

**POLITYKA BEZPIECZEŃSTWA  
PRZETWARZANIA DANYCH  
OSOBOWYCH**

**W**

**Oxymoron Sp. z o.o.**



## Spis treści

I. Informacje ogólne .....	4
II. Definicje .....	5
III. Dokumenty powiązane .....	6
IV. Cel i zakres Polityki .....	6
V. Obowiązki i odpowiedzialność .....	8
VI. Zarządzanie ochroną danych osobowych .....	9
VII. Szkolenia użytkowników .....	10
VIII. Upoważnienie do przetwarzania danych osobowych .....	10
IX. Ewidencja osób upoważnionych .....	11
X. Udostępnianie danych osobowych .....	11
XI. Dokonanie obowiązku informacyjnego .....	11
XII. Przetwarzanie danych osobowych. Wymagania bezpieczeństwa. ....	12
XIII. Sprawdzenie stanu systemu ochrony danych osobowych .....	13
XIV. Postępowanie w sytuacji naruszenia bezpieczeństwa danych osobowych .....	13
XV. Zgodność .....	14
XVI. Postanowienia końcowe .....	14

# I. Informacje ogólne

1. Głównym celem wprowadzenia Polityki Bezpieczeństwa jest zapewnienie zgodności działania firmy Oxymoron Sp. z o. o. jako Administratora Danych Osobowych z przepisami prawa regulującymi kwestię administrowania i przetwarzania danych osobowych. Niniejsza Polityka Bezpieczeństwa opisuje w szczególności zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem.
2. Dokument Polityki Bezpieczeństwa został opracowany w oparciu o wytyczne zawarte w następujących aktach prawnych:
  - Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922);
  - Rozporządzeniu 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 [rozporządzenie ogólne o ochronie danych];
  - Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (U. 2004 nr 100 poz. 1024),
3. Obszarem przetwarzania danych osobowych przez Oxymoron Sp. z o.o. jest każdorazowy adres siedziby firmy.
4. Ochrona danych osobowych realizowana jest poprzez stosowanie zabezpieczeń w postaci środków organizacyjnych, środków ochrony fizycznej oraz środków technicznych systemu informatycznego w ramach procedur zawartych w instrukcji zarządzania systemem informatycznym.
5. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w Oxymoron Sp. z o.o. rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.
6. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów:
  - 1) Poufność danych – zapewnienie, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,
  - 2) Integralność danych – zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
  - 3) Dostępność danych – zapewnienie osiągalności danych i możliwości ich wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot,
  - 4) Rozliczalność danych – zapewnienie, że działania podmiotu mogą być przy pisane w sposób jednoznaczny tylko temu podmiotowi,
  - 5) Autentyczność danych – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana,
  - 6) Integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiegokolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;

- 7) Zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.
7. Administrator Danych Osobowych gromadzi przetwarza dane osobowe w następujących celach:
- 1) Wykonywanie obowiązków pracodawcy w zakresie zatrudnienia pracowników (dokumentacja i przebieg zatrudnienia oraz płace pracowników);
  - 2) Przetwarzanie danych kontrahenta dla którego realizowane są usługi w zakresie działań promocyjnych i marketingowych
  - 3) Pozyskiwanie danych od podwykonawców celem realizacji usług marketingowych dla kontrahentów.

## **II. Definicje**

1. Przez użyte w Polityce Bezpieczeństwa określenia należy rozumieć:
  - 1) Polityka Bezpieczeństwa – rozumie się przez to Politykę Bezpieczeństwa Ochrony Danych Osobowych w firmie Oxymoron Sp. z o.o.
  - 2) Administrator Danych Osobowych – Administratorem Danych Osobowych w rozumieniu niniejszej Polityki Bezpieczeństwa jest firma Oxymoron Sp. z o.o., która reprezentowana jest przez trzech członków zarządu.
  - 3) Administrator Bezpieczeństwa Informacji – osoba, która dba o należyte zabezpieczenie danych osobowych oraz o kompleksowe zapewnianie u danego administratora danych przestrzegania przepisów o ochronie danych osobowych. Administratora Bezpieczeństwa Informacji powołuje Administrator Danych Osobowych;
  - 4) Biuro – firmy Oxymoron Sp. z o.o.;
  - 5) Ustawa – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922);
  - 6) Rozporządzenie – rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024) z późniejszymi zmianami;
  - 7) RODO - Rozporządzeniu 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 [rozporządzenie ogólne o ochronie danych]
  - 8) Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

- 9) Zbiór danych osobowych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
- 10) Baza danych osobowych – zbiór uporządkowanych powiązanych ze sobą tematycznie zapisanych np. w pamięci wewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze – rekordów lub obiektów, w których są zapisywane dane osobowe;
- 11) Usuwanie danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dotyczą.
- 12) Przetwarzanie danych - rozumie się przez to jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
- 13) System informatyczny - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
- 14) Bezpieczeństwo systemu informatycznego – wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed nieuprawnionym przetwarzaniem danych;
- 15) Administrator Systemu Informatycznego – osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych (może to być administrator sieci lokalnej, systemu operacyjnego, bazy danych itp.).
- 16) Użytkownik - rozumie się przez to osobę wyznaczoną i upoważnioną przez Administratora danych do przetwarzania danych osobowych, przeszkoloną w zakresie ochrony tych danych.
- 17) Stacja robocza – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.

### **III. Dokumenty powiązane**

Dokumentem powiązany z Polityką bezpieczeństwa przetwarzania danych osobowych w firmie Oxymoron Sp. z o.o. jest, zgodnie z wymogami § 3 ust. 1 Rozporządzenia, Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w firmie Oxymoron Sp. z o.o.

### **IV. Cel i zakres Polityki**

1. Ustawa o ochronie danych osobowych nakłada na Administratora Danych obowiązek stosowania odpowiednich środków technicznych i organizacyjnych zapewniających

ochronę przetwarzanych danych osobowych oraz zabezpieczenie ich między innymi przed udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem ustawy, a także zmianą, utratą, uszkodzeniem lub zniszczeniem. Celem niniejszej Polityki Bezpieczeństwa przetwarzania danych osobowych jest opracowanie optymalnych i zgodnych z wymogami prawa zasad przetwarzania danych, których zbieranie i przetwarzanie jest niezbędne dla funkcjonowania firmy Oxymoron Sp. z o.o. zgodnie z obowiązującymi przepisami prawa w zakresie przetwarzania danych osobowych.

-----

2. W firmie Oxymoron Sp. z o.o. przetwarzane są przede wszystkim dane osobowe osób zatrudnionych w firmie, osób współpracujących z firmą na podstawie umów cywilnoprawnych, samozatrudnienia, kontrahentów oraz potencjalnych klientów.
3. Dane osobowe we wskazanych powyżej zbiorach danych są przetwarzane i składowane zarówno w postaci dokumentacji tradycyjnej jak i elektronicznej.
4. Politykę Bezpieczeństwa stosuje się przede wszystkim do:
  - 1) Wszystkich informacji dotyczących danych firmy Oxymoron Sp. z o.o. oraz osób współpracujących z Oxymoron Sp. z o.o na podstawie umów cywilnoprawnych, w tym danych osobowych i treści zawieranych umów.
  - 2) Wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji.
  - 3) Informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych.
  - 4) Rejestru osób dopuszczonych do przetwarzania danych osobowych.
  - 5) Innych dokumentów zawierających dane osobowe.
5. Zakres ochrony danych osobowych określony w Polityce Bezpieczeństwa ma zastosowanie do systemów informatycznych firmy Oxymoron Sp. z o.o., w których są przetwarzane dane osobowe, a w szczególności do:
  - 1) Wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie.
  - 2) Wszystkich lokalizacji - pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.

- 3) Wszystkich osób świadczących pracę bądź usługi cywilnoprawne na rzecz Administratora Danych Osobowych, które uzyskały upoważnienie do przetwarzania danych osobowych.
6. Do stosowania zasad określonych w Polityce Bezpieczeństwa zobowiązani są wszyscy Użytkownicy danych, w tym w szczególności pracownicy Biura, zleceniobiorcy, stażyści oraz wszelkie inne osoby mające dostęp do informacji podlegających ochronie, w tym zwłaszcza członkowie zarządu firmy Oxymoron Sp. z o.o

## **V. Obowiązki i odpowiedzialność**

1. Do najważniejszych obowiązków Administratora Danych realizowanych przez Administratora Bezpieczeństwa Informacji należy:
  - 1) Organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych oraz innych przepisów regulujących zasady bezpieczeństwa i ochrony danych osobowych;
  - 2) Zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki Bezpieczeństwa;
  - 3) Wydawanie i anulowanie upoważnień do przetwarzania danych osobowych;
  - 4) Przeprowadzanie szkoleń użytkowników przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe;
  - 5) Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
  - 6) Prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych;
  - 7) Nadzór nad bezpieczeństwem danych osobowych;
  - 8) Kontrola działań pracowników pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
  - 9) Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych;
  - 10) Bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych;
  - 10) Optymalizację wydajności systemu informatycznego, baz danych, instalacje i konfiguracje sprzętu sieciowego i serwerowego;
  - 11) Instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego;
  - 12) Konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem;
  - 13) Współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych;



- 14) Zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego;
  - 15) Przeciwdziałanie próbom naruszenia bezpieczeństwa informacji;
  - 16) Zmiana lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń;
  - 17) Zarządzanie licencjami oraz procedurami ich dotyczącymi;
  - 18) Prowadzenie profilaktyki antywirusowej.
2. Do najważniejszych obowiązków osób upoważnionych do przetwarzania danych osobowych należy:
- 1) Znajomość, zrozumienie i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony danych osobowych oraz uniemożliwienie osobom nieuprawnionym dostępu do swojej stacji roboczej;
  - 2) Przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami;
  - 3) Postępowania zgodnie z ustalonymi regulacjami wewnętrznymi dotyczącymi przetwarzania danych osobowych;
  - 4) Zachowania w tajemnicy danych osobowych, do których uzyskały dostęp oraz informacji o sposobach ich zabezpieczenia;
  - 5) Ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;
  - 6) Informowania Administratora Danych Osobowych o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe;
  - 7) Zapoznanie się z Polityką Bezpieczeństwa przetwarzania danych osobowych oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

## **VI. Zarządzanie ochroną danych osobowych**

1. Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z upoważnieniem oraz rolą sprawowaną w procesie przetwarzania danych.
2. Dostęp do danych osobowych powinien być przyznawany zgodnie z zasadą wiedzy koniecznej.
3. Każda z osób mająca styczność z danymi osobowymi jest zobowiązana do ochrony danych osobowych oraz przetwarzania ich w granicach udzielonego jej upoważnienia.
4. Należy zapewnić poufność, integralność i rozliczalność przetwarzanych danych osobowych.

5. Należy stosować adekwatny do zmieniających się warunków i technologii poziom bezpieczeństwa przetwarzania danych osobowych.
6. Dane osobowe powinny być chronione przed nieuprawnionym dostępem i modyfikacją.
7. Dane osobowe należy przetwarzać wyłącznie za pomocą autoryzowanych urządzeń służbowych.
8. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane na mocy art. 37 Ustawy. Upoważnienia wydawane są indywidualnie przez Administratora Danych Osobowych.

## **VII. Szkolenia użytkowników**

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Za przeprowadzenie szkolenia odpowiada Administrator Danych Osobowych.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz Polityką Bezpieczeństwa danych i Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych obowiązującymi u Administratora Danych. Po zaznajomieniu się z powyższymi regulacjami, użytkownik, przed dopuszczeniem do przetwarzania danych, powinien zobowiązać się do ich przestrzegania przez podpisanie oświadczenia użytkownika.

## **VIII. Upoważnienie do przetwarzania danych osobowych**

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane na mocy art. 37 Ustawy.
2. Upoważnienia są wydawane indywidualnie przed rozpoczęciem przetwarzania danych osobowych przez Administratora Danych Osobowych.
3. W celu otrzymania przez Użytkownika upoważnienia do przetwarzania danych osobowych, należy dostarczyć do Administratora Danych podpisane oświadczenie użytkownika.
4. Na podstawie otrzymanego oświadczenia Administrator Danych Osobowych upoważnia Użytkownika do przetwarzania danych osobowych i wydaje upoważnienie do przetwarzania danych osobowych. Upoważnienia, o których mowa powyżej przechowywane są w Biurze.

5. Upoważnienie może być w każdym czasie odwołane przez Administratora Danych Osobowych. Oświadczenie o odwołaniu upoważnienia do przetwarzania danych osobowych powinno być sporządzone na piśmie. Upoważnienie do przetwarzania danych osobowych wygasa z chwilą ustania przesłanki będącej podstawą wydania upoważnienia, w tym w szczególności wygaśnięcia stosunku pracy lub umowy cywilnoprawnej łączącej Użytkownika z Administratorem Danych Osobowych.

## **IX. Ewidencja osób upoważnionych**

Ewidencja osób upoważnionych do przetwarzania danych osobowych w firmie Oxymoron Sp. z o.o. jest prowadzona przez Administratora Danych zgodnie ze wzorem formularza stanowiącym załącznik nr 1 do Polityki Bezpieczeństwa przetwarzania danych osobowych w firmie.

## **X. Udostępnianie danych osobowych**

1. Dane osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz osobom, których dotyczą.
2. Udostępnianie danych osobowych może nastąpić wyłącznie za zgodą Administratora Danych Osobowych.
3. Informacje zawierające dane osobowe powinny być przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru listem poleconym za pokwitowaniem odbioru lub innym bezpiecznym sposobem, określonym wymogiem prawnym lub umową.
4. Udostępniając dane osobowe, należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

## **XI. Dokonanie obowiązku informacyjnego**

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, w wypadkach przewidzianych Ustawą należy poinformować tę osobę o:
  - 1) Pełnej nazwie Firmy;
  - 2) Celu zbierania danych, a w szczególności o znanych w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych;
  - 3) Prawie dostępu do swoich danych oraz ich poprawiania;
  - 4) Dobrowolności lub obowiązku podania danych - jeżeli taki obowiązek istnieje, o jego podstawie prawnej;

## **XII. Przetwarzanie danych osobowych. Wymagania bezpieczeństwa.**

1. Dane osobowe w firmie Oxymoron Sp. z o.o. przetwarzane są przy zastosowaniu zabezpieczeń zapewniających ich ochronę w postaci środków organizacyjnych, technicznych i środków ochrony fizycznej.
2. Dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych stosuje się następujące środki:
  - A. Środki organizacyjne:
    - wdrożenie Polityki bezpieczeństwa przetwarzania danych osobowych oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w firmie;
    - ustalona, indywidualna procedura udzielania upoważnień przez Administratora Danych poprzedzonego szkoleniem z zakresu przepisów i zasad ochrony danych osobowych;
    - prowadzenie ewidencji osób uprawnionych do przetwarzania danych osobowych,
    - procedura postępowania w sytuacji naruszenia ochrony danych osobowych; konieczność składania deklaracji poufności przez Użytkowników danych; procedury przechowywania zbiorów danych;
  - B. Środki techniczne:
    - Zbiory danych osobowych przetwarzane są wyłącznie na autoryzowanym sprzęcie służbowym;
    - Stacje robocze wyposażone są w indywidualną ochronę antywirusową;
    - Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
  - C. Środki ochrony fizycznej:
    - Pomieszczenia, w których znajdują się zbiory danych osobowych, są zamykane na klucz, a dostęp do nich odbywa się wyłącznie w obecności pracowników Biura firmy;
    - Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system przeciwwłamaniowy;
    - Drzwi zwykle (niewzmocnione, nie przeciwpożarowe) do pomieszczeń, w których przetwarzane są dane osobowe znajdują się wewnątrz budynku w strefie ograniczonego dostępu;
    - Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej niemetalowej szafie;
    - Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej niemetalowej szafie;

- Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek.

### **XIII. Sprawdzenie stanu systemu ochrony danych osobowych**

2. Okresowy przegląd Polityki Bezpieczeństwa powinien mieć na celu stwierdzenie, czy postanowienia Polityki odpowiadają aktualnej i planowanej działalności firmy oraz stanowi prawnemu aktualnemu w momencie dokonywania przeglądu.

### **XIV. Postępowanie w sytuacji naruszenia bezpieczeństwa danych osobowych**

1. Każdy użytkownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest o tym poinformować Administratora Danych.
2. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
  - 1) Niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
  - 2) Niewłaściwe zabezpieczenie sprzętu, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
  - 3) Nieprzestrzeganie zasad ochrony danych osobowych przez pracowników.
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
  - 1) Zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
  - 2) Zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twarde dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/ zagubienie danych);
  - 3) Umysłne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
4. W przypadku stwierdzenia wystąpienia zagrożenia, Administrator Danych prowadzi postępowanie wyjaśniające w toku, którego:
  - 1) Ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki;
  - 2) Inicjuje ewentualne działania dyscyplinarne;

- 3) Rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości;
- 4) Dokumentuje prowadzone postępowania.
5. W przypadku stwierdzenia incydentu (naruszenia), Administrator Danych prowadzi postępowanie wyjaśniające, w toku którego:
  - 1) Ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały;
  - 2) Zabezpiecza ewentualne dowody;
  - 3) Ustala osoby odpowiedzialne za naruszenie;
  - 4) Podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody);
  - 5) Inicjuje działania dyscyplinarne;
  - 6) Wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości;
  - 7) Dokumentuje prowadzone postępowania zgodnie ze wzorem Raportu z naruszenia bezpieczeństwa danych osobowych

## **XV. Zgodność**

Niniejsza Polityka powinna być aktualizowana wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w ramach firmy Oxymoron Sp. z o.o., które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.

## **XVI. Postanowienia końcowe**

1. Administrator Danych ma obowiązek zapoznać z treścią Polityki każdego użytkownika.
2. Wszystkie regulacje dotyczące systemów informatycznych, określone w Polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiegokolwiek innej formie.
3. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce.
4. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.

5. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
6. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy oraz rozporządzenia.