**ZASADY POSTĘPOWANIA UŻYTKOWNIKA OBOWIĄZUJĄCE PODCZAS PRZETWARZANIA DANYCH OSOBOWYCH W SZKOLE PODSTAWOWEJ IM. ORŁA BIAŁEGO W MICHAŁÓWCE  
MICHAŁÓWKA 3, 08-400 GARWOLIN**

Niniejsze zasady stanowią wyciąg z najistotniejszych zapisów zawartych w Polityce bezpieczeństwa danych osobowych oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Obowiązują pracowników etatowych, osoby świadczące pracę na podstawie umowy cywilnoprawnej (współpracowników), kontrahentów i usługodawców wykonujących usługi wymagające dostępu do danych osobowych Administratora Danych, stażystów, praktykantów i wolontariuszy, którzy wykonują zadania lub realizują obowiązki związane z przetwarzaniem danych osobowych w Szkole Podstawowej im. Orła Białego w Michałówce (dalej: ADO)

**SPIS TREŚCI**

1 Zasady bezpiecznego użytkowania sprzętu IT 1

2 Zasady korzystania z oprogramowania 3

3 Zasady korzystania z Internetu ……………………………………………………………………… ..3

4 Polityka haseł ……………………………………………………………………………………….……..4

5 Zasady korzystania z poczty elektronicznej 4

6 Ochrona antywirusowa 5

7 Przestrzeganie zasad bezpieczeństwa podczas korzystania z elektronicznego sprzętu mobilnego…………………………………………………………………………………………………. .6

8 Nadawanie upoważnień i uprawnień do przetwarzania danych osobowych 6

9 Zasady rozpoczecia, zawieszenia i zakończenia pracy 7

10 Postepowanie z informatycznymi nośnikami zawierajacymi dane osobowe 7

11 Postępowanie z dokumentami papierowymi zawierającymi dane osobowe 7

12 Zasady czystego biurka i zasada czystego pulpitu……………………………………………………7

13Zapewnienie poufnosci danych osobowych…………………………………………………………….8

14 Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych   
 osobowych 8

15 Postępowanie dyscyplinarne 9

1. **Zasady bezpiecznego użytkowania sprzętu IT**
   1. Sprzęt IT służący do przetwarzania zbioru danych osobowych jest zasobem informatycznym rzeczywistym (sprzętowym) bądź wirtualnym. Zasób obejmuje serwery, komputery stacjonarne lub mobilne, wydzielone ich części (przestrzeń dyskowa, udział sieciowy), urządzenia peryferyjne i komunikacji elektronicznej (telefony komórkowe), informatyczne nośniki danych (dyskietki, dyski CD, DVD, Blu-ray, pamięci USB), drukarki.
   2. Użytkownik zobowiązany jest korzystać ze sprzętu informatycznego w sposób zgodny z jego przeznaczeniem i chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem. W przypadku zaistnienia takiego zdarzenia niezwłocznie zgłasza ten fakt przełożonemu.
   3. Samowolne otwieranie (demontaż) sprzętu IT, instalowanie bez zezwolenia przełożonego dodatkowych urządzeń lub podłączanie do zasobu informatycznego jakichkolwiek urządzeń o niepotwierdzonej legalności jest zabronione. Zabronione jest zdejmowanie plomb gwarancyjnych a także dokonywanie samowolnych zmian w konfiguracji sprzętowej.
   4. W przypadku konieczności zabrania do naprawy sprzętu zawierającego na dyskach twardych informacje chronione, dane te muszą być przez ADO, Informatyka lub osobę wyznaczoną przez ADO lub firmę serwisową wymontowane pod nadzorem odpowiedzialnego pracownika i pozostawione u użytkownika (zamontowane ponownie po dokonanie naprawy). W przypadku uszkodzenia dysku twardego zawierającego informacje chronione w sposób uniemożliwiający ich odzyskanie dysk taki należy zniszczyć w sposób uniemożliwiający ponowne odczytanie. Sposób trwałego usunięcia danych uzgodnić z ADO, Informatykiem lub osobą wyznaczoną przez ADO. Odrębnego postępowania wymaga sytuacja, gdy dysk jest na gwarancji.
   5. Zasady zabezpieczenia osobistego sprzętu komputerowego, danych oraz ich nośników (pen-drive, przenośny dysk twardy, dyskietki, taśmy, CD-ROM’y, karty pamięci itp. ) przed dostępem osób niepowołanych do zasobów informacyjnych obejmują:
      1. Wyłączenie albo wylogowanie się z używanych aktualnie systemów każdorazowo w sytuacji opuszczenia stanowiska pracy z komputerem (dla sprzętu PC zaleca się stosowanie aplikacji klasy save-screen (wygaszacz ekranu) z aktywną opcją „password” lub inne równoważne zabezpieczenie);
      2. Zabezpieczenie tworzonych przez siebie danych (plików) na własnych komputerach, okresowe przeglądanie ich zawartości i usuwanie danych zbędnych. Dane uznane przez użytkownika za szczególnie chronione np. dane osobowe muszą być przechowywane miejscach określonych przez ADO a ponadto sposób ich zabezpieczenia uzgodnić należy każdorazowo z ADO, Informatykiem lub osobą wyznaczoną przez ADO.
      3. Wykonywanie kopii bezpieczeństwa jest obowiązkiem użytkownika końcowego w przypadku tworzenia dokumentów w pamięci swojej stacji roboczej, poza zasobami sieciowymi udostępnionymi przez Administratora Danych, dla których wykonywane są kopie bezpieczeństwa centralnie przez uprawnionych pracowników;
      4. Asystowanie przy prowadzonych pracach serwisowych przy sprzęcie za który odpowiedzialność ponosi pracownik;
      5. Wnioskowanie (w ramach posiadanych kompetencji i zgodnie z uzgodnionymi i obowiązującymi w danym Projekcie procedurami) o dostęp do zasobów i usług dla przypadków rzeczywiście uzasadnionych (zasada „need to know” - minimum tego co konieczne);
      6. Niezwłoczne informowanie ADO o zmianach lub odebraniu wcześniej wnioskowanych przez użytkownika uprawnień (dostęp do systemów, aplikacji, folderów…)   
         w przypadku ustania przyczyn (zmiana stanowiska, komórki organizacyjnej, zakończenia pracy itp.);
      7. Udostępnianie własnych zasobów (dzielenie (share) dysków komputerów własnych) w sieci jedynie   
         w sytuacjach wyjątkowych i na czas możliwie najkrótszy tylko dla współpracowników w projekcie posiadających odpowiednie uprawnienia i upoważnienia, za zgodą odpowiedniego kompetentnego przełożonego. Za ewentualne skutki wynikłe z takiej sytuacji odpowiedzialny jest użytkownik.
   6. Korzystanie z wszelkiego rodzaju łącz i serwisów modemowych w czasie realizacji swoich obowiązków przy korzystaniu z bazy danych stanowiących informacje chronione, wymaga uzyskania zgody ADO. Użytkownik odpowiedzialny jest za wykorzystanie takich połączeń w sposób zgodny z otrzymanym pozwoleniem.
   7. Użytkowanie mobilnych nośników informatycznych do przetwarzania danych osobowych możliwe jest za zgodą przełożonego. Takie nośniki jak laptop, smartfon, tablet czy pen-drive jest przypisany imiennie do użytkownika i podlega ewidencjonowaniu jeśli zawiera dane osobowe. Zaleca się, by dostęp do składowanych tam danych osobowych wymuszał podanie indywidualnego hasła, PIN-u lub innego kodu dostępu. Fakt używania przenośnych informatycznych nośników danych do przetwarzania danych osobowych, wymaga zgłoszenia do ADO, Informatyka lub osoby wyznaczonej przez ADO, która prowadzi centralną ewidencję takich nośników.
   8. Pracownik użytkujący mobilny sprzęt informatyczny do wykonywania pracy na odległość (telepraca) przetwarzający dane osobowe, powinien posiadać zgodę kompetentnego przełożonego i na tej podstawie zgłosić zamiar wykonywania pracy zdalnej do ADO w celu zestawienia bezpiecznych kanałów do łączenia się z serwerem firmowym i bezpiecznego korzystania z zasobów firmowych. Użytkownik zachowuje szczególną ostrożność podczas transportu, przechowywania i użytkowania sprzętu IT poza obszarem bezpiecznego przetwarzania.
   9. Do podstawowych zasad bezpiecznego użytkowania informatycznego sprzętu mobilnego (komputery przenośne, urządzenia PDA – palmtopy, smartfony itp.) należy:
      1. Utrzymywanie w tajemnicy kodów PIN posiadanych kart SIM i kart tokenowych RSA;
      2. Stosowanie przygotowanych przez ADO mechanizmów zabezpieczających klasy firewall, zabezpieczeń antywirusowych i szyfrowania zawartości dysków;
      3. Stosowanie w uzgodnieniu z ADO, Informatykiem lub osobą wyznaczoną przez ADO dedykowanego mechanizmu ochrony danych chronionych, polegającego na synchronizacji katalogów na dyskach lokalnych z ich odpowiednikami na serwerach;
      4. Przestrzeganie zakazu aktywowania modemów i kart transmisji danych GSM z jednoczesnym wpięciem do sieci komputerowej;

1.9.5. Zakaz udostępnienia sprzętu osobom postronnym;

1.9.6. Niezwłocznego poinformowania ADO, Informatyka lub osoby wyznaczonej przez ADO w przypadku zagubienia lub kradzieży komputera, palmtopu czy karty tokenowej.

* 1. Zabronione jest podejmowanie prób włamywania się lub omijania zabezpieczeń, instalacji   
     i wykorzystywania oprogramowania penetracyjnego i skanującego. Zakaz obejmuje również instalację   
     i wykorzystywanie urządzeń aktywnych, dostępu do innych sieci.
  2. Zabronione jest przesyłanie za pośrednictwem sieci, danych niemających związku z wykonywanymi obowiązkami (w systemie poczty elektronicznej), powielania i przekazywania danych użytkownikom, których one nie dotyczą.

# Zasady korzystania z oprogramowania

* 1. Używanie jedynie oprogramowania pochodzącego z legalnych źródeł i zgodnie z warunkami udzielonej licencji. (na podstawie ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych. Użytkownicy oprogramowania wykorzystują udostępnione im zasoby informatyczne jedynie do celów służbowych związanych z ich działalnością zawodową.
  2. Instalowanie oprogramowania w zasobach informatycznych oraz wykonywanie kopii zapasowych oprogramowania może się odbywać na warunkach umowy licencyjnej oraz w zgodzie z przepisami ustawy   
     o prawie autorskim i prawach pokrewnych.
  3. Instalowanie lub używanie oprogramowania innego niż przekazanego bądź udostępnionego użytkownikom przez Administratora Danych, zwłaszcza prywatnie zakupionych dyskietek, płyt CD, programów ściąganych ze stron internetowych jak również odpowiadanie na samoczynnie pojawiające się reklamy internetowe jest zabronione.
  4. Użytkownik nie ma prawa do powielania danych lub programów zainstalowanych w komputerze przez administratora oprogramowania (licencji) na swoje własne potrzeby ani na potrzeby osób trzecich.
  5. Zabronione jest samowolne instalowanie oprogramowania i dokonywanie zmian w ustawieniach sieciowych komputera (np. zmiana nazwy czy przyznanego adresu IP, itp.). oraz aktywowanie modemów również tych stanowiących stały element konstrukcyjny urządzeń.
  6. Wyznaczony Informatyk (również z firmy zewnętrznej) lub osoba wyznaczona przez ADO jest zobowiązana do prowadzenia okresowych kontroli legalności oprogramowania.
  7. W przypadku podejmowania prób przełamywania lub omijania zabezpieczeń oprogramowania i sieci lub naruszenia któregokolwiek z powyższych postanowień, kierownik jednostki organizacyjnej ma prawo (bez uprzedzenia) zażądać usunięcia nielegalnie lub niewłaściwie zainstalowanego oprogramowania. Ponadto, niezależnie od odpowiedzialności dyscyplinarnej lub porządkowej może dochodzić naprawienia poniesionej szkody na podstawie kodeksu cywilnego.

1. **Zasady korzystania z Internetu**
   1. Korzystanie z zasobów sieci Internet dozwolone jest jedynie w zakresie związanym z wykonywaniem obowiązków służbowych.
   2. Wszystkie dane otrzymane poprzez Internet, w tym pocztą elektroniczną muszą być traktowane ze szczególną ostrożnością pod kątem obecności wirusów oraz ich autentyczności i prawdziwości.
   3. Korzystanie z aplikacji, usług i serwisów oferowanych przez Internet niesie ryzyko łatwej identyfikacji użytkownika.
   4. Przesyłanie danych (np. zestawień finansowych, danych osobowych, informacji stanowiących tajemnicę przedsiębiorstwa, strategii, projektów itp.), których przechwycenie może stanowić zagrożenie dla interesów lub prestiżu organizacji za pomocą zewnętrznej (internetowej) poczty elektronicznej bez specjalnych zabezpieczeń jest niedozwolone. Sposób zabezpieczeń (szyfrowanie) zostało opisane w pkt.4.
   5. Przechowywanie danych i korzystanie z kont pocztowych na serwerach zewnętrznych (w tym darmowych) jest niedopuszczalne.
   6. Pracodawca zastrzega sobie prawo do kontrolowania i monitorowania pracowników w zakresie sposobu korzystania przez nich z Internetu, w tym kontroli czasu spędzonego przez pracowników w Internecie oraz przestrzegania przez nich wyżej wymienionych zasad bezpieczeństwa.
   7. Umieszczanie w Internecie informacji zawierających dane osobowe kierownictwa, pracowników, klientów, dostawców lub kontrahentów, wymaga zgody zarówno osoby fizycznej, której dane dotyczą, jak i kierownika jednostki organizacyjnej.
   8. Pracodawca zastrzega sobie prawo do blokowania dostępu do niektórych portali, stron lub treści dostępnych za pośrednictwem Internetu bez uprzedzenia użytkowników.
2. **Polityka haseł**
   1. Użytkownik sam definiuje hasło dostępu zarówno do systemu operacyjnego, jak również do systemów   
      i aplikacji w których są przetwarzane dane osobowe. Hasło musi składać się co najmniej z **8 znaków** (wielkich i małych liter oraz z cyfr lub znaków specjalnych). Użytkownik osobiście odpowiada za utrzymanie hasła w tajemnicy (zakaz ujawniania innym osobom).
   2. Zmiana hasła następuje nie rzadziej, niż co **30 dni** oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione. Zmianę hasła może być wymuszana przez system IT. Jeśli system nie posiada takiej funkcji, to użytkownik jest zobowiązany do jego zmiany we własnym zakresie.
   3. Należy unikać stosowania tego samego hasła w przypadku posiadania uprawnień do wielu zasobów, systemów lub aplikacji.
   4. Użytkownik jest zobowiązany się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
   5. Zabronione jest pozostawianie haseł w formie jawnej w postaci, zbiorów (plików) tekstowych, nalepek na monitorach itp.
   6. Hasła nie mogą być zbyt łatwe do odgadnięcia. W szczególności nie należy ich tworzyć z powszechnie używanych pojęć i znaczeń, jak np. daty, imiona, nazwiska, inicjały stanowisk, numery rejestracyjne samochodów, numery telefonów, itp.
   7. W razie konieczności przekazania hasła w celach serwisowych (naprawy lub instalacji oprogramowania) dokonania jego zmiany niezwłocznie po zakończeniu takich prac.
   8. Należy staranni wykonywać proces logowania (następujące po sobie błędne wprowadzenie hasła traktowane jest przez systemy jako próby włamania, skutkiem czego następuje czasowa lub całkowita blokada konta użytkownika – w takich przypadkach na żądanie administratora systemu użytkownik zobowiązany jest do złożenia dodatkowych wyjaśnień**).**
   9. Aktywacja zablokowanych kont (zmiana hasła), zmiany udostępnień do folderów, serwisów drukarkowych itp. wymagają zgłoszenia tego faktu do ADO, Informatyka lub osoby wyznaczonej przez ADO
3. **Zasady korzystania z poczty elektronicznej** 
   1. System poczty elektronicznej (SPE) powinien być wykorzystywany do prowadzenia korespondencji służbowej, stąd listy elektroniczne wysyłane za pośrednictwem SPE traktowane są jako korespondencja służbowa konieczna do wykonywania zadań i obowiązków służbowych.
   2. Użytkownicy mają prawo korzystać z SPE dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
   3. Korzystanie z poczty elektronicznej dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.
   4. Użytkownicy nie mają prawa korzystać z poczty elektronicznej w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub nieetycznym i naruszającym cudzą godność i prywatność
   5. Zabrania się dokonywanie w sieci zakupów, rezerwacji usług lub świadczeń na rzecz użytkownika oraz dokonywania bankowych z prywatnego konta.
   6. Administrator Danych ma prawo do monitorowania SPE. W przypadku nieobecności pracownika oraz konieczności wglądu do korespondencji nieobecnego pracownika, celem ochrony prywatności pracownika ma zastosowanie wytyczna wyrażona w Załączniku nr 1 do Rozporządzenia Ministra Pracy i Polityki Socjalnej z dnia 1 grudnia 1998 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe (pkt 10e).
   7. Użytkownik bez zgody Pracodawcy nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.
   8. Wszelkie przesyłanie dokumentów, opracowań, jak i innych treści przesyłane przez użytkownika podlegają zasadom ochrony prawa autorskiego i prawa własności przemysłowej, które użytkownik jest obowiązany przestrzegać.
   9. Niedozwolone jest przesyłanie wiadomości e-mail do więcej niż jednego adresata w taki sposób, że dla każdego z nich widoczne są, bądź będą adresy poczty elektronicznej pozostałych odbiorców,   
      w szczególności gdy zawierają w swej treści dane osobowe klientów organizacji.

Przy wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW”. Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości”.

* 1. Każdy użytkownik przed wysłaniem poczty jest zobowiązany sprawdzić poprawność adresu odbiorcy dokumentu.
  2. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę   
     o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
  3. Nakazuje się okresowe czyszczenie poczty z nieaktualnych e- mali i opróżnianie kosza.
  4. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
  5. Użytkownicy nie powinni otwierać przesyłek e-mail i uruchamiać wykonywalnych załączników dołączonych do korespondencji elektronicznej nadesłanej od nieznanych sobie nadawców, których adres nie wskazuje na związek z wypełnianymi przez nich obowiązkami służbowymi. Zabrania się, bez weryfikacji wiarygodności nadawcy „klikać” na hiperlinki w mailach. Nieprzestrzeganie tej zasady może doprowadzić do zainfekowania komputera użytkownika i innych pracujących w sieci.
  6. W przypadku przesyłania plików zawierających dane osobowe, użytkownik zobowiązany jest do ich spakowania i zabezpieczenia hasłem, tj. wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych dokumentów lub plików zzipowanych) . W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.
  7. Dokumenty źródłowe zawierające dane osobowe sporządzone jednorazowo, przesyłane innym jednostkom/odbiorcom powinny być zniszczone po ich wykorzystaniu.
  8. Wszystkie przypadki e-maili budzących podejrzenie należy zgłaszać administratorowi sieci/ informatykowi.
  9. Skrzynki pocztowe osób, które przestają być pracownikami, stażystami, praktykantami lub współpracownikami, niezwłocznie podlegają procedurze ich zamykania.

1. **Ochrona antywirusowa**
   1. Każdy system informatyczny musi być wyposażony w program antywirusowy oraz firewall, stanowiące kluczowy środek zabezpieczenia przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego. Takie same zabezpieczenia muszą być stosowane na urządzeniach mobilnych używanych służbowo.
   2. Zabronione jest zgrywanie na dysk twardy komputera oraz uruchamianie nielegalnych programów i plików pobranych z niewiadomego źródła.
   3. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym zainstalowanym na danym komputerze.
   4. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe**.**
   5. W przypadku stwierdzenia zainfekowania systemu, użytkownik obowiązany jest wyłączyć komputer z sieci, poinformować niezwłocznie o tym fakcie ADO.
   6. Bieżące aktualizowanie systemu operacyjnego komputera, systemu antywirusowego oraz firewalli odbywa się pod nadzorem ADO, Informatyka (również z firmy zewnętrznej) lub osoby wyznaczonej przez ADO
   7. W przypadku braku reakcji użytkownika i stwierdzenia przez administratora obecności wirusów, w trosce   
      o bezpieczeństwo pracy pozostałych użytkowników, zablokowany zostanie dostęp do sieci, a za skutki wynikłe z takiej sytuacji odpowiedzialny będzie użytkownik.
2. **Przestrzeganie zasad bezpieczeństwa podczas korzystania z elektronicznego sprzętu mobilnego (komputery przenośne, palmtopy, smartfony itp.)**
   1. Utrzymywanie w tajemnicy kodów PIN posiadanych kart SIM i kart tokenowych RSA,
   2. Stosowanie przygotowanych przez Administratora systemu informatycznego mechanizmów zabezpieczających klasy firewall, zabezpieczeń antywirusowych i szyfrowania zawartości dysków,
   3. Stosowanie, w uzgodnieniu z Administratorem systemu, mechanizmu ochrony danych, polegającego na synchronizacji katalogów na dyskach lokalnych z ich odpowiednikami na serwerach,
   4. Zakaz aktywowania modemów i kart transmisji danych GSM i jednoczesnego wpięcia do sieci komputerowej,
   5. Zakaz udostępnienia sprzętu osobom postronnym,
   6. Niezwłocznego informowania ADO w przypadku zagubienia lub kradzieży komputera, palmtopu czy karty tokenowej.
3. **Nadawanie upoważnień i uprawnień do przetwarzania danych osobowych**
   1. Za nadawanie i odwoływanie upoważnień do przetwarzania danych osobowych (dalej upoważnienie) odpowiada Administrator Danych Osobowych dalej ADO
   2. Upoważnienia mogą być nadawane w postaci papierowej lub elektronicznej,
   3. Upoważnienia nadawane są do poszczególnych zbiorów danych osobowych prowadzonych w formie papierowej i elektronicznej umieszczonych w wykazie (rejestrze czynności przetwarzania danych osobowych) prowadzonych przez ADO
   4. ADO prowadzi w formie papierowej i elektronicznej centralną ewidencję osób upoważnionych do przetwarzania danych osobowych
   5. Pracownik przetwarzający dane osobowe w formie papierowej oraz użytkownik systemu informatycznego używanego do przetwarzania danych osobowych przed nadaniem upoważnienia musi:
   6. zostać zaznajomiony z przepisami o ochronie danych osobowych oraz obowiązującymi w Firmie dokumentami takimi jak: polityka bezpieczeństwa danych osobowych i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
   7. podpisać stosowne oświadczenie o zachowaniu w poufności danych umieszczone na upoważnieniu.
   8. W przypadku, gdy upoważnienie nadawane jest pracownikowi do procesu - zbioru w formie elektronicznej, ADO otwiera konto oraz przydziela uprawnienia oraz identyfikator w danym systemie. .
   9. Zwolnienie z pracy lub zmiana stanowiska pracy związana ze zmianą dostępu do określonych procesów - zbiorów danych osobowych, wiąże się z koniecznością odwołania danego upoważnienia oraz zablokowania konta lub anulowania uprawnień w systemie.

# Zasady rozpoczęcia, zawieszenia i zakończenia pracy

* 1. Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła,
  2. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, innym pracownikom) wgląd do danych wyświetlanych na monitorach komputerowych stosując zasadę czystego ekranu,
  3. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu,
  4. Po zakończeniu pracy, użytkownik zobowiązany jest:
  5. wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy
  6. zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz elektroniczne nośniki danych, na których znajdują się dane osobowe.

1. **Postępowanie z informatycznymi nośnikami zawierającymi dane osobowe**
   1. Informatyczne nośniki danych są mobilną częścią zasobów informatycznych Podmiotu. Są nimi głównie dyskietki, dyski CD-R, DVD, Blu-ray, rodzaje pamięci USB, które podlegają oznaczeniu i ewidencji,
   2. ADO prowadzi rejestr elektronicznych nośników zawierających dane osobowe,
   3. Posługiwanie się tego rodzaju nośnikami zawierającymi dane osobowe wymaga zgody ADO. Podobnie, jak w przypadku konieczności przetwarzania danych na odległość, przy użyciu komputera przenośnego zawierającego dane osobowe,
   4. Użytkownicy tego typu nośników szyfrują część lub całość dysku urządzenia, kiedy transportują, przechowują i użytkują je poza obszarem przetwarzania.
   5. W przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe należy je przekazać do ADO celem dalszego procedowania.
2. **Postępowanie z dokumentami papierowymi zawierającymi dane osobowe** 
   1. Pracownicy upoważnieni do przetwarzania danych w formie tradycyjnej papierowej, odpowiadają za zabezpieczenie i ochronę danych osobowych przetwarzanych w kartotekach, skorowidzach, księgach czy wykazach,
   2. Tego typu papierowe urządzenia ewidencyjne oraz sporządzone z nich wydruki chroni się przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, zmianą, utratą, uszkodzeniem lub zniszczeniem
   3. Dokumenty i wydruki zawierające dane osobowe przechowuje się w zamykanych na klucz szafach kartotekowych, zamykanych regałach biurowych lub biurkach znajdujących się w zamykanych pomieszczeniach, stanowiących obszar przetwarzania danego zbioru,
   4. Przetwarzający dane są zobowiązani do stosowania „polityki czystego biurka”. Polega ona na bieżącym użytkowaniu dokumentów tylko niezbędnych do wykonania zadania, przechowywaniu dokumentów   
      w zamykanych regałach, szafach i biurkach oraz stosowaniu zabezpieczeń przed kradzieżą lub wglądem osób nieupoważnionych w trakcie godzin pracy jak i po jej zakończeniu,
   5. Użytkownicy zobowiązani są do niszczenia dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.
3. **Zasady czystego biurka i zasada czystego pulpitu** 
   1. Wszystkie dokumenty i ruchome nośniki danych (płyty CD, dyski przenośne, pamięć zewnętrzna itp.) nie są pozostawiane na biurku. W momencie, gdy przestają być używane – chowane są do szafek i biurek. W przypadku informacji wrażliwych / zastrzeżonych, zamykane są na klucz, a dane z nich usuwa się gdy stają się niepotrzebne.
   2. Na biurku znajdują się jedynie dokumenty aktualnie wykorzystywane przez pracownika/personel.   
      W przypadku opuszczenia stanowiska pracy (wyjście do WC, na przerwę śniadaniową / obiadową, poza siedzibę) wszystkie dokumenty i ruchome nośniki danych oraz pieczęcie znajdują się w szafkach   
      i szufladach. W przypadku informacji wrażliwych i zastrzeżonych, ruchome nośniki i pieczęcie, zamykane są na klucz.
   3. Dyrektor lub pracownik wyznaczony przez Administratora Danych Osobowych przeprowadza po godzinach pracy okresowe przeglądy z zakresu stosowania postanowień czystego biurka i pulpitu oraz zabezpieczenia informacji wrażliwych/zastrzeżonych przed nieuprawnionym dostępem.
   4. W odniesieniu do urządzeń przetwarzających informacje (komputer) stosuje się zasadę czystego pulpitu – nie prowadzi się zapisywania, tymczasowego zapisywania plików. Na pulpicie znajdują się tylko skróty do plików oraz katalogów.
   5. Po odejściu od stanowiska pracy należy się wylogować (przełączenie użytkownika)
   6. Dyrektor lub pracownik wyznaczony przez Administratora Danych Osobowych przeprowadza po godzinach pracy okresowe przeglądy z zakresu stosowania postanowień czystego pulpitu oraz wylogowania się z sieci w przypadku opuszczenia stanowiska pracy
4. **Zapewnienie poufności danych osobowych**
   1. Przetwarzający dane osobowe zobowiązany jest do zachowania w tajemnicy danych osobowych, do których ma lub będzie miał dostęp w związku z wykonywaniem zadań służbowych lub zadań zleconych przez przełożonego,
   2. Użytkownik zobowiązany jest do niewykorzystywania danych osobowych w celach pozasłużbowych bądź niezgodnych ze świadczoną pracą, o ile nie są one jawne,
   3. Użytkownik zobowiązany jest do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,   
      o ile nie są one jawne,
   4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieuprawnionym do ich poznania.
5. **Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych**
   1. W przypadku, gdy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci mogą wskazywać na naruszenie zabezpieczeń tych danych, każdy pracownik niezależnie do formy zatrudnienia przy przetwarzaniu danych osobowych, zobowiązany jest niezwłocznie powiadomić o tym ADO,
   2. Administrator wprowadza procedurę postępowania w przypadku naruszenia ochrony danych, którą osoba upoważniona przez Administratora do przetwarzania danych osobowych powinna bezwzględnie przestrzegać.
   3. Niektóre typowe sytuacje, które wskazują na możliwość zaistnienia incydentu:

* utrata lub przejęcie przez osoby nieuprawnione danych chronionych takich jak: dane osobowe pracowników, klientów, kontrahentów, danych powierzonych organizacji związanych z jej działalnością lub stanowiących tajemnicę przedsiębiorstwa;
* nieautoryzowany dostęp do informacji chronionych oraz ich modyfikacja;
* zagubienie lub zniszczenie informacji chronionej;
* ślady na drzwiach, oknach i szafach wskazujące na próbę włamania;
* dokumentacja jest niszczona bez użycia niszczarki;
* przebywanie osób bez nadzoru w budynku lub pomieszczeniach obszaru przetwarzania, zachowujących się podejrzanie, zwłaszcza jeśli nie towarzyszy im przedstawiciel – pracownik organizacji;
* otwarte drzwi do pomieszczeń, gdzie przechowywane są dokumenty, nieobecność pracownika na stanowisku pracy, gdy dokumenty są dostępne w zasięgu ręki, po zakończeniu pracy nie zamknięte szafy i nie wylogowany komputer;
* ustawienie monitorów komputerów pozwala na wgląd w ich zawartość przez osoby postronne;
* wynoszenie dokumentów zawierających dane osobowe w wersji papierowej lub elektronicznej na zewnątrz firmy bez upoważnienia przełożonego;
* próba skopiowania bazy danych (np. pracowników, klientów, kontrahentów) i przekazania ich podmiotowi nieuprawnionemu;
* ustne przekazywanie informacji mających znamiona informacji osobowych osobom nieuprawnionym;
* telefoniczne próby wyłudzenia danych osobowych;
* kradzież komputerów lub innych urządzeń stanowiących zasób informatyczny organizacji;
* maile zachęcające do ujawnienia identyfikatora i/lub hasła;
* pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
* hasła do systemów przyklejone są w post-it lub dostępne w innym miejscu w pobliżu komputera;
* logowanie się kilku pracowników do jednej stacji roboczej przy użyciu ogólnie dostępnego hasła.

1. **Ciągłość działania** 
   * Zapewnienie ciągłości działania i ochrona procesów przed skutkami zdarzeń losowych i sytuacji kryzysowych.
   1. Szkoła Podstawowa w Michałówce posiada Plan Ochrony ppoż. i ustalony sposób komunikacji na wypadek klęsk żywiołowych zalanie, pożar itp.;
   2. W zakresie ciągłości funkcjonowania Jednostka wykonuje kopie zapasowe w wersji elektronicznej wszystkich istotnych danych dotyczących działalności Szkoły Podstawowej w Michałówce;
   3. Archiwizowane dane elektroniczne przechowane są w szafie pancernej;
   4. Dokumenty papierowe archiwizowane są w archiwum – nie wykonuje się kopii zapasowej tych dokumentów;
   5. Pomieszczenie zabezpieczone jest odpowiednim zamkiem oraz systemem alarmowym i ppoż.,
   6. Instrukcja ppoż. jest opracowywana i aktualizowana przez inspektora BHP, który odpowiedzialny jest za jej dostępność oraz przeszkolenie pracowników szkoły;
   7. Instrukcje ppoż. przeglądane są pod kątem ich adekwatności i aktualności przez Inspektora BHP;
   8. Dyrektor odpowiada za bezpieczeństwo pracy użytkowanych pomieszczeń i aktualną instrukcje ppoż., by była dostępna w miejscu jej stosowania oraz za organizację szkoleń pracowników w tym zakresie.
   9. w przypadku utraty danych elektronicznych dane te są odtwarzane z kopii zapasowych;
   10. Dyrektor odpowiada za organizację, wyznaczenie osób odpowiedzialnych za ewakuację z pomieszczeń szkoły dokumentów, danych i sprzętu w przypadku pożaru lub zalania użytkowanych pomieszczeń.
   11. W przypadku stwierdzenia awarii łącza zapewniającego dostęp do Internetu, należy niezwłocznie skontaktować się z dostawca usługi i ustalić przyczynę awarii oraz uzyskać informacje o planowanym terminie przywrócenia poprawnego działania łącza;
   12. w przypadku przerwa w dostawie zasilania prądu należy powiadomić Administratora Danych Osobowych o awarii, zlokalizować w miarę swoich możliwości powód wystąpienia awarii zgłosić fakt wystąpienia awarii do pogotowia energetycznego zamknięcia wszystkie maszyn i urządzania , wliczając oraz urządzenia sieciowe i telekomunikacyjne.
2. **Postępowanie dyscyplinarne**
   1. W przypadku naruszeń zasad bezpieczeństwa w procesie przetwarzania danych osobowych pracownik ponosi odpowiedzialność porządkową, dyscyplinarną lub karną w zależności od wagi naruszenia,   
      z zastosowaniem właściwych przepisów prawa.
   2. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub domniemania takiego naruszenia, nie podjęła działania określonego w niniejszym opracowaniu zasad, a w szczególności nie powiadomiła przełożonego , a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, mogą mieć zastosowanie przepisy odpowiedzialności porządkowej i materialnej.

……………………………………………………..

*Podpis ADO*