POLITYKA BEZPIECZEŃSTWA INFORMACJI ZE SZCZEGÓLNYM UWZGLĘDNIENIEM OCHRONY DANYCH OSOBOWYCH

Galeria Quadrilion

Carmen Tarcha

NIP 5212858888

(nazwa administratora – firmy)

Z A T W I E R D Z A M

Warszawa, dnia 25 maja 2018 roku

(data i podpis Administratora danych)

Spis treści

I. POSTANOWIENIA OGÓLNE

§1

DEKLARACJA I ZASTOSOWANIE

1. Administrator danych ma świadomość znaczenia przetwarzanych informacji dla realizacji celów firmy i potrzeby ochrony informacji, ze szczególnym uwzględnieniem ochrony danych osobowych, poprzez budowę systemu zarządzania bezpieczeństwem informacji.
2. Zasady, działania, kompetencje i zakresy odpowiedzialności opisane w niniejszej Polityce Bezpieczeństwa Informacji (zwanej dalej „Polityką"), obowiązują wszystkich pracowników i współpracowników firmy.
3. Procedury i dokumenty związane z Polityką będą weryfikowane i dostosowywane w celu zapewnienia odpowiedniego poziomu bezpieczeństwa. Przeglądy dokumentacji odbywają się nie rzadziej niż raz w roku.
4. Polityka określa środki techniczne i organizacyjne zastosowane przez Administratora Danych dla zapewnienia ochrony danych oraz tryb postępowania w przypadku stwierdzenia naruszenia zabezpieczenia danych w systemie informatycznym lub w kartotekach albo w sytuacji podejrzenia o takim naruszeniu.
5. Polityka została opracowana z uwzględnieniem metod i środków ochrony danych, których skuteczność w czasie ich zastosowania jest powszechnie uznawana. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania charakteru poufnego wraz z zachowaniem ich integralności i rozliczalności, ze szczególnym uwzględnieniem obowiązujących przepisów prawa dotyczących ochrony danych osobowych.
6. Zakres obowiązywania dokumentu.
    1) Niniejsza Polityka obowiązuje wszystkich pracowników, współpracowników, a także partnerów handlowych firmy.
    2) Każdy z pracowników ma obowiązek zapoznania się z treścią Polityki.
    3) Polityka bezpieczeństwa dotyczy wyposażenia, systemów, urządzeń przetwarzających informacje w formie elektronicznej, papierowej lub jakiejkolwiek innej.
    4) Nieprzestrzeganie postanowień zawartych w dokumentacji bezpieczeństwa informacji może skutkować sankcjami w pełnym zakresie dopuszczonym przez stosunek pracy pomiędzy Administratorem Danych a pracownikiem oraz obowiązujące przepisy prawa.
    5) W celu skutecznego zapoznania pracowników i współpracowników z zasadami zawartymi w niniejszej Polityce wprowadza się zestaw reguł stanowiący wyciąg najistotniejszych zapisów zawartych w Polityce Bezpieczeństwa Informacji oraz Instrukcji zarządzania systemami informatycznymi. Zasady użytkowania zasobów komputerowych i sieci komunikacyjnych opisane są w Załączniku nr 2 do Instrukcji zarządzania systemami informatycznymi.

§ 2

DEFINICJE

Ilekroć w Polityce jest mowa o:

1) Administratorze danych (ADO) - rozumie się przez to Carmen Tarcha, prowadzącą działalność gospodarczą pod firmą Galeria Quadrilion Carmen Tarcha, której nadano numer NIP 521 285 88 88. Dane teleadresowe: ul. Mokotowska 59, 00-542 Warszawa, info@quadrilion, +48 22 522 78 78.

   Administrator danych nadzoruje przestrzeganie zasad ochrony przetwarzanych danych osobowych i innych informacji prawem chronionych. Nadzoruje on stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem, lub zniszczeniem, a także przeprowadzi kontrole w zakresie określonym regulacjami wewnętrznymi.

   Zakres obowiązków ADO opisuje **załącznik nr 1** do niniejszej Polityki.

2) Administratorze Systemu Informatycznego – rozumie się przez to osobę nadzorującą prawidłowe funkcjonowanie sprzętu, oprogramowania i jego konserwację, odpowiadającą za koordynowanie techniczno-organizacyjnej obsługi systemów teleinformatycznych, zwanego dalej „Informatykiem" lub „ASI".

   Zadania Administratora Systemu Informatycznego opisuje **załącznik nr 2** do niniejszej Polityki.

3) Aktywach – wszystko, co ma wartość dla organizacji (wartość materialna: np. pracownicy. Komputery, bazy danych itp.; wartość niematerialna: dobre imię, rozpoznawalność i wizerunek organizacji itp.);

4) Zbiorze danych – 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,

5) Kartotece – rozumie się przez to zewidencjonowany, usystematyzowany zbiór wykazów, skoroszytów, wydruków komputerowych i innej dokumentacji gromadzonej w formie papierowej, zawierającej dane osobowe,

6) Przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

7) Systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

8) Bezpieczeństwie danych - zachowanie poufności, integralności i dostępności informacji;
   dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność,

9) Usuwanie danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

10) Użytkowniku – rozumie się przez to osobę upoważnioną przez Administratora danych do przetwarzania informacji i danych osobowych.

11) Komórce organizacyjnej – rozumie się przez to każdą wydzieloną organizacyjnie i funkcjonalnie komórkę wewnętrzną, zgodnie z podziałem organizacyjnym przeprowadzonym przez Administratora danych.

12) Pomieszczeniach – rozumie się przez to budynki i pomieszczenia określone przez Administratora danych, tworzące obszar, w którym przetwarzane są dane osobowe i inne informacje prawem chronione.

    Obszar przetwarzania danych opisany jest w **załączniku nr 3** do niniejszej Polityki.

13) Planie kontroli, audycie wewnętrznym – przedmiot, zakres oraz termin przeprowadzenia sprawdzenia zgodności przetwarzania danych z przepisami z zakresu ochrony danych osobowych.

    Wzór Planu kontroli przedstawia **załącznik nr 8** do niniejszej Polityki.

14) Incydencie – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.

    Raport z naruszenia ochrony danych stanowi **załącznik nr 9**, a rejestr naruszeń stanowi **załącznik nr 10** do niniejszej Polityki.

15) Teczce ODO – zbiór dokumentów, instrukcji, regulaminów, załączników opisujących sposób przetwarzania i ochrony danych, składający się na Politykę Bezpieczeństwa Informacji, gromadzonych i nadzorowanych przez Administratora danych osobowych.

§ 3

ZASADY OCHRONY DANYCH

System zarządzania bezpieczeństwem informacji zgodny z wymaganiami niniejszej polityki opiera się na następujących niezaprzeczalnych zasadach ochrony informacji:

1) **Zasada znajomości wymagań Polityki Bezpieczeństwa Informacji**. Każdy pracownik powinien zostać zapoznany z regułami oraz z kompletnymi i aktualnymi procedurami ochrony informacji i podpisać stosowne oświadczenie o zapoznaniu się z zasadami obowiązującej polityki.
2) **Zasada uprawnionego dostępu.** Każdy pracownik stosuje się do obowiązujących zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji.
3) **Zasada przywilejów koniecznych**. Każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań.
4) **Zasada wiedzy koniecznej**. Każdy pracownik posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań.
5) **Zasada usług koniecznych**. Systemy informacyjne świadczą tylko te usługi, które są konieczne do realizacji zadań biznesowych i operacyjnych.
6) **Zasada asekuracji**. Każdy mechanizm zabezpieczający musi być ubezpieczony drugim, (podobnym). Jako mechanizmy zabezpieczeń dopuszczalne jest stosowanie zarówno zabezpieczeń technicznych, jak i organizacyjnych.
7) **Zasada świadomości zbiorowej**. Wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych i aktywnie uczestniczą w tym procesie.
8) **Zasada indywidualnej odpowiedzialności**. Za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby.
9) **Zasada obecności koniecznej**. Prawo przebywania w określonych miejscach mają tylko osoby do tego upoważnione.
10) **Zasada stałej gotowości**. System jest przygotowany na wszelkie zagrożenia. Niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających.
11) **Zasada najsłabszego ogniwa**. Poziom bezpieczeństwa wyznacza najsłabszy (najmniej zabezpieczony) element. Elementy takie są wyznaczane na podstawie analizy ryzyka.

12) **Zasada kompletności**. Skuteczne zabezpieczenie jest tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania informacji.

13) **Zasada ewolucji**. Każdy system musi ciągle dostosowywać mechanizmy wewnętrzne do zmieniających się warunków zewnętrznych.

14) **Zasada odpowiedniości**. Używane mechanizmy muszą być adekwatne do sytuacji.

15) **Zasada świadomej konwersacji**. Nie zawsze i wszędzie trzeba mówić, co się wie, ale zawsze i wszędzie trzeba wiedzieć, co, gdzie i do kogo się mówi.

§ 4

1. W celu zwiększenia efektywności ochrony informacji dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Ochrona informacji jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu poniższych celów i zapewnić:
   1) **rozliczalność** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
   2) **integralność** – rozumie się przez to właściwość zapewniającą, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   3) **poufność** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
   4) **integralność** systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
   5) **dostępność** – gwarantuje, że osoby, które są upoważnione i którym informacje są potrzebne, mają do nich dostęp w odpowiednim miejscu i czasie;
   6) **uwierzytelnienie** - uwiarygodnienie swojej tożsamości względem systemu teleinformatycznego;
   7) **autentyczność** - właściwość zapewniająca, że tożsamość podmiotu lub procesu jest taka, jak deklarowana.
3. Cele i strategie bezpieczeństwa:
   1) zgodność z prawem;
   2) ochrona zasobów informacyjnych i innych aktywów;
   3) uzyskanie i utrzymanie odpowiednio wysokiego poziomu bezpieczeństwa zasobów, rozumiane jako zapewnienie poufności, integralności i dostępności zasobów oraz zapewnienie rozliczalności podejmowanych działań;
   4) zapewnienie ciągłości działania procesów i właściwej reakcji na incydenty;
   5) zapewnienie odpowiedniego poziomu wiedzy dotyczącej bezpieczeństwa informacji wśród pracowników i współpracowników poprzez zapewnienie odpowiednich szkoleń.

§ 5

ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO INFORMACJI

1. Za bezpieczeństwo informacji odpowiedzialni są wszyscy pracownicy i współpracownicy upoważnieni do przetwarzania danych osobowych. W szczególności odpowiadają oni za przestrzeganie zasad bezpieczeństwa wynikających z niniejszej Polityki oraz zgłaszanie incydentów i wykonywanie zaleceń Administratora danych osobowych.

2. We wszystkich umowach, które mogą dotyczyć przetwarzania danych w jednostce, należy uwzględnić zapisy zobowiązujące drugą stronę do przestrzegania odpowiednich zapisów Polityki Bezpieczeństwa Informacji.

Administrator danych osobowych prowadzi wykaz podmiotów zewnętrznych, z którymi realizacja umów/porozumień/zamówień lub aneksów do nich zobowiązuje lub umożliwia zleceniobiorcy/wykonawcy dostęp do informacji zawierających dane osobowe. Wykaz podmiotów zewnętrznych stanowi **załącznik nr 7** do niniejszej Polityki.

3. Za nadzór nad przestrzeganiem postanowień niniejszej Polityki odpowiada Administrator danych osobowych.

§ 6

Realizację zamierzeń określonych w § 3 powinny zagwarantować następujące założenia:

1) Wdrożenie procedur określających postępowanie osób dopuszczonych do przetwarzania informacji oraz ich odpowiedzialność za ochronę danych.
2) Przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony informacji.
3) Przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory).
4) Podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń.
5) Okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych.
6) Opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii.
7) Okresowe aktualizowanie Polityki Bezpieczeństwa Informacji.
8) Identyfikacja zagrożeń i analiza ryzyka.

OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH

§ 7

Podział zagrożeń:

1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych;
2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych;
3) zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

§ 8

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są informacje, to głównie:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy,
3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych,
7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony informacji - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu itp.,
11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. bocznej furtki itp.,
12) podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane,
13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych itp.).

§ 9

Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.

PRZEDSIĘWZIĘCIA ZABEZPIECZAJĄCE PRZED NARUSZENIEM OCHRONY DANYCH

§ 10

1. Każdy użytkownik – przed dopuszczeniem do przetwarzania informacji podlega przeszkoleniu z przepisów w zakresie ochrony informacji oraz wynikających z nich zadań i obowiązków.
2. Wszyscy użytkownicy podlegają okresowym szkoleniom.
3. Za organizację szkoleń odpowiedzialny jest Administrator danych osobowych.

§ 11

1. Do zapewnienia bezpieczeństwa danych i informacji zastosowano następujące środki organizacyjne:

1) Dostęp do danych osobowych mogą mieć tylko i wyłącznie pracownicy posiadający pisemne, imienne upoważnienia nadane przez Administratora danych.
2) Każdy z pracowników powinien zachować szczególną ostrożność przy przenoszeniu wszelkich nośników z danymi.
3) Należy chronić dane przed wszelkim dostępem do nich osób nieupoważnionych.
4) Pomieszczenia, w których są przetwarzane dane osobowe, powinny być zamykane na klucz.
5) Dostęp do kluczy posiadają tylko upoważnieni pracownicy.
6) Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy. W wypadku gdy jest wymagany poza godzinami pracy – możliwy jest tylko na podstawie zezwolenia Administratora danych lub Administratora bezpieczeństwa informacji.
7) Dostęp do pomieszczeń, w których są przetwarzane dane osobowe, mogą mieć tylko upoważnieni pracownicy.
8) W przypadku pomieszczeń, do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności.
9) Szafy, w których przechowywane są dane, powinny być zamykane na klucz.
10) Klucze do tych szaf posiadają tylko upoważnieni pracownicy.
11) Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych, a następnie powinny być zamykane.
12) Dane w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych, a następnie muszą być chowane do szaf.

2. Do zapewnienia bezpieczeństwa danych i informacji zastosowano następujące środki techniczne:
   1) Dostęp do komputerów, na których są przetwarzane dane, mają tylko upoważnieni pracownicy.
   2) Monitory komputerów, na których przetwarzane są dane, są tak ustawione, aby osoby nieupoważnione nie miały wglądu w dane.
   3) Po zakończeniu pracy komputery przenośne (np. typu notebook) zawierające dane osobowe powinny być zabezpieczone w zamykanych na klucz szafach.
   4) W wypadku potrzeby wyniesienia komputera przenośnego (np. typu notebook) zawierającego dane osobowe lub inne informacje chronione, komputer taki musi być odpowiednio dodatkowo zabezpieczony, a dane zaszyfrowane.
   5) Nie należy udostępniać osobom nieupoważnionym tych komputerów.
   6) W przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności.
   7) Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie), aby nie zostały na nich dane osobowe.
   8) W wypadku niemożliwości skasowania danych z nośnika (płyta CD-ROM) należy taką płytę zniszczyć fizycznie.
   9) W przypadku wykorzystania do przenoszenia dysków dane należy kasować z tych dysków.
   10) Niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną.
   11) Sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz.

12) Błędne lub nieaktualne wydruki i wersje papierowe zawierające dane osobowe lub inne informacje chronione niszczone są za pomocą niszczarki lub w inny mechaniczny sposób uniemożliwiający powtórne ich odtworzenie.

DOSTĘP DO INFORMACJI i DANYCH OSOBOWYCH

§ 12

1. Przetwarzanie, w tym udostępnianie danych osobowych, jest prawnie dopuszczalne, jeżeli jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.
2. W przypadku udostępnienia informacji w celach innych niż włączenie do zbioru Administrator danych udostępnia posiadane informacje osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
3. Dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
4. Podmiot występujący o udostępnienie informacji powinien wskazać podstawę prawną upoważniającą go do otrzymania tych danych albo uzasadnioną potrzebę żądania ich udostępnienia. Tylko w takiej sytuacji można dokonać oceny, czy w określonym przypadku udostępnienie danych jest prawnie dopuszczalne i czy nie będzie ono stanowić naruszenia zasad ochrony informacji.
5. Przetwarzanie, w tym udostępnianie informacji w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje w celu badań naukowych, dydaktycznych, historycznych oraz statystycznych, z zachowaniem praw i wolności osób, których dane dotyczą i po zanonimizowaniu danych osobowych.
6. Udostępnienie informacji może nastąpić jedynie za zgodą Administratora danych i powinno być odpowiednio udokumentowane.

§ 13

Porozumienia i kontakty ze stronami zewnętrznymi

1. W przypadku zawierania umów z firmami zewnętrznymi mającymi wpływ na funkcjonowanie kluczowych elementów systemu zarządzania bezpieczeństwem informacji zalecane jest zawarcie umowy powierzenia i określenie w niej następujących wymagań bezpieczeństwa:
   1) Zakres i cel czynności oraz danych mających być przedmiotem współpracy z firmą zewnętrzną.
   2) Zakresy odpowiedzialności w przypadku utraty lub ujawnienia danych.
   3) Własność informacji i oprogramowania oraz obowiązki w zakresie ochrony danych osobowych.
   4) Specjalne zabezpieczenia, które mogą być wymagane do ochrony informacji szczególnie chronionych, takich jak dane finansowe czy też identyfikatory i hasła dostępu.
   5) Warunki dostępu do informacji, zobowiązanie do zachowania w tajemnicy czynnika uwierzytelniającego.
   6) Definicji informacji, które mają być chronione (np. informacji poufnych).
   7) Spodziewanego czasu trwania umowy, łącznie z przypadkami, w których obowiązek zachowania poufności może być bezterminowy.
   8) Wymaganych działań w momencie zakończenia umowy.
   9) Zasad zwrotu lub niszczenia informacji przy zakończeniu umowy.
   10) Działań podejmowanych w przypadku naruszenia warunków umowy.

11) Ustaleń dotyczących licencji, własności kodu i prawa do własności intelektualnej.

12) Zasad testowania przed instalacją w celu wykrycia kodu złośliwego i koni trojańskich.

2. Administrator danych osobowych prowadzi wykaz podmiotów zewnętrznych. Wykaz stanowi **załącznik nr 7** do niniejszej Polityki

PRAWO TAJEMNICY PRZEDSIĘBIORSTWA

§ 14

Informacje stanowiące tajemnicę przedsiębiorstwa

1. Przez tajemnicę przedsiębiorstwa rozumie się nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności.
2. Informacje objęte prawem tajemnicy przedsiębiorstwa:
   1) Sprzedaż:
      a) Lista klientów
      b) Informacje o klientach
      c) Ceny transakcyjne, poufne cenniki
      d) Terminy obowiązywania lub odnawiania umów
      e) Fakt prowadzenia negocjacji i ich przebieg
   2) Marketing:
      a) Informacje uzyskane podczas badania klientów
      b) Plany kampanii marketingowych
   3) Dostawcy, podwykonawcy, pracownicy:
      a) Informacje o dostawcach i stosowanych cenach;
      b) Informacja stosowanych zakazach konkurencji;
      c) Informacje o wynagrodzeniach pracowników.
   4) Badania i rozwój:
      a) Plany rozwoju, kierunki rozwoju;
      b) Wyniki badań;
      c) Pozytywne *know-how* w zakresie badań i rozwoju;
      d) Negatywne *know-how*, czyli informacje o niepowodzeniach.
   5) Informacje finansowe:
      a) Wewnętrzne dokumenty finansowe;
      b) Budżety, prognozy, raporty;
      c) Nieujawniane rachunki zysków i strat;
      d) Obowiązkowe sprawozdania finansowe przed ujawnieniem.
   6) Wewnętrzne informacje o firmie:
      a) Sposób organizacji pracy

b) Biznesplany
c) Oprogramowanie stosowane przez firmę
d) Dokumenty wydawane przez firmę
e) Dokumentacja techniczna i dokumenty pochodzenia zewnętrznego.

3. Wszyscy pracownicy, współpracownicy, partnerzy Administratora danych są zobowiązani do zachowania w tajemnicy wszelkich informacji stanowiących tajemnicę przedsiębiorstwa.

4. Za umyślne bądź nieumyślne ujawnienie informacji objętych prawem tajemnicy przedsiębiorstwa grozi odpowiedzialność dyscyplinarna, odszkodowawcza, karna, nałożona zgodnie z obowiązującymi przepisami prawa w tym zakresie.

5. Wzory umów o zachowaniu poufności przechowuje Administratora danych osobowych w Teczce ODO.

POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH

§ 15

Działania korygujące i zapobiegawcze

1. Działania korygujące podejmowane są w przypadku wykrycia niezgodności w działalności bądź nieprawidłowego działania procesu.
   Przesłanką do podjęcia działań korygujących mogą być wyniki audytów, zgłoszenia niezgodności, zdarzenia i incydenty związane z bezpieczeństwem informacji, zapisy, wyniki badania zadowolenia klientów, analiza reklamacji klientów.
   Działania zapobiegawcze mają na celu zapobiec wystąpieniu potencjalnych niezgodności.
   Podejmowanie działań korygujących oraz zapobiegawczych powinno być dokumentowane w odpowiednich rejestrach działań korygujących i zapobiegawczych. Za prowadzenie rejestru działań zapobiegawczych i korygujących odpowiedzialny jest Administratora danych osobowych lub osoba przez niego formalnie upoważniona.
2. Administrator danych osobowych opracowuje Plan kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

§ 16

W przypadku stwierdzenia naruszenia:

1) zabezpieczenia systemu informatycznego,

2) technicznego stanu urządzeń,

3) zawartości zbioru danych osobowych,

4) ujawnienia metody pracy lub sposobu działania programu,

5) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,

6) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.) każda osoba zatrudniona przy przetwarzaniu danych jest obowiązana niezwłocznie powiadomić o tym fakcie Administratora danych osobowych.

§ 17

W razie niemożliwości zawiadomienia Administratora danych osobowych lub osoby przez niego upoważnionej należy powiadomić bezpośredniego przełożonego.

§ 18

Do czasu przybycia na miejsce naruszenia ochrony danych Administratora danych osobowych lub upoważnionej przez niego osoby należy:

1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
3) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
4) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
5) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
6) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku.

§ 19

Po przybyciu na miejsce naruszenia Administrator danych osobowych lub osoba go zastępująca:

1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania, mając na uwadze ewentualne zagrożenia dla prawidłowości pracy,
2) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
3) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, z zewnętrznymi specjalistami.

§ 20

1. Administrator danych osobowych dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który powinien zawierać w szczególności:
   1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
   2) określenie czasu i miejsca naruszenia i powiadomienia,
   3) określenie okoliczności towarzyszących i rodzaju naruszenia,
   4) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
   5) wstępną ocenę przyczyn wystąpienia naruszenia,
   6) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.
2. Administrator danych osobowych opracowuje Raport. Wzór raportu z naruszenia ochrony danych stanowi **załącznik nr 9**.

§ 21

Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator danych osobowych zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje

się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

§ 22

1) Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Administratora danych, Informatyka oraz osób wyznaczonych przez Administratora danych.
2) Analiza powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.
3) W przypadku naruszenia ochrony danych osobowych skutkującym ryzykiem naruszenia praw lub wolności osób fizycznych administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Wzór zgłoszenia naruszenia do organu nadzorczego stanowi załącznik nr 9a.

GRUPY INFORMACJI PODLEGAJĄCE OCHRONIE

§ 23

1. Grupa informacji dotycząca działalności:
   1) dane osobowe klientów
   2) dane osobowe kontrahentów
   3) informacje dotyczące współpracy i rozliczeń z podmiotami współpracującymi
   4) skargi, zażalenia, reklamacje

2.Grupa informacji dotycząca pracowników:
   1) dane osobowe pracowników
   2) dane osobowe rodzin pracowników
   3) dane osoby - kandydata do zatrudniania
   4) informacje dot. obsługi kadrowo-płacowej pracownika (wynagrodzenia, ewidencja czasu pracy, informacja a urlopach)

3.Grupa informacji dotycząca infrastruktury fizycznej i teleinformatycznej:
   1) informacje dotyczące zarządzania zasobami (plany i rozmieszczenia i ilość zasobów – środki trwałe, informacja o nieruchomościach)
   2) dane na temat postępowania w sytuacji krytycznej (ewakuacja)
   3) informacje dotyczące stanu infrastruktury
   4) dane o zabezpieczeniach systemu informatycznego
   5) dane o zabezpieczeniach infrastruktury fizycznej
   6) informacje dotyczące systemów zarządzania
   7) dokumentacja techniczna infrastruktury

4. Grupa informacji dotycząca finansów organizacji:
   1) informacje finansowe
   2) dane z kontroli i audytów
   3) informacje dotyczące kontrahentów

5. Administrator danych osobowych prowadzi wykaz zbiorów danych. Wykaz zbiorów danych stanowi **załącznik nr 4** do niniejszej Polityki.

6. W Wykazie zbiorów zawarty jest opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między oraz wykaz programów i systemów komputerowych wykorzystywanych do przetwarzania danych w tych zbiorach.

7. Opis struktury baz danych oraz sposób przepływu danych pomiędzy poszczególnymi systemami jest w posiadaniu Administratora Systemu Informatycznego (ASI),a także u dostawców i autorów oprogramowania służącego do przetwarzania danych.

BEZPIECZEŃSTWO OSOBOWE

§ 24

Etap naboru pracownika / współpracownika

1. Do przetwarzania danych osobowych i do dostępu do innych informacji chronionych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora danych. Administrator danych może wydać pełnomocnictwo do nadawania upoważnień.
2. Wzór upoważnienia do przetwarzania danych osobowych i zobowiązania do zachowania tajemnicy przedsiębiorstwa stanowi **załącznik nr 6** do niniejszej Polityki.
3. Zakres upoważnienia może również być określony w umowie o pracę lub współpracę.
4. Osoba upoważniona zobowiązana jest podpisać oświadczenie lub umowę, która dokładnie określa odpowiedzialność w zakresie bezpieczeństwa informacji. Role i zakresy odpowiedzialności powinny uwzględniać:
   1) działania zgodne z Polityką Bezpieczeństwa Informacji;
   2) ochronę aktywów przed nieuprawnionym dostępem, ujawnieniem, modyfikacją lub zniszczeniem;
   3) wykonywanie działań związanych z bezpieczeństwem informacji;
   4) odpowiedzialność pracownika za jego działania lub niepodejmowanie działań;
   5) raportowanie zdarzeń związanych z bezpieczeństwem informacji;
   6) zapisy o zachowaniu poufności i nieujawnianiu informacji;
   7) prawa i obowiązki w odniesieniu do praw autorskich i ochrony danych osobowych;
   8) obowiązek klasyfikacji informacji i zarządzania aktywami organizacji związanymi z systemami informacyjnymi i usługami;
   9) odpowiedzialność w zakresie przetwarzania informacji otrzymywanej z zewnątrz;
   10) odpowiedzialność organizacji w zakresie przetwarzania danych osobowych;
   11) odpowiedzialność rozszerzoną, np. praca w domu, po godzinach pracy;
   12) konsekwencje nieprzestrzegania procedur bezpieczeństwa;
5. Wszyscy kandydaci do pracy, wykonawcy oraz podwykonawcy powinni podlegać weryfikacji, zgodnie z przepisami prawnymi i regulacjami wewnętrznymi, adekwatnie do wymagań biznesowych, klasyfikacji udostępnionych informacji oraz zidentyfikowanego ryzyka. Weryfikacja nie może naruszać prywatności, ochrony danych osobowych ani regulacji prawnych dotyczących zatrudnienia i może obejmować:
   1) dostępność referencji osobistych i świadectw pracy;
   2) sprawdzenie przedstawionego życiorysu;
   3) potwierdzenie deklarowanego wykształcenia i kwalifikacji zawodowych;
   4) niezależne potwierdzenie tożsamości, np. paszport.

§ 25

Zatrudnienie / współpraca

1. Pracownicy, wykonawcy i podwykonawcy powinni być świadomi swoich obowiązków i odpowiedzialności prawnej oraz zagrożeń związanych z bezpieczeństwem informacji. W tym celu należy zapewnić wszystkim zatrudnionym właściwy poziom świadomości poprzez kształcenie i szkolenie z zakresu bezpieczeństwa informacji, ze szczególnym uwzględnieniem procedur bezpieczeństwa. Dokumentują to: lista obecności ze szkoleń, oświadczenia pracowników, umowy o poufności, posiadane zaświadczenia, dyplomy lub certyfikaty.
2. W przypadku naruszenia zasad bezpieczeństwa jest uruchomiana odpowiednia procedura postępowania dyscyplinarnego, która powinna być poprzedzona potwierdzeniem naruszenia zasad bezpieczeństwa i zgromadzeniem materiału dowodowego.
3. Postępowanie dyscyplinarne powinno uwzględniać: rodzaj i wagę naruszenia zasad bezpieczeństwa, wpływ na procesy biznesowe, przypadek incydentalny, czy jest to kolejne naruszenie oraz jakość odbytego przeszkolenia.
4. Procedura przyznawania uprawnień i zakresu dostępu do informacji i systemów opisana jest w Instrukcji zarządzania systemem informatycznym.
5. W przypadku pracy mobilnej i na odległość z wykorzystaniem urządzeń przenośnych zastosowano odpowiednie, dodatkowe środki bezpieczeństwa.
6. Przekazywanie sprzętu i urządzeń służących do przetwarzania danych odbywa się na podstawie protokołów przekazania sprzętu.

§ 26

Zakończenie zatrudnienia / współpracy

1. Odchodzenie z Firmy lub zmiana stanowiska pracy wewnątrz organizacji powinny odbywać się w sposób zorganizowany.
2. Odchodzenie z firmy lub zmiana stanowiska pracy wiąże się ze zwrotem posiadanego przez pracownika sprzętu i odebraniem lub zmianą praw dostępu.
3. Odebranie lub ograniczenie praw dostępu jest poprzedzone analizą ryzyka uwzględniającą następujące uwarunkowania:
   1) ustalenie inicjatora (pracownik, wykonawca czy właściciel firmy) i przyczyn zakończenia lub zmiany zatrudnienia;
   2) aktualny zakres czynności pracownika, wykonawcy lub podwykonawcy;
   3) wartość aktualnie dostępnych aktywów.

§ 27

Ogólne zasady bezpieczeństwa osobowego

1. Każdy pracownik przy wykonywaniu swoich obowiązków służbowych jest zobowiązany do przestrzegania postanowień niniejszej Polityki oraz postanowień innych części dokumentacji bezpieczeństwa informacji, a także poleceń dotyczących bezpieczeństwa otrzymywanych od Administratora danych osobowych (ADO) oraz Administratora systemu informatycznego (ASI).
2. Administrator danych osobowych i przełożeni zobowiązani są do nadzoru nad przestrzeganiem postanowień niniejszej Polityki.
3. Każdy z pracowników jest zobowiązany do uczestniczenia w organizowanych okresowych szkoleniach z zakresu bezpieczeństwa informacji. Administrator danych osobowych oraz ASI są zobowiązani do utrzymywania i podnoszenia poziomu wiedzy dotyczącej bezpieczeństwa informacji.

4. Każdy pracownik jest zobowiązany do podjęcia bezpośrednich działań dla zapobiegania incydentom lub minimalizowania skutków incydentów w miarę swoich możliwości i kompetencji, w razie potrzeby zawiadamiając Administratora danych osobowych lub przełożonych. W razie potrzeby o zgłoszeniu incydentu Policji decyduje Administrator danych.

§ 28

Zasady przyznawania dostępu

1. Przyznawanie zakresu uprawnień powinno być w ścisłym związku z zakresem obowiązków danego pracownika.

2. Zarządzanie dostępem na etapie nadawania, zmiany i cofania praw dostępu pracowników w obszarze przetwarzania danych oraz do systemów teleinformatycznych powinno się odbywać na wniosek bezpośredniego przełożonego Użytkownika.

3. Na wniosek przełożonego lub specjalisty ds. kadrowych upoważnionemu użytkownikowi Administrator Systemu Informatycznego zakłada konto w systemie z adekwatnym poziomem uprawnień.

4. W zarządzaniu dostępem obowiązuje zasada, że dostęp użytkownika powinien opierać na spełnieniu zasady rozliczalności oraz zasady niezaprzeczalności. W przypadku systemów informatycznych obowiązują następujące wymagania:

1) wymóg jednoznacznej identyfikacji pracownika - tj. w systemach informatycznych każdy użytkownik pracuje wyłącznie na swoim indywidualnym koncie, nie są stosowane konta anonimowe lub współdzielone poza wyjątkami, gdzie z przyczyn technicznych nie ma innej możliwości,
2) wymóg uwierzytelnienia pracownika przy korzystaniu z systemu informatycznego,
3) autoryzacji przyznania praw dostępu do systemów informatycznych.
4) zasady przywilejów, wiedzy i usług koniecznych.

5. Procedury przyznawania upoważnień i dostępów do danych opisane są w instrukcjach zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

BEZPIECZENSTWO TELEINFORMATYCZNE

§ 29

Autoryzacja i dopuszczalne wykorzystanie zasobów

1. Przy ochronie zasobów kluczowe jest stosowanie podstawowej zasady bezpieczeństwa, że nie jest dozwolone wykorzystywanie zasobów w sposób inny niż jawnie dozwolony.
2. Do wykonywania obowiązków służbowych związanych z przetwarzaniem informacji dozwolone jest używanie systemów, urządzeń i oprogramowania dopuszczonych do użytku zgodnie z wymogami Polityki Bezpieczeństwa Informacji oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
3. Pracownicy są uprawnieni do korzystania z zasobów teleinformatycznych niezbędnych do wykonywania ich obowiązków. Za określenie takich zasobów dla każdego pracownika i wnioskowanie o przyznanie dostępu odpowiedzialny jest bezpośredni przełożony pracownika. Szczegółowa procedura przyznawania dostępu opisana jest w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
4. Zakazane jest użytkowanie na terenie obszaru przetwarzania danych lub przy wykonywaniu obowiązków służbowych poza obszarem przetwarzania danych innych niż dopuszczone urządzeń, systemów i oprogramowania bez zgody Administratora systemu informatycznego (ASI).

5. Zakazane jest bez zgody ASI:
   1) użytkowanie urządzeń skutkujących połączeniem systemów Administratora danych z sieciami teleinformatycznymi innych podmiotów, w tym publicznymi sieciami teleinformatycznymi,
   2) użytkowanie urządzeń lub oprogramowania mających na celu zakłócenie działania innych systemów, urządzeń lub oprogramowania,
   3) użytkowanie urządzeń lub oprogramowania do testowania bezpieczeństwa lub wykrywania podatności,
   4) użytkowanie urządzeń lub oprogramowania mogących naruszyć bezpieczeństwo innych systemów lub urządzeń,
   5) wprowadzanie zmian konfiguracji urządzeń, systemów lub oprogramowania.
6. Zakazane jest bez zgody Administratora danych osobowych wykorzystywanie urządzeń do niejawnego przekazywania lub rejestracji danych dotyczących informacji chronionych, w tym głosu i obrazu, tj.: magnetofonów, dyktafonów, aparatów fotograficznych, kamer, telefonów komórkowych z opcją rejestrowania dźwięku i obrazu, rejestratorów ruchu sieciowego, rejestratorów pracy klawiatur itp.
7. Powyższy zakaz nie dotyczy sytuacji, gdy rejestrowane są dane pochodzące z systemu testowego, a działania pracownika nie prowadzą, i w sposób oczywisty nie mogą prowadzić, do odczytywania jakichkolwiek poufnych informacji, do których pracownik nie ma dostępu.
8. Wykorzystanie należących do Administratora danych urządzeń, systemów i oprogramowania oraz innych zasobów do prywatnych celów pracowników jest dozwolone jedynie na uzasadniony wniosek pracownika i za zgodą Administratora danych osobowych i ASI.
9. Zasoby Administratora danych powinny być przechowywane w taki sposób, aby zapobiec możliwości ich kradzieży lub uszkodzenia przez osoby postronne oraz przypadkowe uszkodzenia przez osoby lub czynniki środowiskowe.
10. Wynoszenie aktywów (zasobów i informacji) poza obszar przetwarzania danych możliwe jest za zgodą Administratora danych osobowych lub bezpośredniego przełożonego użytkownika poza przypadkami, gdy jest to ujęte w planie praw dostępu.
11. Zakazane jest przesyłanie informacji podlegających ochronie na prywatne adresy poczty elektronicznej oraz prowadzenie korespondencji służbowej z wykorzystaniem prywatnego adresu e-mail użytkownika.
12. Zakazane jest używanie prywatnych nośników zewnętrznych (np. typu pendrive) i tworzenie nieautoryzowanych kopii z baz danych.
13. Pracownicy zobowiązani są stosować zasadę czystego biurka - wszystkie dokumenty i materiały powinny być po zakończeniu pracy chowane w przeznaczonych do tego szafkach, szufladach itp. W przypadku braku dostatecznej ilości dostępnego miejsca dokumenty i materiały powinny być pozostawiane na biurku uporządkowane.
14. Pracownicy są zobowiązani do ochrony zasobów będących własnością innych podmiotów, a powierzonych lub oddanych do dyspozycji Administratorowi danych lub udostępnionych pracownikom na czas wykonywania przez nich czynności służbowych w takim samym stopniu jak w przypadku zasobów będących własnością Administratora danych.
15. Procedury i instrukcje dotyczące bezpieczeństwa teleinformatycznego opracowuje ASI i przechowuje w Teczce ODO.

POSTANOWIENIA KOŃCOWE

§ 30

1. Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa Informacji zobowiązani są wszyscy pracownicy w rozumieniu przepisów Kodeksu pracy, konsultanci, stażyści i inne osoby mające dostęp do informacji podlegającej ochronie.
2. Z treścią niniejszego dokumentu powinni zapoznać się wszyscy pracownicy i inne osoby mające dostęp do informacji przetwarzanej w firmie, przed przystąpieniem do przetwarzania danych.
3. Niniejszy dokument może być przedstawiany podmiotom i jednostkom współpracującym, z którymi współpraca może skutkować możliwością dostępu do informacji chronionych.
4. Wobec osoby, która w przypadku naruszenia bezpieczeństwa informacji 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, wszczyna się postępowanie dyscyplinarne lub porządkowe.
5. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora danych osobowych.
6. W przypadku naruszenia postanowień Polityki Bezpieczeństwa Informacji pracownik, który dopuścił się takiego naruszenia lub przyczynił do niego (umyślnie lub nieumyślnie), może zostać ukarany zgodnie z obowiązującym regulaminem pracy, obowiązującymi przepisami prawa z zakresu ochrony informacji, a w skrajnych przypadkach pociągnięty do odpowiedzialności karnej.
7. Umyślne lub nieumyślne naruszenie postanowień Polityki Bezpieczeństwa Informacji lub niestosowanie się do poleceń służbowych w tym zakresie może być potraktowane jako naruszenie obowiązków pracowniczych.

§ 31

1. Polityka jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie.
2. Użytkownicy są zobowiązani zapoznać się z treścią Polityki.
3. Użytkownik zobowiązany jest złożyć oświadczenie o tym, iż został zaznajomiony z zasadami i przepisami o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych, z niniejszą Polityką, a także zobowiązać się do ich przestrzegania.
4. Wzór oświadczenia potwierdzającego zaznajomienie użytkownika z przepisami w zakresie ochrony informacji oraz z dokumentacją obowiązującą u Administratora danych, a także o zobowiązaniu się do ich przestrzegania, stanowi **załącznik nr 5** do niniejszej Polityki.
5. Oświadczenia przechowywane są w aktach osobowych.

§ 32

1. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie aktualnie obowiązujące przepisy prawa w zakresie ochrony informacji.
2. Użytkownicy zobowiązani są do bezwzględnego stosowania postanowień zawartych w niniejszej Polityce. W wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obowiązujących u Administratora danych użytkownicy mają obowiązek stosowania unormowań dalej idących, których stosowanie zapewni wyższy poziom ochrony informacji.