LUBELSKI PARK NAUKOWO TECHNOLOGICZNY

ZARZĄDZENIE

Prezesa Zarządu
Lubelskiego Parku Naukowo-Technologicznego S.A.
z dnia 25.10.2021 r.

w sprawie wdrożenia dokumentacji ochrony danych osobowych

W związku z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych – RODO) oraz w celu ochrony danych osobowych pracowników i klientów, Zarząd Lubelskiego Parku Naukowo-Technologicznego S.A. w Lublinie postanawia wdrożyć następujące działania:

§1

1. Przyjmuje się Politykę Ochrony Danych Osobowych wraz z załącznikami opisanymi w jej treści, stanowiącą Załącznik nr 1 do niniejszego Zarządzenia oraz Instrukcję Zarządzania Systemem Informatycznym w Lubelskim Parku Naukowo-Technologicznym S.A. stanowiącą Załącznik nr 2 do niniejszego Zarządzenia.
2. Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemem Informatycznym wchodzą w życie w dniu podpisania niniejszego zarządzenia.
3. Pracownicy zobowiązani są do zapoznania się z dokumentami, o których mowa w pkt 1 oraz ścisłego przestrzegania ich zapisów.

§2

1. Zarządzenie wchodzi w życie z dniem podpisania.

Prezes Zarządu
Magdalena Stachyra

Lubelski Park Naukowo-Technologiczny S.A.
ul. Dobrzańskiego 3, 20-262 Lublin
tel.: 81 534 61 00, fax: 81 351 85 48, e-mail: biuro@lpnt.pl, www.lpnt.pl,
KRS 0000228715, NIP 712 29 14 578, REGON: 060005172
Sąd Rejonowy w Lublinie, XI Wydział Gospodarczy,
Kapitał zakładowy 60 903 000,00 zł, kapitał wpłacony 60 903 000,00 zł.

Załącznik nr 1 do Zarządzenia Prezesa Zarządu Lubelskiego Parku Naukowo-Technologicznego S.A. z dnia 25.10.2021 r. ws. wdrożenia dokumentacji ochrony danych osobowych.

Polityka Ochrony Danych Osobowych
w
Lubelskim Parku Naukowo Technologicznym S.A.

LUBELSKI PARK NAUKOWO TECHNOLOGICZNY

Wersja nr 1		**Pieczęć:**	
Opracował:	**Data:**	**Zatwierdził:**	**Data:**
Inspektor Ochrony Danych: Bartosz Starzomczyk		Administrator Danych Osobowych Prezes Zarządu Magdalena Stachyra	

Spis treści

I. Wstęp

Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania System Informatycznym wraz z załącznikami, są podstawowymi dokumentami opisującym zasady ochrony danych osobowych stosowane w Lubelskim Parku Naukowo Technologicznym S. A. (dalej jako LPNT S.A.). Dokumentacja powstała w celu spełnienia wymagań Art. 24 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, dalej „RODO") oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

Dokumentacja ochrony danych w LPNT S.A. opisuje sposób przetwarzania danych osobowych oraz zastosowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

Celem wdrożenia Instrukcji Zarządzania Systemem Informatycznym jest także określenie podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz wymagań w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.

Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

- poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
- integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
- rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
- integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

Każda osoba mającą dostęp do danych osobowych z upoważnienia LPNT S.A, ma obowiązek zapoznania się z dokumentem Polityki Ochrony Danych Osobowych. Dotyczy to w szczególności pracowników zatrudnionych przez Administratora Danych. Osoby, o których mowa w zdaniu poprzednim, mają obowiązek złożenia na piśmie oświadczenia o zapoznaniu się z treścią Polityki oraz zachowaniu danych osobowych w tajemnicy.

II. Definicje:

1. **Administrator Danych** – Lubelski Park Naukowo Technologiczny S.A. z siedzibą ul. Bohdana Dobrzańskiego 3, 20-262 Lublin;
2. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
3. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych;
4. **Użytkownik** – osoba upoważniona przez Administratora Danych do przetwarzania danych osobowych;
5. **Zbiór danych** – każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów;
6. **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na Danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie w formie tradycyjnej oraz w systemach informatycznych;
7. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie Przetwarzania danych osobowych w takim systemie;
8. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (Użytkownikowi) w razie przetwarzania danych osobowych w takim systemie;
9. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (Użytkownika).

III. Zakres stosowania:

1. Politykę Ochrony Danych Osobowych w LPNT S.A stosuje się do wszelkich czynności mających charakter przetwarzania danych osobowych w rozumieniu art. 4 ust. 2) ogólnego rozporządzenia o ochronie danych RODO.
2. Bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania, stosowane są zasady przetwarzania danych osobowych ujęte w niniejszym dokumencie.
3. Polityka dotyczy wszystkich danych osobowych niezależnie od formy ich przetwarzania (przetwarzane tradycyjnie zbiory ewidencyjne, systemy informatyczne) oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.
4. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora.
5. Polityka jest udostępniana do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych na ich wniosek, a także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z jej treścią.

IV. Organizacja przetwarzania danych osobowych:

4.1 Administrator Danych Osobowych:

Administrator danych osobowych (ADO) realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:

1) Podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji zasad pracy ADO oraz technik zabezpieczenia danych osobowych;
2) Upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków;
3) Wyznacza Inspektora Ochrony Danych (IOD) oraz określa zakres jego zadań i czynności jako właściwego do prowadzenia dokumentacji z zakresu ochrony danych, o ile jako właściwy do jej prowadzenia nie zostanie wskazany w niniejszym dokumencie inny podmiot;
4) Zapewnia użytkownikom odpowiednie środki w ramach stanowiska pracy, w tym sprzęt informatyczny, umożliwiające bezpieczne i zgodne z obowiązującym prawem przetwarzanie danych osobowych;
5) Podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych;
6) Inicjuje proces szacowania ryzyka dla przetwarzania danych osobowych
7) Zarządza naruszeniami ochrony danych osobowych i w przypadkach określonych w przepisach kontaktuje się z Prezesem Urzędu Ochrony Danych Osobowych;

4.2 Inspektor Ochrony Danych:

Inspektor Ochrony Danych (IOD) sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych, w tym zwłaszcza:

1) Sprawuje nadzór nad wdrożeniem i funkcjonowaniem adekwatnych środków fizycznych, a także organizacyjnych i technicznych – w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych;
2) Odpowiada za wydawanie upoważnień do przetwarzania danych osobowych;
3) Prowadzi Ewidencję osób upoważnionych do przetwarzania danych osobowych;
4) Koordynuje wewnętrzne audyty i sprawdzenia w zakresie obszaru ochrony danych osobowych;
5) Nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom;
6) Prowadzi w imieniu ADO Rejestr Czynności Przetwarzania oraz Rejestr Kategorii Danych Osobowych;
7) Przygotowuje wzory dokumentów dotyczące ochrony danych osobowych;
8) Prowadzi oraz aktualizuje dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych;
9) Wspólnie z ADO i ASI podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa przetwarzania danych osobowych ze szczególnym uwzględnieniem systemu informatycznego;
10) Nadzoruje wykonywanie oceny skutków dla ochrony w sytuacji, gdy wymagane jest to przepisami prawa;

11) Uczestniczy w procesie szacowania ryzyka dla ochrony danych;
12) W porozumieniu z ADO na czas swojej nieobecności wyznacza w formie pisemnej swojego zastępcę;
13) Inicjuje i podejmuje przedsięwzięcia mające na celu doskonalenie i rozwijanie systemu ochrony danych osobowych u ADO;
14) Szkoli personel w zakresie obowiązujących zasad przetwarzania danych osobowych;
15) Rejestruje wszelkie naruszenia i incydenty oraz pełni funkcję punktu kontaktowego w sytuacji wystąpienia naruszenia ochrony danych osobowych;

Inspektor Ochrony Danych ma prawo:

1) Wstępu do pomieszczeń, w których zlokalizowane są zbiory danych osobowych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z obowiązującymi procedurami i przepisami prawa;
2) Żądać od pracowników i podmiotów współpracujących złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego;
3) Żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli;
4) Przeprowadzenia kontroli dokumentacji, urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych, których właścicielem jest ADO oraz do przeprowadzenia kontroli u podmiotów przetwarzających powierzone przez ADO dane osobowe;

4.3 Administrator Systemu Informatycznego:

Administrator systemu informatycznego (ASI) realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym Administratora Danych Osobowych, w tym zwłaszcza:

1) Zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, poprzez posługiwanie się hasłami administracyjnymi zapewniającymi dostęp do wszystkich stacji roboczych i serwerów z poziomu administratora;
2) Przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe;
3) Na wniosek ADO lub IOD przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
4) Nadzoruje prawidłowe działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;
5) Podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego;
6) Wyrejestrowuje użytkowników na polecenie ADO;
7) W sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje ADO i IOD o naruszeniu oraz współdziała z nimi przy usuwaniu skutków naruszenia;
8) Prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym;
9) Wykonuje oraz sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją

urządzeń komputerowych, na których przetwarzane są dane osobowe;

10) Wykonuje oraz sprawuje nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;
11) Podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji;

4.4 Obowiązki pracowników LPNT S.A.:

1) Pracownik może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez ADO (zgodnie z nadanym upoważnieniem do przetwarzania danych osobowych) i tylko w celu wykonywania nałożonych na niego obowiązków;
2) Zakres uprawnień do zbiorów danych osobowych przetwarzanych z wykorzystaniem systemu informatycznego przypisany jest do indywidualnego i niepowtarzalnego identyfikatora użytkownika, niezbędnego do pracy w systemie;
3) Rozwiązanie stosunku pracy lub odwołanie z pełnionej funkcji jest podstawą do wycofania upoważnienia do przetwarzania danych osobowych;
4) Pracownicy upoważnieni do przetwarzania danych osobowych, pisemnie oświadczają, że zobowiązują się do zachowania w tajemnicy danych osobowych oraz przestrzegania procedur ich bezpiecznego przetwarzania, a także zachowania w tajemnicy zastosowanych u ADO środków bezpieczeństwa;
5) Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u ADO, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji;
6) Naruszenie przez pracowników upoważnionych do przetwarzania danych osobowych, procedur bezpiecznego przetwarzania, w szczególności świadome udostępnienie danych osobie niepowołanej, jest ciężkim naruszeniem obowiązków pracowniczych i może uzasadnić rozwiązanie umowy o pracę w trybie art. 52 Kodeksu Pracy.

Wszyscy pracownicy są zobowiązani do:

1) Zapoznania się z przepisami prawa w zakresie ochrony danych osobowych, w tym zapisami niniejszej Polityki Ochrony Danych oraz Instrukcji Zarządzania Systemem Informatycznym,
2) Stosowania określonych przez ADO oraz IOD procedur oraz wytycznych mających na celu zgodne z prawem, w tym zwłaszcza adekwatne przetwarzanie danych osobowych,
3) Odpowiedniego zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym.

V. Środki organizacyjne i techniczne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych:

5.1 Obszar przetwarzania danych osobowych:

Na obszar przetwarzania danych osobowych składa się budynek mieszczący się pod adresem ul. Bohdana Dobrzańskiego 3, 20-262 Lublin. LPNT S.A. jest operatorem Inkubatora

Przedsiębiorczości znajdującego się w tym samym budynku pod adresem ul. Bohdana Dobrzańskiego 1.

5.2 Środki ochrony fizycznej:

1) Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
2) W budynku zastosowano system kontroli dostępu, każdy pracownik oraz najemca posiada przypisaną do niego kartę magnetyczną. Nadzór nad systemem oraz osobami wchodzącymi bo budynku sprawuje służba ochrony;
3) Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przez ADO i posiadającej ważne upoważnienie do przetwarzania danych osobowych;
4) Dane osobowe znajdujące się na nośnikach tradycyjnych (papierowych) są przechowywane w pomieszczeniach zabezpieczonych drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi);
5) Nośniki tradycyjne są przechowywane w szafach zamykanych na klucz. Pracownicy są zobowiązani do niepozostawiania kluczy w zamkach oraz do przechowywania ich w miejscach minimalizujących ryzyko dostępu przez osoby niepowołane;
6) Pomieszczenie, w którym znajduje się serwer jest zabezpieczone drzwiami przeciwwłamaniowymi o podwyższonej odporności ogniowej;
7) Pomieszczeniach wyposażone są w czujki przeciwwłamaniowe. Budynek jest objęty systemem alarmowym przeciwwłamaniowym;
8) Budynek został objęty monitoringiem wizyjnym, podstawa funkcjonowania monitoringu wraz z zasadami jego wykorzystania i okresem przechowywania danych została określona w Regulaminie Funkcjonowania Monitoringu Wizyjnego LPNT S.A.;
9) Budynek znajduje się pod stałym 24-godzinnym nadzorem sprawowanym przez służbę ochrony, z która została zawarta stosowna umowa;
10) Kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są w zamkniętej metalowej szafie w pomieszczeniu zamykanym na klucz;
11) Dostęp do pomieszczeń, w których przetwarzane są dane osobowe jest możliwy po uprzednim pobraniu klucza. Po zakończeniu pracy każdy pracownik ma obowiązek zdania klucza w miejscu wyznaczonym przez Zarząd. ADO prowadzi listę osób, którym nadano upoważnienie do wynoszenia kluczy poza teren LPNT S.A.;
12) Pomieszczenia, w których przetwarzane są zbiory danych osobowych zabezpieczone są przed skutkami pożaru za pomocą systemu czujek przeciwpożarowych oraz wolnostojących gaśnic;
13) Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów zawierających odpowiedni atest, minimalizujących ryzko odtworzenia niszczonego dokumentu;
14) Dokumenty podlegające przepisom o archiwach są przechowywane w archiwum zakładowym znajdującym się w budynku głównym należącym do LPNT.

5.3 Środki sprzętowe, informatyczne i telekomunikacyjne:

1) Co najmniej jedno urządzenie systemu informatycznego służącego do przetwarzania danych osobowych połączone jest z siecią publiczną;
2) Lokalizacja urządzeń informatycznych (komputerów, laptopów, terminali, drukarek) uniemożliwia osobom niepowołanym dostęp do nich oraz wgląd do danych wyświetlanych na monitorach komputerowych;
3) Komputery przenośne, wykorzystywane do przetwarzania danych osobowych, po zakończonej pracy są przechowywane w warunkach zapewniających im odpowiedni poziom bezpieczeństwa. ADO prowadzi listę osób upoważnionych do wynoszenia urządzeń poza teren LPNT S.A.;
4) Zastosowano środki adekwatne do możliwości technicznych i organizacyjnych ADO, uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych;
5) Zastosowano lokalne urządzenia podtrzymujące zasilanie typu UPS, chroniące system informatyczny służący do przetwarzania danych osobowych, przed skutkami awarii zasilania;
6) Sprzęt komputerowy służący do przetwarzania danych osobowych połączony jest z siecią publiczną za pośrednictwem urządzeń z wbudowanym firewallem pełniących rolę bramy zabezpieczającej przed niepowołanym dostępem;
7) Zastosowano kryptograficzne środki ochrony nośników (szyfrowanie całej powierzchni nośników) na urządzeniach przenośnych, na których odbywa się przetwarzanie danych osobowych (laptopy, pendrive, dyski przenośne);
8) Okablowanie sieciowe zostało zaprojektowane w ten sposób, że dostęp do linii teletransmisyjnych jest możliwy tylko z pomieszczeń zamykanych na klucz i nadzorowanych przez pracowników LPNT S.A. oraz pracowników ochrony;
9) Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelniania;
10) Bieżąca konserwacja sprzętu wykorzystywanego przez ADO do przetwarzania danych jest prowadzona tylko przez podmioty, z którymi zawarto odpowiednie umowy powierzenia przetwarzania danych osobowych. Prace konserwacyjnego wykonywane są pod nadzorem ASI lub innego, wyznaczonego przez ADO pracownika;
11) Poważne naprawy wykonywane przez personel zewnętrzny są realizowane w siedzibie ADO po zawarciu z podmiotem wykonującym naprawę umowy o powierzenie przetwarzania danych osobowych;
12) ASI dopuszcza konserwowanie i naprawę sprzętu poza siedzibą ADO jedynie po trwałym usunięciu danych osobowych lub pozostawieniu w siedzibie ADO nośników zawierających dane osobowe;
13) Zużyty sprzęt służący do przetwarzania danych osobowych może być zbywany dopiero po trwałym usunięciu danych osobowych lub pozostawieniu w siedzibie ADO nośników zawierających dane osobowe, a urządzenia uszkodzone są przekazywane właściwym podmiotom w celu utylizacji, po zawarciu odpowiedniej umowy;

5.3.1 Środki ochrony w ramach systemu operacyjnego:

1) Dostęp do systemów operacyjnych komputerów i laptopów, w których są przetwarzane dane osobowe, jest zabezpieczony za pomocą procesu uwierzytelniania z wykorzystaniem indywidualnego identyfikatora użytkownika (loginu) oraz hasła;

2) Rodzaj systemu operacyjnego i sposób jego konfiguracji zapewnia odpowiednie restrykcje w zakresie dostępu do danych i aplikacji;
3) W systemach operacyjnych zastosowano mechanizm wymuszający okresową zmianę haseł;
4) Użytkownicy systemu informatycznego nie posiadają praw do wykonywania kopii zapasowych zbiorów danych osobowych;
5) Zastosowano oprogramowanie zabezpieczające przed nieuprawnionym dostępem do systemu informatycznego;
6) Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe;
7) Zastosowano zabezpieczone hasłem wygaszanie ekranu w przypadku nieaktywności użytkownika dłuższej niż 15 minut;
8) Każdy komputer i laptop został zabezpieczony działającym w tle programem antywirusowym;
9) Skonfigurowano i zapewniono automatyczne pobieranie aktualizacji do systemów operacyjnych;

5.3.2 Środki ochrony w ramach narzędzi programowych:

1) Serwery obsługujące bazy danych, w których przetwarzane są dane osobowe dostępne są wyłącznie po przeprowadzeniu prawidłowego procesu autoryzacji przez ASI;
2) Dostęp do zbiorów danych osobowych zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika (loginu) oraz hasła;
3) Zastosowano system rejestracji dostępu do zbioru danych osobowych (logi);
4) Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbiorów danych osobowych;
5) Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego;
6) Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych;
7) Zastosowano mechanizm umożliwiający rejestrację identyfikatora użytkownika wprowadzającego dane osobowe;
8) Zapewniono rejestrację czasu nieudanych logowań do systemów przetwarzających dane osobowe;
9) Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zasobów gromadzonych w systemie informatycznym;

Ponadto każdy pracownik lub użytkownik upoważniony do przetwarzania danych osobowych ma obowiązek:

1) Nieużywania jednostronnie zadrukowanych dokumentów zawierających dane osobowe;
2) Zachowania tajemnicy danych przetwarzanych w siedzibie ADO, w tym także wobec osób najbliższych;
3) Zapewnienia odpowiedniego poziomu bezpieczeństwa powierzonych mu dokumentów, akt, płyt, pamięci przenośnych, komputerów przenośnych oraz innych nośników elektronicznych;

4) Niepozostawiania bez kontroli dokumentów, nośników danych i sprzętu w hotelach oraz innych miejscach publicznych, a w szczególności nie pozostawiania ich bez nadzoru w samochodach;
5) Ustawiania ekranów komputerowych tak, aby osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia;
6) Niezapisywania hasła wymaganego do uwierzytelniania się w systemie na papierze lub innym nośniku przechowywanym razem z urządzeniem służącym do przetwarzania danych osobowych;
7) Niepodłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych mogących powodować spięcia w sieci elektrycznej;
8) Dbania o prawidłową wentylację komputerów;
9) Przestrzegania swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń ASI;
10) Niepozostawiania osób nie będących pracownikami LPNT S.A w pomieszczeniu, w którym przetwarza się dane osobowe, bez osoby upoważnionej do przetwarzania danych osobowych;
11) Opuszczania stanowiska pracy dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;
12) Udostępniania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej;
13) Nie wynoszenia na jakichkolwiek nośnikach dokumentacji zawierającej dane osobowe, nawet w postaci zaszyfrowanej;
14) Kończenia pracy na stacji roboczej po zapisaniu wszystkich zmian i prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera;
15) Zamykania okien w razie różnych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych;
16) Zamykania okien w razie opuszczenia pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy;

5.5 Zabezpieczenie dokumentacji papierowej:

1) Upoważnieni pracownicy są zobowiązani do stosowania tzw. „**Polityki czystego biurka**". Polega ona na zabezpieczaniu (zamykaniu) dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy;
2) Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach lub utylizacji ich w specjalnych bezpiecznych pojemnikach z przeznaczeniem do bezpiecznej utylizacji;
3) Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych;
4) Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np., na terenach publicznych;

5.6 Polityka kluczy:

1) W związku z funkcjonującą w budynku ochroną, za zamykanie i otwieranie głównych drzwi poza godzinami pracy parku odpowiada wyznaczony pracownik ochrony;
2) Administrator Danych Osobowych wyznacza pracowników, którzy są upoważnieni do otwierania i zamykania głównych wejść do budynku;
3) Wyznaczonym pracownikom ADO nadaje pisemne upoważnienie;
4) Wszystkie klucze do pomieszczeń wewnątrz strefy administracyjnej znajdują się w metalowej skrzynce na klucze;
5) Od momentu pobrania kluczy do momentu ich zdania na pracownikach spoczywa pełna odpowiedzialność za ich zabezpieczenie;
6) Po otwarciu pomieszczeń biurowych, przed przystąpieniem do pracy pracownicy sprawdzają stan zastosowanych zabezpieczeń sprzętu biurowego i komputerowego, a także składowanej w tych pomieszczeniach dokumentacji i innego wyposażenia;
7) W przypadku stwierdzenia zmian lub naruszeń stanu zabezpieczeń pracownik, który to stwierdził natychmiast powiadamia o tym swojego bezpośredniego przełożonego lub Inspektora Ochrony Danych;
8) Klucze do biurek stanowiskowych i szaf biurowych są w posiadaniu pracowników, którzy po zakończonej pracy zobowiązani się do zdeponowania ich we wcześniej ustalonym miejscu;

VI. Prawa osób, których dane dotyczą:

1) Osobie, której Dane Osobowe dotyczą, przysługują wobec Administratora Danych Osobowych (przy spełnieniu warunków opisanych w Rozporządzeniu) następujące uprawnienia:
   a) prawo dostępu do danych osobowych;
   b) prawo do sprostowania danych osobowych;
   c) prawo do usunięcia danych osobowych („prawo do bycia zapomnianym");
   d) prawo do ograniczenia przetwarzania danych osobowych;
   e) prawo do przenoszenia danych osobowych;
   f) prawo do sprzeciwu wobec przetwarzania danych osobowych;
   g) prawo do niepodlegania decyzji polegającej na zautomatyzowanym przetwarzaniu, w tym profilowaniu;
2) Funkcję punktu kontaktowego w zakresie realizacji praw osób, których dane dotyczą pełni Inspektor Ochrony Danych;
3) Komunikacja z osobami możliwa jest za pomocą korespondencji tradycyjnej lub elektronicznej pod adresem e-mail: iod@lpnt.pl
4) Komunikacja możliwa jest również na na piśmie (listem poleconym lub przesyłką kurierską). W razie, gdy żądanie zostało przekazane do Administratora drogą elektroniczną, odpowiedź udzielana jest w tej samej formie, chyba, że osoba, której dane dotyczą żąda innej formy komunikacji;
5) Komunikacja z osobą, której dane dotyczą odbywa się w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem;
6) Każdy z pracowników i współpracowników Administratora, w razie otrzymania w jakikolwiek sposób informacji/oświadczenia/komunikatu, które mogą stanowić żądanie w zakresie praw osoby, jest zobowiązany w trybie niezwłocznym do przekazania ich w drodze korespondencji e-mail do Inspektora Ochrony Danych bądź do innej osoby wyznaczonej przez ADO lub gdy

osoba taka nie ma dostępu do poczty elektronicznej, zawiadomienia Inspektora Ochrony lub innej Osoby Kontaktowej;

7) ADO jest zobowiązany w terminie nie późniejszym niż 30 dni od otrzymania żądania, udzielić osobie, której dane osobowe dotyczą, informacji o działaniach podjętych w związku z jej żądaniem;
8) W uzasadnionym przypadku, wyżej wskazany termin, może zostać przedłużony o kolejne 30 dni (nie więcej niż 60 dni od dnia otrzymania żądania) z uwagi na skomplikowany charakter żądania lub dużą ich liczbę. W takiej sytuacji ADO informuje osobę, której dane osobowe dotyczą, o przedłużeniu terminu wraz z podaniem przyczyn opóźnienia;
9) Komunikacja prowadzona z osobą, której dane osobowe dotyczą jak i realizacja żądań takiej osoby, są wolne od opłat, chyba że mają charakter nieuzasadniony lub są nadmierne w swojej treści np. ze względu na swój ustawiczny charakter. W takiej sytuacji Administrator jest uprawniony do pobrania rozsądnej opłaty, uwzględniającej administracyjne koszty prowadzenia komunikacji lub podjęcia żądanych działań. Administrator informuje osobę, której dane dotyczą o zasadach obliczania i wysokości opłaty;
10) Przed udzieleniem odpowiedzi na wniosek lub żądanie, Administrator, IOD lub inna wyznaczony pracownik zobowiązany jest do weryfikacji tożsamości osoby, której dane dotyczą.
11) Jeżeli Administrator ma uzasadnione wątpliwości co do tożsamości osoby, która złożyła żądanie, może zażądać dodatkowych informacji niezbędnych do potwierdzenia jej tożsamości (tj. wykorzystać dane osobowe, w których jest w posiadaniu do ustalenia tożsamości i weryfikacji osoby);

VII. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych:

1) Niezastosowanie się do prowadzonej przez ADO Polityki Ochrony Danych Osobowych, i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może zostać potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez zachowania okresu wypowiedzenia na podstawie art. 52 Kodeksu pracy;
2) Niezależnie od rozwiązania stosunku pracy osoby popełniające przestępstwo mogą zostać pociągnięte do odpowiedzialności karnej zwłaszcza na podstawie art. 107 ustawy o ochronie danych osobowych oraz art. 266 Kodeksu karnego;

VIII. Szkolenia osób upoważnionych do przetwarzania danych osobowych:

1) IOD prowadzi szkolenia dla pracowników upoważnionych do przetwarzania danych osobowych w przypadku:
   a) zmiany przepisów prawa odnoszących się do przetwarzania danych osobowych,
   b) zmiany obowiązującej w LPNT S.A dokumentacji ochrony danych;
   c) każdorazowo w związku z zatrudnieniem nowego pracownika, stażysty, praktykanta, wolontariusza itp.;
   d) na indywidualne polecenie ADO;
2) Tematyka szkoleń obejmuje:
   a) przepisy i instrukcje dotyczące ochrony danych osobowych, sporządzania i przechowywania ich kopii, niszczenia wydruków i zapisów na nośnikach,

b) sposoby ochrony danych przed osobami postronnymi i procedury udostępniania danych osobom, które one dotyczą,
c) obowiązki osób upoważnionych do przetwarzania danych osobowych,
d) zasady i procedury określone w polityce bezpieczeństwa informacji,
e) zmiany w przepisach o ochronie danych osobowych.

3) ADO może każdorazowo skorzystać z pomocy zewnętrznego wyspecjalizowanego podmiotu w zakresie przeprowadzenia szkolenia z obszaru ochrony danych osobowych.

IX. Procedura nadawania upoważnień do przetwarzania danych osobowych:

Do przetwarzania danych osobowych mogą mieć dostęp jedynie osoby posiadające pisemne upoważnienie do przetwarzania danych osobowych nadane przez Administratora Danych Osobowych.

1) Za przygotowanie upoważnienia do przetwarzania danych osobowych odpowiada pracownik ds. kadr oraz Inspektor Ochrony Danych Osobowych.
2) Zakres upoważnienia do przetwarzania danych osobowych ustalany jest każdorazowo przez bezpośredniego przełożonego, nowozatrudnionego pracownika w porozumieniu z Administratorem Danych Osobowych.
3) Bezpośredni przełożony przekazuje pracownikowi ds. kadr zakres obowiązków oraz zakres dostępu do zbiorów danych osobowych przetwarzanych do których powinien mieć dostęp nowy pracownik. Bezpośredni przełożony przekazuje również informacje o potrzebie nadania dostępu do systemów informatycznych oraz do poczty służbowej dla nowego pracownika.
4) Pracownik ds. kadr przekazuje informacje o potrzebie dostępu do systemów informatycznych oraz do poczty służbowej do Administratora Systemu Informatycznego.
5) Administrator Systemu Informatycznego nadaje dostępy, a w uzasadnionych przypadkach kontaktuje się z bezpośrednim przełożonym pracownika, w celu ustalenia szczegółów i doprecyzowania zakresu nadania planowanych dostępów. Po nadaniu odpowiednich dostępów ASI przekazuje informacje do pracownika ds. kadr.
6) Pracownik ds. kadr opracowuje dokument upoważnienia do przetwarzania danych osobowych i przedstawia go do podpisu Administratorowi Danych Osobowych (wzór upoważnienia znajduje się w załączniku do niniejszego dokumentu).
7) Administrator Danych Osobowych zatwierdza dokument upoważnienia. Podpisane upoważnienie do przetwarzania danych osobowych jest przechowywane w aktach osobowych pracownika, a jego kopia zostaje wydana pracownikowi.
8) W przypadku zmiany stanowiska i/lub zamiany zakresu obowiązków która wpływa bezpośrednio na rodzaj i zakres przetwarzanych danych osobowych, pracownik ds. kadr jest zobowiązany do przygotowania nowego upoważnienia lub jego aktualizacji.

X. Procedura postępowania w przypadku incydentów i naruszeń ochrony danych osobowych:

1) Naruszeniem bezpieczeństwa danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawniania danych osobowych, udostępniania lub umożliwiania dostępu do nich osobom

nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

a) nieautoryzowanego dostępu do danych,
b) nieautoryzowane modyfikacje lub zniszczenie danych,
c) udostępnianie danych nieautoryzowanym podmiotom,
d) nielegalne ujawnianie danych,
e) pozyskiwanie danych z nielegalnych źródeł;

2) W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie powiadomić o tym fakcie IOD oraz bezpośredniego przełożonego, a następnie stosować się do podjętych przez nich decyzji;
3) Zgłoszenie naruszenia ochrony danych osobowych powinno zawierać:
   a) opis symptomów naruszenia ochrony danych osobowych,
   b) określenie sytuacji i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych,
   c) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę tego naruszenia,
   d) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.
4) IOD lub inna upoważniona przez niego osoba podejmuje wszelkie działania mające na celu:
   a) minimalizację negatywnych skutków zdarzenia,
   b) wyjaśnienie okoliczności zdarzenia,
   c) zabezpieczenie dowodów zdarzenia,
   d) umożliwienie dalszego bezpiecznego przetwarzania danych.
5) W celu realizacji procedury postępowania w przypadku naruszenia bezpieczeństwa danych osobowych IOD lub inna upoważniona przez niego osoba ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:
   a) żądania wyjaśnień od pracowników,
   b) korzystania z pomocy konsultantów (w tym zewnętrznych podmiotów),
   c) nakazanie przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.
   d) polecenia IOD wydawane w czasie realizacji zadań wynikających z Polityki Ochrony Danych są priorytetowe i powinny być wykonywane w pierwszej kolejności, zapewniając ochronę danych osobowych.
6) Odmowa udzielenia wyjaśnień lub współpracy z IOD traktowana będzie jako naruszenie obowiązków pracowniczych.
7) IOD po zagrożeniu sytuacji nadzwyczajnej opracowuje raport, w którym przedstawia przyczyny i skutki zdarzenia oraz zawiera rekomendacje ograniczające możliwość wystąpienia zdarzenia w przyszłości.
8) Nieprzestrzeganie zasad określonych w Polityce Ochrony Danych stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej określonej w Kodeksie Pracy.
9) Jeżeli skutkiem działania określonego w ustępie 9 jest szkoda, sprawca ponosi odpowiedzialność materialną na warunkach określonych w Kodeksie Pracy oraz Prawa Cywilnego.

10) W przypadku stwierdzenia naruszenia ochrony danych osobowych, o którym mowa w art. 4 pkt 12) RODO skutkującego 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, którym jest Prezes Urzędu Ochrony Danych Osobowych.
11) Wykonując działania określone w pkt. 11 ADO informuje osoby dotknięte naruszeniem o jego potencjalnych, negatywnych skutkach oraz przekazuje im zalecenia dotyczące ochrony prywatności.

XI. Przegląd polityki ochrony danych osobowych:

1) Polityka Ochrony Danych Osobowych powinna być poddawana przeglądowi przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych IOD może zarządzić przegląd polityki bezpieczeństwa informacji stosownie do potrzeb;
2) Do kontroli stanu ochrony danych osobowych w LPNT S.A upoważnieni są:
   a) Administratora Danych Osobowych;
   b) Inspektor Ochrony Danych;
   c) Administrator Systemu Informatycznego;
3) IOD analizuje, czy polityka i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:
   a) zmian w budowie systemu informatycznego,
   b) zmian organizacyjnych ADO, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,
   c) zmian w obowiązującym prawie.
4) Raz do roku kontroli podlegają wszystkie systemy informatyczne przetwarzające dane osobowe oraz zabezpieczenia fizyczne i bezpieczeństwo osobowe;
5) ASI przygotowuje plan kontroli uwzględniając zakres oraz potrzeby fizyczne, czasowe i osobowe;
6) Kontroli podlega sprzęt, system teleinformatyczny, realizacja zabezpieczeń przez pracowników oraz przestrzeganie polityki bezpieczeństwa informacji;
7) IOD po uzgodnieniu z ADO może, stosownie do potrzeb, przeprowadzić wewnętrzny audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
8) Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z ADO i ASI. Zakres, przebieg i rezultaty audytu dokumentowane są na piśmie w protokole podpisywanym przez IOD i ASI i przedstawiane w formie pisemnej do wiadomości ADO;
9) ADO biorąc pod uwagę wnioski administratorów, może zlecić przeprowadzenie audytu zewnętrznego realizowanego przez wyspecjalizowany podmiot;

XII. Postanowienia końcowe:

1) Niniejsza Polityka Ochrony Danych jest dokumentem wewnętrznym i nie może być udostępniania osobom nieupoważnionym w żadnej formie.
2) Użytkownik zobowiązany jest złożyć oświadczenie o tym, iż został zaznajomiony z przepisami RODO, ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami

wykonawczymi oraz instrukcjami i procedurami obowiązującymi u Administratora Danych Osobowych, a także o zobowiązaniu się do ich przestrzegani;.

3) Oświadczenie potwierdzające zaznajomienie użytkownika z przepisami RODO, ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami i procedurami obowiązującymi u Administratora Danych Osobowych, a także o zobowiązaniu się do ich przestrzegania, przechowywane jest w aktach osobowych pracownika;
4) Wszystkie regulacje dotyczące systemów informatycznych określone w Polityce Ochrony Danych dotyczą również przetwarzania danych osobowych w bazach danych prowadzonych w jakiejkolwiek innej formie;
5) Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce Ochrony Danych;
6) Niezastosowanie się do prowadzonej przez Administratora Danych Osobowych, której założenia określa niniejszy dokument i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym.

XII. Spis załączników:

1) **Załącznik nr 1 – Wzór upoważnienia do przetwarzania danych osobowych**
2) **Załącznik nr 2 – Wzór oświadczenia o zachowaniu danych w poufności**
3) **Załącznik nr 3 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych**
4) **Załącznik nr 4 – Wzór rejestru incydentów i naruszeń ochrony danych osobowych**
5) **Załącznik nr 5 – Wzór rejestru udostępnień danych osobowych**
6) **Załącznik nr 6 – Wzór Rejestru Czynności Przetwarzania Danych Osobowych**

UPOWAŻNIENIE/ANULOWANIE UPOWAŻNIENIA* Nr .....

do przetwarzania danych osobowych oraz obsługi systemu informatycznego i urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

Nadaję / odbieram* upoważnienie Pani/Panu:

.....,
(imię i nazwisko nr PESEL)

.....
(nazwa stanowiska)

do przetwarzania danych osobowych w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku tj. określonych w zawartej umowie.

Zobowiązuję Panią*/Pana* do przestrzegania przepisów dotyczących ochrony danych osobowych oraz wdrożonych do stosowania przez Administratora Danych Osobowych „Polityki Ochrony Danych Osobowych" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do zachowania w tajemnicy danych osobowych i sposobu ich zabezpieczenia również po odwołaniu upoważnienia, a także ustaniu stosunku pracy.

(data, podpis Administratora Danych Osobowych)	***(podpis osoby upoważnionej)***

**niepotrzebne skreślić*

.....
(imię i nazwisko)

.....
(miejscowość, data)

OŚWIADCZENIE O ZACHOWANIU DANYCH W POUFNOŚCI

Oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności ogólnego Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r. oraz Ustawy o Ochronie Danych Osobowych oraz z dokumentacją ochrony danych osobowych, na która składa się „Polityka Ochrony Danych Osobowych" oraz „Instrukcja Zarządzania Systemem Informatycznym".

W szczególności zobowiązuję się do:

- przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach i obowiązkach służbowych,
- zachowania w tajemnicy danych osobowych do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań powierzonych przez Administratora,
- niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Administratora,
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
- ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Administratora za naruszenie przepisów RODO oraz ustawy o ochronie danych osobowych z dnia 10 maja 2018 r.

.....
(podpis oświadczającego)

Ewidencja osób upoważnionych do przetwarzania danych osobowych
Lubelski Park Naukowo Technologiczny S.A.

L.P.	Nr upoważnienia	Imię	Nazwisko	Stanowisko	Data nadania upoważnienia	Data ustania upoważnienia	Data modyfikacji upoważnieniaIdenfytikator	Identyfikator

Rejestr incydentów i naruszeń ochrony danych osobowych
Lubelski Park Naukowo Technologiczny S.A.

L.P.	Data wystąpienia incydentu	Rodzaj incydentu	Osoba zgłaszająca	Opis zdarzenia	Skutki incydentu / naruszenia	Podjęte działania	Czy poinformowano osoby dotknięte incydentem/ naruszeniem?	Czy zawiadomiono UODO?

Rejestr Udostępnień Danych Osobowych Lubelski Park Naukowo Technologiczny S.A.				
L.P.	Nazwa podmiotu	Zakres udostępnienia	Podstawa udostępnienia	Data udostępnienia

Załącznik nr 2 do Zarządzenia Prezesa Zarządu Lubelskiego Parku Naukowo-Technologicznego S.A. z dnia 25.10.2021 r. ws. wdrożenia dokumentacji ochrony danych osobowych.

Instrukcja Zarządzania Systemem Informatycznym w Lubelskim Parku Naukowo Technologicznym S.A.

LUBELSKI PARK NAUKOWO TECHNOLOGICZNY

Wersja nr 1		**Pieczęć:**	
Opracował:	**Data:**	**Zatwierdził:**	**Data:**
Inspektor Ochrony Danych: Bartosz Starzomczyk		Administrator Danych Osobowych Prezes Zarządu Magdalena Stachyra	

Spis treści

I. Wstęp

Instrukcja Zarządzania System Informatycznym oraz Polityka Ochrony Danych Osobowych wraz z załącznikami, są podstawowymi dokumentami opisującym zasady ochrony danych osobowych stosowanymi przez Lubelski Park Naukowo Technologiczny S.A. (dalej LPNT S.A.) w celu spełnienia wymagań ochrony danych osobowych w rozumieniu Art. 24 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, dalej „RODO"). oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

Dokumentacja ochrony danych w LPNT S.A. opisuje sposób przetwarzania danych osobowych oraz zastosowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

Celem wdrożenia Instrukcji Zarządzania Systemem Informatycznym jest także określenie podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz wymagań w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.

Każda osoba mającą dostęp do danych osobowych z upoważnienia LPNT S.A., ma obowiązek zapoznania się z Polityką Ochrony Danych Osobowych. Dotyczy to w szczególności pracowników zatrudnionych przez Administratora Danych. Osoby, o których mowa w zdaniu poprzednim, mają obowiązek złożenia na piśmie oświadczenia o zapoznaniu się z treścią Polityki oraz zachowaniu danych osobowych w tajemnicy.

II. Definicje:

1) **Administrator Danych** – Lubelski Park Naukowo Technologiczny S.A. z siedzibą ul. Bohdana Dobrzańskiego 3, 20-262 Lublin;
2) **Administrator Systemu Informatycznego (ASI)** – osoba wyznaczona przez ADO do zarządzania określonym systemem informatycznym, odpowiadająca za jego bezpieczeństwo oraz sprawne i ciągłe działanie;
3) **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
4) **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych;
5) **Użytkownik** – osoba upoważniona przez Administratora Danych do przetwarzania danych osobowych;
6) **Zbiór danych** – każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów;

7) **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na Danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie w formie tradycyjnej oraz w systemach informatycznych;
8) **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie Przetwarzania danych osobowych w takim systemie;
9) **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (Użytkownikowi) w razie przetwarzania danych osobowych w takim systemie
10) **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (Użytkownika).

III. Informacje ogólne:

1) Administrator Danych Osobowych (ADO) wyznacza Administratora Systemów Informatycznych (ASI) w drodze pisemnego upoważnienia lub zarządzenia. ADO może powołać więcej niż jednego ASI;
2) ASI jest odpowiedzialny za przestrzeganie zasad bezpieczeństwa przetwarzania danych osobowych w zakresie systemu informatycznego służącego do tego celu;
3) Do obowiązków ASI należy także kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej i systemu informatycznego;
4) Obowiązkiem ASI jest również zabezpieczenie sprzętu komputerowego przed nieuprawnionym dostępem oraz przeprowadzanie analizy ryzyka uwzględniającej realne zagrożenia dla systemu informatycznego;
5) W zakresie przestrzegania zasad określonych w niniejszym dokumencie oraz Polityce Ochrony Danych Osobowych, ASI współpracuje z Inspektorem Ochrony Danych (IOD) i przekazuje mu wszelkie informacje niezbędne do kontroli zgodności stanu faktycznego z przepisami ochrony danych osobowych.

IV. Nadawanie i rejestrowanie uprawnień do systemów informatycznych oraz przetwarzania danych w systemie informatycznym:

4.1. Nadawanie uprawnień:

1) Przed nadaniem dostępu do systemu informatycznego służącego do przetwarzania danych osobowych każdy użytkownik (pracownik, stażysta, kontraktor) zostaje zapoznany przez Inspektora Ochrony Danych (IOD) z obowiązującymi zasadami i przepisami o ochronie danych osobowych;
2) Przed uzyskaniem dostępu określonego w pkt 1) użytkownikowi zostaje nadane upoważnienie do przetwarzania danych osobowych określone w Załączniku nr 1 do *Polityki Ochrony Danych Osobowych*, jednocześnie użytkownik podpisuje określone w Załączniku nr 2 Oświadczenie o zachowaniu danych w poufności.

3) Dostęp do systemu informatycznego każdy użytkownik uzyskuje na wniosek bezpośredniego przełożonego skierowany do pracownika ds. kadr, który przekazuje informacje do Administratora Systemu Informatycznego.
4) Rejestracja użytkownika, polega na nadaniu niepowtarzalnego identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.
5) Rejestracji użytkowników w systemach informatycznych dokonuje ASI którzy przekazują informację o nadanym użytkownikowi identyfikatorze, Administratorowi Danych Osobowych oraz Inspektorowi Ochrony Danych.
6) Uprawnienia użytkownikom systemu zostają określone w Upoważnieniu do przetwarzania danych osobowych stanowiącym Załącznik nr 1 do Polityki Ochrony Danych Osobowych.
7) Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych, zarejestrowana jako użytkownik w tym systemie przez Administratora Systemu na wniosek ADO.

4.2. Wyrejestrowywanie uprawnień:

1) Wyrejestrowania użytkownika z systemu informatycznego dokonuje Administrator Systemu na wniosek pracownika ds. kadr, IOD lub bezpośrednio Administratora Danych.
2) Wyrejestrowanie, o którym mowa w ust.1, może mieć charakter czasowy lub trwały.
3) Wyrejestrowanie następuje poprzez:
   a) Zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
   b) Usuniecie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).
4) Czasowe wyrejestrowanie użytkownika z systemu informatycznego musi nastąpić w razie:
   a) nieobecności użytkownika pracy trwającej dłużej niż 30 dni kalendarzowych,
   b) zawieszenia w pełnieniu obowiązków służbowych,
   c) wypowiedzenia umowy o pracy,
   d) wszczęcia postepowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych osobowych.
5) Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśniecie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.
6) O nieobecnościach (np. urlop czy zwolnienie lekarskie, itp.), zawieszeniu w pełnieniu obowiązków służbowych, wypowiedzeniu umowy czy postepowaniu dyscyplinarnym w stosunku do pracownika informuje (np. drogą e-mailową) Administratora Systemu osoba zajmującą się kadrami lub bezpośrednio ADO.
7) Osoby zatrudnione na czas określony wszystkie uprawnienia otrzymują do momentu ustania zatrudnienia. W przypadku przedłużenia stosunku pracy pracownik zachowuje uprawnienia po okazaniu umowy o pracę lub innego dokumentu stwierdzającego kontynuację zatrudnienia.
8) O zmianie zakresu uprawnień, ADO lub kierownik komórki organizacyjnej informuje Inspektora Ochrony Danych oraz Administratora Systemu Informatycznego wypełniając stosownie upoważnienie do przetwarzania danych osobowych.

V. Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem:

5.1 Identyfikator:

1) Identyfikator i hasło użytkownika są podstawowym elementem ochrony danych osobowych przetwarzanych w systemach baz danych osobowych.
2) Identyfikator składa się z minimum czterech znaków, z których pierwszy odpowiada pierwszej literze imienia użytkownika, a kolejne – literom jego nazwiska (w przypadku nazwisk dwuczłonowych używa się liter członu pierwszego).
3) W identyfikatorze pomija się polskie znaki diakrytyczne.
4) W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika administrator systemu, za zgodą administratora bezpieczeństwa informacji, nadaje inny identyfikator, odstępując od zasady określonej w pkt2.
5) Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu nie może być przydzielony innej osobie.

5.2 Hasła:

1) Hasło musi składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem.
2) System informatyczny wymusza zmianę hasła co 30 dni;
3) Administrator Systemu Informatycznego lub IOD może, w uzasadnionych sytuacjach, polecić wcześniejsze dokonanie zmiany hasła przez użytkownika.
4) Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowych z identyfikatora lub hasła innego użytkownika.
5) Przy wpisywaniu hasło nie może być wyświetlane na ekranie.
6) Użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności.
7) Zabrania się przechowywania haseł w miejscach, do których dostęp jest niezabezpieczony oraz zapisywanie go w miejscach ogólnie widocznych.
8) Komputery nie pracujące w sieci musza mieć hasło założone na BIOS.

5.3 Hasła administratorów systemu:

1) Hasła poziomu administratora do wszystkich wykorzystywanych systemów i aplikacji zostały zdeponowane u Administratora Danych Osobowych i są przechowywane w miejscu niedostępnym dla osób nieupoważnionych.
2) Hasła poziomu administratora powinny spełniać minimalne wymagania określone w niniejszym dokumencie, jednak zaleca się aby ich złożoności i długość była dłuższa od standardowych.

VI. Procedury rozpoczęcia, zawieszenia i zakończenia pracy, przeznaczone dla użytkowników systemu:

6.1 Tryb pracy na poszczególnych stacjach roboczych:

1) Pracownik przed przystąpieniem do pracy powinien dokonać oględzin pomieszczenia i zwrócić uwagę na ewentualne ślady, które mogłyby świadczyć o nieautoryzowanym naruszeniu zabezpieczeń.
2) Każdy użytkownik może zalogować się do systemu informatycznego tylko w godzinach pracy określonych w Regulaminie Pracy. Poza tymi godzinami logowanie do systemu jest zabronione
3) Na pracę poza standardowymi godzinami musi wyrazić zgodę ADO lub kierownik poszczególnej komórki organizacyjnej posiadający stosowne upoważnienie ADO.
4) Rozpoczęcie pracy na stacji roboczej następuje poprzez włączenie komputera, a następnie wprowadzenie indywidualnego, znanego tylko użytkownikowi, hasła i identyfikatora.
5) W systemie informatycznym stosuje się podwójną autoryzację użytkownika. Pierwszej autoryzacji należy dokonać w momencie uzyskania dostępu do serwera, podając login użytkownika i hasło. Drugiej autoryzacji należy dokonać uruchamiając program użytkowy, podając login użytkownika i hasło.
6) W pomieszczeniu, w którym przetwarzane są dane osobowe, mogą znajdować się osoby postronne tylko za zgodą i w obecności użytkownika.
7) Przed osobami postronnymi należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać podgląd), wydruki lezące na biurkach oraz dokumenty w szafach.
8) Monitory komputerów wyposażone są w wygaszacze ekranu włączające się po 15 minutach od przerwania pracy. Wznowienie wyświetlenia następuje po wprowadzeniu odpowiedniego hasła.
9) W przypadku opuszczenia stanowiska pracy użytkownik obowiązany jest aktywować wygaszacz ekranu lub w inny sposób zablokować stację roboczą. Użytkownikowi nie wolno dokonywać modyfikacji w konfiguracji systemu komputera.
10) Obowiązuje zakaz robienia kopii całych zbiorów danych; całe zbiory danych mogą być kopiowane tylko przez administratora systemu lub automatycznie przez system, z zachowaniem procedur ochrony danych osobowych.
11) Obowiązuje zakaz wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej.
12) Zakończenie pracy na stacji roboczej następuje po prawidłowym zamknięciu wszystkich aplikacji, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera.
13) Przed opuszczeniem miejsca pracy należy:
    a) schować do zamykanych na klucz szaf wszelkie wykonane wydruki zawierające dane osobowe lub zniszczyć w niszczarce zbędne wydruki pomocnicze i wadliwe:
    b) schować do zamykanych na klucz szaf wszelkie dokumenty zawierające dane osobowe,
    c) umieścić klucze do szaf w ustalonym, przeznaczonym do tego miejscu,
    d) zamknąć okna.
14) Opuszczając miejsce pracy, należy zamknąć za sobą drzwi na klucz.

6.2 Tryb pracy na komputerach przenośnych:

1) Tylko osoby posiadające upoważnienie Administratora Danych Osobowych mogą przetwarzać dane osobowe na komputerach przenośnych powierzonych i należących do ADO.
2) Przed rozpoczęciem przetwarzania danych osobowych na urządzeniach przenośnych, pamięć tych urządzeń powinna zostać zaszyfrowana przy pomocy aktualnie dostępnych i uznanych metod.
3) Użytkownicy, którym zostały powierzone komputery przenośne, powinni chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych, szczególną ostrożność należy zachować podczas ich transportu.
4) Użytkownicy, którzy przetwarzają dane osobowe na komputerach przenośnych mają zakaz pozostawiania urządzeń bez nadzoru np. w autach.
5) Obowiązuje zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone.
6) Praca na komputerze przenośnym możliwa jest po wprowadzeniu indywidualnego identyfikatora użytkownika oraz hasła.
7) Użytkownicy są zobowiązani zmieniać hasła w komputerach przenośnych nie rzadziej niż raz na 30 dni.
8) Obowiązuje zakaz samodzielnej modernizacji oprogramowania i sprzętu w powierzonych komputerach przenośnych. Wszelkie zmiany mogą być dokonywane tylko pod nadzorem administratora systemu, stosownie do wymagań niniejszej instrukcji. W razie wystąpienia usterek w pracy komputerów przenośnych lub w razie wystąpienia konieczności aktualizacji ich oprogramowania należy zgłosić to Administratorowi Systemu.
9) Komputery przenośne wyposażone są w odpowiednie programy ochrony antywirusowej, których aktualizację sugeruje automatycznie system.

VII. Procedury tworzenia kopii zapasowych danych oraz programów i narzędzi programowych służących do przetwarzania danych osobowych:

7.1 Zasady tworzenia kopii zapasowych:

1) Nadzór nad wykonywaniem kopii zapasowych sprawuje ASI;
2) Kopie baz danych programów dziedzinowych wykonywane są automatycznie i zapisywane na serwerze;
3) W związku z wykorzystywaniem usługi Exchange, kopie zapasowe maili przechowywane są na serwerze dostawcy usługi, oraz w zakresie indywidualnych użytkowników, na ich komputerach służbowych w programie Outlook;

7.2 Procedury tworzeni kopii zapasowych:

1) Każdy pracownik przetwarzający dane osobowe lokalnie lub na komputerze przenośnym zobowiązany jest do wykonywania kopii tych zbiorów na dysk serwera, przypisany danemu użytkownikowi, na koniec dnia pracy.
2) Kopię taką zobowiązany jest również wykonać przed każdorazowym wyniesieniem komputera przenośnego poza teren przetwarzania danych.

3) Za sporządzanie kopii danych zgromadzonych na serwerze odpowiedzialny jest administrator systemu lub osoba przez niego upoważniona.
4) W celu zapewnienia poprawności wykonywanych kopii bezpieczeństwa należy je poddawać cyklicznym testom. Próba polega na odtworzeniu danych w warunkach testowych i sprawdzeniu, czy jest możliwość odczytania danych.
5) Zaleca się, aby użytkownicy przechowywali dane na zaszyfrowanych urządzeniach z wykorzystaniem usługi MS OneDrive;

7.3 Przechowywanie kopii zapasowych:

1) Kopie zapasowe danych w systemach informatycznych obejmują serwer AD, serwer ERP oraz dane archiwum.
2) Ze względu na dużą ilość danych kopie bezpieczeństwa tworzone są na dyskach serwera backup'owego.
3) Zaleca się przechowywanie kopii zapasowych w pomieszczeniach innych niż przeznaczone do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu, co najmniej w dwóch odrębnych od siebie lokalizacjach.
4) Kopie zapasowe powinny regularnie testowane pod względem poprawności ich wykonania – nie rzadziej niż raz na rok.
5) Nośniki zawierające kopie zapasowe zbiorów danych przekazane do archiwum zakładowego należy sprawdzać pod względem ich działania.

7.4 Likwidacja nośników zawierających kopie zapasowe:

1) Nie należy magazynować zbędnych plików i wydruków, kopie bezpieczeństwa po upływie okresu przechowywania muszą być skasowane lub fizycznie zniszczone w sposób uniemożliwiający odczytanie danych.
2) Kontrolę nad niszczeniem zbędnych wydruków i innych dokumentów zawierających dane osobowe powierza się kierownikom poszczególnych komórek organizacyjnych.
3) Każdy zbędny dokument zawierający takie dane powinien zostać niezwłocznie zniszczony w przygotowanej do tego niszczarce dokumentów.
4) Za niszczenie nośników elektronicznych odpowiedzialny jest ASI, który powinien odpowiednio zabezpieczyć nośniki wycofane z użytkowania.
5) Nośniki zawierające nieaktualne kopie danych, będące poza wykazem cyklicznych kopii, likwiduje się. W przypadku nośników jednorazowych, takich jak płyty CD-R, DVD-R, likwidacja polega na ich fizycznym zniszczeniu w taki sposób, by nie można było odczytać ich zawartości. Nośniki wielorazowego użytku, takie jak dyski twarde można wykorzystać ponownie do celów przechowywania kopii bezpieczeństwa po uprzednim usunięciu ich zawartości.
6) Nośniki wielorazowego użytku nienadające się do ponownego użycia należy zniszczyć fizycznie w sposób uniemożliwiający odczyt zapisanych wcześniej danych.
7) Administrator Danych Osobowych wyznacza osobę odpowiedzialną za archiwizację i prowadzenie archiwum zakładowego.

VIII. Przechowywanie elektronicznych nośników informacji zawierających dane osobowe:

1) Zbiory danych przechowywane są na serwerze obsługującym system informatyczny Administratora Danych Osobowych. Wszelkie dane przetwarzane w pamięci poszczególnych stacji roboczych oraz komputerów przenośnych są niezwłocznie umieszczane w odpowiednich miejscach na serwerze, przydzielonych każdemu użytkownikowi przez ASI.
2) W przypadku przetwarzania zbiorów danych osobowych przez firmy zewnętrzne ich bezpieczeństwo zagwarantowane jest stosowną umową.
3) Zabrania się przetwarzania zbiorów danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych i innych oraz ich przesyłania pocztą elektroniczną.
4) W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym na wyznaczonym w tym celu stanowisku komputerowym oraz do oznakowania tego nośnika.
5) Nośniki magnetyczne raz użyte do przetwarzania danych osobowych nie mogą być wykorzystywane do innych celów mimo usunięcia danych i podlegają ochronie w trybie niniejszej instrukcji.
6) Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione do przetwarzania danych osobowych.

IX. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego:

1) Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania zainstalowanego na serwerach, stacjach roboczych oraz komputerach przenośnych przez Administratora Systemu Informatycznego.
2) Oprogramowanie, o którym mowa w pkt1, sprawuje ciągły nadzór (praca w tle) nad pracą systemu i jego zasobami oraz serwerem i stacjami roboczymi.
3) Niezależnie od ciągłego nadzoru, o którym mowa w pkt 2, Administrator Systemu przeprowadza kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również na serwerze i stacjach roboczych.
4) Do obowiązków ASI należy aktualizacja oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów, dokonywanych przez to oprogramowanie.
5) Użytkownik jest obowiązany zawiadomić ASI o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.
6) Użytkownicy mogą korzystać z zewnętrznych nośników danych zawierających dane służbowe, pochodzących z pewnego źródła po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym.

X. Kontrola nad wprowadzaniem, dalszym przetwarzaniem i udostępnianiem danych osobowych:

1) System informatyczny administratora danych umożliwia automatycznie:
   a) przypisanie wprowadzanych danych użytkownikowi (identyfikatorowi użytkownika), który te dane wprowadza do systemu,
   b) sygnalizację wygaśnięcia czasu obowiązywania hasła dostępu do stacji roboczej (dotyczy to także komputerów przenośnych),
   c) sporządzenie i wydrukowanie dla każdej osoby, której dane są przetwarzane w systemie, raportu zawierającego:
   d) datę pierwszego wprowadzenia danych do systemu administratora danych,
   e) identyfikator użytkownika wprowadzającego te dane,
   f) źródła danych – w przypadku zbierania danych nie od osoby, której one dotyczą,
   g) informacje o odbiorcach danych, którym dane osobowe zostały udostępnione,
2) Odnotowanie informacji, o których mowa w pkt 1 następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

XI. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych:

1) Przeglądu i konserwacji systemu dokonuje Administrator Systemu Informatycznego na bieżąco.
2) Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale ASI nie rzadziej niż raz na miesiąc.
3) Zapisy logów systemowych powinny być przeglądane wyrywkowo przez ASI codziennie oraz każdorazowo po wykryciu naruszenia zasad bezpieczeństwa.
4) Kontrole i testy przeprowadzane przez Inspektora Ochrony Danych oraz ASI powinny obejmować zarówno dostęp do zasobów systemu, jak i profile oraz uprawnienia poszczególnych użytkowników.

XII. Naprawy urządzeń komputerowych z chronionymi danymi osobowymi:

1) Wszelkie naprawy urządzeń komputerowych oraz zmiany w systemie informatycznym Administratora Danych Osobowych przeprowadzane są przez ASI lub przez specjalistyczne firmy, z którymi zawarto odpowiednie umowy, pod nadzorem ASI.
2) Naprawy i zmiany w systemie informatycznym Administratora Danych Osobowych przeprowadzane przez serwisanta prowadzone są pod nadzorem ASI w siedzibie ADO, po uprzednim nieodwracalnym usunięciu danych w nich przetwarzanych, a jeśli wiązałoby się to z nadmiernymi utrudnieniami, to po podpisaniu umów powierzenia przetwarzania danych osobowych.
3) Jeśli nośnik danych (np. dysk, płyta) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć mechanicznie np. w niszczarce.

XIII. Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego:

1) Użytkownik zobowiązany jest zawiadomić Inspektora Ochrony Danych i Administratora Systemu Informatycznego o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności o:
   a) naruszeniu hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzenia hasła),
   b) częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień,
   c) braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera,
   d) wykryciu wirusa komputerowego,
   e) zauważeniu elektronicznych śladów próby włamania do systemu informatycznego,
   f) znacznym spowolnieniu działania systemu informatycznego,
   g) podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe,
   h) zmianie położenia sprzętu komputerowego,
   i) zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf.
2) Inspektor Ochrony Danych oraz Administrator Systemu Informatycznego po otrzymaniu zawiadomienia, o którym mowa w pkt 1, powinni:
   a) Przeprowadzić postepowanie wyjaśniające w celu ustalenia okoliczności naruszenia ochrony danych osobowych,
   b) Podjąć działania chroniące system przed ponownym naruszeniem,
   c) W przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu sporządzić raport naruszenia bezpieczeństwa systemu informatycznego i przekazać jego kopię administratorowi danych osobowych.
3) Inspektor Ochrony Danych w uzgodnieniu z Administratorem Systemu Informatycznego może zarządzić, w razie potrzeby, odłączenie części systemu dotkniętej incydentem od pozostałej części systemu informatycznego.
4) W razie odtwarzania danych z kopii zapasowych ASI zobowiązany jest upewnić się, że odtwarzane dane zapisane zostały przed wystąpieniem incydentu (dotyczy to zwłaszcza przypadków infekcji wirusowej i ataków typu ransomware).
5) ADO po zapoznaniu się z raportem z naruszenia, podejmuje decyzję o dalszym trybie postepowania, powiadomieniu właściwych organów oraz podjęciu innych szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego administratora danych bądź zastosowaniu dodatkowych środków ochrony fizycznej.
6) IOD oraz ASI zobowiązani są do informowania Administratora Danych Osobowych o awariach systemu informatycznego, zauważonych przypadkach naruszenia niniejszej instrukcji przez użytkowników, a zwłaszcza o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami, nieprzestrzegania zasad używania oprogramowania antywirusowego, niewłaściwego wykorzystania sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych.
7) Inspektor Ochrony Danych oraz Administrator Systemu Informatycznego uczestniczą w procesie zarządzania ryzykiem dotyczącym systemu informatycznego i przetwarzanych w nim danych osobowych i innych danych zawierających informacje prawnie chronione.

8) ASI dokonuje raz w roku kontroli przestrzegania zasad użytkowania oraz zarządzania systemem informatycznym, której wyniki przekazuje Administratorowi Danych Osobowych.

XIV. Procedura postępowania na wypadek wystąpienia sytuacji awaryjnych w pomieszczeniach, w których przetwarzane są dane osobowe:

1) Sytuacją awaryjną w sprawach ochrony obiektów są sytuacje spowodowane uszkodzeniem instalacji ciepłowniczej, wodociągowej, elektrycznej, urządzeń i sieci telekomunikacyjnej, urządzeń zabezpieczenia technicznego w tym systemów alarmowych albo powstała na skutek pożaru, klęsk żywiołowych (burz i gwałtownych opadów atmosferycznych) bądź zdarzeń losowych stwarzających zagrożenie dla zdrowia i życia ludzi, mienia w tym nieprzewidzianego oddziaływania czynników zewnętrznych na zasoby systemu (sprzęt informatyczny służący do przetwarzania zbiorów danych osobowych). Sytuację awaryjną może spowodować również niepożądane działanie osób trzecich takie jak napad, kradzież, włamanie, działania terrorystyczne, niewłaściwa ingerencja ekipy remontowej.
2) W razie wystąpienia sytuacji awaryjnej należy:
   a) ocenić zaistniałą sytuację i stopień zagrożenia oraz wykonać przedsięwzięcia niecierpiące zwłoki np. wyprowadzenie ludzi z rejonu zagrożenia, udzielenie pierwszej pomocy przedlekarskiej osobom poszkodowanym, wyłączenie prądu elektrycznego itp.
   b) powiadomić o awarii właściwe służby ratunkowe i techniczne,
   c) powiadomić o zdarzeniu właściwych przełożonych,
   d) objąć wzmożoną ochroną zagrożony rejon obiektu mając na uwadze minimalizację skutków wystąpienia danego zdarzenia,
   e) po przybyciu służb ratunkowych wykonywać polecenia kierującego akcją ratowniczą,
   f) po zakończeniu działań sporządzić pisemną informację dla administratora danych szczegółowo opisującą przebieg zdarzeń.
3) Drogi ewakuacyjne, miejsce zbiórki oraz szczegółowy sposób postepowania w przypadku ewakuacji wynikającej z pożaru lub wystąpienia innej sytuacji awaryjnej określa Plan ochrony przeciwpożarowej.

XV. Postanowienia końcowe:

1) Instrukcja Zarządzania Systemem Informatycznym stanowi integralną część Polityki Ochrony Danych Osobowych.
2) W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.
3) Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się z niniejszą Instrukcją oraz złożyć stosowne oświadczenie, potwierdzające znajomość jej treści.
4) Niezastosowanie się do procedur określonych w niniejszej Instrukcji przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 kodeksu pracy.