**POLITYKA BEZPIECZEŃSTWA INFORMACJI**

**W ZESPOLE SZKÓŁ PONADGIMNAZJALNYCH**

**W ŁODZIERZY**

## Metryka dokumentu

|  |  |  |  |
| --- | --- | --- | --- |
| **Data** | **Wersja** | **Opis** | **Autor** |
|  | 2.00 | Aktualizacja dokumentu zgodnie z aktualnymi wymogami UODO oraz polskich norm. | Katarzyna Kawczyńska |

**Rozdział 1 Wprowadzenie**

Podstawą do opracowania i wdrożenia dokumentu są:  
a) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 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 nazywanego ogólnym Rozporządzeniem o ochronie danych osobowych [dalej: RODO];  
b) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 r., poz. 1000) [dalej: Ustawa].

wprowadza się w **Zespole Szkół Ponadgimnazjalnych w Łodzierzy,** zwanym dalej **ZSP,** zestaw reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej pozwalający na zapewnienie ochrony danych osobowych.

Celem Polityki Bezpieczeństwa jest zapewnienie ochrony danych osobowych przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi, jak i zewnętrznymi, świadomymi lub nieświadomymi.

Jako załącznik do niniejszej polityki opracowano i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwaną dalej „Instrukcją zarządzania systemem informatycznym”. Określa ona sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem zapewnienia ich bezpieczeństwa.

Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez samych użytkowników.

Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić: poufność, integralność i dostępność.

**Rozdział 2 Definicje**

Przez użyte w niniejszym dokumencie określenia należy rozumieć:

|  |  |  |  |
| --- | --- | --- | --- |
| L.p. | Nazwa | Skrót | Opis |
| 1 | Administrator danych | AD | Podmiot decydujący o celach i środkach przetwarzania danych osobowych, czyli **ZSP.** |
| 2 | Administrator bezpieczeństwa informacji | ABI | Osoba powołana przez AD i zgłoszona do GIODO, odpowiedzialna za zapewnienie przestrzegania przepisów o ochronie danych osobowych oraz prowadzenie rejestru zbiorów przetwarzanych przez AD. |
| 3 | Administrator systemu informatycznego -> pracownik firmy zewnętrznej | ASI | Osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień – informatyk firmy zewnętrznej. |
| 4 | Analiza ryzyka |  | Proces identyfikacji ryzyka, określenia jego wielkości i wyodrębnienia obszarów wymagających zabezpieczeń. |
| 5 | Bezpieczeństwo informacji | BI | Bezpieczeństwo informacji określa zapewnienie  zachowania atrybutów: poufności, integralności i dostępności. Dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. |
| 6 | Dane osobowe |  | Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. |
| 7 | Dostępność |  | Zapewnienie, że dostęp do danych jest zapewniony wtedy, kiedy jest to potrzebne. |
| 8 | Generalny Inspektor Ochrony Danych Osobowych | GIODO | Organ do spraw ochrony danych osobowych powołany przez Sejm Rzeczypospolitej Polskiej. |
| 9 | Incydent naruszenia bezpieczeństwa |  | Każde zdarzenie lub działanie naruszające bezpieczeństwo lub zasady ochrony danych osobowych. |
| 10 | Integralność |  | Zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany. |
| 11 | Naruszenie bezpieczeństwa |  | Przypadek, w którym użytkownik lub inna osoba pomija lub niszczy środki nadzoru systemu teleinformatycznego w celu pozyskania nieuprawnionego dostępu do informacji w nim zawartej lub do jego zasobów. |
| 12 | Obszar podwyższonego bezpieczeństwa | Obszar PB | Pomieszczenia o podwyższonym bezpieczeństwie - na potrzeby bezpieczeństwa sieci informatycznej wyznaczone są strefy o podwyższonych zabezpieczeniach, w których znajdują się systemy serwerowe, urządzenia aktywne sieci komputerowej, urządzenia centrali telefonicznej, główne węzły sieci teleinformatycznej oraz archiwum nośników danych i licencji oprogramowania. |
| 13 | Obszar PDO |  | Pomieszczenia stanowiące obszar, w którym przetwarzane są dane osobowe. |
| 14 | Polityka bezpieczeństwa informacji | PBI | Polityka bezpieczeństwa danych osobowych |
| 15 | Poufność |  | Zapewnienie dostępu osobom tylko uprawnionym. |
| 16 | Przetwarzanie danych |  | wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie. |
| 17 | Rozporządzenie |  | Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych |
| 18 | System informatyczny | SI | Zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych. |
| 19 | UODO | UODO | Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych. |
| 20 | Upoważniony |  | Przetwarzający dane osobowe na podstawie upoważnienia AD. |
| 21 | Usuwanie danych |  | Rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą. |
| 22 | Urządzenia mobilne |  | Komputery przenośne (notebooki), a także urządzenia multimedialne (projektory oraz aparaty i kamery cyfrowe) i telefony komórkowe. |
| 23 | Użytkownik |  | Pracownik posiadający uprawnienia do pracy w systemie informatycznym zgodnie ze swoim zakresem obowiązków. |
| 24 | Zabezpieczenie systemu informatycznego |  | Należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą. |
| 25 | Zasada czystego biurka |  | Zasada, według której użytkownik opuszczając stanowisko pracy usuwa z blatu biurka dokumenty zawierające informacje w tym dane osobowe, chowając je do przeznaczonych do tego celu szaf, szuflad lub sejfów, w celu wyeliminowania ryzyka przypadkowego lub celowego odczytania, skopiowania, zniszczenia lub zmodyfikowania (np. poprzez podmianę kartki) przez osoby nieuprawnione. |
| 26 | Zasada czystego ekranu |  | Zasada, według której użytkownik przerywając pracę, wyloguje się z systemu operacyjnego lub uruchamia chroniony hasłem wygaszacz ekranu, w celu uniemożliwienia innym osobom pracy z jego uprawnieniami. |
| 27 | Zbiór danych |  | Zestaw danych osobowych posiadający określoną strukturę, uporządkowany według określonych kryteriów oraz celów. |
| 28 | Zgoda osoby, której dane dotyczą |  | Rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie, zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści |

**Rozdział 3 Podstawy prawne**

|  |  |
| --- | --- |
| L.p. | NAZWA AKTU PRAWNEGO |
| WYKAZ AKTÓW PRAWNYCH ZWIĄZANYCH Z PBI | |
| 1. | Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych |
| 2. | Ustawa z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną |
| 3. | Ustawa z dnia 27 lipca 2001 roku o ochronie baz danych |
| 4. | Ustawa z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych |
| 5. | Ustawa z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne |
| 6. | Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie określenia wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych |
| 7. | Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 roku w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji |
| 8. | Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych |
| 9. | Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji |
| 10. | Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zwane dalej Rozporządzeniem. |
| 11. | Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych |
| 12. | Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 kwietnia 2011 r. w sprawie zasad potwierdzania, przedłużania ważności, wykorzystania i unieważniania profilu zaufanego elektronicznej platformy usług administracji publicznej |
| 13. | Rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych |
| 14. | Rozporządzenie 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 |
| PRZEPISY SZCZEGÓŁOWE: | |
| 1. | Ustawa z dnia 27 czerwca 1997 r. o bibliotekach |
| 2. | Ustawa z dnia 26 stycznia 1982 r. - Karta Nauczyciela |
| 3. | Ustawa z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy |
| 4. | Ustawa z dnia 21 listopada 2008r. o pracownikach samorządowych |
| 5. | Ustawa z dnia 7 września 1991 r. o systemie oświaty |
| 6. | Ustawa z dnia 26 czerwca 1974 r. - Kodeks pracy |
| 7. | Ustawa z dnia 23 maja 1991 r. o związkach zawodowych |
| 8. | Rozporządzenie Rady Ministrów z dnia 19 grudnia 1992 r. w sprawie pracowniczych kas zapomogowo-pożyczkowych oraz spółdzielczych kas oszczędnościowo-kredytowych w zakładach pracy |
| WYKAZ POLSKICH NORM ZWIĄZANYCH Z PBI | |
| 1. | PN-ISO/IEC 27001:2014 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania |
| 2. | PN-ISO/IEC 27002: 2014 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji |
| 3. | PN-ISO/IEC 27005: 2014 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji |
| 4. | PN-ISO/IEC 24762:2010 Technika informatyczna - Techniki bezpieczeństwa – Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie |
| 5. | PN-ISO/IEC 27000:2014 Technika informatyczna – Techniki bezpieczeństwa –Systemy zarządzania bezpieczeństwem informacji – przegląd i terminologia |

**Rozdział 4 Zakres danych objętych ochroną**

Aktywami informacyjnymi objętych ochroną są dane osobowe przetwarzane w **ZSP,** zidentyfikowane zbiory danych osobowych, systemy informatyczne za pomocą których są przetwarzane oraz przepływ pomiędzy tymi systemami przedstawione są w załącznikach numer 1 do niniejszego dokumentu – osobno dla każdego zbioru:

* 1. ABSOLWENCI
  2. DANE OSOBOWE RODZICÓW
  3. KANDYDACI DO PRACY
  4. KANDYDACI NA UCZNIÓW
  5. KONKURSY
  6. KSIĄŻKA KONTROLI
  7. PRACOWNICY I BYLI PRACOWNICY
  8. REJESTR KORESPONDENCJI
  9. SKŁADNICA AKT
  10. STAŻ
  11. SYSTEM INFORMACJI OŚWIATOWEJ
  12. UCZNIOWIE
  13. UMOWY CYWILNOPRAWNE
  14. WNIOSKODAWCY UBIEGAJĄCY SIĘ O UDOSTĘPNIENIE INFORMACJI PUBLICZNEJ
  15. WYPADKI PRZY PRACY
  16. WYPADKI UCZNIÓW
  17. ZAMÓWIENIA PUBLICZNE I PRZETARGI

**Rozdział 5 Struktura zarządzania przetwarzanych danych**

* 1. Administratorem Danych (AD) jest **ZSP**, który odpowiada za:
* przetwarzanie danych osobowych na podstawie legalnych przesłanek.
* realizację obowiązku informacyjnego.
* dołożenie szczególnej staranności przy przetwarzaniu danych osobowych.
* ochronę danych osobowych.
* realizację obowiązku rejestracyjnego.
  1. Administratorem Bezpieczeństwa Informacji (ABI) jest osoba powołana przez AD, który odpowiada za:
* nadzór nad przestrzeganiem zasad ochrony informacji, a w szczególności zapewnianie przestrzegania przepisów o ochronie danych osobowych;
* nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2, oraz przestrzegania zasad w niej określonych,
* zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
* prowadzenie rejestru zbiorów danych osobowych.
  1. Administratorem Systemu Informatycznego (ASI) jest pracownik **ZSP/firmy zewnętrznej (proszę wybrać poprawne),** z którą AD podpisał umowę **o pracę/cywilnoprawną**, który odpowiada za:
* zapewnienie poprawności oraz ciągłości działania systemów informatycznych.
* realizuje zadania dotyczące systemu informatycznego wykonywane zgodnie z PBI.
* koordynuje również współpracę z dostawcami usług, sprzętu informatycznego.
* przeciwdziała próbom naruszenia bezpieczeństwa informacji oraz zapewnia najwyższy poziom bezpieczeństwa i dostępności dostępnych usług.
  1. Upoważnionym jest osoba upoważniona do przetwarzania danych osobowych przez AD (wzór upoważnienia znajduje się w załączniku nr 6), który odpowiada za:
* bezpieczeństwo danych osobowych, w tym w szczególności zabezpieczenie:
  + danych osobowych – także po zakończeniu godzin pracy;
  + pomieszczeń, w których przetwarza się informacje – także w godzinach pracy
* przestrzeganie PBI.
* zgłaszanie do ABI sytuacji związanych z naruszeniem zasad ochrony danych osobowych oraz innych informacji
* zachowanie w tajemnicy chronionych danych oraz sposobów ich zabezpieczenia, także po ustaniu zatrudnienia;
  1. Użytkownikiem SI jest osoba pracująca w systemie informatycznym, która odpowiada za:
* zachowanie w tajemnicy swojego hasła;
* przestrzeganie terminu zmiany hasła co 30 dni, w przypadku, używania identyfikatora i hasła do uwierzytelniania w SI;
* zwracanie uwagi oraz zgłaszanie do ASI nietypowego zachowania SI;
* zgłaszanie do ASI wypadków wykrycia wirusów komputerowych, które nie dają się usunąć przy pomocy dostępnego oprogramowania antywirusowego;
* zabezpieczenie urządzeń przenośnych.
  1. Użytkownik urządzeń mobilnych – pracownik pracujący na służbowym laptopie, smartfonie lub innych urządzeniach mobilnych – instrukcja zapewnienia bezpieczeństwa urządzeń mobilnych w załączniku numer 2.

**Rozdział 6 Zasady przetwarzania danych osobowych:**

* 1. **Zasada legalności**

Podstawy przetwarzania zbiorów danych osobowych w **ZSP** są zgodne z art. 23 ust. 1 oraz 27 ust. 2 UODO. Dla każdego zidentyfikowanego zbioru podstawy prawne opisane są w załącznikach numer 1.

W **ZSP** stosuje się pisemne umowy powierzenia przetwarzania danych przy współpracy z podmiotami zewnętrznymi przetwarzającymi dane osobowe (wzór umowy - załącznik nr 17

Załącznik nr 18 zawiera wzór oświadczenia osoby, której wizerunek jest wykorzystywany w celu promowania **ZSP**.

* 1. **Zasada wypełniania obowiązku informacyjnego**
     1. Przy zbieraniu danych osobowych bezpośrednio od osoby obowiązek informacyjny spełniany jest poprzez pisemne (ogólny wzór załącznik nr 4, informacja dla pracowników załącznik nr 4a, informacja dla kandydatów do pracy – załącznik nr 4b) lub ustne poinformowanie zgodnie z art. 24 ust. 1 UODO.
     2. Każda osoba fizyczna, której dane są przetwarzane, ma prawo zwrócić się z wnioskiem o udzielenie informacji związanych z przetwarzaniem tych danych, prawo do kontroli i poprawiania swoich danych osobowych, a także w przypadkach określonych w art. 32 ust 1 pkt 7 i 8 UODO prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz sprzeciwu wobec przekazywania ich innym podmiotom.
     3. Informację o monitoringu wizyjnym zawiera załącznik nr 19.
  2. **Zasada zapewnienia szczególnej staranności**
     1. Dane osobowe przetwarzane są zgodnie z prawem.
     2. Dla każdego zbioru określony jest cel przetwarzania.
     3. Dane osobowe są merytorycznie poprawne oraz adekwatne co do celów przetwarzania.
     4. Dane osobowe przetwarzane są przez okres niezbędny do realizacji celu, po czym są niezwłocznie zanonimizowane lub usuwane.
  3. **Zasada ochrony danych osobowych**
     1. Ochrona – bezpieczeństwo fizyczne:
* Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.
* Przebywanie osób nieupoważnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych lub na podstawie pisemnej zgody otrzymanej od AD wg wzoru, który stanowi załącznik nr 15. Wzór odwołania zgody znajduje się w załączniku nr 16.
* Pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych pozostają zawsze pod bezpośrednim nadzorem osoby upoważnionej. Opuszczone pomieszczenia są zamknięte na klucz.
* Klucze do szaf, w których przechowywane są dane osobowe mają jedynie pracownicy upoważnieni do przetwarzania danych osobowych.
* Wykaz pomieszczeń zawarty jest w załączniku numer 7.
  + 1. Ochrona - bezpieczeństwo osobowe:
* Powołano administratora bezpieczeństwa informacji.
* Upoważnienia nadawane są każdej osobie, która będzie przetwarzać dane osobowe.
* ABI prowadzi ewidencję osób upoważnionych do przetwarzania danych zgodnie ze wzorem stanowiącym załącznik numer 5.
* Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane zostały do zachowania ich w tajemnicy.
* ABI zapewnia zapoznanie osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Dokumentem potwierdzającym zapoznanie się z przepisami dotyczącymi ochrony danych osobowych oraz z treścią niniejszego dokumentu jest oświadczenie użytkownika, którego wzór stanowi załącznik numer 6. Kompendium wiedzy na temat ochrony danych osobowych stanowi załącznik numer 13.
* Korzystanie ze zbiorów danych osobowych przez osoby inne niż pracownicy, odbywa się po uzyskaniu upoważnienia do przetwarzania tych danych na podstawie ogólnie obowiązujących przepisów.
  + 1. Ochrona - bezpieczeństwo techniczne:
* Zastosowano środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii danych osobowych. W systemach informatycznych obowiązuje wysoki poziom bezpieczeństwa. Zasady bezpiecznego użytkowania systemu informatycznego zawarte są w Instrukcji zarządzania systemem informatycznym stanowiącym załącznik numer 8.
* Wszyscy użytkownicy systemu informatycznego są przeszkoleni z zasad bezpieczeństwa informacji,
  + 1. Ochrona – realizacja zadań administratora bezpieczeństwa informacji wskazanych w pkt. 5.2.
  1. **Sprawdzenia zgodności przetwarzania danych osobowych**
     1. Sprawdzenia zgodności przetwarzania danych osobowych przeprowadza ABI.
     2. Sprawdzenia przeprowadzane są w trybie:
        1. sprawdzenia planowego – według planu sprawdzeń,
        2. sprawdzenia doraźnego – w przypadku nieprzewidzianym w planie sprawdzeń, w sytuacji powzięcia przez administratora bezpieczeństwa informacji wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia,
        3. art. 19b ust. 1 UODO – w przypadku zwrócenia się o dokonanie sprawdzenia przez Generalnego Inspektora.
     3. Z przeprowadzonych czynności sprawdzających ABI opracowuje sprawozdanie dla AD.
     4. Sprawdzenie planowe:
        1. ABI przygotowuje plan sprawdzeń na okres nie krótszy niż kwartał i nie dłuższy niż rok,
        2. ABI przedstawia AD plan sprawdzeń danych nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem.
     5. Sprawdzenie doraźne:
        1. jest przeprowadzane niezwłocznie po powzięciu wiadomości przez ABI informacji o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia,
        2. ABI zawiadamia AD o rozpoczęciu sprawdzenia doraźnego przed podjęciem pierwszej czynności w toku sprawdzenia.
     6. Sprawdzenie w trybie art. 19b UODO:
        1. GIODO może zwrócić się do ABI o przeprowadzenie sprawdzenia,
        2. ABI za pośrednictwem AD przekazuje do GIODO sprawozdanie.
  2. **Zasada rejestracji i aktualizacji zbiorów danych**

Rejestracja zbioru oraz aktualizacja rejestracji zbioru polega na zgłaszaniu do ABI zbiorów do rejestracji na druku, którego wzór stanowi załącznik numer 10.

* ABI prowadzi ewidencję zbiorów przetwarzanych w **ZSP**.
* ABI prowadzi rejestr zbiorów.
  1. **Zasady udostępniania i powierzania danych**
     1. AD po otrzymaniu wniosku o udostępnienie danych osobowych postępuje zgodnie z procedurą udostępniania danych osobowych, która stanowi załącznik numer 9***.***
     2. Przy zawieraniu umów cywilnoprawnych z podmiotami, z realizacją których wiąże się przetwarzanie danych osobowych, powierzenie przetwarzania danych osobowych temu podmiotowi, następuje w drodze umowy zawartej na piśmie, zgodnie z art. 31 UODO. Osoba przyjmująca przetwarzanie danych zobowiązuje się do przestrzegania obowiązujących przepisów ustawy o ochronie danych osobowych.
* Procedurę powierzania przetwarzania danych osobowych stanowi załącznik numer 3***.***
* Wykaz umów powierzenia prowadzi ABI zgodnie ze wzorem wskazanym w załączniku numer 12.
  + 1. Instrukcja dotycząca zasad bezpieczeństwa informacji przy korzystaniu z usług podmiotów zewnętrznych znajduje się w załączniku nr 14.
  1. **Zasady postępowania w sytuacji naruszenia**

Naruszenie bezpieczeństwa informacji to sytuacja zaistniała w wyniku niepożądanego lub nieoczekiwanego zdarzenia lub serii zdarzeń, skutkująca potencjalnie zwiększonym prawdopodobieństwem utraty lub faktyczną utratą przez informację (zarówno w postaci elektronicznej, papierowej i każdej innej) dowolnej z cech charakteryzujących jej bezpieczeństwo:

* poufności – poprzez nieuprawniony dostęp do informacji,
* integralności – poprzez nieuprawnioną modyfikację, usunięcie lub ujawnienie informacji,
* dostępności – poprzez brak dostępu w określonym czasie,
* autentyczności – poprzez nieuprawnioną zmianę autora informacji.

Na możliwość wystąpienia naruszenia bezpieczeństwa informacji mogą wskazywać:

* nietypowy stan pomieszczeń przetwarzania (naruszone plomby, otwarte pomieszczenia, okna, drzwi od szaf, biurek, włączone urządzenia, podłączane lub inaczej przełączone przewody sieci logicznej, itp.),
* zaginięcie sprzętu lub nośników informacji (elektronicznych oraz papierowych),
* podejrzewane nieuzasadnione modyfikacje lub usunięcie danych,
* nieprawidłowe lub nietypowe działanie systemu informatycznego między innymi:
  + nietypowe komunikaty wyświetlane na monitorze,
  + odstająca od normy wydajność (prędkość) działania systemu,
  + brak możliwości zalogowania do systemu,
* próby uzyskania informacji przez nieuprawnione osoby stosujące metody socjotechniczne.

W przypadku wystąpienia naruszenia bezpieczeństwa informacji każda osoba jest zobowiązana do powiadomienia o tym fakcie bezpośredniego przełożonego oraz ABI.

ABI wszczyna postępowanie w trybie sprawdzenia doraźnego.

Instrukcja postępowania w sytuacji naruszenia bezpieczeństwa znajduje się w załączniku nr 11.

**Rozdział 7 Postanowienia końcowe**

* 1. Polityka Bezpieczeństwa jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.
  2. Kierownicy komórek organizacyjnych są zobowiązani zapoznać z treścią Polityki Bezpieczeństwa każdego pracownika.
  3. Wszystkie regulacje dotyczące systemów informatycznych określone w Polityce Bezpieczeństwa dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
  4. Pracownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.
  5. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.
  6. 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 gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
  7. Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia, nie wyklucza odpowiedzialności karnej tej osoby zgodnie z UODO oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
  8. W sprawach nieuregulowanych w niniejszej Polityce Bezpieczeństwa mają zastosowanie przepisy UODO oraz wydane na jej podstawie akty wykonawcze.
  9. Polityka bezpieczeństwa, wchodzi w życie z dniem ……………………. r.
  10. Traci moc dokument „………………………………………………. z dnia ……………………. wprowadzony w życie zarządzeniem nr …… dyrektora szkoły z dnia …………………. .

**Załączniki:**

|  |  |
| --- | --- |
| Załącznik numer 1 | Wykaz oraz rejestr zbiorów danych osobowych wraz z systemami przetwarzającymi te dane |
| Załącznik numer 2 | Instrukcja korzystania z urządzeń mobilnych |
| Załącznik numer 3 | Procedura powierzenia przetwarzania danych osobowych |
| Załącznik numer 4 | Wzór pisemnej formy obowiązku informacyjnego |
| Załącznik numer 4a | Wzór pisemnej formy obowiązku informacyjnego wobec pracownika |
| Załącznik numer 4b | Wzór pisemnej formy obowiązku informacyjnego wobec kandydata do pracy |
| Załącznik numer 5 | Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych |
| Załącznik numer 6 | Wzór upoważnienia do przetwarzania danych osobowych |
| Załącznik numer 7 | Obszar przetwarzania |
| Załącznik numer 8 | Instrukcja zarządzania systemem informatycznym |
| Załącznik numer 9 | Procedura udostępniania danych osobowych |
| Załącznik numer 10 | Wzór zgłoszenia zbioru do rejestracji |
| Załącznik numer 11 | Postępowanie w przypadku naruszenia bezpieczeństwa |
| Załącznik numer 12 | Wzór ewidencji umów powierzenia |
| Załącznik numer 13 | Kompendium wiedzy na temat ochrony danych osobowych |
| Załącznik numer 14 | Korzystanie z podmiotów zewnętrznych |
| Załącznik numer 15 | Wzór zgody na przebywanie w obszarze przetwarzania |
| Załącznik numer 16 | Wzór odwołania zgody na przebywanie w obszarze przetwarzania |
| Załącznik numer 17 | Wzór umowy powierzenia |
| Załącznik numer 18 | Zezwolenie na wykorzystanie wizerunku |
| Załącznik numer 19 | Informacja o monitoringu wizyjnym |