

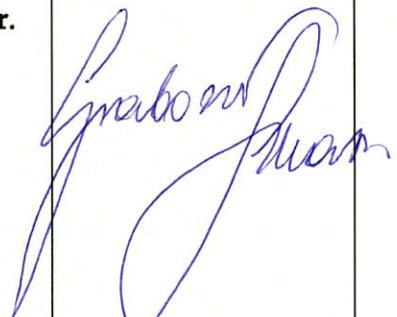
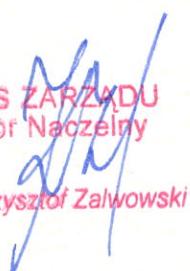


# **POLITYKA PRACY ZDALNEJ ORAZ SYSTEMU INFORMATYCZNEGO W RPWIK TYCHY S.A.**

<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 polityka reguluje sposób zarządzania pracą zdalną oraz systemem informatycznym w firmie RPWiK Tychy S.A. w związku z bezpieczeństwem informacji, zwłaszcza w odniesieniu do przetwarzania danych osobowych.*



Tytuł dokumentu	Polityka Pracy Zdalnej oraz Systemu Informatycznego w RPWiK Tychy S.A.		
Opracował	Imię Nazwisko: <b>Łukasz Grabowski</b> Pieczętka:  Inspektor Ochrony Danych  Łukasz Grabowski	Data: <b>22.11.2018 r.</b>	Podpis: 
Zatwierdził	Imię Nazwisko: <b>Krzysztof Zalwowski</b> Pieczętka:	Data: <b>22.11.2018 r.</b>	Podpis:  <b>PREZES ZARZĄDU</b> <b>Dyrektor Naczelnny</b>  <b>mgr inż. Krzysztof Zalwowski</b> 
<b>Dokument obowiązuje od dnia podpisania dokumentu przez wskazane powyżej strony</b>			

RPWiK Tychy S. A.  
Kierownik Działu Informatyki i Bezpieczeństwa Informacji  
mgr inż. Dariusz Mrowiec  


WICEPREZES ZARZĄDU  
Dyrektor ds. Technicznych  
**mgr inż. Marek Dygoń**  




## SPIS TREŚCI

POSTANOWIENIA OGÓLNE .....	5
PROCEDURY NADAWANIA UPRAWNIĘŃ .....	6
NADANIE UPRAWNIĘŃ.....	8
MODYFIKACJA UPRAWNIĘŃ.....	9
ODEBRANIE UPRAWNIĘŃ.....	10
ZARZĄDZANIE PRZYWILEJAMI.....	11
ZASADY POSTĘPOWANIA Z HASŁAMI ADMINISTRACYJNYMI.....	12
STOSOWANE METODY I ŚRODKI UWIERZYTELNIEŃNIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM .....	13
POLITYKA HASEŁ.....	14
PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU.....	15
PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA, PROWADZENIA I ZAKOŃCZENIA PRACY	16
ZASADY KORZYSTANIA ZE SŁUŻBOWEJ POCZTY ELEKTRONICZNEJ .....	17
ZASADY KORZYSTANIA Z SIECI PUBLICZNEJ (INTERNET).....	19
ZASADY POSTĘPOWANIA Z NOŚNIKAMI ELEKTRONICZNYMI ORAZ VPN PODCZAS PRACY POZA OBSZAREM PRZETWARZANIA DANYCH .....	20
SPOSÓB, MIEJSCE I OKRES PRZEHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE.....	22
UŻYTKOWANIE SPRZĘTU KOMPUTEROWEGO, OPROGRAMOWANIA, NOŚNIKÓW DANYCH.....	22
KORZYSTANIE Z URZĄDZEŃ KOMUNIKACJI GŁOSOWEJ I WIZYJNEJ .....	24
ZABEZPIECZENIE SYSTEMU INFORMATYCZNEGO PRZED UTRATĄ DANYCH SPOWODOWANĄ PODRÓŻĄ PRACOWNIKA ZDALNEGO .....	25
SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO.....	25
OCHRONA PRZED SZKODLIWYM OPROGRAMOWANIEM .....	26
SPOSÓB REALIZACJI WYMOGÓW ODNOTOWANIA INFORMACJI O ODBIORCACH, KTÓRYM DANE OSOBOWE ZOSTAŁY UDOSTĘPNIONE .....	28
PROCEDURY WYKONYWANIA PRZEGŁĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH .....	28



POSTANOWIENIA KOŃCOWE ..... 29



## POSTANOWIENIA OGÓLNE

### § 1

1. Niniejsza Polityka Bezpieczeństwa Pracy Zdalnej oraz Systemu Informatycznego (zwana dalej Polityką) zawiera sposób zarządzania pracą zdalną, służącą do ochrony danych osobowych podczas tego rodzaju zatrudnienia oraz zarządzania systemem informatycznym wykorzystywany w Spółce.
2. Polityka została zatwierdzona przez kierownictwo RPWiK Tychy S.A. i przyjęta do stosowania przez wszystkich pracowników, którzy mają dostęp do zasobów firmy zarówno w siedzibie jak i poza nią.
3. Zawarte w niej procedury i wytyczne powinny być przekazane osobom odpowiedzialnym w przedsiębiorstwie za ich realizację, stosownie do przydzielonych uprawnień, zakresu obowiązków i odpowiedzialności.
4. W Polityce zostały przedstawione podstawowe działania zmierzające do zapewnienia wymaganego poziomu bezpieczeństwa informacji, m.in.:
  - a. zabezpieczenie obszaru, w którym przetwarzane są dane osobowe poprzez uniemożliwienie dostępu do nich osobom nieuprawnionym,
  - b. zastosowanie mechanizmów kontroli dostępu do przetwarzanych danych osobowych,
  - c. monitorowanie wdrożonych zabezpieczeń systemów,
  - d. określenie procedur nadawania, zmieniania, odbierania dostępu do danych osobowych,
  - e. określenie procedur zarządzania hasłami,
  - f. określenie sposobów korzystania z sieci publicznych,
  - g. określenie procedur użytkowania oraz przechowywania sprzętu poza siedzibą przedsiębiorstwa.



## PROCEDURY NADAWANIA UPRAWNIEŃ

### § 2

1. Poniżej zostały opisane zasady przyznawania dostępu informatycznego oraz sprzętowego dla pracowników mających dostęp do sieci za pośrednictwem urządzeń.
2. Zawarte poniżej procedury obejmują:
  - a. operacje związane z nadawaniem użytkownikom uprawnień do pracy w systemie informatycznym, począwszy od utworzenia użytkownikowi dostępu do zasobów firmy poprzez połączenie VPN, poprzez przydzielanie i modyfikację jego uprawnień, aż do momentu odebrania sprzętu przez organizacje,
  - b. zasady postępowania w trakcie pracy zdalnej,
  - c. zasady zabezpieczenia sprzętu podczas trwania stosunku zatrudnienia.

### § 3

1. Przydzielanie uprawnień do systemu informatycznego realizowane jest w oparciu o następujące zasady:
  - a. każdy z użytkowników posiada prawa dostępu do zasobów ograniczone wyłącznie do tych, które są niezbędne do wykonywania powierzonych mu obowiązków poprzez połączenie VPN,
  - b. pracownicy posiadają wiedzę o zasobach ograniczoną wyłącznie do zagadnień, które są niezbędne do realizacji powierzonych im zadań,
  - c. wszystkie działania, które nie są jawnie dozwolone, są zabronione.
2. Dostęp do zasobów sprzętowych oraz systemu informatycznego mogą posiadać pracownicy lub współpracownicy, w szczególności:
  - a. osoby zatrudnione na podstawie umowy cywilnoprawnej,
  - b. pracownicy lub osoby działające w imieniu podmiotu zewnętrznego, świadczącego usługi na rzecz Administratora Danych,
  - c. stażyści, na podstawie umowy z Urzędem Pracy,



- d. praktykanci, na podstawie umowy ze szkołą wyższą, ew. wolontariusze, na podstawie umowy o wolontariat.
3. Użytkownik systemu informatycznego jest jednoznacznie identyfikowany poprzez nadany mu indywidualny identyfikator użytkownika.
4. Niedopuszczalne jest korzystanie z tego samego identyfikatora przez więcej niż jednego użytkownika.
5. Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi.
6. Uprawnienia dostępu są nadawane wyłącznie w zakresie wynikającym z zajmowanego stanowiska i potrzeby wykonywania obowiązków służbowych na danym stanowisku pracy. Bezzasadne nadawanie uprawnień Administratora (przywilejów) będzie kwalifikowane jako incydent związany z Bezpieczeństwem Informacji.

#### § 4

1. Użytkownikowi zostaje nadany dostęp do zasobów sprzętowych oraz informatycznych po:
  - a. zapoznaniu się z niniejszą Polityką,
  - b. zapoznaniu się ze wszystkimi załącznikami do Polityki,
  - c. zapoznaniu się z Polityką Transportu Dokumentów oraz bezpieczeństwa teleinformatycznego,
  - d. podpisaniu oświadczenia o zapoznaniu się z dokumentacją przetwarzania danych osobowych,
  - e. podpisaniu oświadczenia o zachowaniu informacji (w tym danych osobowych), do których użytkownik będzie miał dostęp podczas wykonywania obowiązków służbowych lub zobowiązań umownych oraz środków ich zabezpieczania, w tajemnicy (również po ustaniu łączącej strony umowy), w tym powstrzymanie się od wykorzystywania ich w celach pozasłużbowych,



- f. otrzymaniu upoważnienia do przetwarzania danych osobowych.
2. Rejestr użytkowników wraz z uprawnieniami do systemu i/lub aplikacji prowadzi Administrator Systemu Informatycznego (ASI). Prowadzi on również rejestr powierzonego sprzętu teleinformatycznego pracownikom poza siedzibę Przedsiębiorstwa.
3. Rejestry, o których mowa powyżej prowadzone są w postaci elektronicznej lub papierowej.
4. Weryfikację aktualności rejestrów, o których mowa powyżej, prowadzi ASI we współdziałaniu z osobami odpowiedzialnymi za wnioskowanie o nadanie/modyfikację/odebranie uprawnień do systemu informatycznego oraz sprzętu teleinformatycznego.
5. Administrator Systemu Informatycznego, raz na 30 dni, dokonuje przeglądu stanu aktywności kont użytkowników.

## NADANIE UPRAWNIEŃ

### § 5

1. Kierownik jednostki organizacyjnej zobowiązany jest do złożenia wniosku o nadanie uprawnień do systemu informatycznego dotyczącego danego środowiska informatycznego Administratora Danych. Wniosek powinien zawierać informacje komu, w jakim stopniu i na jaki czas, mają zastać przyznane uprawnienia.
2. Po dopełnieniu powyższych wymagań wniosek powinien zostać przekazany do Administratora Systemu Informatycznego.
3. Administrator Systemu Informatycznego realizuje otrzymany wniosek lub odmawia nadania uprawnień do systemu informatycznego w przypadku powzięcia podejrzeń, co do przekroczenia uprawnień wymaganych na danym stanowisku.
4. W przypadku powzięcia podejrzenia, co do przekroczenia uprawnień wymaganych na danym stanowisku, ASI jest obowiązany zgłosić ten fakt najwyższemu kierownictwu firmy oraz Inspektorowi Ochrony Danych (IOD).



5. W przypadku nadania uprawnień wymagających logowania, Administrator Systemu Informatycznego przekazuje użytkownikowi informację zawierającą wymienione z nazwy systemy informatyczne, do których użytkownik otrzymał dostęp oraz login i hasło na potrzeby pierwszego logowania.
6. Wniosek o nadanie uprawnień może zostać sporządzony i przekazany Administratorowi Systemu Informatycznego także za pomocą poczty elektronicznej.

## MODYFIKACJA UPRAWNIEŃ

### § 6

1. Kierownik jednostki organizacyjnej jest zobowiązany do złożenia wniosku o zmianę uprawnień do systemu informatycznego dotyczącego modyfikacji uprawnień do danego zasobu informatycznego.
2. Wniosek modyfikujący uprawnienia pracownika powinien zostać złożony do Administratora Systemu Informatycznego w możliwie najkrótszym czasie po wystąpieniu zapotrzebowania na dostęp do danego zasobu informatycznego.
3. W zależności od obszaru zmian, wniosek powinien zawierać uzasadnienie wnoszonych zmian oraz informację o przedmiocie modyfikacji:
  - a. zmiana/dodanie/usunięcie uprawnień w profilu uprawnień,
  - b. przekierowanie skrzynki poczтовej,
  - c. założenie dodatkowej skrzynki poczтовej,
  - d. dodanie/usunięcie do grupy użytkowników,
  - e. zestawienie łącza VPN,
  - f. nadanie indywidualnych uprawnień do systemów poza zdefiniowanym profilem.
4. Administrator Systemu Informatycznego realizuje otrzymany wniosek lub odmawia nadania uprawnień do systemu informatycznego w przypadku powzięcia podejrzeń, co do przekroczenia uprawnień wymaganych na danym stanowisku.



5. W przypadku powzięcia podejrzenia, co do przekroczenia uprawnień wymaganych na danym stanowisku, Administrator Systemu Informatycznego jest obowiązany zgłosić ten fakt najwyższemu kierownictwu firmy oraz IOD.
6. W przypadku nadania uprawnień wymagających logowania, Administrator Systemu Informatycznego przekazuje użytkownikowi informację zawierającą wymienione z nazwy systemy informatyczne, do których użytkownik otrzymał dostęp oraz login i hasło na potrzeby pierwszego logowania.
7. Wniosek o modyfikację uprawnień może zostać sporządzony i przekazany Administratorowi Systemu Informatycznego także za pomocą poczty elektronicznej.
8. W przypadku modyfikacji uprawnień, ASI zmienia Wykaz upoważnień do systemów informatycznych.

## ODEBRANIE UPRAWNIĘŃ

### § 7

1. Kierownik danej jednostki administracyjnej jest zobowiązany do złożenia wniosku o odebranie uprawnień do systemu informatycznego dotyczącego odebrania użytkownikowi uprawnień do danego zasobu teleinformatycznego.
2. Terminami obowiązującymi przy składaniu wniosku są w szczególności:
  - a. w przypadku ustania stosunku pracy należy złożyć wniosek odbierający wszystkie uprawnienia oraz sprzęt – natychmiast, jednak nie później, niż ostatniego dnia pracy zatrudnionego,
  - b. w przypadku długotrwałego zwolnienia lekarskiego należy złożyć wniosek odbierający wszystkie uprawnienia oraz sprzęt - natychmiast po upływie 30 (trzydziestu) dni kalendarzowych zwolnienia lekarskiego,
  - c. w przypadku zmiany stanowiska pracy należy złożyć wniosek odbierający część uprawnień - natychmiast, jednak nie później, niż ostatniego dnia



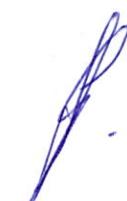
pracy przed zmianą stanowiska na stanowisko wymagające zmniejszenia uprawnień.

3. Po spełnieniu powyższych wymagań wniosek powinien zostać przekazany do Administratora Systemu Informatycznego.
4. Administrator Systemu Informatycznego przyjmuje wniosek o odebranie uprawnień do systemu informatycznego, spełniający wymogi opisane powyżej.
5. ASI dokonuje weryfikacji poprawności wniosku o odebranie uprawnień do systemu informatycznego oraz sprzętu teleinformatycznego.
6. Administrator Systemu Informatycznego bezzwłocznie realizuje otrzymany wniosek.
7. Wniosek o odebranie uprawnień może zostać sporządzony i przekazany Administratorowi Systemu Informatycznego także za pomocą poczty elektronicznej.

## ZARZĄDZANIE PRZYWILEJAMI

### § 8

1. Nadawane przywileje (większe uprawnienia, niż wynika to z realizowanych, rutynowych zadań użytkownika), podlegają ścisłej ewidencji prowadzonej przez Administratora Systemu Informatycznego.
2. Przywileje w systemie nadaje Administrator Systemu Informatycznego.
3. Uprzywilejowane konto nie może służyć do realizacji przez użytkownika rutynowych zadań.
4. Przywileje podlegają cofnięciu niezwłocznie po ustaniu potrzeby uzasadniającej ich nadanie.
5. Nadawane przywileje podlegają regularnym przeglądom i kontroli.





## ZASADY POSTĘPOWANIA Z HASŁAMI ADMINISTRACYJNYMI

### § 9

1. W stosunku do haseł użytkowników uprzywilejowanych stosuje się zaostrzone standardy bezpieczeństwa.
2. Standardy, o których mowa powyżej, stosuje się również do haseł:
  - a. elementów aktywnych sieci teleinformatycznych;
  - b. konfiguracji komputerów, w tym hasła do BIOS.
3. Hasła, o których mowa w ust. 1 i 2 przechowuje się w postaci zaszyfrowanej.
4. Do przechowywania haseł zapisanych na papierze stosuje się wyłącznie koperty, uniemożliwiają otwarcie bez uszkodzenia ich struktury (tzw. „koperty bezpieczne”).
5. Koperty z hasłami przechowuje się w zamkniętych szafach (ewentualnie w sejfach), w miejscu zapewniającym dostęp tylko osobom upoważnionym.
6. Dane umieszczone na bezpiecznej kopercie zawierają:
  - a. numer koperty adekwatny do numeru ewidencyjnego podanego w ewidencji haseł;
  - b. datę jej złożenia i podpis osoby składającej kopertę;
  - c. skróconą nazwę przynależności hasła.
7. Koperty z hasłami podlegają ścisłej ewidencji prowadzonej przez Administratora Systemu Informatycznego.
8. Ewidencja haseł przechowywana jest w miejscu zabezpieczonym przed dostępem osób niepowołanych.
9. Za aktualność przechowywanych haseł odpowiedzialny jest Administrator Systemu Informatycznego.
10. Awaryjne otwarcie bezpiecznej koperty oraz pobranie kopii hasła znajdującego się w kopercie wymaga uprzedniej pisemnej akceptacji IOD lub osoby przez niego upoważnionej i jest udokumentowane w ewidencji kopert.



11. Po użyciu, hasło ulega zniszczeniu, a w to miejsce jest generowane nowe hasło, którego kopia jest przechowywana na identycznych zasadach, jak w przypadku zniszczonego hasła.

## **STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM**

### **§ 10**

1. Poniżej zostały uregulowane m.in. tryb przydzielania haseł, wymogi dotyczące stopnia ich złożoności oraz wskazanie osoby odpowiedzialnej za przydział haseł.
2. Zawarte poniżej procedury odnoszą się również do:
  - a. możliwych zagrożeń i konsekwencji związanych z tzw. utratą tożsamości elektronicznej (tj. utratą danych służących uwierzytelnieniu, co może skutkować pozyskaniem tych danych przez osoby nieuprawnione),
  - b. zalecanych sposobów korzystania z przeglądarek internetowych.

### **§ 11**

1. Każdy użytkownik systemu informatycznego musi posiadać unikalny identyfikator i wprowadzone przez siebie hasło autoryzujące jego osobę w systemie informatycznym.
2. Hasła użytkowników lub inne dane uwierzytelniające podlegają szczególnej ochronie.
3. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła (oprócz pierwszego hasła do systemu, nadawanego przez Administratora Systemu Informatycznego) i jego przechowywanie.
4. Osoba pełniąca funkcję ASI powinna posiadać dodatkowo odrębne konto służące tylko i wyłącznie do administracji danym systemem informatycznym, o ile dany system udostępnia taką funkcjonalność.



## POLITYKA HASEŁ

### § 12

Każdy użytkownik posiadający dostęp do systemów informatycznych jest obowiązany do:

1. zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających, wykorzystanych do pracy w systemie informatycznym;
2. niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia;
3. niezwłocznej zmiany hasła tymczasowego, przekazanego przez Administratora Systemu Informatycznego;
4. poinformowania Administratora Systemu Informatycznego oraz Inspektora Ochrony Danych o podejrzeniu lub rzeczywistym ujawnieniu hasła;
5. stosowania haseł o minimalnej długości 8 znaków, zawierających kombinacją małych i dużych liter oraz cyfr lub znaków specjalnych;
6. stosowania haseł nie posiadających w swojej strukturze części loginu;
7. stosowania haseł nie będących zbliżonymi do poprzednich (np. RPWIK2018 – RPWIK2019);
8. zmiany wykorzystywanych haseł, nie rzadziej niż raz na 90 dni.

### § 13

1. Hasła zachowują swoją poufność również po ustaniu ich użyteczności.
2. Zabronione jest:
  - a. zapisywanie haseł w sposób jawnym i umieszczania ich w miejscach dostępnych dla innych osób;
  - b. stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.;
  - c. używanie tych samych haseł w różnych systemach operacyjnych i aplikacjach;
  - d. udostępnianie haseł innym użytkownikom;



- e. przeprowadzanie prób łamania haseł;
- f. wpisywanie haseł „na stałe” (np. w skryptach logowania) oraz wykorzystywania opcji auto-zapamiętywania haseł (np. w przeglądarkach internetowych).

#### **§ 14**

1. Administrator Systemu Informatycznego zobowiązany jest do skonfigurowania systemu tak, aby próby dostępu do tego systemu były limitowane zarówno w ujęciu ilościowym, jak i czasowym, jeżeli system umożliwia wymienioną konfigurację.
2. W przypadku, gdy system umożliwia limitowanie wprowadzenia błędного hasła, należy przyjąć próg ilości wprowadzonych błędnych haseł na 3, po czym ustanowić blokadę konta.
3. Należy ograniczyć możliwość wielokrotnego logowania, gdzie użytkownik loguje się na kilku komputerach równocześnie wykorzystując ten sam identyfikator.
4. Administrator Systemu Informatycznego odblokowuje/zresetuje hasło do danego systemu informatycznego, w przypadku przekroczenia przez użytkownika ustalonej ilości prób logowania.
5. Po dokonaniu czynności przez Administratora Systemu Informatycznego stosowna informacja o odblokowaniu dostępu do konta użytkownika zostanie przekazana użytkownikowi.

### **PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU**

#### **§ 15**

1. Poniżej zostały opisane kolejne czynności, jakie należy wykonać, w celu uruchomienia systemu informatycznego, a w szczególności, zasady postępowania użytkowników podczas przeprowadzania procesu uwierzytelniania się (logowania się do systemu).



2. Przestrzeganie określonych w instrukcji zasad ma na celu zachowanie poufności haseł oraz uniemożliwienie nieuprawnionego przetwarzania danych.
3. Zawarte poniżej procedury obejmują również:
  - a. metody postępowania w sytuacji tymczasowego zaprzestania pracy, na skutek opuszczenia stanowiska pracy;
  - b. metody postępowania w sytuacji, kiedy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba;
  - c. sposób postępowania w sytuacji podejrzenia naruszenia bezpieczeństwa systemu, np. w razie braku możliwości zalogowania się użytkownika na jego konto, czy też w sytuacji stwierdzenia fizycznej ingerencji w przetwarzane dane bądź użytkowane narzędzia programowe lub sprzętowe.

## **PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA, PROWADZENIA I ZAKOŃCZENIA PRACY**

### **§ 16**

1. Rozpoczęcie pracy w systemie informatycznym następuje po wprowadzeniu unikalnego identyfikatora i hasła.
2. Zawieszenie pracy w systemie informatycznym tj. brak wykonywania jakichkolwiek czynności, przez okres 10 minut, w systemie informatycznym powoduje automatycznie uruchomienie systemowego wygaszacza ekranu blokowanego hasłem. Zastosowanie powyższego mechanizmu nie zwalnia użytkownika z obowiązku każdorazowego blokowania ekranu wygaszaczem chronionym hasłem po odejściu od stanowiska.
3. Przed zakończeniem pracy należy upewnić się, czy dane zostały zapisane, aby uniknąć utraty danych.
4. Po zakończeniu pracy, użytkownik obowiązany jest wylogować się z systemu informatycznego przetwarzającego dane osobowe i, z systemu operacyjnego,



zabezpieczyć nośniki informacji (elektroniczne i papierowe) oraz wyłączyć komputer.

5. W sytuacji, gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba, należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlana treść.
6. Użytkownik systemu informatycznego przetwarzającego dane osobowe niezwłocznie powiadamia ASI w przypadku, gdy:
  - a. wygląd systemu, sposób jego działania, zakres danych lub sposób ich przedstawienia przez system informatyczny odbiega od standardowego stanu, uznawanego za typowy dla danego systemu informatycznego;
  - b. niektóre opcje, dostępne użytkownikowi w normalnej sytuacji, przestały być dostępne lub opcje niedostępne użytkownikowi w normalnej sytuacji, stały się dostępne.

## ZASADY KORZYSTANIA ZE SŁUŻBOWEJ POCZTY ELEKTRONICZNEJ

### § 17

1. Użytkownikowi zostaje nadany dedykowany adres skrzynki poczty elektronicznej działający w domenie Administratora Danych Osobowych (ADO).
2. Informacja o służbowym adresie skrzynki poczty jest jawną i ogólną, w tym może być dostępna na łamach witryny internetowej ADO, w postaci książki adresowej.
3. Nadany użytkownikowi adres skrzynki poczty elektronicznej służy wyłącznie do realizacji celów służbowych lub umownych. Korespondencja realizowana drogą elektroniczną, z wykorzystaniem systemów informatycznych ADO podlega rejestracji i może być monitorowana. Informacje przesyłane za pośrednictwem sieci Administratora Danych Osobowych (w tym do, i z Internetu) nie stanowią własności prywatnej użytkownika.



4. Wszelka korespondencja elektroniczna, niezwiązana z działalnością ADO, powinna być prowadzona przez prywatną skrzynkę poczty elektronicznej użytkownika.
5. Korzystanie z systemu poczty elektronicznej, dla celów prywatnych, nie może wpływać na wydajność systemu poczty elektronicznej.
6. Użytkownicy dokonujący wysyłki korespondencji masowej poza organizację, obowiązani są do ukrywania odbiorów w kopii (pole BCC lub UDW).
7. Zabronione jest:
  - a. wysyłanie materiałów służbowych na konta prywatne (np. celem pracy nad dokumentami w domu);
  - b. wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi Administratora Danych Osobowych;
  - c. odbieranie wiadomości z nieznanych źródeł;
  - d. otwieranie załączników z plikami samorozpakowującymi się, bądź wykonalnymi typu .exe, .com, itp.;
  - e. przesyłanie pocztą elektroniczną plików wykonywalnych typu: .com, .exe, plików multimedialnych oraz plików graficznych;
  - f. ukrywanie lub dokonywanie zmian tożsamości nadawcy;
  - g. czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika;
  - h. odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem;
  - i. posługiwanie się służbowym adresem e-mail, w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy lub obowiązków umownych;
  - j. wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej, niż wynikającej z potrzeb



Administratora Danych Osobowych lub do poszukiwania dodatkowego zatrudnienia.

## **ZASADY KORZYSTANIA Z SIECI PUBLICZNEJ (INTERNET)**

### **§ 18**

1. Zdalne korzystanie z systemów informatycznych poprzez sieć publiczną może mieć miejsce po zastosowaniu systemu uwierzytelniania użytkownika i szyfrowanego kanału transmisji.
2. Zdalny dostęp do serwerów, w celach administracyjnych, może mieć miejsce po zastosowaniu systemu uwierzytelniania użytkownika i szyfrowanego kanału transmisji.
3. Systemy informatyczne powinny korzystać z szyfrowanych protokołów wymiany danych, w szczególności połączeń sftp i https.
4. Dostęp użytkowników do sieci publicznej (Internet) powinien być ograniczony do niezbędnego minimum na danym stanowisku pracy.
5. Dostęp do przeglądania stron internetowych możliwy jest po nadaniu odpowiednich uprawnień (USER, VIP, GUEST).
6. Na stanowiskach komputerowych, na których zbiera się, przetwarza lub przechowuje dane osobowe, a które podłączone są do sieci publicznej (Internet) zabrania się korzystać ze stron internetowych, portali społecznościowych, platform zakupowych i innych serwisów, których odwiedzanie nie jest związane i potrzebne do wykonania obowiązków służbowych, a które może spowodować zagrożenie naruszenia tych danych.
7. Wprowadza się całkowite ograniczenia w dostępie do treści uznanych za pornograficzne, rasistowskie, traktujące o przemocy, przestępstwach, jak również do protokołów umożliwiających wymianę plików w sieciach z naruszeniem przepisów prawa.



8. Dostęp do protokołu wymiany plików możliwy jest w uzasadnionych przypadkach, po nadaniu odpowiednich uprawnień.
9. Dalsze ograniczenia dostępu do sieci Internet mogą być rekomendowane przez Inspektora Ochrony Danych.

## **ZASADY POSTĘPOWANIA Z NOŚNIKAMI ELEKTRONICZNYMI ORAZ VPN PODCZAS PRACY POZA OBSZAREM PRZETWARZANIA DANYCH**

### **§ 19**

Każdy użytkownik wymiennych nośników elektronicznych oraz użytkownicy zdalnych dostępów do sieci służbowej ADO (VPN) oraz użytkownicy elektronicznych kart dostępu, ponoszą całkowitą odpowiedzialność za powierzony do użytkowania sprzęt oraz są zobowiązani do stosowania się do poniższych zasad:

1. zabrania się pozostawiania bez opieki w miejscach publicznych nośników wymiennych przetwarzających informacje Administratora Danych Osobowych;
2. komputery przenośne należy przewozić jako bagaż podręczny i w miarę możliwości, je maskować;
3. zaleca się zachowanie ostrożności podczas używania urządzeń do przetwarzania mobilnego w miejscach publicznych, salach spotkań i innych niechronionych miejscach poza siedzibą organizacji;
4. w przypadkach używania urządzeń mobilnych w miejscach publicznych, zaleca się użytkownikom unikania ryzyka podglądania ze strony nieuprawnionych osób;
5. zaleca się regularne wykonywanie kopii zapasowych krytycznych informacji biznesowych;
6. zaleca się właściwy sposób ochrony kopii zapasowych, np. przed kradzieżą lub utratą informacji;
7. zaleca się, aby był dostępny sprzęt umożliwiający szybkie i łatwe wykonywanie kopii zapasowych informacji;



8. zaleca się, aby urządzenia przetwarzania mobilnego wyposażyć w fizyczne zabezpieczenia przed kradzieżą, zwłaszcza gdy są pozostawiane, np. w samochodach i innych środkach transportu, pokojach hotelowych, centrach konferencyjnych i salach spotkań;
9. użytkownik, wykonując czynności zawodowe lub umowne w domu, powinien zadbać o należyte zabezpieczenie powierzonego sprzętu oraz dostępu do informacji przed nieautoryzowanym dostępem osób trzecich;
10. zabrania się spożywania posiłków i picia podczas pracy z powierzonym sprzętem;
11. należy wprowadzić specjalną procedurę, uwzględniającą wymagania prawne, ubezpieczeniowe lub inne wymagania bezpieczeństwa, na wypadek kradzieży lub utraty urządzeń przetwarzania mobilnego;
12. sprzęt zawierający ważne, wrażliwe lub krytyczne informacje biznesowe, nie należy pozostawiać bez nadzoru i tam, gdzie jest to możliwe, zaleca się jego fizyczne zamknięcie lub odpowiednie zabezpieczenie za pomocą specjalnych zamków;
13. zaleca się zorganizowanie szkoleń dla personelu stosującego przetwarzanie mobilne, aby zwiększyć świadomość występowania dodatkowego ryzyka związanego z tym sposobem pracy oraz zabezpieczeń, które trzeba wprowadzić. Jest to najtańsza, z biznesowego punktu widzenia, forma zabezpieczenia ochrony danych osobowych;
14. zabrania się udostępniania, osobom trzecim, nośników elektronicznych informacji oraz powierzonego sprzętu będącego własnością ADO;
15. w przypadku utraty nośnika elektronicznego lub sprzętu komputerowego, należy ten fakt, bezzwłocznie, zgłosić do bezpośredniego przełożonego lub IOD lub Administratora Systemu Informatycznego. Bezpośredni przełożony lub Administrator Systemu Informatycznego bezzwłocznie zgłasza taki fakt do Inspektora Ochrony Danych, ponieważ zgubienie nośnika przetwarzającego dane może wiązać się z utratą poufności informacji chronionych przez ADO;



16. problemy wynikające z nieprawidłowego funkcjonowania sprzętu komputerowego należy zgłaszać Administratorowi Systemu Informatycznego;
17. połączenia w sieciach bezprzewodowych są podobne do połączeń w sieciach innych typów, jednak przy wyborze zabezpieczeń zaleca się uwzględnić istotne różnice. Niektóre bezprzewodowe protokoły zabezpieczeń są niedojrzałe i mają znane słabości. Kopie zapasowe informacji przechowywanych w komputerach przenośnych mogą nie być wykonywane, ponieważ pasmo sieciowe jest ograniczone lub urządzenie nie jest podłączone do sieci w momencie, w którym zaplanowano wykonanie kopii.

## **SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE**

### **§ 20**

1. Poniżej zostały opisane sposoby i czas przechowywania wszelkiego rodzaju nośników informacji (dyskietki, płyty CD, taśmy magnetyczne, dyski twarde) wykorzystywanych przez ADO.
2. Zawarte w niniejszym rozdziale procedury obejmują również:
  - a. zdefiniowanie pomieszczeń przeznaczonych do ich przechowywania;
  - b. sposoby ich zabezpieczenia przed nieuprawnionym przejęciem, odczytem, skopiowaniem lub zniszczeniem.

## **UŻYTKOWANIE SPRZĘTU KOMPUTEROWEGO, OPROGRAMOWANIA, NOŚNIKÓW DANYCH**

### **§ 21**

1. Do sprzętu komputerowego zalicza się między innymi:
  - a. komputery stacjonarne;
  - b. komputery przenośne;
  - c. tablety;



- d. smartphony;
  - e. drukarki;
  - f. modemy;
  - g. monitory;
  - h. routery;
  - i. sprzęt dostarczony razem z wyżej wymienionym sprzętem lub zakupiony oddzielnie, a w szczególności, zasilacze, torby, klawiatury, myszki komputerowe.
2. Administrator Systemu Informatycznego odpowiada za poprawne działanie sprzętu komputerowego. Czynność tą ASI może wykonywać poprzez pracowników lub współpracowników ADO, lub poprzez podmioty zewnętrzne.
  3. W przypadku wykorzystywania urządzeń mobilnych (m. in. tablet, smartphone) wymaga się zastosowania następujących środków bezpieczeństwa:
    - a. blokada ekranu (pin/hasło/symbol graficzny/odcisk palca),
    - b. szyfrowanie pamięci/karty pamięci,
    - c. program antywirusowy,
    - d. wyłączanie nieużywanych usług (wi-fi, gprs/lte, bluetooth, nfc),
    - e. instalowanie oprogramowania z zaufanego źródła (np. App Store, Google Play),
    - f. używanie szyfrowania, np.: poczty lub VPN podczas korzystania z publicznych hotspot-ów.
  4. Przekazanie sprzętu jest to czynność polegająca na dostarczeniu sprzętu komputowego wraz z odpowiednim oprogramowaniem użytkownikowi.
  5. Administrator Systemu Informatycznego odpowiedzialny jest za przygotowanie sprzętu komputerowego do prawidłowej i zgodnej z przeznaczeniem pracy.
  6. ASI jest zobowiązany do prowadzenia spisu posiadanego pod opieką sprzętu komputerowego oraz oprogramowania wraz z dostarczoną dokumentacją.



7. Administrator Systemu Informatycznego ma obowiązek przechowywać karty gwarancyjne, klucze i licencje do oprogramowania.
8. Administrator Systemu Informatycznego prowadzi rejestr wydanego sprzętu komputerowego, wraz z wyszczególnieniem użytkownika. ASI udziela pomocy użytkownikowi w obsłudze sprzętu i oprogramowania.
9. W przypadku niepoprawnego i niezgodnego z przeznaczeniem użytkowania przez użytkownika sprzętu komputerowego, Administrator Systemu Informatycznego informuje o powyższym IOD.
10. ASI ma prawo instalować wyłącznie licencjonowane oprogramowanie lub oprogramowanie, które nie wymaga opłaty licencyjnej, zgodnie z warunkami licencji.
11. Użytkownik jest zobowiązany do dbałości o sprzęt oraz oprogramowanie, a także odpowiedzialny za zabezpieczenie go przed używaniem przez osoby nieuprawnione oraz do ochrony przed kradzieżą lub zagubieniem.
12. Użytkownik nie może samodzielnie zmieniać konfiguracji przekazanego sprzętu komputerowego oraz instalować lub usuwać oprogramowania, w tym nie może używać na przekazanym sprzęcie prywatnego oprogramowania.
13. Użytkownik nie może udostępniać powierzonego mu sprzętu służbowego, w szczególności urządzeń mobilnych, osobom trzecim.

## **KORZYSTANIE Z URZĄDZEŃ KOMUNIKACJI GŁOSOWEJ I WIZYJNEJ**

### **§ 22**

1. Każdy użytkownik zobowiązany jest do przestrzegania zakazu prowadzenia rozmów, podczas których może dochodzić do wymiany informacji, danych osobowych lub informacji poufnych, jeśli rozmowy te odbywają się w miejscach publicznych, otwartych pomieszczeniach biurowych lub takich, które nie gwarantują zachowania poufności rozmów.



2. Odczytanie wiadomości z faksów, automatycznych sekretarek lub systemów poczty głosowej powinno być możliwe wyłącznie po wprowadzeniu indywidualnego hasła. W przypadku braku takiej możliwości urządzenia należy zabezpieczyć przed dostępem osób nieuprawnionych.
3. Zabronione jest wykorzystywanie domyślnych („fabrycznych”) haseł dla ww. urządzeń.

## **ZABEZPIECZENIE SYSTEMU INFORMATYCZNEGO PRZED UTRATĄ DANYCH SPOWODOWANĄ PODRÓŻĄ PRACOWNIKA ZDALNEGO**

### **§23**

W trakcie podróży zaleca się:

1. pilnowanie bagażu zawierającego sprzęt elektroniczny w pociągu oraz samolocie;
2. niepozostawianie sprzętu w samochodzie w widocznych miejscach;
3. korzystanie z automatycznej blokady zamków w trakcie użytkowania pojazdu służbowego;
4. umieszczanie sprzętu przed transportem w specjalnie dedykowanym futerale ochronnym.

## **SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO**

### **§ 24**

1. Poniżej zostały opisane sposoby zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, wraz ze zdefiniowaniem obszaru systemu informatycznego, narażonego na ingerencję wirusów komputerowych oraz wszelkiego rodzaju innego szkodliwego oprogramowania.



2. Zawarte poniżej procedury obejmują również:

- a. zdefiniowane źródła przedostania się szkodliwego oprogramowania do systemu oraz działania, jakie należy podejmować, aby minimalizować możliwość jego zainstalowania się;
- b. zastosowane narzędzia programowe, których zadaniem jest przeciwdziałanie skutkom szkodliwego oprogramowania;
- c. metody i częstotliwość aktualizacji definicji wirusów oraz osoby odpowiedzialne za zarządzanie oprogramowaniem antywirusowym;
- d. sposób postępowania użytkowników na okoliczność zidentyfikowania zagrożeń.

## OCHRONA PRZED SZKODLIWYM OPROGRAMOWANIEM

### § 25

1. Zidentyfikowanymi obszarami systemu informatycznego ADO, narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania, są dyski twarde lub karty pamięci urządzeń, pamięć RAM oraz elektroniczne nośniki informacji.
2. Drogą przedostania się wirusów lub szkodliwego oprogramowania może być sieć publiczna, wewnętrzna sieć teleinformatyczna lub elektroniczne nośniki informacji.
3. Stacje robocze, komputery przenośne oraz serwery objęte są ochroną, w czasie rzeczywistym, za pomocą oprogramowania antywirusowego oraz zapory (firewall), zapewniających integralność zasobów przechowywanych i przetwarzanych w systemie informatycznym.
4. Za prawidłowe funkcjonowanie oprogramowania antywirusowego odpowiada Administrator Systemu Informatycznego.
5. Oprogramowanie antywirusowe uruchamiane jest przy starcie systemu, a użytkownik nie posiada uprawnień do jego wyłączenia.



6. Konfiguracja programu antywirusowego zapewnia ciągłe monitorowanie otrzymywanych i wysyłanych, a także uruchamianych plików, pod kątem występowania oprogramowania złośliwego.
7. Stacje robocze i komputery przenośne, przynajmniej raz w miesiącu, skanowane są pod kątem występowania na nich złośliwego oprogramowania.
8. Serwery plikowe podlegają skanowaniu pod kątem występowania na nich złośliwego oprogramowania, przynajmniej raz w tygodniu.
9. Użytkownicy systemu mają obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.
10. W przypadku stwierdzenia pojawienia się wirusa i braku możliwości usunięcia go przez program antywirusowy, użytkownik powinien skontaktować się z Administratorem Systemu Informatycznego.
11. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, Administrator Systemu Informatycznego podejmuje działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:
  - a. usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego;
  - b. odtworzenie plików z kopii zapasowych, po uprzednim sprawdzeniu, czy dane zapisane na kopiiach zapasowych nie są zainfekowane;
  - c. samodzielną ingerencję w zawartość pliku - w zależności od posiadanych kwalifikacji, lub skonsultowanie się z odpowiednim serwisem.



## SPOSÓB REALIZACJI WYMOGÓW ODNOTOWANIA INFORMACJI O ODBIORCACH, KTÓRYM DANE OSOBOWE ZOSTAŁY UDOSTĘPNIONE

### § 26

Dla każdej osoby, której dane osobowe przetwarzane są w systemie informatycznym, system ten powinien zapewnić odnotowanie informacji o udostępnieniach danych odbiorcom, zawierające informacje komu, kiedy i w jakim zakresie dane osobowe zostały udostępnione.

## PROCEDURY WYKONYWANIA PRZEGŁĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

### § 27

1. Poniżej zostały określone cel, zakres, częstotliwość oraz procedury wykonywania przeglądów i konserwacji systemu informatycznego oraz podmioty i osoby do tego uprawnione.
2. Zawarte poniżej procedury obejmują również:
  - a. sposób nadzoru nad osobami spoza organizacji wykonującymi czynności konserwacyjne systemu;
  - b. tryb przekazywania sprzętu komputerowego do naprawy lub zniszczenia.
3. Konserwacja sprzętu komputerowego, systemów informatycznych oraz nośników informacji, należących do ADO, ma na celu zapewnienie nieprzerwanej i bezpiecznej pracy tych systemów, zapobieganie utraty, uszkodzenia lub naruszenia bezpieczeństwa.
4. Sprzęt podlega konserwacji według ustalonego planu, wynikającego z zaleceń producentów.
5. Wszelkie naprawy oraz konserwacje urządzeń komputerowych oraz zmiany w systemie informatycznym ADO przeprowadzane są - o ile to możliwe - przez upoważnionych pracowników.



6. Naprawy, konserwacje i zmiany w systemie informatycznym przeprowadzane przez serwisanta zewnętrznego prowadzone są pod nadzorem Administratora Systemu Informatycznego w siedzibie ADO (jeśli to możliwe) lub poza siedzibą ADO, po uprzednim usunięciu elementów zawierających dane osobowe, o ile nie wiąże się to z nadmiernymi utrudnieniami.
7. Wszelkie prace, o których mowa powyżej, wykonywane przez podmiot zewnętrznego, powinny odbywać się na zasadach określonych w szczegółowej umowie pomiędzy ADO, a tymże podmiotem, z uwzględnieniem klauzuli powierzenia przetwarzania danych lub klauzuli dotyczącej zachowania poufności przez wykonawcę wszelkich informacji, do których ma dostęp w czasie wykonywania usługi;
8. Podmiot zewnętrzny powinien prowadzić swoją działalność zgodnie z zaleceniami RODO.
9. W przypadku zdalnej obsługi serwisowej systemów informatycznych ADO, porty komunikacyjne powinny być włączane jedynie na wyraźne żądanie dostawcy takich usług, za zgodą Administratora Systemu Informatycznego i muszą być ponownie odłączone tuż po zakończeniu prac serwisowych.
10. Jeśli nośnik danych (dysk, płyta lub inne) zostanie uszkodzony i nie można go odczytać, ani usunąć z niego danych, należy go zniszczyć mechanicznie w niszczarce spełniającej wymagania normy DIN 66399.

## POSTANOWIENIA KOŃCOWE

### § 28

1. Dokumentacja przetwarzania danych osobowych stanowi wewnętrzną regulację ADO i obowiązuje wszystkich pracowników i współpracowników Administratora wykonujących pracę w systemach teleinformatycznych.



- 
2. Każdy, kto przetwarza dane posiadane przez ADO, zobowiązany jest do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce oraz w pozostałych, obowiązujących w firmie, dokumentach.
  3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego innego, niż stosunek pracy.
  4. W sprawach nieuregulowanych w niniejszej Polityce, zastosowanie mają zapisy zawarte w Polityce Bezpieczeństwa Informacji RPWiK Tychy S.A. oraz w pozostałych załącznikach do PBI.

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

Imię i nazwisko: Łukasz Grabowski  
Adres e-mail: odo@rpwik.tychy.pl  
Telefon stacjonarny: 48 883 942 060

**Kontakt do Administratora Systemów Informatycznych (ASI):**

Imię i nazwisko: Jerzy Trzepała  
Adres e-mail: j.trzepala@rpwik.tychy.pl  
Telefon komórkowy: 48 501 178 700

Imię i nazwisko: Dariusz Mrowiec  
Adres e-mail: d.mrowiec@rpwik.tychy.pl  
Telefon komórkowy: 48 501 379 177



Załącznik nr 8a do Polityki Bezpieczeństwa Informacji RPWiK Tychy S.A.

## RAPORT Z NARUSZENIA OCHRONY DANYCH OSOBOWYCH W ZWIĄZKU Z PRACĄ ZDALNĄ

Informuję, że:

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:  
.....

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

5. Podjęte działania:  
.....

6. Wstępna ocena przyczyn wystąpienia naruszenia:  
.....

7. Postępowanie wyjaśniające i naprawcze:  
.....

.....  
(podpis pracownika)

.....  
(data i podpis Inspektora  
Ochrony Danych)