

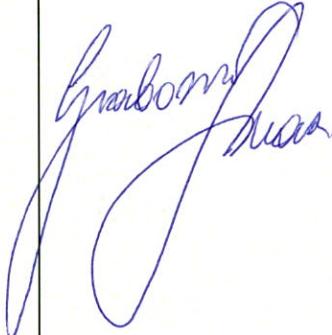
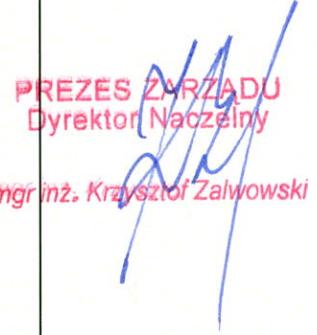


# PROCEDURA ZARZĄDZANIA INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI W RPWIK TYCHY S.A.

<b>Wersja:</b>	01/2018
<b>Data wersji:</b>	22.11.2018 r.
<b>Utworzony przez:</b>	mgr inż. Łukasz Grabowski
<b>Zatwierdzony przez:</b>	Krzysztof Zalwowski – Prezes Zarządu
<b>Poziom poufności:</b>	1

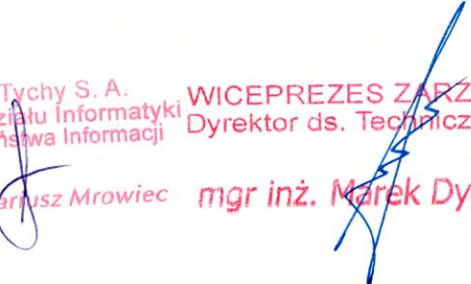
*Niniejsza instrukcja reguluje postępowanie pracowników RPWiK Tychy S.A. w związku z bezpieczeństwem informacji, definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu informacji, w tym bezpieczeństwu danych osobowych, oraz opisuje sposób reagowania na nie.*



Tytuł dokumentu	Procedura zarządzania incydentami związanymi z Bezpieczeństwem Informacji w RPWiK Tychy S.A.		
Opracował	Imię Nazwisko: <b>Łukasz Grabowski</b>	Data: <b>22.11.2018</b>	Podpis: 
Zatwierdził	Imię Nazwisko: <b>Krzysztof Zalwowski</b>	Data: <b>22.11.2018</b>	Podpis:  PREZES ZARZĄDU Dyrektor Naczelnny mgr inż. Krzysztof Zalwowski
Dokument obowiązuje od dnia podpisania dokumentu przez wskazane powyżej strony			

RPWiK Tychy S. A. WICEPREZES ZARZĄDU  
Kierownik Działu Informatyki Dyrektor ds. Technicznych  
i Bezpieczeństwa Informacji

mgr inż. Dariusz Mrowiec mgr inż. Marek Dygoń





## Spis treści

CEL PROCEDURY .....	4
ZAKRES STOSOWANIA.....	4
KLASYFIKACJA INCYDENTÓW .....	4
ZGŁASZANIE INCYDENTÓW NARUSZENIA BEZPIECZEŃSTWA INFORMACJI .....	8
ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH.....	9
ZGŁASZANIE NARUSZENIA ORGANOWI NADZORCZEMU.....	9
ZAWIADAMIANIE OSOBY, KTÓREJ DANE DOTYCZĄ, O NARUSZENIU .....	10
POSTĘPOWANIE Z INCYDENTAMI .....	11
PROCEDURA DZIAŁAŃ KORYGUJĄCYCH I ZAPOBIEGAWCZYCH .....	13



## CEL PROCEDURY

### §1

1. Celem Procedury Zarządzania Incydentami Związanymi z Bezpieczeństwem Informacji jest określenie zadań pracowników w zakresie:
  - a. ochrony wszystkich informacji przed ich modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem, a także utratą oraz ochroną zasobów technicznych;
  - b. prawidłowego reagowania pracowników przy przetwarzaniu danych, w przypadku stwierdzenia ich naruszenia (zwłaszcza naruszenia ochrony danych osobowych) lub naruszenia zabezpieczeń systemu informatycznego;
  - c. ograniczenia ryzyka powstania zagrożeń oraz minimalizacji skutków wystąpienia zagrożeń.
2. Pośrednim celem tej Procedury jest zapewnienie, że zdarzenia związane z Bezpieczeństwem Informacji oraz słabości systemów informacyjnych, są zgłoszane w sposób umożliwiający szybkie podjęcie działań korygujących.

## ZAKRES STOSOWANIA

### §2

Działania opisane w niniejszej procedurze obowiązują, we wszystkich oddziałach, działach, biurach i pozostałych komórkach organizacyjnych firmy. Niniejsza procedura jest elementem Polityki Bezpieczeństwa Informacji ustanowionej w RPWiK Tychy S.A.

## KLASYFIKACJA INCYDENTÓW

### §3

1. Naruszenie systemu ochrony danych może zostać stwierdzone na podstawie oceny:
  - a. stanu urządzeń technicznych;
  - b. zawartości zbiorów informacji;



- c. sposobu działania programu lub jakości komunikacji w sieci teleinformatycznej;
  - d. metod pracy (w tym obiegu dokumentów).
2. Naruszeniem danych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, pozyskania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego.
  3. Incydentem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.
  4. Do typowych zagrożeń Bezpieczeństwa Informacji należą:
    - a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
    - b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
    - c. nieprzestrzeganie zasad ochrony informacji przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
  5. Do typowych incydentów zagrażających bezpieczeństwu danych osobowych należą:
    - a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności); ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej, zakłócenia ciągłości pracy systemów, nie dochodzi jednak do naruszenia poufności danych;
    - b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, niezamierzzone pomyłki Operatorów, Administratorów, Informatyków, Użytkowników utrata/zagubienie danych, błędy w oprogramowaniu); może dojść do zniszczenia danych,



może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych;

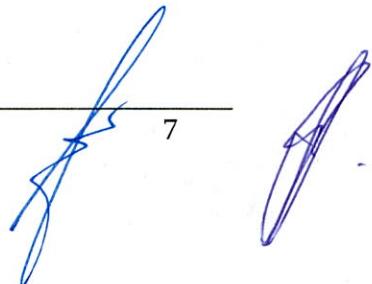
- c. zdarzenia zamierzone, świadome i celowe (włamanie do systemu informatycznego lub pomieszczeń z zewnątrz lub z sieci wewnętrznej, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania); stanowią najpoważniejsze zagrożenie naruszenia poufności danych, choć zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy.

6. Przykłady zdarzeń, które mogą być zakwalifikowane jako uzasadnione podejrzenie naruszenia bezpieczeństwa informacji:

- a. sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na infrastrukturę teleinformatyczną jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.;
- b. niewłaściwe parametry środowiska, jak zbyt wysoka temperatura lub nadmierna wilgotność (w szczególności dotyczy to serwerowni);
- c. awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie systemu, a w tym sam fakt pozostawienia serwisantów bez nadzoru;
- d. pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
- e. jakość danych w systemie lub inne odstępstwo od stanu oczekiwanej wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożadaną modyfikację w systemie;



- f. naruszenie lub próba naruszenia integralności systemu, lub bazy danych w tym systemie;
- g. próba lub modyfikacja danych, lub zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
- h. niedopuszczalna manipulacja danymi w systemie;
- i. ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą elementów systemu zabezpieczeń;
- j. praca w systemie lub w sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy, wskazujące na przełamanie lub zaniechanie ochrony danych osobowych, np.: praca w systemie lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.;
- k. ujawnienie istnienia nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki”, itp.;
- l. podmienienie lub zniszczenie nośników z danymi bez odpowiedniego upoważnienia lub kasowanie albo kopiowanie danych osobowych w niedozwolony sposób;
- m. rażące naruszenie dyscypliny pracy w zakresie przestrzegania PBI (niewylogowanie się, pozostawienie włączonego komputera po zakończeniu pracy, nie zamknięcie pokoju z komputerem, niewykonywanie w ustalonych terminach kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.);
- n. stwierdzenie nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych, w tym także osobowych (otwarte szafy, regały, biurka).





## ZGŁASZANIE INCYDENTÓW NARUSZENIA BEZPIECZEŃSTWA INFORMACJI

### §4

1. Wszyscy pracownicy firmy, którzy mają dostęp do informacji/systemów teleinformatycznych, i zobowiązali się do przestrzegania regulacji wewnętrznych związanych z PBI, w przypadku stwierdzenia jakiegokolwiek zagrożenia lub naruszenia Bezpieczeństwa Informacji, mają obowiązek bezwłocznie powiadomić bezpośredniego przełożonego oraz/lub Inspektora Ochrony Danych. W takim wypadku Pracownik jest również zobowiązany podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia. **Zgłaszający incydent nie powinien podejmować żadnych działań na własną rękę, jednak w miarę możliwości powinien zabezpieczyć materiał dowodowy.**
2. Bezpośredni przełożony pracownika, po stwierdzeniu naruszenia bezpieczeństwa danych osobowych, jest zobowiązany niezwłocznie powiadomić najwyższe kierownictwo, a także Inspektora Ochrony Danych, chyba, że zrobił to pracownik, który stwierdził naruszenie.
3. Zgłoszenie zagrożenia lub naruszenia Bezpieczeństwa Informacji może nastąpić drogą ustną, mailową lub pisemną. W przypadku powiadomień ustnych sporządzana jest notatka, która powinna zostać przedstawiona do podpisania przez pracownika zgłaszającego.
4. Zgłoszenie to musi zawierać:
  - a. imię i nazwisko zgłaszającego;
  - b. miejsce i datę wystąpienia incydentu;
  - c. opis zdarzenia.
5. Administrator Systemu Informatycznego jest zobowiązany do informowania Inspektora Ochrony Danych o wszelkich anomaliiach w pracy administrowanych



przez siebie urządzeń, mogących być przyczyną lub skutkiem incydentu, w zakresie danych osobowych.

## **ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH**

### **§5**

W przypadku naruszenia ochrony danych osobowych należy wykonać tożsame czynności co w §4 oraz, zgodnie z Rozporządzeniem 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 (ogólne rozporządzenie o ochronie danych), zgłosić to naruszenie właściwemu organowi nadzorcemu, a także w uzasadnionych przypadkach, wszystkim osobom, których to naruszenie dotyczy.

## **ZGŁASZANIE NARUSZENIA ORGANOWI NADZORCZEMU**

### **§6**

1. W przypadku naruszenia ochrony danych osobowych, Inspektor Ochrony Danych bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Urzędowi Ochrony Danych Osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorcemu, po upływie 72 godzin, dołącza się wyjaśnienie przyczyn opóźnienia. Wzór zgłoszenia – Załącznik nr 23b.
2. Zgłoszenie, o którym mowa w ust. 1, musi zawierać co najmniej:
  - a. opis charakteru naruszenia ochrony danych osobowych, w tym, w miarę możliwości, wykaz kategorii i przybliżoną liczbę osób, których dane



- dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- b. imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
  - c. opis możliwych konsekwencji naruszenia ochrony danych osobowych;
  - d. opis środków zastosowanych lub proponowanych przez Administratora, w celu zaradzenia naruszeniu ochrony danych osobowych, w tym, w stosownych przypadkach, środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
3. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
  4. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszych zapisów.

## **ZAWIADAMIANIE OSOBY, KTÓREJ DANE DOTYCZĄ, O NARUSZENIU**

### **§7**

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Inspektor Ochrony Danych bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa w ust. 1 niniejszego podrozdziału, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej następujące informacje i środki:



- a. imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
  - b. opis możliwych konsekwencji naruszenia ochrony danych osobowych;
  - c. opis środków zastosowanych lub proponowanych przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym, w stosownych przypadkach, środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:
- a. Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
  - b. Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w pkt. 1;
  - c. wymagałoby ono niewspółmiernie dużego wysiłku.
4. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

## **POSTĘPOWANIE Z INCYDENTAMI**

### **§8**

1. W przypadku stwierdzenia wystąpienia zagrożenia bezpieczeństwa danych, IOD prowadzi postępowanie wyjaśniające, w toku którego dokumentuje czynności



podjęte w prowadzonym postępowaniu poprzez sporządzenie pisemnego raportu z zagrożenia bezpieczeństwa danych wg załączonego wzoru (Załącznik 23c) który zawiera co najmniej:

- a. datę, czas, miejsce wystąpienia naruszenia, jego zakres, przyczyny ujawnienia, jego ewentualne skutki oraz wielkość szkód, które zaistniały;
  - b. ewentualne dowody winy (IOD gromadzi materiał dowodowy umożliwiający ustalenie przyczyn oraz skutków naruszenia, który może być potrzebny w przypadku ewentualnego postępowania sądowego – Załącznik 23d.);
  - c. osoby odpowiedzialne za naruszenia i inicjuje ewentualne działania dyscyplinarne;
  - d. działania naprawcze (usuwa skutki incydentu i ogranicza szkody);
  - e. działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości.
2. Firma przechowuje sporządzony raport i ewidencjonuje go w „Rejestrze incydentów i zagrożeń” (Załącznik 1 do PBI.).
  3. Gromadzenie materiału dowodowego:
    - a. dla dokumentów papierowych: oryginał jest bezpiecznie przechowywany wraz z informacją, kto znalazł dokument, gdzie, kiedy i kto by był świadkiem tego zdarzenia; każde śledztwo może wykazać, że oryginał nie został naruszony;
    - b. dla dokumentów na nośnikach komputerowych zaleca się: utworzenie obrazu lub kopii (zależnie od stosownych wymagań); zaleca się zapisanie informacji znajdujących się na dyskach twardych lub w pamięci komputera, aby zapewnić ich dostępność, zaleca się zachowanie zapisów wszelkich działań podczas procesu kopiowania oraz aby proces ten odbywał się w obecności świadków; zaleca się przechowywanie oryginalnego nośnika



i dziennika zdarzeń w sposób bezpieczny i nienaruszony (jeśli to niemożliwe, to co najmniej jeden obraz lustrzany lub kopię).

4. W przypadku, gdy zgłoszone zdarzenie nie zostało zaklasyfikowane jako Incydent Bezpieczeństwa Informacji, ma charakter fałszywego alarmu, Inspektor Ochrony Danych powiadamia zgłaszającego o zdarzeniu, że zdarzenie nie stanowi incydentu bezpieczeństwa.
5. W przypadku stwierdzenia działań umyślnych i ustaleniu sprawcy incydentu, IOD przekazuje wyniki analizy wraz z zabezpieczonym materiałem dowodowym najwyższemu kierownictwu, w celu wyciągnięcia konsekwencji dyscyplinarnych wobec sprawcy, ewentualnego zawiadomienia organów ścigania lub podjęcia kroków prawnych wobec osób trzecich.
6. Wobec osoby, która w przypadku naruszenia Bezpieczeństwa Informacji nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby, zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne lub porządkowe. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu Bezpieczeństwa Informacji nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z aktualnie obowiązującym przepisami oraz możliwością wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

## **PROCEDURA DZIAŁAŃ KORYGUJĄCYCH I ZAPOBIEGAWCZYCH**

### **§9**

1. Celem procedury jest uporządkowanie i przedstawienie czynności związanych z inicjowaniem oraz realizacją działań korygujących i zapobiegawczych,



wynikających z zaistnienia naruszeń lub zagrożeń bezpieczeństwa danych, oraz zagrożeń systemu ochrony danych osobowych.

2. Procedura działań korygujących i zapobiegawczych obejmuje wszystkie te procesy, w których incydenty bezpieczeństwa lub zagrożenia mogą wpływać na zgodność z wymaganiami prawnymi, jak również na poprawne funkcjonowanie systemu ochrony danych.
3. Osobą odpowiedzialną za nadzór nad procedurą jest IOD.
4. Definicje:
  - a. incydent – naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność;
  - b. zagrożenie – potencjalna możliwość wystąpienia incydentu;
  - c. korekcja – działanie w celu wyeliminowania skutków incydentu;
  - d. działanie korygujące – jest to działanie przeprowadzone w celu wyeliminowania przyczyny incydentu lub innej niepożądanej sytuacji;
  - e. działania zapobiegawcze – jest to działanie, które należy przedsiewziąć, aby wyeliminować przyczyny zagrożenia lub innej potencjalnej sytuacji niepożądanej;
  - f. kontrola – systematyczna, niezależna i udokumentowana ocena skuteczności systemu ochrony danych osobowych, na podstawie wymagań ustawowych, polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym.

## §10

1. IOD jest odpowiedzialny za analizę incydentów bezpieczeństwa lub zagrożeń ochrony danych. Typowymi źródłami informacji o incydentach, zagrożeniach lub słabościach są:
  - a. zgłoszenia od kierowników komórek organizacyjnych lub pracowników;



- b. wyniki kontroli w tym ustalone przyczyny i okoliczności naruszenia bezpieczeństwa informacji.
2. W przypadku, gdy IOD stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych, określa:
  - a. źródło powstania incydentu lub zagrożenia;
  - b. zakres działań korygujących lub zapobiegawczych;
  - c. termin realizacji oraz osobę odpowiedzialną.
3. Wiedzę zdobytą podczas analizy i rozwiązywania Incydentów Związanych z Bezpieczeństwem Informacji należy wykorzystać do zredukowania prawdopodobieństwa wystąpienia lub zmniejszenie skutków przyszłych incydentów.
4. IOD zapewnia właściwe wykorzystanie informacji o Incydentach Związanych z Bezpieczeństwem Informacji dla celów szkoleniowych i doskonalenia systemu zarządzania bezpieczeństwem informacji.



Załącznik nr 23a do Polityki Bezpieczeństwa Informacji RPWiK Tychy S.A.

## KATALOG ZAGROŻEŃ I INCYDENTÓW ZAGRAŻAJĄCYCH BEZPIECZEŃSTWU INFORMACJI

Formy naruszeń	Sposób postępowania	
	Kierownik komórki organizacyjnej	Inspektor Ochrony Danych
<b>Formy naruszenia danych osobowych przez pracownika zatrudnionego przy przetwarzaniu danych</b>		
<b>W zakresie wiedzy</b>		
Ujawnienie sposobu działania aplikacji i systemu jej zabezpieczeń osobom niepowołanym.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Powiadomić IOD.	Sporządza raport z opisem, jaka informacja została ujawniona.
Ujawnienie informacji o sprzęcie i pozostałej infrastrukturze informatycznej.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Powiadomić IOD.	Sporządza raport z opisem, jaka informacja została ujawniona.
Dopuszczenie i stwarzanie warunków, aby ktokolwiek mógł pozyskać informację o sprzęcie i pozostałej infrastrukturze informatycznej np. z obserwacji lub dokumentacji.	Natychmiast przerwać czynność prowadzącą do ujawnienia informacji. Powiadomić IOD.	Sporządza raport z opisem, jaka informacja została ujawniona.
<b>W zakresie sprzętu i oprogramowania</b>		
Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.	Niezwłocznie zakończyć działanie aplikacji. Pouczyć osobę, która dopuściła do takiej sytuacji. Przekazać	Przyjmuje informacje od kierownika komórki organizacyjnej i sporządza raport.



	informacje do IOD.	
Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inną osobę niż osoba, której identyfikator został przydzielony.	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Pouczyć osobę, która dopuściła się do takiej sytuacji. Sporządzić raport.	Przyjmuje raport od kierownika komórki organizacyjnej.
Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych i sieci.	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Niezwłocznie powiadomić IOD.	Sporządza raport.
Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych przez osoby nie będące pracownikami.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska pracy. Ustalić jakie czynności zostały wykonane przez osobę nieuprawnioną. Niezwłocznie powiadomić IOD.	Sporządza raport
Samodzielne instalowanie i wykorzystanie nielegalnego oprogramowania oraz narzędzi służących do obchodzenia zabezpieczeń w systemach informatycznych.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD.	Wzywa Administratora systemu informatycznego w celu odinstalowania programów. Sporządza raport.
Zmiana konfiguracji sprzętowej oraz programowej systemów oraz stacji roboczych przez	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie	Wzywa Administratora systemu informatycznego w celu przywrócenia stanu



niepowołane osoby.	powiadomić IOD.	pierwotnego. Sporządza raport.
Odczytywanie nośników przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę popełniającą wymienioną czynność, aby zaczęła stosować się do wymogów bezpieczeństwa pracy.	Wzywa Administratora systemu informatycznego w celu wykonania kontroli antywirusowej. Sporządza raport.
Wykorzystanie ogólnodostępnych serwisów pocztowych (np. Wirtualna Polska, Onet.pl, o2.pl) w celach służbowych.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD.	Sporządza raport.
Wykorzystanie służbowej poczty elektronicznej do celów prywatnych.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD.	Sporządza raport.

**W zakresie dokumentów i obrazów zawierające dane osobowe**

Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty. Przekazać informację do IOD.	Przyjmuje informację od Kierownika komórki organizacyjnej.
Przechowywanie dokumentów zabezpieczonych w niedostatecznym stopniu przed dostępem osób niepowołanych.	Spowodować poprawienie zabezpieczeń. Przekazać informacje do IOD.	Przyjmuje raport od Kierownika komórki organizacyjnej.
Wyrzucanie dokumentów w niedostatecznym stopniu zniszczonych, co umożliwia ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Sporządzić raport.	Przyjmuje raport od Kierownika komórki organizacyjnej.
Dopuszczenie do kopiowania	Zaprzestać kopiowania.	Przyjmuje raport od



dokumentów i utraty kontroli nad kopią.	Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić IOD. Sporządzić raport.	Kierownika komórki organizacyjnej.
Dopuszczenie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały ważne dane – sporządzić raport.	Przyjmuje raport od Kierownika komórki organizacyjnej.
Sporządzanie kopii danych na nośnikach danych w sytuacji nie przewidzianych procedurą.	Spowodować zaprzestanie kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić IOD.	Przyjmuje informacje od Kierownika jednostki organizacyjnej.
Utrata kontroli nad kopią danych osobowych.	Podjąć próbę odzyskania kopii. Powiadomić IOD.	Przyjmuje informacje raport od Kierownika komórki organizacyjnej.

**W zakresie pomieszczeń i infrastruktury służących do przetwarzania danych osobowych**

Opuszczenie i pozostawienie bez dozoru niezamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych.	Zabezpieczyć (zamknąć) pomieszczenie. Sporządzić raport.	Przyjmuje raport od kierownika komórki organizacyjnej.
Wpuszczenie do pomieszczenia	Wezwać osoby bezprawnie	Przyjmuje raport od



osób nieznanych i dopuszczenie ich do kontaktu ze sprzętem komputerowym.	przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość. IOD. Sporządzić raport.	kierownika komórki organizacyjnej.
Dopuszczenie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakiekolwiek urządzenia do sieci komputerowej, demontowały elementy obudów do gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji.	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i IOD. Sporządzić raport.	Przyjmuje raport od kierownika komórki organizacyjnej.
Pozostawienie otwartych okien, drzwi po zakończeniu pracy.	Zabezpieczyć (zamknąć) pomieszczenie. Sporządzić raport.	Przyjmuje raport od Kierownika komórki organizacyjnej.
Pożar, zalanie.	Podjąć próbę odzyskania dokumentacji i sprzętu. Powiadomić IOD.	Przyjmuje informacje od Kierownika jednostki organizacyjnej.
Nieprzestrzeganie polityki czystego biurka oraz czystego ekranu	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD.	Sporządza raport.
Pozostawienie dokumentów w koszu na śmieci.	Zabezpieczyć dokumenty. Przekazać informację do IOD.	Przyjmuje informację od Kierownika komórki organizacyjnej.
Pozostawienie wydruków na ogólnodostępnej drukarce.	Zabezpieczyć dokumenty. Przekazać informację do	Przyjmuje informację od Kierownika komórki



	IOD.	organizacyjnej.
Nieautoryzowane wykonanie kopii klucza do pomieszczeń biurowych.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD	Sporządza raport.
Wyniesienie kluczy od pomieszczeń biurowych po zakończonej pracy.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD	Sporządza raport.
<b>W zakresie pomieszczeń w których znajdują się komputery centralne i urządzenia sieci</b>		
Dopuszczenie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakiekolwiek manipulacji przy urządzeniach lub okablowaniach sieci komputerowej w miejscach publicznych (hole, korytarze, itp)	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania i ew. opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić Ślużby informatyczne i IOD.	Przyjmuje informacje od Kierownika komórki organizacyjnej.
Dopuszczenie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych lub ignorowania takiego faktu.	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i IOD.	Przyjmuje informacje od Kierownika komórki organizacyjnej.
<b>Zjawiska świadczące o możliwości naruszenia ochrony danych osobowych</b>		



Ślady manipulacji przy układach sieci komputerowej lub komputerach.	Powiadomić niezwłocznie IOD oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od Kierownika komórki organizacyjnej. Sporządza raport.
Obecność nowych kabli o nieznanym przeznaczeniu lub pochodzeniu.	Powiadomić niezwłocznie IOD oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od Kierownika komórki organizacyjnej. Sporządza raport.
Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.	Powiadomić niezwłocznie IOD oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od Kierownika komórki organizacyjnej. Sporządza raport.
Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od Kierownika komórki organizacyjnej.
Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania	Powiadomić niezwłocznie IOD oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od Kierownika komórki organizacyjnej. Sporządza raport.
Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe	Postępować zgodnie z właściwymi przepisami. Powiadomić niezwłocznie IOD.	Przyjmuje informacje od kierownika komórki organizacyjnej. Sporządza raport.
Zidentyfikowano środek	Powiadomić niezwłocznie	Przyjmuje informacje od



przetwarzający informacje nieznanego pochodzenia (sprzęt, nośnik.)	IOD oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Kierownika komórki organizacyjnej. Sporządza raport.
Wykorzystano niezinwentaryzowany środek przetwarzania informacji (nie będący własnością pracodawcy).	Powiadomić niezwłocznie IOD oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od Kierownika komórki organizacyjnej. Sporządza raport.
Przechowywanie haseł w niewłaściwy sposób.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD.	Wzywa administratora systemu informatycznego w celu przywrócenia stanu pierwotnego. Sporządza raport.
Przekazywanie haseł innym osobom.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD.	Wzywa administratora systemu informatycznego w celu przywrócenia stanu pierwotnego. Sporządza raport.
Pojawienie się nieautoryzowanej informacji na stronie internetowej.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od kierownika komórki organizacyjnej.
Niewłaściwe niszczenie nośników z danymi pozwalającymi na ich odczyt.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD	Wzywa administratora systemu informatycznego w celu przywrócenia stanu pierwotnego. Sporządza raport.
Wykorzystanie służbowych	Powiadomić niezwłocznie	Sporządza raport.



środków przetwarzania informacji do celów prywatnych.	IOD oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji	
Nadmierne uprawnienia w systemach w stosunku do wykonywanej pracy.	Powiadomić niezwłocznie IOD oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od kierownika komórki organizacyjnej. Sporządza raport.
Nieuprawniona zmiana danych lub ich uszkodzenie.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić IOD.	Sporządza raport.
Fizyczne zniszczenie lub uszkodzenie sprzętu oraz nośników przetwarzających informacje.	Powiadomić niezwłocznie IOD oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od Kierownika komórki organizacyjnej. Sporządza raport.
Kradzież sprzętu przetwarzającego informacje.	Niezwłocznie powiadomić IO oraz służby informatyczne.	Przyjmuje informacje od Kierownika komórki organizacyjnej.
Błędy w obsłudze i konserwacji sprzętu komputerowego służącego do przetwarzania informacji.	Powiadomić niezwłocznie IOD oraz służby informatyczne. Nie używać sprzętu ani oprogramowania	Przyjmuje informacje od Kierownika komórki organizacyjnej. Sporządza raport.



	do czasu wyjaśnienia sytuacji.	
W wyniku rozwiązania umowy z pracownikiem nie podjęto działań związanych z odebraniem uprawnień	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.	Przyjmuje informacje od Kierownika komórki organizacyjnej. Sporządza raport.
Nieuprawniony dostęp do strefy administracyjnej.	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i IOD. Sporządzić raport.	Przyjmuje raport od Kierownika komórki organizacyjnej.

**Formy naruszenia ochrony danych osobowych przez obsługę informatyczną  
w kontaktach z użytkownikiem**

Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej.	Powiadomić IOD.	Przyjmuje informacje od Kierownika komórki organizacyjnej.
Próba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych osobowych za pomocą aplikacji w bazie danych identyfikatorem i hasłem użytkownika.	Powiadomić IOD. Sporządzić raport.	Przyjmuje raport od Kierownika komórki organizacyjnej.
Niewykonanie kopii zapasowych	Powiadomić IOD. Sporządzić raport.	Przyjmuje raport od Kierownika komórki organizacyjnej.



Zał. 23 do Polityki Bezpieczeństwa Informacji RPWiK Tychy S.A.

Niezweryfikowanie możliwości odtworzenia danych z kopii zapasowych.	Powiadomić IOD. Sporządzić raport.	Przyjmuje raport od Kierownika komórki organizacyjnej.
---	------------------------------------	--



Załącznik nr 23b do Polityki Bezpieczeństwa Informacji RPWiK Tychy S.A.

**ZGŁOSZENIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH ORGANOWI  
NADZORCZEMU**

1. Data ..... Godzina .....(naruszenia)
2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe,):  
.....
3. Lokalizacja zdarzenia (nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):  
.....
4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu (*opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie*):  
.....
5. Podjęte działania:  
.....
6. Wstępna ocena przyczyn wystąpienia naruszenia (*opisywać możliwe konsekwencje naruszenia ochrony danych osobowych*):  
.....
7. Postępowanie wyjaśniające i naprawcze (*opisywać środki zastosowane lub proponowane przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków*):



.....

Imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji:

.....

(data i podpis Administratora)



Załącznik nr 23c do Polityki Bezpieczeństwa Informacji RPWiK Tychy S.A.

## RAPORT Z NARUSZENIA OCHRONY DANYCH

1. Data ..... Godzina .....

2. Osoba powiadająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe,):  
.....

3. Lokalizacja zdarzenia (nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):  
.....

4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:  
.....

5. Zabezpieczone materiały lub inne dowody związane z wydarzeniem:  
.....

6. Podjęte działania:  
.....

7. Wstępna ocena przyczyn wystąpienia naruszenia:  
.....



**8. Postępowanie wyjaśniające i naprawcze:**

.....  
.....  
.....

*(podpis pracownika)*

*(data i podpis Inspektora Ochrony Danych)*



Załącznik nr 23d do Polityki Bezpieczeństwa Informacji RPWiK Tychy S.A.

## PROTOKÓŁ ZABEZPIECZENIA MATERIAŁU DOWODOWEGO

Wykonano w dniu ..... o godzinie ..... w obecności:

Świadek 1: <imię i nazwisko, stanowisko, komórka organizacyjna Firmy>

Świadek 2: <imię i nazwisko, stanowisko, komórka organizacyjna Firmy>

Świadek 3: <imię i nazwisko, niezależny ekspert>

### I. Rodzaj materiału dowodowego

(zaznaczyć właściwe kwadraty i wpisać odpowiednie nazwy i oznaczenia)

Dokument papierowy	<input type="checkbox"/>	Rodzaj i Nazwa dokumentu: .....		
Dokument elektroniczny	<input type="checkbox"/>	Rodzaj i Nazwa dokumentu: .....		
Kopia zapasowa	<input type="checkbox"/>	System operacyjny <input type="checkbox"/> <i>Nazwa i wersja systemu:</i> .....	Aplikacja <input type="checkbox"/> <i>Nazwa i wersja aplikacji:</i> .....	
		Baza danych <input type="checkbox"/> <i>Nazwa i wersja bazy:</i> .....	Oznaczenie nośnika .....	
Obraz dysku	<input type="checkbox"/>	Lokalizacja dysku (adres IP/IPX): .....		
		Typ i nr seryjny dysku: .....		
Pliki konfiguracyjne	<input type="checkbox"/>	System operacyjny <input type="checkbox"/>	Aplikacja <input type="checkbox"/>	



i/lub systemowe		<i>Nazwa i wersja systemu:</i> .....	<i>Nazwa i wersja aplikacji:</i> .....
		Baza danych <input type="checkbox"/> <i>Nazwa i wersja bazy:</i> .....	Nazwa(y) Pliku(ów) ..... .....
Kopie zawartości dzienników (logów) zdarzeń .....	<input type="checkbox"/>	System operacyjny <input type="checkbox"/> <i>Nazwa i wersja systemu:</i> .....	Aplikacja <input type="checkbox"/> <i>Nazwa i wersja aplikacji:</i> .....
		Baza danych <input type="checkbox"/> <i>Nazwa i wersja bazy:</i> .....	Nazwa(y) Pliku(ów) ..... .....
Kopia zawartości skrzynki poczтовej	<input type="checkbox"/>	zewnętrzna <input type="checkbox"/> <i>Nazwa skrzynki poczтовej:</i> .....	wewnętrzna <input type="checkbox"/> <i>Za okres od:</i> .....

## II. Opis czynności

(opisać kolejne czynności z zaznaczeniem Wykonawcy(ów))

## III. Wytworzony materiał dowodowy

Wykonano kopie materiału dowodowego w 2 egzemplarzach, którym nadano etykiety:

....., Egzemplarz nr 1"

....., Egzemplarz nr 2"



(wprowadzić krótkie oznaczenie zabezpieczonego materiału dowodowego, zgodnie z kategorią wskazaną w pkt. I, datą i godziną wykonania)

**IV. Zabezpieczenie materiału dowodowego**

(opisać sposób zabezpieczenia jednego z egzemplarzy)

.....  
.....  
.....

Protokół sporządził: .....

Podpisano:

Świadek 1 .....

Świadek 2 .....

Świadek 3 .....



**Kontakt do Inspektora Ochrony Danych (IOD):**

Imię i nazwisko: Łukasz Grabowski

Adres e-mail: odo@rpwik.tychy.pl

Telefon stacjonarny: 48 883 942 060