul Oficerskiej 16a Budynek B



Nazwa komórki organizacyjnej	Podsystem/Zbiory w których przetwarzane są dane osobowe	Zakres uprawnień	Nr/opis pomieszczenia
Dział Utrzymania Ruchu	Kadry-Płace, AxPeople, Zapotrzebowania i zamówienia, kartoteki i aplikacje w formie papierowej	Odczyt danych osobowych klientów oraz pracowników działu	Gł. Mechanik, Mistrzówka, 23
Dział Transportu – Warsztat	Kadry-Płace, AxPeople, Zapotrzebowania i zamówienia, kartoteki i aplikacje w formie papierowej	Odczyt danych osobowych klientów oraz pracowników działu	Warsztat samochodowy

- Siedziba firmy przy ul Oficerskiej 16a Budynek C



Nazwa komórki organizacyjnej	Podsystem/Zbiory w których przetwarzane są dane osobowe	Zakres uprawnień	Nr/opis pomieszczenia
Dział Transportu	Fakturowanie, Transport, Kadry-Płace, AxPeople, Zapotrzebowania i zamówienia	Odczyt danych osobowych klientów oraz pracowników firmy	12
Dział Techniczny	Fakturowanie, Kom-Media, Kom-Bok, Kom-Net, Kadry-Płace, AxPeople, Zapotrzebowania i zamówienia, kartoteki i aplikacje w formie papierowej	Odczyt-zapis danych osobowych klientów oraz pracowników działu	2,5,6,7,8
Dział Jakości Wody i Ścieków	Fakturowanie, Kadry-Płace, AxPeople, Zapotrzebowania i zamówienia, kartoteki i aplikacje w formie papierowej	Odczyt danych osobowych pracowników działu oraz klientów firmy	101,108,109
Dział Informatyki	Wszystkie podsystemy ZSI	Odczyt-zapis danych osobowych pracowników firmy oraz klientów	3b,3c,3d, pomieszczenie serwerowni

- Siedziba firmy przy ul Oficerskiej 16a Budynek E



Nazwa komórki organizacyjnej	Podsystem/Zbiory w których przetwarzane są dane osobowe	Zakres uprawnień	Nr/opis pomieszczenia
Dział Inwestycji i Remontów	Fakturowanie, Kadry-Płace, AxPeople, dane przetwarzane poza ZSI w postaci dokumentów elektronicznych składowanych na komputerach lokalnych, kartoteki i aplikacje w formie papierowej, Zapotrzebowania i zamówienia	Odczyt-zapis danych pracowników działu oraz klientów	119-125
Dyrekcja	Dane przetwarzane poza ZSI w postaci dokumentów	Odczyt-zapis danych osobowych	204, 205

	Instrukcja ZSZ	Nr	I-3/03	
	Polityka bezpieczeństwa informacji w PWiK Sp. z o.o. Olsztyn	Strona: 20	Stron: 27	

	elektronicznych składowanych na komputerach lokalnych, kartoteki i aplikacje w formie papierowej, poczta e-mail	pracowników firmy, klientów oraz osób aplikujących	
Dział Przetargów	Kadry-Płace, AxPeople, Zapotrzebowania i zamówienia, dane przetwarzane poza ZSI w postaci dokumentów elektronicznych składowanych na komputerach lokalnych, kartoteki i aplikacje w formie papierowej	Odczyt-zapis danych pracowników działu oraz klientów	114,115
Dział Ochrony Środowiska	Kadry-Płace, AxPeople, dane przetwarzane poza ZSI w postaci dokumentów elektronicznych składowanych na komputerach lokalnych, Zapotrzebowania i zamówienia, kartoteki i aplikacje w formie papierowej	Odczyt-zapis danych pracowników działu oraz klientów	201-203
Pełnomocnik Zarządu ds. Zintegrowanego Systemu Zarządzania	Dane przetwarzane poza ZSI w postaci dokumentów elektronicznych składowanych na komputerach lokalnych, poczta e-mail, kartoteki i aplikacje w formie papierowej, NND Integrum	Odczyt-zapis danych członków Regionalnego Stowarzyszenia Wodociągowego, dostęp do danych klientów, pracowników w czasie przeprowadzania audytów systemu zarządzania jakością	223
Zespół ds. BHP Racjonalizacji i P.Poż.	BHP-Wypadki, dane osobowe pracowników firmy przetwarzane poza ZSI w postaci dokumentów elektronicznych składowanych na komputerach lokalnych, kartoteki i aplikacje w formie papierowej, poczta e-mail, Zapotrzebowania i zamówienia	Odczyt-zapis danych pracowników firmy oraz klientów	227
Dział Sprzedaży	Kom-Media, Kom-Bok, Kom-Net, Axapta, Kadry-Płace, AxPeople, kartoteki i aplikacje w formie papierowej, poczta e-mail, Zapotrzebowania i zamówienia.	Odczyt-zapis danych osobowych klientów oraz pracowników działu	206-213
Zespół ds. Windykacji	Kom-Media, Kom-Bok, Kom-Net, Finanse-Księgowość, AxPeople, kartoteki i aplikacje w formie papierowej, poczta e-mail, Zapotrzebowania i zamówienia	Odczyt-zapis danych osobowych klientów oraz pracowników działu	224

	Instrukcja ZSZ	Nr	I-3/03	
	Polityka bezpieczeństwa informacji w PWiK Sp. z o.o. Olsztyn	Strona: 21	Stron: 27	

Dział Administracji	Fakturowanie, Kadry-Płace, AxPeople, kartoteki i aplikacje w formie papierowej, Zapotrzebowania i zamówienia	Odczyt danych osobowych pracowników firmy oraz klientów	217-221
Dział Zaopatrzenia	Zapotrzebowania i zamówienia, Gospodarka Materiałowa/Zarządzane Zapasami, Środki Trwałe, Kadry-Płace, AxPeople, kartoteki i aplikacje w formie papierowej, poczta e-mail	Odczyt danych osobowych klientów oraz pracowników firmy	116, 117
Zespół ds. Kontroli Wewnętrznej	Dostęp do podsystemów ZSI w ramach prowadzonych kontroli, dane przetwarzane poza ZSI w postaci dokumentów elektronicznych składowanych na komputerze lokalnym, Zapotrzebowania i zamówienia	Odczyt danych osobowych klientów oraz pracowników firmy	225
Zarządzanie Kryzysowe	Kartoteki formacji obrony cywilnej przedsiębiorstwa przetwarzane w formie papierowej oraz w postaci dokumentów elektronicznych	Odczyt-zapis danych osobowych pracowników przedsiębiorstwa	214
Dział Sieci Wodociągowej	Fakturowanie, Kom-Bok, Kom-Media, Kom-Net, Kadry-Płace, AxPeople, Zapotrzebowania i zamówienia, poczta e-mail, kartoteki i aplikacje w formie papierowej	Odczyt danych pracowników działu oraz klientów firmy	101-106
Dział Sieci Kanalizacyjnej	Fakturowanie, Kom-Bok, Kom-Media, Kom-Net, Kadry-Płace, AxPeople, Zapotrzebowania i zamówienia, poczta e-mail, kartoteki i aplikacje w formie papierowej	Odczyt danych pracowników działu oraz klientów firmy	109-110
Pogotowie WOD-KAN	Fakturowanie, Kom-Bok, Kom-Media, Kom-Net, Kadry-Płace, AxPeople, kartoteki i aplikacje w formie papierowej, Zapotrzebowania i zamówienia	Odczyt-zapis danych pracowników działu oraz klientów	03-05
Centralna Dyspozytornia	Kom-Bok, Kom-Media, Kom-Net, AxPeople, Zapotrzebowania i zamówienia	Odczyt-zapis danych pracowników działu oraz klientów; dane Zarządu, Kierownictwa, pracowników Spółki	01-02
Zespół ds. Geodezji	Kom-Bok, Kom-Media, Kom-Net, AxPeople, Zapotrzebowania i zamówienia	Odczyt danych pracowników działu oraz klientów firmy	107,108

	Instrukcja ZSZ	Nr	I-3/03	
	Polityka bezpieczeństwa informacji w PWiK Sp. z o.o. Olsztyn	Strona: 22	Stron: 27	

- Siedziba firmy przy ul Oficerskiej 16a Budynek F

Nazwa komórki organizacyjnej	Podsystem/Zbiory w których przetwarzane są dane osobowe	Zakres uprawnień	Nr/opis pomieszczenia
Dział Logistyki -Magazyn	Gospodarka Materiałowa, Kadry-Płace, AxPeople, Zapotrzebowania i zamówienia	Odczyt danych pracowników działu oraz klientów	Pomieszczenie magazynierów

- Dział Produkcji Wody Budynek G/H

Nazwa komórki organizacyjnej	Podsystem/Zbiory w których przetwarzane są dane osobowe	Zakres uprawnień	Nr/opis pomieszczenia
Dział Produkcji Wody	Kadry-Płace, AxPeople, Zapotrzebowania i zamówienia, kartoteki i aplikacje w formie papierowej, poczta e-mail	Odczyt danych pracowników działu oraz klientów	Kierownik, Mistrzowie

- Zakład Gospodarki Ściekowej Budynek I

Nazwa komórki organizacyjnej	Podsystem/Zbiory w których przetwarzane są dane osobowe	Zakres uprawnień	Nr/opis pomieszczenia
Zakład Gospodarki Ściekowej	Kadry-Płace, AxPeople, Zapotrzebowania i zamówienia, kartoteki i aplikacje w formie papierowej, poczta e-mail	Odczyt danych pracowników działu oraz klientów	Sekretariat, Mistrzowie
Dział Jakości Wody i Ścieków	Zapotrzebowania i zamówienia, kartoteki i aplikacje w formie papierowej	Odczyt-zapis danych klientów firmy	Strefa Laboratorium

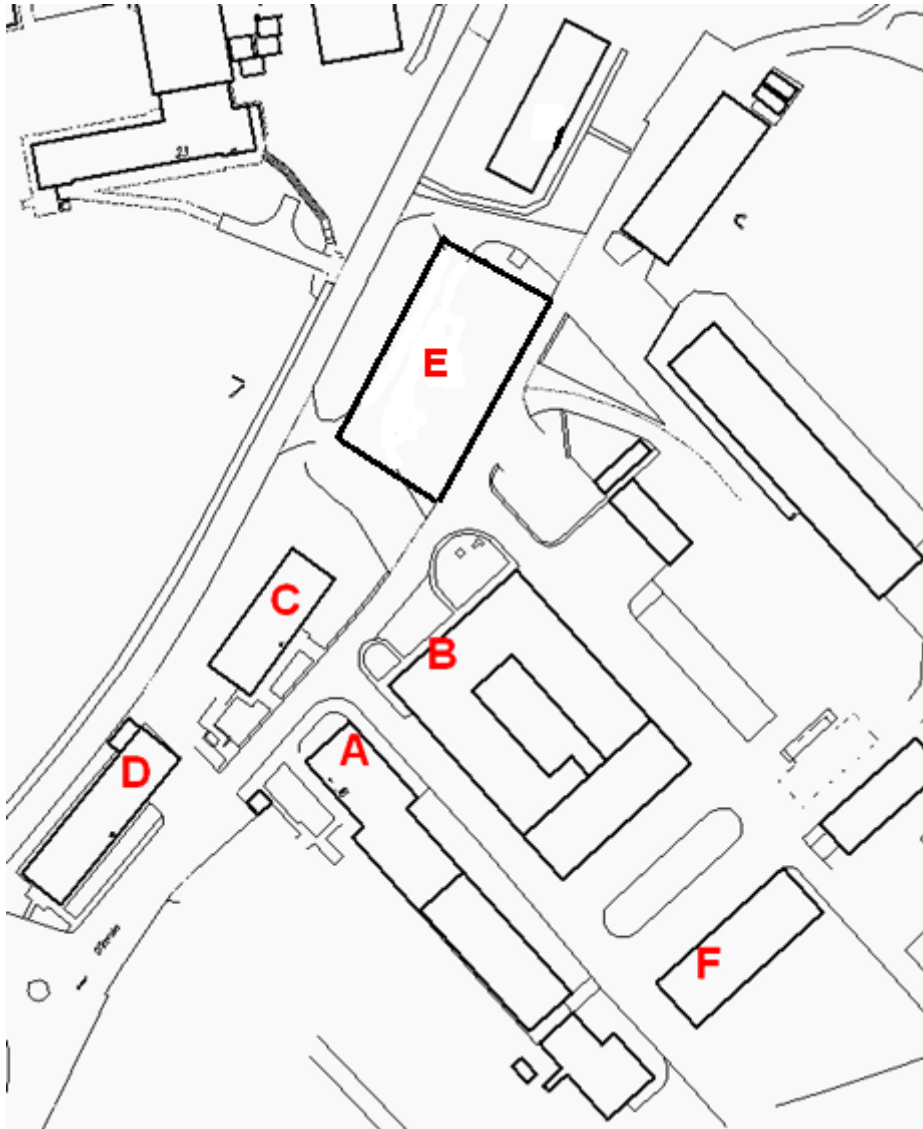
- Spalarnia i Suszarnia Osadów Budynek J



Nazwa komórki organizacyjnej	Podsystem, w którym przetwarzane są dane osobowe	Zakres uprawnień	Nr /opis pomieszczenia
Instalacja Termicznego Przekształcania Osadów	Kadry-Płace, AxPeople, Zapotrzebowania i zamówienia, kartoteki i aplikacje w formie papierowej, poczta e-mail	Odczyt danych pracowników działu oraz klientów	Dyspozytornia, pomieszczenie kierownika działu Budynek I



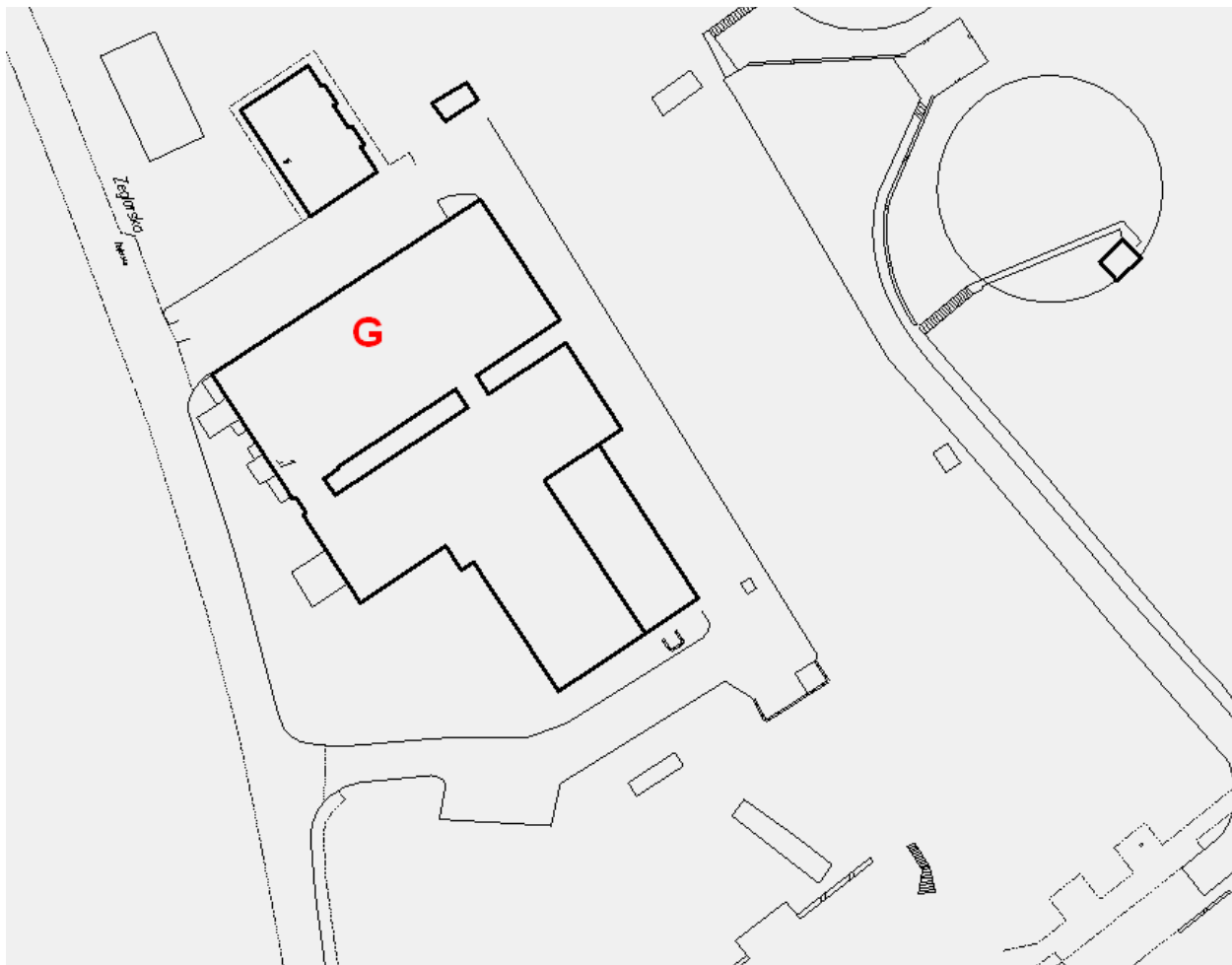
Lokalizacja budynków

- Baza firmy ul. Oficerska 16a Olsztyn



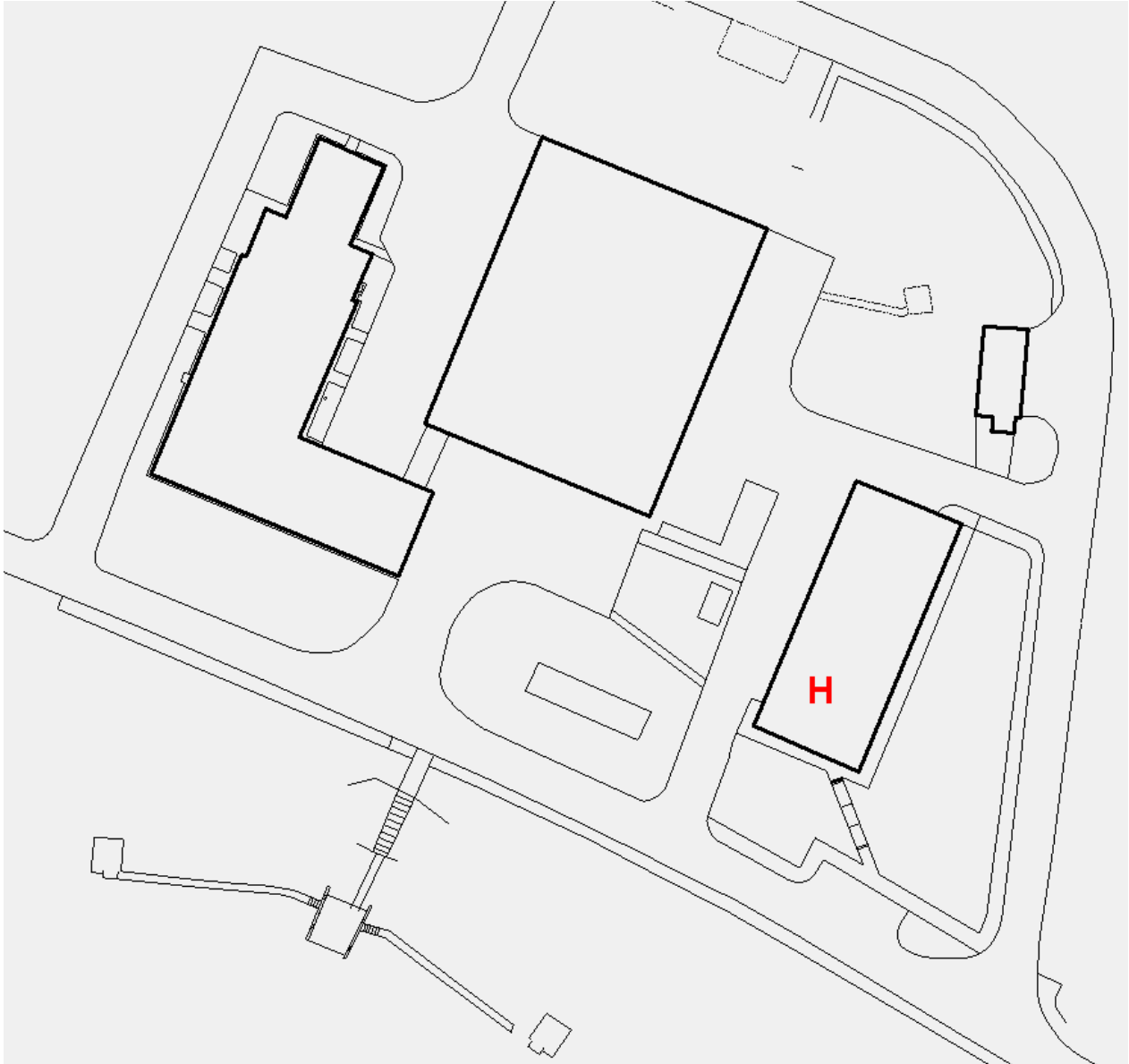
	Instrukcja ZSZ	Nr	I-3/03	
	Polityka bezpieczeństwa informacji w PWiK Sp. z o.o. Olsztyn	Strona: 24	Stron: 27	



- Dział Produkcji Wody ul. Żeglarska 1 Olsztyn



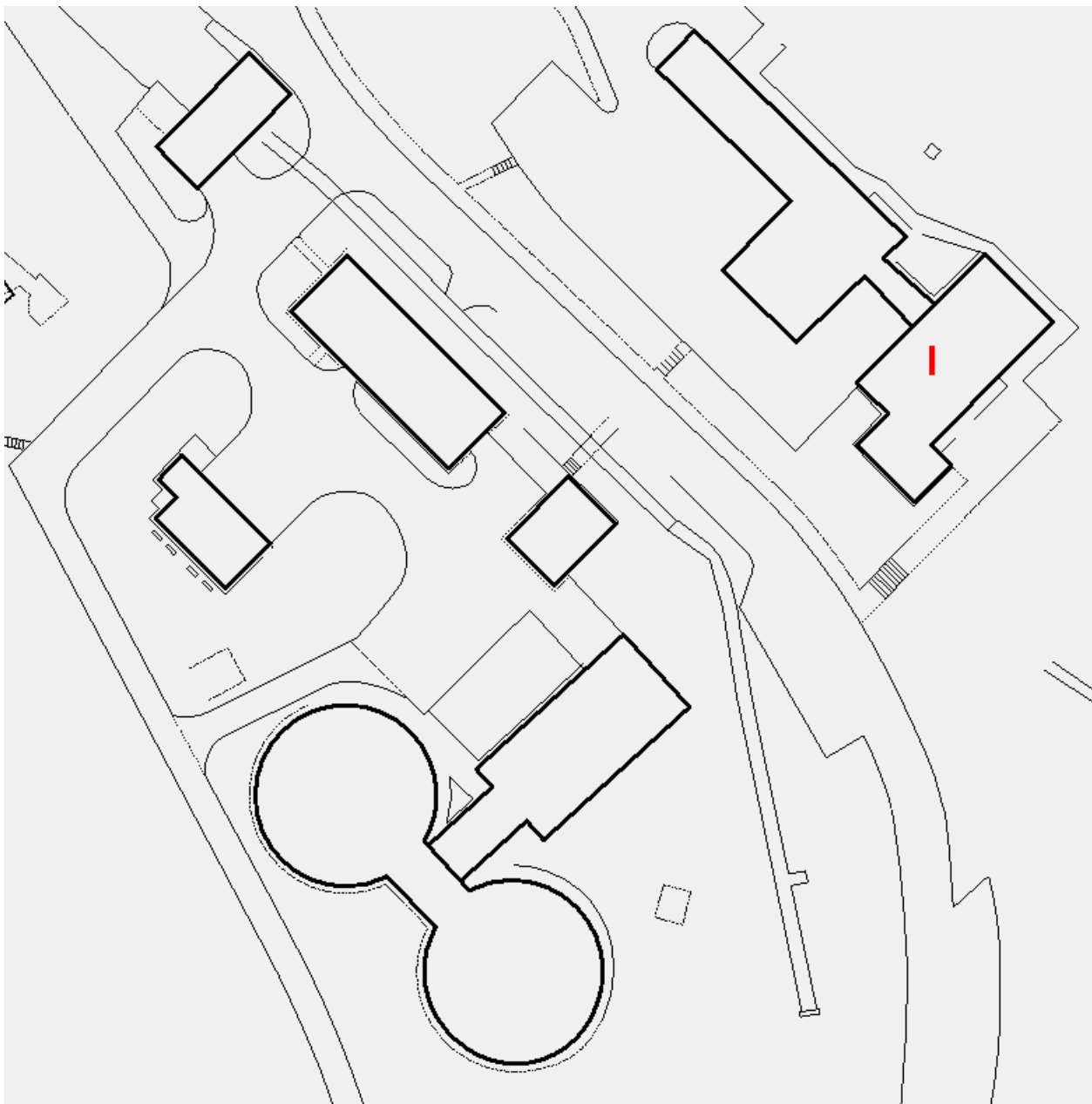


- Dział Produkcji Wody ul. Wiosenna 1 Olsztyn



	Instrukcja ZSZ	Nr	I-3/03	
	Polityka bezpieczeństwa informacji w PWiK Sp. z o.o. Olsztyn	Strona: 26	Stron: 27	

- Zakład Gospodarki Ściekowej ul. Leśna 1 Olsztyn





- Suszarnia i Spalarnia Osadów ul. Leśna 1 Olsztyn

