# Instrukcja Zarządzania Systemami Informatycznymi

*ZESPÓŁ SZKOLNO - PRZEDSZKOLNY w Stanowicach*

*ul. Świebodzka 6-9*
*58-150 Stanowice*

# Wprowadzenie

Instrukcja Zarządzania Systemem Informatycznym wraz z Polityką Bezpieczeństwa stanowi dokumentację przetwarzania danych osobowych w rozumieniu § 5 ust.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) (Dz. Urz. UE L 119 z 5 kwietnia 2016 r.).

Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów niniejszego dokumentu Instrukcji Zarządzania Systemem Informatycznym powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych zawartych w systemach informatycznych w **Zespole Szkolno - Przedszkolnym w Stanowicach**, zwanym dalej „**Zespołem**”, reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę **Zespołu.**

Instrukcja obowiązuje wszystkich pracowników placówki. Wykonywanie postanowień tego dokumentu zapewnia właściwą ochronę danych oraz ewentualną reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa przetwarzanych danych.

Nadto dokument ten określa tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznych **Zespołu**.

Należy przez powyższe rozumieć w szczególności realizację w niniejszym dokumencie wymogu opisania sposobu przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. Zadaniem 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.

# Rozdział I

## Zakres informacji objętych Instrukcją Zarządzania Systemem Informatycznym

Dokument Instrukcji Zarządzania Systemem Informatycznym opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem. Obejmuje on ogólne informacje o systemie informatycznym i zbiorach danych osobowych, które są przy ich użyciu przetwarzane, o zastosowanych rozwiązaniach technicznych, jak również o procedurach eksploatacji i zasady użytkowania, jakie zastosowano w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych.
Na Instrukcję Zarządzania składają się w szczególności następujące informacje:

1. PROCEDURY nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
2. stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
3. procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
4. procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
5. sposób, miejsce oraz okres przechowywania:
   1) elektronicznych nośników informacji zawierających dane osobowe,
   2) kopii zapasowych, o których mowa w pkt 4,
6. sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania szkodliwego,
7. procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych,
8. opis incydentów naruszenia bezpieczeństwa danych osobowych i procedura zarządzania.

Instrukcję Zarządzania Systemem Informatycznym stosuje się do wszelkich czynności, stanowiących w myśl rozporządzenia przetwarzanie danych osobowych. Bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania.

Rygorowi Instrukcji Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych podlegają także dane powierzone przez **zespół** do przetwarzania na podstawie pisemnej umowy powierzenia przetwarzania danych osobowych oraz dane osobowe, których szkoła jest odbiorcą w rozumieniu rozporządzenia.

# Rozdział II

## Charakterystyka Systemu

System informatyczny służący do przetwarzania danych osobowych obejmuje wszystkie pracujące w szkole serwery, komputery stacjonarne i przenośne, a także urządzenia peryferyjne i sieciowe.

# Rozdział III

## Procedura nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym

1. Użytkowników systemów informatycznych tworzy oraz usuwa osoba odpowiedzialna za infrastrukturę informatyczną szkoły na podstawie zgody Administratora Danych Osobowych.
2. Do przetwarzania danych osobowych zgromadzonych w systemie informatycznym jak również w rejestrach tradycyjnych wymagane jest upoważnienie wydane przez Administratora Danych Osobowych ( załącznik nr 2 PBDO)
3. Upoważnienie sporządza Inspektor Ochrony Danych, zgodnie ze wzorem stanowiącym załącznik załącznik nr 2 PBDO Upoważnienie do przetwarzania danych osobowych sporządzane jest w 2 egzemplarzach, jeden otrzymuje pracownik, drugi przechowywany jest w aktach osobowych pracownika.
4. Upoważnienie do przetwarzania danych osobowych jest rejestrowane przez Inspektora Ochrony Danych w ewidencji upoważnień stanowiący Załącznik nr 10 PBDO
5. Upoważnienie osobie upoważnionej wydawane jest po podpisaniu przez nią oświadczenia o zapoznaniu się z obowiązującymi przepisami w zakresie ochrony danych osobowych ( załącznik nr 2 PBDO ) oraz zobowiązaniu się do zachowania w tajemnicy, także po ustaniu realizacji zadań oraz po ustaniu stosunku pracy, poznanych danych osobowych oraz informacji związanych z funkcjonowaniem systemu ochrony danych osobowych. Wzór oświadczenia określa (załącznik nr 2 PBDO) Oświadczenie sporządzane jest w 2 egzemplarzach, jeden przechowywany jest w aktach osobowych pracownika, drugi przechowywany jest w dokumentacji RODO.
6. Uprawnienia do pracy w systemie informatycznym odbierane są czasowo, poprzez zablokowanie konta w przypadku zawieszenia w pełnieniu obowiązków służbowych.
7. Uprawnienia do przetwarzania danych osobowych odbierane są trwale w przypadku ustania stosunku pracy.

# Rozdział IV

## Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. System informatyczny przetwarzający dane osobowe wykorzystuje mechanizm identyfikatora i hasła jako narzędzi umożliwiających bezpieczne uwierzytelnienie.
2. Hasła użytkowników lub inne dane uwierzytelniające podlegają szczególnej ochronie.
3. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego przechowywanie.

4. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu hasła, które jest związane z jego identyfikatorem.
5. Każdy użytkownik posiadający dostęp do systemów teleinformatycznych szkoły zobowiązany jest do:
   1) zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystanych do pracy w systemie informatycznym.
   2) niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia,
   3) niezwłocznej zmiany hasła tymczasowego, przekazanego przez Administratora Systemów Informatycznych,
   4) poinformowania Inspektora Ochrony Danych o podejrzeniu lub rzeczywistym ujawnieniu hasła i natychmiastowej zmiany hasła,
   5) stosowania haseł o minimalnej długości 8 znaków, zawierających kombinację małych i wielkich liter, cyfr i znaków specjalnych,
   6) zmiany wykorzystywanych haseł nie rzadziej niż co 3 miesiące.
   7) 3-krotna błędna próba wprowadzenia hasła powinna skutkować zablokowaniem konta użytkownika oraz odpowiednią adnotacją w systemie monitoringu zawierająca co najmniej:
   8) identyfikator komputera/urządzenia na którym próbowano dokonać logowania oraz czas wykrycia zdarzenia.
   9) Hasła nie powinny być tworzone według stałego schematu, np.: Kowal_01, Kowal_02 itp.
   10) Hasła powinny być wprowadzane w sposób maskowany.
   11) Powinna zostać tworzona historia haseł (przynajmniej 10 wstecz) w celu zablokowania ich powtarzania.
6. **Zabronione jest:**
   1) zapisywanie haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób,
   2) stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.,
   3) używanie tych samych haseł w różnych systemach operacyjnych i aplikacjach,
   4) udostępnianie haseł innym użytkownikom,
   5) przeprowadzanie prób łamania haseł,
   6) wpisywanie haseł w postaci jawnej.
7. Hasłami najwyższego poziomu dysponuje Administrator Danych i przechowuje je w zamkniętej kopercie w sejfie.
8. UWAGA! Hasła powinny być trudne do odgadnięcia (zaleca się nie stosować nazw potocznych, imion, nazwisk, dat urodzenia, numerów dokumentów, innych danych osobistych oraz standardowych kombinacji znaków, np. 12345678).

# Rozdział V

## Ogólne zasady pracy w systemie informatycznym

1. Przetwarzanie danych w systemie informatycznym może być realizowane wyłącznie poprzez dopuszczone przez Administratora Danych do eksploatacji licencjonowane oprogramowanie.
2. Do eksploatacji dopuszcza się systemy informatyczne wyposażone w:
   1) mechanizmy kontroli dostępu umożliwiające autoryzację pracownika wykorzystującego system informatyczny na indywidualnym komputerowym stanowisku pracy zwanego dalej użytkownikiem, z pominięciem narzędzi do edycji tekstu,
   2) mechanizmy ochrony poufności, dostępności i integralności informacji, z uwzględnieniem potrzeby ochrony kryptograficznej,
   3) mechanizmy umożliwiające wykonanie kopii bezpieczeństwa oraz archiwizację danych, niezbędne do przywrócenia prawidłowego działania systemu po awarii,
   4) urządzenia niwelujące zakłócenia i podtrzymujące zasilanie,
   5) mechanizmy monitorowania w celu identyfikacji i zapobiegania zagrożeniom, w szczególności pozwalające na wykrycie prób nieautoryzowanego dostępu do informacji lub przekroczenia przyznanych uprawnień w systemie,
3. Użytkownikom zabrania się:
   1) korzystania ze stanowisk komputerowych podłączonych do sieci informatycznej poza godzinami i dniami pracy szkoły bez zgody na pracę w godzinach nadliczbowych lub odpracowanie czasu nieprzepracowanego w związku z załatwianiem spraw osobistych w godzinach pracy,
   2) udostępniania stanowisk roboczych osobom nieuprawnionym,
   3) wykorzystywania sieci komputerowej **Zespołu** w celach innych niż wyznaczone przez Administratora Danych Osobowych ,
   4) samowolnego instalowania i używania programów komputerowych,
   5) korzystania z nielicencjonowanego oprogramowania oraz wykonywania jakichkolwiek działań niezgodnych z ustawą o ochronie praw autorskich,
   6) umożliwiania dostępu do zasobów wewnętrznej sieci informatycznej szkoły oraz sieci Internetowej osobom nieuprawnionym,
   7) używania komputera bez zainstalowanego oprogramowania antywirusowego.
4. Regulamin korzystania z przeglądarek internetowych stanowi **załącznik nr 1 IZSI**
5. Regulamin korzystania z poczty elektronicznej stanowi **załącznik nr 2 IZSI**

# Rozdział VI

## Procedury rozpoczęcia, zawieszenie i zakończenia pracy

1. Każdy pracownik korzystający z systemu informatycznego przystępując do pracy powinien podać swoje dane dostępu do komputera i systemu, tj. identyfikator i hasło.

2. Zawieszenie pracy polega na opuszczeniu stanowiska pracy bez wylogowania się i jest dopuszczalne tylko w przypadku pozostania w pomieszczeniu. Użytkownik jest zobowiązany w takiej sytuacji do włączenia wygaszacza ekranu odblokowywanego hasłem.
3. Zakończenie pracy w systemie następuje poprzez prawidłowe, wymagane przez daną aplikację oraz system operacyjny, wykonanie czynności kończących. Niedopuszczalne jest zakończenie pracy poprzez wyłączenie napięcia zasilającego bez pełnej procedury zamknięcia komputera.
4. Ekrany monitorów stanowisk komputerowych, na których odbywa się przetwarzanie danych osobowych powinny być w miarę możliwości tak umieszczone, aby uniemożliwić wgląd w dane osobom postronnym przebywającym w pomieszczeniu oraz powinny automatycznie się wyłączać poprzez stosowanie wygaszaczy ekranowych uruchamiających blokadę pracy na komputerze.
5. Osoba przetwarzająca dane osobowe w przypadku konieczności opuszczenia pomieszczenia, obowiązana jest prawidłowo, zgodnie z instrukcją obsługi systemu, zakończyć pracę w systemie.
6. Czas rozpoczynania i kończenia pracy w systemach sieciowych, w tym systemach przetwarzających dane osobowe, określa **Regulamin Pracy**.

## Rozdział VII

### Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi służących do ich przetwarzania

1. Dla wszystkich aktywów informatycznych określa się zasady archiwizacji i tworzenia kopii zapasowych. Przy określaniu zasad bierze się pod uwagę:
   1) kategoryzację aktywu,
   2) zagrożenia i ryzyka związane z utratą integralności i dostępności danych,
   3) możliwości techniczne,
   4) wymogi prawne.
2. Archiwizacja zasobów i wykonywanie kopii zapasowych odbywa się według planu archiwizacji i wykonywania kopii zapasowych.
3. Plan archiwizacji i wykonywania kopii zapasowych stanowi **załącznik nr 3 IZSI**
4. Dane osobowe zabezpiecza się poprzez wykonywanie kopii zapasowych.
5. Ochronie poprzez wykonanie kopii podlegają także programy i narzędzia programowe służące przetwarzaniu danych. Kopie programów i narzędzi wykonywane są zaraz po instalacji oraz po każdej aktualizacji na zewnętrznych, elektronicznych nośnikach informacji.
6. Zabezpieczeniu poprzez wykonywanie kopii zapasowych podlegają także dane konfiguracyjne systemu informatycznego przetwarzającego dane osobowe, w tym uprawnienia użytkowników systemu.
7. Za proces tworzenia kopii programów i narzędzi programowych oraz danych konfiguracyjnych systemu odpowiedzialna jest osoba odpowiedzialna za infrastrukturę informatyczną szkoły. Kopie przechowywane są w zamkniętej szafie w wydzielonym i zabezpieczonym pomieszczeniu.

8. Kopie zapasowe mogą być sporządzane automatycznie lub manualnie z wykorzystaniem specjalistycznych urządzeń do wykonywania kopii lub standardowych narzędzi oferowanych przez stacje robocze.
9. Kopie baz danych gromadzonych na serwerach wykonywane są przez osoba odpowiedzialna za infrastrukturę informatyczną szkoły zapisywane na dysk sieciowy lub zewnętrzne nośniki danych i przechowywane w zamkniętej szafie.
10. Kopie zbiorów danych osobowych zlokalizowanych na komputerach lokalnych wykonywane są przez poszczególnych użytkowników ostatniego dnia każdego miesiąca i zapisywane na dyskach lokalnych w ustalonej z osobą odpowiedzialną za infrastrukturę informatyczną szkoły, lokalizacji lub zapisywane na nośnikach zewnętrznych
11. Pliki edytorów tekstu lub arkuszy kalkulacyjnych traktowane są jak kopie zbiorów, z których pochodzą przetwarzane w nich dane i nie są objęte procedurami wykonywania kopii zapasowych.
12. Nośniki, na których są przechowywane kopie danych osobowych muszą być wyraźnie oznaczone datami.
13. Za bezpieczeństwo kopii zapasowych przetwarzanych lokalnie odpowiadają poszczególni użytkownicy systemu, którzy je wykonali. Kopie usuwa się niezwłocznie po ustaniu ich użyteczności w sposób uniemożliwiający odtworzenie danych.
14. Informację zawierająca dane osobowe, które nie będą wykorzystywane a nie podlegają archiwizacji lub dla której upłynął okres przechowywania należy usunąć.
15. Zewnętrzne nośniki kopii zapasowych, które zostały wycofane z użycia, podlegają zniszczeniu po usunięciu danych osobowych, w odpowiednim urządzeniu niszczącym.
16. Za właściwe usuniecie informacji zawartej na nośniku przenośnym lub w pamięci masowej stacji roboczej odpowiada użytkownik.
17. Za usuwanie informacji z pamięci masowych serwerów oraz nośników kopii archiwalnych i zapasowych odpowiada osoba odpowiedzialna za infrastrukturę informatyczną **Zespołu.**
18. Użytkownik tworzy wydruki związane z przetwarzaniem danych osobowych wyłącznie w zakresie i ilości niezbędnej dla celów służbowych w uzgodnieniu z przełożonym.
19. Wszystkie dokumenty, zestawienia i wydruki zawierające dane osobowe powinny być chronione przed dostępem osób nieupoważnionych. Użytkownik przechowuje je w zamkniętej szafie w pomieszczeniu zabezpieczonym przed nieuprawnionym dostępem.

## Rozdział VIII

**Sposób, miejsce i okres przechowywania elektronicznych nośników informacji**

1. Dane osobowe mogą być przetwarzane na serwerach, a także na dyskach lokalnych komputerów. **Zabrania się gromadzenia danych osobowych na**

**innych, nie autoryzowanych przez Administratora Danych nośnikach danych.**

2. W uzasadnionych przypadkach, za zgodą Inspektora Ochrony Danych, dane osobowe można przetwarzać na zewnętrznych nośnikach informacji, autoryzowanych przez Administratora Danych.
3. Informacje zawierające dane osobowe przechowywane na zewnętrznych nośnikach informacji **muszą być szyfrowane.**
4. W celu zwiększenia bezpieczeństwa danych i systemu informatycznego ogranicza się w szkole obieg pendrive-ów i innych nośników informatycznych poprzez ich oznaczenie i zarejestrowanie w ewidencji wewnętrznej. Wzór ewidencji nośników stanowi **załącznik nr 4 do IZSI**
5. Ewidencję nośników prowadzi Administrator Danych.
6. Wprowadza się zakaz obiegu nośników nie oznakowanych w sposób, o którym mowa w pkt 4, a wszystkie nośniki pochodzące od jednostek zewnętrznych mogą być wykorzystane tylko do jednorazowego odczytu ich zawartości po uprzednim sprawdzeniu programem antywirusowym.
7. Serwery oraz komputery, na których odbywa się przetwarzanie danych osobowych, powinny być zabezpieczone przed utratą danych spowodowaną awarią zasilania poprzez stosowanie specjalnych urządzeń podtrzymujących zasilanie i eliminujących zakłócenia sieci zasilającej.
8. Komputery przenośne oraz inne mobilne nośniki danych osobowych muszą być zabezpieczone ochroną kryptograficzną – **muszą być zaszyfrowane.**

## Rozdział IX

### Zasady ochrony kryptograficznej

1. W celu ochrony poufności danych osobowych stosuje się zabezpieczenia kryptograficzne.
2. Za właściwą ochronę kryptograficzną odpowiedzialny jest osoba odpowiedzialna za infrastrukturę informatyczną **Zespołu**.
3. Zabezpieczenia kryptograficzne stosuje się przy:
   1) wymianie danych z podmiotami zewnętrznymi,
   2) szyfrowaniu informacji na nośnikach zewnętrznych,
   3) przy korzystaniu z komputerów przenośnych,
   4) szyfrowaniu wiadomości poczty elektronicznej,
   5) szyfrowaniu baz danych.
4. Do szyfrowania połączeń stosuje się:
   1) połączenia szyfrowane SSL/TLS,
   2) tunele VPN.
5. Do szyfrowania informacji na nośnikach zewnętrznych stosuje się:
   1) szyfrowanie plików technologią PGP,
   2) szyfrowanie plików w kontenerach.
6. Do szyfrowania informacji na dyskach komputerów przenośnych stosuje się funkcje wbudowane systemu operacyjnego lub produkty firm zewnętrznych.
7. W wypadku przesyłania danych osobowych przez sieć internetową pocztą elektroniczną należy **każdy z załączników zabezpieczyć ochroną**

**kryptograficzną** poprzez nadanie hasła odczytu. Hasło należy przesłać lub podać odbiorcy w innej przesyłce, a najlepiej z wykorzystaniem innych metod komunikacji (tel., sms, bezpośrednia rozmowa).

8. Do szyfrowania baz danych stosuje się funkcje wbudowane serwera baz danych lub produkty firm zewnętrznych.
9. Zabrania się przekazywania danych przez aplikacje internetowe nie wykorzystujące odpowiedniego protokołu szyfrowania (adres internetowy musi być poprzedzony zapisem „https").

## Rozdział X

**Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu.**

1. Serwery i stacje robocze w szkole są objęte ochroną w czasie rzeczywistym za pomocą oprogramowania antywirusowego oraz zapory ( firewall), zapewniających integralność zasobów przechowywanych i przetwarzanych w systemie informatycznym **Zespołu**.
2. Wymienne nośniki pamięci, przed rozpoczęciem pracy z tymi nośnikami w systemie informatycznym szkoły, są sprawdzane za pomocą aktualnego oprogramowania antywirusowego.
3. Aktualizacja baz wirusów odbywa się automatycznie.
4. System antywirusowy jest skonfigurowany w sposób zapewniający na bieżąco skanowanie wszystkich informacji przetwarzanych w systemie, a zwłaszcza poczty elektronicznej i stron internetowych.
5. Po każdej naprawie i konserwacji urządzenia a przed ponownym włączeniem do systemu informatycznego **Zespołu** zawartość stałych nośników informacji jest sprawdzana za pomocą oprogramowania antywirusowego.
6. Wystąpienie infekcji traktowane jest jako incydent bezpieczeństwa i podlega procedurze postępowania w sytuacji naruszenia ochrony danych osobowych.
7. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, osoba odpowiedzialna za infrastrukturę informatyczną szkoły podejmuje działania zmierzające do usunięcia zagrożenia.

## Rozdział XI

**Informacje o odbiorcach, którym dane osobowe zostały udostępnione.**

1. Dla każdej osoby, której dane są przetwarzane w systemie informatycznym powinny być automatycznie odnotowane następujące informacje:
   1) dane o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba, że dane te traktuje się jako dane jawne,
   2) sprzeciwu osoby, której dane dotyczą w przypadku zamierzenia przetwarzania jej danych w celach marketingowych lub zamierzenia przekazania jej danych innemu administratorowi.

2. Zapis pkt 1 nie dotyczy systemów służących do przetwarzania danych ograniczonych do edycji tekstu w celu udostępnienia go na piśmie i niezwłocznym usunięciu z systemu.
3. Dla każdej osoby, której dane są przetwarzane w systemie informatycznym, system powinien zapewniać sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w pkt 1.
4. W uzasadnionych przypadkach uniemożliwiających automatyczne odnotowywanie, o którym mowa w pkt 1, prowadzi się odrębny „rejestr udostępniania", stanowiący **załącznik nr 7 PBDO**
5. Za udostępnianie danych zgodnie z przepisami prawa odpowiedzialny jest Administrator Danych Osobowych. – Każde udostepnienie Danych Osobowych powinno być zaewidencjonowane w rejestrze stanowiącym **załącznik nr 7 PBDO**

## Rozdział XII

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

1. Konserwacja sprzętu i urządzeń pracujących w systemie informatycznym szkoły ma na celu zapewnienie nieprzerwanej i bezpiecznej pracy tego systemu, zapobieganie utraty, uszkodzenia danych lub naruszenie bezpieczeństwa systemu.
2. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   1) **likwidacji** — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
   2) **przekazania podmiotowi nieuprawnionemu do przetwarzania danych** — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
   3) **naprawy** — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby odpowiedzialnej za infrastrukturę informatyczną **Zespołu**.
3. Instalacji, konserwacji oraz napraw sprzętu komputerowego dokonuje osoba odpowiedzialna za infrastrukturę informatyczną szkoły lub podmiot zewnętrzny świadczący usługi konserwacyjne na podstawie umowy lub w ramach gwarancji.
4. Przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez Administratora Danych Osobowych lub posiadające umowy na powierzenie przetwarzania danych lub udostepnienie w zakresie konserwacji i napraw jeśli naprawa odbywa się na terenie ADO
5. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wy-

maganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych, w szczególności poprzez bezpośredni nadzór prowadzony przez osobę odpowiedzialną za infrastrukturę informatyczną szkoły. Jeżeli zaś taki nadzór nie jest możliwy, to informacje zawierające dane osobowe są, po zapewnieniu możliwości ich odtworzenia, skutecznie usuwane z nośnika.

# Rozdział XIII

## Zdarzenia Naruszające Bezpieczeństwo Informacji

1. Wszyscy pracownicy Szkoły oraz pracownicy reprezentujący podmiot zewnętrzny, którzy mają dostęp do systemów informatycznych **Zespołu** i zobowiązali się do przestrzegania jej regulacji wewnętrznych związanych z bezpieczeństwem informacji, mają obowiązek zgłaszania wszelkich zdarzeń, które naruszają lub mogą naruszyć przepisy prawa oraz polityki, regulaminy i procedury **Zespołu** dotyczące bezpieczeństwa informacji.
2. Przed przystąpieniem do pracy użytkownik obowiązany jest sprawdzić stację roboczą i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie lub próbę naruszenia bezpieczeństwa informacji.
3. Podział zagrożeń:
   1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych,
   2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora systemu informatycznego, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,
   3) zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:
      a) nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
      b) nieuprawniony dostęp do systemu z jego wnętrza,
      c) pogorszenie jakości sprzętu i oprogramowania,
      d) nieuprawniony przekaz danych,
      e) bezpośrednie zagrożenie materialnych składników systemu.
4. Do przykładów mogących świadczyć lub świadczących o naruszeniu bezpieczeństwa, niewłaściwym funkcjonowaniu oprogramowania lub podatności systemu informatycznego zalicza się:
   1) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach (np. zacinające się zamki, naruszone plomby, niedomknięte okno itp.), w których odbywa się przetwarzanie danych osobowych.

2) utratę usługi, urządzenia lub funkcjonalności aplikacji/systemu,
3) nieautoryzowaną utratę lub zniszczenie danych,
4) spowolnienie pracy komputera,
5) pojawienie się nietypowych komunikatów na ekranie,
6) niemożność zalogowania się do systemu informatycznego,
7) objawy niestabilnej pracy systemu informatycznego,
8) nagłe przyspieszenie lub zwolnienie transmisji danych,
9) brak reakcji systemu na działania użytkownika,
10) ponowny start lub zawieszania się komputera,
11) ograniczenie funkcjonalności komputera.
12) brak możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp do danych osobowych,
13) ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika aplikacji (np. brak możliwości wykonywania pewnych operacji normalnie dostępnych użytkownikowi) lub uprawnienia poszerzone w stosunku do normalnej sytuacji,
14) wygląd aplikacji inny niż normalnie,
15) inny zakres danych niż normalnie dostępny dla użytkownika - dużo więcej lub dużo mniej danych,
16) znaczne spowolnienie działania systemu informatycznego,
17) zgubienie lub kradzież nośnika danych osobowych,
18) kradzież sprzętu informatycznego, w którym przechowywane były dane osobowe,
19) informację z systemu antywirusowego o zainfekowaniu systemu informatycznego wirusami,
20) fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia siły wyższej.
21) podejrzenie nieautoryzowanej modyfikacji danych osobowych.

5. Za naruszenie ochrony danych osobowych i wystąpienie incydentu bezpieczeństwa uważa się w szczególności:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
2) awarię sprzętu lub oprogramowania, która wskazuje na umyślne działanie w kierunku naruszenia ochrony danych,
3) dopuszczenie do przetwarzania danych osobowych pracowników nie posiadających odpowiednich uprawnień,
4) niewłaściwe niszczenie nośników informacji, na których przechowywane są dane osobowe,
5) ujawnienie indywidualnych haseł,
6) stwierdzenie nieupoważnionego dostępu do systemu informatycznego przetwarzającego dane osobowe,

7) niedopełnienie obowiązku ochrony danych osobowych (np. pozostawienie danych osobowych, nie zablokowanie dostępu do systemu, brak nadzoru nad serwisantami itp.),
8) wykonanie nieuprawnionych kopii danych osobowych,
9) zaniechanie działań zmierzających do eliminacji wirusów komputerowych i innego rodzaju niepożądanego oprogramowania,
10) przesyłanie niezabezpieczonych informacji zawierających dane osobowe drogą elektroniczną,
11) stwierdzenie próby lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
12) ujawnienie istnienia nieautoryzowanych kont dostępu do danych.
13) utratę zewnętrznego nośnika pamięci,
14) utratę komputera przenośnego,
15) dopuszczenie do braku aktualnych kopii bezpieczeństwa danych i ustawień systemu informatycznego,
16) korzystanie z nielicencjonowanego oprogramowania,
17) dopuszczenie do możliwości korzystania z sieci informatycznej.

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

# Rozdział XIV

**Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych**

1. Osoba, która zauważyła niepokojące zdarzenie, wystąpienie poniżej wymienionych symptomów lub innych objawów, które jej zdaniem mogą spowodować zagrożenie bądź mogą być przyczyną naruszenia ochrony danych osobowych i bezpieczeństwa informacji, zobowiązana jest do natychmiastowego poinformowania Administratora Danych.
2. Osoba odpowiedzialna za infrastrukturę informatyczną **Zespołu** dokonuje wstępnej identyfikacji zdarzenia i na podstawie dostępnych informacji oraz analizy okoliczności zdarzenia kwalifikuje zdarzenie (lub serię zdarzeń) jako:
   1) zdarzenie nie mające cech naruszenia bezpieczeństwa informacji,
   2) incydent związany z naruszeniem bezpieczeństwa informacji.
3. potencjalnym wystąpieniu incydentu związanego z naruszeniem bezpieczeństwa informacji osoba odpowiedzialna za infrastrukturę informatyczną szkoły powiadamia niezwłocznie Inspektora Ochrony Danych.
4. Inspektor Ochrony Danych we współpracy z osobą odpowiedzialną za infrastrukturę informatyczną szkoły przeprowadza analizę incydentu.
5. Analiza incydentu uwzględnia następujące kryteria:
   1) charakter incydentu i jego znaczenie związane z bezpieczeństwem danych,
   2) miejsce wystąpienia incydentu – identyfikacja punktu, w którym nastąpiło zdarzenie (lokalizacja, serwer, stacja robocza itp.)

3) zakres incydentu,
4) identyfikację zasobów potrzebnych przy dalszych działaniach w ramach postępowania z incydentem,
5) możliwość rozszerzenia się zakresu incydentu,
6) szacowany poziom szkód,
7) rodzaj ujawnionej informacji,
8) skutki organizacyjne i prawne.

6. W przypadku, gdy incydent posiada skutki przekładające się na możliwość zakłócenia działalności ustawowej bądź statutowej szkoły osoba odpowiedzialna za infrastrukturę informatyczną szkoły informuje niezwłocznie Administratora Danych Osobowych.
7. W przypadku , gdy zasięg i szacunkowy czas trwania powoduje zakwalifikowanie incydentu jako sytuację kryzysową określaną jako zniszczenie lub poważną awarię kluczowych zasobów teleinformatycznych szkoły osoba odpowiedzialna za infrastrukturę informatyczną szkoły niezwłocznie powiadamia Administratora Danych Osobowych.
8. W przypadku, gdy rodzaj i zasięg incydentu zidentyfikowany na którymkolwiek z etapów postępowania uzasadnia potrzebę powiadomienia organów ścigania to decyzje o sposobie i terminie powiadomienia podejmuje Administrator Danych Osobowych.
9. W przypadku, gdy rodzaj i zasięg incydentu zidentyfikowany na którymkolwiek z etapów postępowania uzasadnia podejrzenie utraty danych osobowych Administrator Danych Osobowych powiadamia w terminie 72 godzin Prezesa Urzędu Ochrony Danych i jeżeli to możliwe osoby, których dane osobowe zostały utracone.
10. Inspektor Ochrony Danych prowadzi bieżącą dokumentację incydentu. Dokumentacja ta w szczególności obejmuje:
    1) wszystkie zdarzenia zachodzące w systemie informatycznym ( zapisy z systemowych dzienników),
    2) wszystkie podejmowane działania (opatrzone datą i czasem),
    3) wszystkie przeprowadzone rozmowy ( osoba rozmówcy, data i czas, treść rozmowy).
11. Dokumentacja incydentu podlega rygorom ochrony przez tworzenie autoryzowanych kopii tych elementów systemu, które mają zastosowania przy postepowaniu z incydentem tzn. rejestry urządzeń, systemów operacyjnych i aplikacji, kopie zapasowe, pliki konfiguracyjne i systemowe (zgodnie z rygorami tworzenia materiału dowodowego). Wzór protokołu zabezpieczenia materiału dowodowego stanowi **załącznik nr 5 IZSI**
12. Osoba odpowiedzialna za infrastrukturę informatyczną szkoły przeprowadza działania zmierzające do ograniczenia skutków incydentu i zidentyfikowaniu źródła naruszenia bezpieczeństwa.
13. Przy ograniczaniu skutków incydentu osoba odpowiedzialna za infrastrukturę informatyczną szkoły może korzystać z konsultantów zewnętrznych, jeżeli **zespół** zawarł w umowach z tymi podmiotami stosowne zapisy.
14. Po usunięciu lub zablokowaniu źródła incydentu osoba odpowiedzialna za infrastrukturę informatyczną szkoły przystępuje do odtworzenia systemu.

15. Odtwarzanie systemu odnosi się do punktu odtworzenia, co do którego osoba odpowiedzialna za infrastrukturę informatyczną szkoły ma uzasadnioną pewność, że nie zawiera źródła incydentu.
16. System informatyczny, którego prawidłowe działanie zostało odtworzone powinien zostać poddany szczegółowej obserwacji w celu stwierdzenia całkowitego usunięcia symptomów incydentu.
17. Inspektor Ochrony Danych prowadzi rejestr incydentów zawierający następujące informacje:
    1) datę i godzinę zgłoszenia incydentu,
    2) dane identyfikujące osobę zgłaszającą,
    3) dane osoby przekazującej informację o incydencie,
    4) datę zarejestrowania incydentu,
    5) dane identyfikujące osobę rejestrującą incydent,
    6) informacje dotyczące sposobu postepowania z incydentem,
    7) informacje o zgromadzonych informacjach dowodowych.
18. Z każdego incydentu bezpieczeństwa Inspektor Ochrony Danych sporządza raport. Wzór dokumentu raportu opisany jest w **załączniku nr 6 IZSI**
19. Inspektor Ochrony Danych odpowiedzialny jest za przeprowadzenie przynajmniej raz w roku analizy zaistniałych incydentów w celu:
    1) określenia skuteczności podejmowanych działań wyjaśniających i naprawczych,
    2) określenia wymaganych działań zwiększających bezpieczeństwo systemu informatycznego i minimalizujących ryzyko zaistnienia incydentów,
    3) określenia potrzeb w zakresie szkoleń administratorów systemu i użytkowników systemu informatycznego przetwarzającego dane osobowe.

## Rozdział XV

### Zasady korzystania z komputerów przenośnych, na których są przetwarzane dane osobowe.

1. Przetwarzanie danych osobowych na komputerach przenośnych powinno być ograniczone do niezbędnych przypadków. Przetwarzanie danych osobowych przy użyciu komputerów przenośnych może odbywać się wyłącznie za zgodą Administratora Danych Osobowych i za wiedzą Inspektora Ochrony Danych. Zakres danych przetwarzanych na komputerze przenośnym oraz zakres uprawnień do przetwarzanych danych ustala przełożony pracownika za wiedzą Inspektora Ochrony Danych.
2. Osoba korzystająca z komputera przenośnego w celu przetwarzania danych osobowych zobowiązana jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych danych, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem.
3. Użytkownik komputera przenośnego zobowiązany jest do:
    1) transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia, a w szczególności:
        a) - transportowania komputera w bagażu podręcznym,
        b) - nie pozostawiania komputera w samochodzie, przechowalni

bagażu, itp.,
   c) - zaleca się przenoszenie komputera w torbie przeznaczonej do przenoszenia
   d) komputerów przenośnych,
2) korzystania z komputera w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby nieupoważnione, w szczególności zabrania się korzystania z komputera w miejscach publicznych i w środkach transportu publicznego,
3) nie zezwalania osobom nieupoważnionym do korzystania z komputera
4) przenośnego, na którym przetwarzane są dane osobowe,
5) zabezpieczania komputera przenośnego hasłem,
6) blokowania dostępu do komputera przenośnego w przypadku, gdy nie jest on wykorzystywany przez pracownika,
7) kopiowania danych osobowych przetwarzanych na komputerze przenośnym do systemu informatycznego w celu umożliwienia wykonania kopii zapasowej tych danych,
8) umożliwienia, poprzez podłączenie komputera do sieci informatycznej szkoły:
   a) - aktualizacji wzorców wirusów w programie antywirusowym,
   b) utrzymania konfiguracji oprogramowania systemowego w sposób wymuszający
   c) korzystanie z haseł,
9) wykorzystywania haseł odpowiedniej jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe,
10) zmiany haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe,
11) zabezpieczania danych osobowych przetwarzanych na komputerach przenośnych poprzez zastosowanie oprogramowania szyfrującego te dane, tak by dostęp do tych danych był możliwy wyłącznie po podaniu hasła,
12) dokonania instalacji i konfiguracji oprogramowania antywirusowego na komputerze przenośnym,
13) przeprowadzania aktualizacji wzorców wirusów zgodnie z zasadami zarządzania programem antywirusowym.

4. W razie zgubienia lub kradzieży komputera przenośnego pracownik zobowiązany jest do **natychmiastowego powiadomienia** Administratora Danych Osobowych lub osoby uprawnionej zgodnie z zasadami informowania o naruszeniu ochrony danych osobowych.

## Rozdział XVI

### Przetwarzanie danych osobowych w systemach informatycznych powierzonych szkole przez inne podmioty

1. Możliwe jest przetwarzanie w systemach informatycznych szkoły danych osobowych powierzonych szkole przez inny podmiot (Zleceniodawcę). W takim przypadku, przetwarzanie danych osobowych odbywa się na podstawie

**umowy pomiędzy placówką a Zleceniodawcą zawartej w formie pisemnej.** Umowa ta musi zawierać ściśle określony zakres przetwarzanych danych. Przetwarzanie danych możliwe jest tylko w ustalonym przez umowę zakresie.

2. Powierzone dane podlegają ochronie na takich samych zasadach jak dane będące własnością szkoły, chyba, że umowa określi inne zasady ochrony danych osobowych. W szczególności może dotyczyć to nadawania uprawnień do przetwarzania danych osobowych. Dostęp do powierzonych danych osobowych z sieci zewnętrznej (np. siedziby Zleceniodawcy) musi odbywać się z zachowaniem odpowiednich zabezpieczeń. Dostęp do danych musi być chroniony identyfikatorem oraz hasłem, a połączenie sieciowe realizujące dostęp do danych musi być odpowiednio szyfrowane.

## Rozdział XVII

### Postanowienia końcowe

1. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.
2. Inspektor Ochrony Danych zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego **załącznik nr 7 IZSI.**
3. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia Inspektora Ochrony Danych nie wyklucza odpowiedzialności karnej tej osoby zgodnie 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) (Dz. Urz. UE L 119 z 5 kwietnia 2016 r.) oraz możliwość wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
4. W sprawach nieuregulowanych niniejszym dokumentem mają zastosowanie przepisy 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) (Dz. Urz. UE L 119 z 5 kwietnia 2016 r.).
5. Postanowienia niniejszej instrukcji stosuje się również do stażystów i praktykantów.
6. Wszelkie zmiany Instrukcji mogą być wprowadzane tylko na podstawie zarządzeń Administratora Danych Osobowych.
7. Zmiany wprowadzane w załącznikach do niniejszego dokumentu nie wymagają zmiany zarządzenia, które wprowadziło niniejszą instrukcję w życie.

## Załączniki:

Załącznik nr 1 - Oświadczenie zapoznania się z Instrukcją Zarządzania Systemami Informatycznymi
Załącznik nr 2 - Regulamin korzystania z przeglądarek internetowych
Załącznik nr 3 – Regulamin korzystania z poczty e-mail
Załącznik nr 4 – Rejestr nośników komputerowych
Załącznik nr 5 - Protokół zabezpieczenia materiału dowodowego
Załącznik nr 6 - Wzór raportu z incydentu
Załącznik nr 7 - Ewidencja osób zapoznanych z Instrukcja zarządzania systemami informatycznymi