INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM PRZETWARZAJĄCYM DANE OSOBOWE

.....	.....	.....
pieczęć firmowa	podpis administratora danych osobowych	data

Wstęp

Mając na uwadze konstytucyjne prawa każdego obywatela Rzeczypospolitej Polskiej
KONSTYTUCJA RZECZYPOSPOLITEJ POLSKIEJ *(ART. 47, 51):*

(art. 47.)

Każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

(art. 51.)

1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.
2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.
3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.
4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.
5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

Zgodnie z ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000, 1669, z 2019 r. poz. 730.), oraz Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE., administrator danych osobowych zobowiązany jest do zapewnienia ochrony przetwarzanych danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Jakość zapewnianej ochrony powinna być odpowiednia do zagrożeń oraz kategorii danych nią objętych. Ponadto administrator danych zobowiązany jest zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. Biorąc pod uwagę te konstytucyjne i ustawowe obowiązki ustanawiamy niniejszą Instrukcję zarządzania systemem informatycznym.

Rozdział 1
Postanowienia ogólne

§ 1. Ilekroć w Instrukcji jest mowa o:

1) **ustawie** – rozumie się przez to ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000, 1669, z 2019 r. poz. 730.)

8) **administratorze danych** – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydujące o celach i środkach przetwarzania danych osobowych;

9) **administratorze systemu** – /ASI/– rozumie się przez to osobę zarządzającą systemem informatycznym w którym przetwarzane są dane osobowe,

10) **użytkowniku systemu** – rozumie się przez to osobę upoważnioną przez administratora danych do przetwarzania danych osobowych, której nadano indywidualny identyfikator i przyznano hasło;

13) **odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, przedstawiciela, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;

14) **państwie trzecim** – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego (ang. *European Economic Area, EEA*) – strefa wolnego handlu i Wspólny Rynek.

16) **wykazie zbiorów** – należy przez to rozumieć wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;

17) **opisie struktury zbiorów** – należy przez to rozumieć opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;

18) **opis struktury zbiorów** – danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;

Rozdział 2
Procedura nadawania uprawnień do przetwarzania danych osobowych.

§ 2. Uwzględniając kategorie przetwarzanych danych oraz występujące zagrożenia bezpieczeństwa przetwarzania tych danych osobowych w systemie informatycznym, mając na uwadze także wszystkie odpowiednie środki do realizacji postawionych sobie celów ochrony danych osobowych, zastosowano poziom bezpieczeństwa wysoki. Procedura opisuje zasady: przyznawania, modyfikacji i usuwania uprawnień użytkownika do przetwarzania zbiorów w systemie informatycznym lub w wersji papierowej.

§ 3. Osobą odpowiedzialną za nadawanie i cofanie bądź zmianę uprawnień w systemie informatycznym jest administrator danych. Przyznanie, anulowanie bądź zmiana upoważnienia do przetwarzania danych osobowych w systemie informatycznym lub w zbiorze papierowym wraz z uprawnieniami do przetwarzania tych danych realizowana jest na pisemne zlecenie Administratora Danych Osobowych.

§ 4. Procedura nadawania, modyfikowania i odbierania uprawnień przez administratora bezpieczeństwa danych użytkownikowi w systemie informatycznym obejmuje w kolejności następujące zadania:

1) zapoznanie osoby uprawnionej przed przystąpieniem do zadań z przepisami dotyczącymi ochrony danych osobowych w regulacjach prawnych oraz z procedurami bezpieczeństwa systemu informatycznego określonego niniejszą instrukcją;

2) sprawdzenia czy dana osoba odbyła szkolenie z zakresu przestrzegania zasad bezpieczeństwa danych osobowych i czy wiedza uzyskana z danego szkolenia jest aktualna;

3) sprawdzenia czy dana osoba podpisała oświadczenie o zachowaniu poufności co do danych, które będą jej powierzone i przestrzega wewnętrznej dokumentacji ochrony danych osobowych;

4) sprawdzenia czy dana osoba będzie przetwarzać dane osobowe w zakresie i celu określonym w polityce bezpieczeństwa i instrukcji zarządzania i ewentualnie w Regulaminie ODO;

5) zwrócenie się z wnioskiem do administratora systemu o przyznanie osobie uprawnionej, uprawnień w systemie informatycznym w niezbędnym zakresie do realizacji powierzonych jej funkcji;

6) modyfikacja i odbieranie uprawnień użytkownika w systemie informatycznym celem zagwarantowania najwyższych standardów ochrony danych osobowych.

§ 5. Procedurę rejestrowania uprawnień użytkownika w systemie informatycznym przeprowadza administrator tego systemu i obejmuje następujące działania:

1) przypisanie indywidualnego identyfikatora użytkownika w systemie informatycznym do konkretnej osoby wraz z datą przyznania i odebrania uprawnień, kontrola poprawności tych uprawnień;

2) przypisanie zakresu przydzielonych uprawnień w systemie informatycznym do konkretnego identyfikatora użytkownika. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielany innej osobie, jest jednorazowy.

Rozdział 3
Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 6. W zakresie uwierzytelniania użytkownika w systemie informatycznym zastosowano identyfikator i hasło. Dostęp do zbioru danych osobowych (do bazy danych i do programu) wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła. Ten podrozdział określa politykę haseł użytkownika przy dostępie do serwera lub sieci, jeśli dane osobowe (np. w Excelu, listy osób, dokumenty z danymi osobowymi) znajdują się bezpośrednio na serwerze lub na poszczególnych stacjach.

§ 7. Hasło zastosowane do uwierzytelnienia użytkownika w systemie informatycznym dla pełniejszej ochrony składa się z co najmniej 8 znaków, w tym musi zawierać co najmniej małe i duże litery oraz liczbę lub znak specjalny. Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych. Hasło jest zmieniane w cyklach nie dłuższych niż 30 dni. Administrator zobowiązany jest do prowadzenia metryk haseł użytkownika. Metryka hasła powinna zawierać: treść hasła, datę jego wprowadzenia do systemu, datę i powód awaryjnego udostępnienia hasła oraz być przechowywana przez okres 5 lat.

§ 8. Zmiana hasła odbywa się cyklicznie.

§ 9. Hasło zastosowane do uwierzytelnienia administratora systemu w systemie informatycznym składa się z co najmniej 10 znaków, w tym musi zawierać co najmniej dwie małe i duże litery oraz liczbę lub znak specjalny. Każdorazowe użycie konta administratora systemu jest odnotowywane w tym systemie w formie logów dostępowych. Hasło jest zmieniane w cyklach nie dłuższych niż 6 miesięcy. Administrator zobowiązany jest do

prowadzenia metryk haseł administratora. Metryka hasła powinna zawierać: treść hasła, datę jego wprowadzenia do systemu, datę i powód awaryjnego udostępnienia hasła oraz być przechowywana przez okres 5 lat.

§ 10. Użytkownicy systemów informatycznych przed przystąpieniem do obowiązków są zapoznawani z zagrożeniami wynikającymi ze stosowania haseł o różnym poziomie skomplikowania/trudności jako formy ich uwierzytelniania w systemie informatycznym. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.

Rozdział 4
Procedura rozpoczęcia, zawieszenia i zakończenia lub zmiany uprawnień pracy użytkowników systemu informatycznego

§ 11. Procedura opisuje szczegółowe zasady: przyznawania, modyfikacji i usuwania uprawnień użytkownika do przetwarzania zbiorów w systemie informatycznym lub w wersji papierowej. Celem procedury jest minimalizacja ryzyka nieuprawnionego dostępu do danych osobowych i utraty poufności przez osoby nieupoważnione. Przed rozpoczęciem pracy w systemie informatycznym uprawniony użytkownik weryfikuje bezpieczeństwo środowiska pracy pod względem treści wyświetlanych na ekranie i przebywanie w ich bezpośrednim sąsiedztwie osób nieupoważnionych.

§ 12. W każdym wypadku zawieszenia pracy lub przerwy w jej wykonywaniu przez pracownika, osobę uprawnioną, użytkownika w systemie informatycznym i odejściem od punktu systemu informatycznego w/w osoba zobowiązana jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu. Jeżeli tego nie uczyni – po upływie 5 minut system automatycznie aktywuje wygaszacz tzw. Polityka czystego ekranu.

§ 13. Osoba uprawniona po zakończeniu pracy zobowiązana jest do zamykania systemu informatycznego poprzez wylogowanie się z niego, a następnie wyłączyć sprzęt komputerowy, zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację.

Rozdział 5
Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

§ 14. Kopie zapasowe danych są tworzone w cyklach: kopia całościowa raz na tydzień.

§ 15. Kopie powyższe są wykonywane metodą nadpisywania na nośniku danych innym niż ten na którym znajduje się baza danych oraz przechowywany jest w pomieszczeniu odrębnym niż zbiór danych głównych.

§ 16. W przypadku zużycia lub uszkodzenia elektronicznego nośnika zawierającego kopie zapasowe, należy ten uszkodzony nośnik zutylizować w sposób uniemożliwiający odczytanie danych na nim zawartych.

Rozdział 6
Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

§ 17. W systemie informatycznym zostało zainstalowane automatycznie aktualizujące się

oprogramowanie antywirusowe.

§ 18. Na styku sieci wewnętrznej z siecią publiczną zastosowano zaporę ogniową: programową – zapora systemowa Microsoft Windows.

§ 19. Użytkownicy systemu niezwłocznie informują administratora systemu o zagrożeniach monitowanych przez oprogramowanie antywirusowe, np. w postaci ujawnionego podejrzanego oprogramowania, cudzej ingerencji w bazę danych.

Rozdział 7
Sposób odnotowania informacji o odbiorcach danych, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia

§ 20. Administrator danych udostępnia dane odbiorcom danych samodzielnie tj. z pominięciem przyznawania dostępu odbiorcom danych do systemu informatycznego administratora danych.

Rozdział 8
Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

§ 21. Administrator systemu informatycznego jest zobowiązany do okresowego przeglądania systemu informatycznego. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI. Działania te podejmowane są w celu określania ich poziomu sprawności, bezpieczeństwa i użyteczności, biorąc pod uwagę racjonalne wykorzystanie sprzętu oraz zapewnienie bezpieczeństwa danych przetwarzanych z jego wykorzystaniem.

§ 22. Administrator systemu przeprowadza w/w przegląd nie rzadziej niż raz na 5 lat. ASI odpowiada za regularną aktualizację oprogramowania, zgodnie z zaleceniami określonymi przez producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji.

§ 23. Wszelkie naprawy i konserwacja systemu odbywają się pod nadzorem i wiedzą ASI.

Rozdział 9
Postanowienia końcowe

§ 24. Wszelkie zasady i procedury opisane w niniejszej Instrukcji są wdrożone i przestrzegane przez uprawnionych użytkowników i administratorów systemów. Głównym wyznacznikiem wszystkich działań jest dobro osób, których dane te dotyczą.

§ 25. Instrukcja obowiązuje od dnia jej zatwierdzenia przez administratora danych.