ZESPÓŁ SZKOLNO-PRZEDSZKOLNY
W LISEWIE

POLITYKA BEZPIECZEŃSTWA

ZESPOŁU SZKOLNO - PRZEDSZKOLNEGO

UL. TORUŃSKA 17, 86-230 LISEWO

REGON - 340266163

Spis treści:

A. INFORMACJE OGÓLNE

1. Cel polityki ochrony danych osobowych

Polityka Bezpieczeństwa w zakresie przetwarzania danych osobowych w Zespole Szkolno – Przedszkolnym w Lisewie zwana dalej „Polityką" jest dokumentem opisującym zasady i procedury przetwarzania danych osobowych stosowane przez Administratora w celu spełnienia wymagań Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE z dnia 27 kwietnia 2016 r., zwanej dalej RODO. Jest to zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych. Polityka odnosi się do problemu zabezpieczenia danych osobowych, tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie (w postaci papierowej), jak i danych przetwarzanych w systemach informatycznych. Politykę ochrony danych osobowych stosuje się do wszystkich czynności bez względu na źródło pochodzenia danych osobowych, ich zakresu, celu zebrania, sposobu przetwarzania. Każda osoba mająca dostęp do danych osobowych zobowiązana jest zapoznać się z niniejszym dokumentem oraz potwierdzić ten fakt na wykazie, którego wzór stanowi załącznik nr 1 do niniejszej Polityki – Wykaz osób zapoznanych z Polityką.

2. Definicje

Administrator Danych Osobowych (ADO)– oznacza jednostkę publiczną, która samodzielnie ustala cele i sposoby przetwarzania danych osobowych w ramach niniejszego dokumentu i jest to: Zespół Szkolno – Przedszkolny w Lisewie, ul. Toruńska 17, 86-230 Lisewo, nr RSPO: 59162; REGON: 340266163

Administrator Bezpieczeństwa Informacji (**ABI)** – osoba wyznaczona przez Administratora Danych, koordynująca działania związane z zapewnieniem bezpieczeństwa systemów informatycznych, w tym również odpowiadająca za nadzór nad zabezpieczeniem danych osobowych przetwarzanych w systemach informatycznych przez Administratora Danych.

Inspektor Ochrony Danych (IOD) – osoba wyznaczona przez Administratora Danych, koordynująca procesy związane z przestrzeganiem zasad ochrony danych osobowych w ramach procesów przetwarzania danych osobowych zachodzących w strukturze Administratora Danych.

Anonimizacja – zmiana danych osobowych, w wyniku której dane te tracą charakter danych osobowych.

Dane osobowe – to wszelkie informacje związane z zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną (osobie, której dane dotyczą), którą można zidentyfikować w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Dane szczególnych kategorii oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej (w tym o korzystaniu z usług opieki zdrowotnej) ujawniające informacje o stanie jej zdrowia, dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne (przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej) oraz dane dotyczące seksualności lub orientacji seksualnej osoby fizycznej.

Polityka – oznacza niniejszą Politykę ochrony danych osobowych.

Przetwarzanie – operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, porządkowanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

Poufność danych – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE z dnia 27 kwietnia 2016 r.
Pseudonimizacja – oznacza przetwarzanie danych osobowych w taki sposób (np. przez zastępowanie nazw – liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. listy nazwisko i numer), pod warunkiem, że takie dodatkowe informacje są przechowywanie oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizyczne.
Użytkownik – osoba posiadająca dostęp do systemu informatycznego przetwarzającego dane osobowe oraz dokumentacji papierowej.

B. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

1. Struktura organizacji ochrony danych osobowych

Za właściwe przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami RODO odpowiadają w Zespole Szkolno – Przedszkolnym w Lisewie:

1. Administrator Danych Osobowych
2. Inspektor Ochrony Danych
3. Administrator Systemów Informatycznych
4. Osoby upoważnione do przetwarzania danych osobowych

1.1. Administrator Danych Osobowych

1. Administrator Danych Osobowych odpowiedzialny jest za :
   a) wyznaczenie Inspektora Ochrony Danych,
   b) wyznaczenie Administratora Bezpieczeństwa Informacji.
   c) zapewnienie odpowiednich środków organizacyjnych i technicznych w celu zapewnienia i wykazania przetwarzania danych osobowych zgodnie z określonymi w RODO zasadami przetwarzania danych osobowych,
   d) wdrożenie odpowiednich procedur ochrony danych osobowych,
   e) nadzorowanie realizacji postanowień w Polityce Bezpieczeństwa,
   f) zapewnienie środków umożliwiających prawidłową realizację praw osób, których dane dotyczą,
   g) wdrożenie rejestru czynności przetwarzania danych osobowych
   h) aktualizacje informacji zawartych w rejestrze czynności przetwarzania,
   i) wdrożenie odpowiednich środków organizacyjnych i technicznych, aby zapewnić stopień bezpieczeństwa odpowiadający istniejącemu ryzyku naruszenia praw lub wolności osób, których dane dotyczą,
   j) wdrożenie Polityki ochrony danych,
   k) zgłaszanie naruszenia ochrony danych osobowych właściwemu organowi nadzorczemu, a w przypadku, gdy zajdą ku temu odpowiednie przesłanki, również osobie, której dane dotyczą,
   l) dokumentowanie wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia, jego skutków oraz podjętych działań zaradczych,

m) zapewnienie odpowiednich środków w celu dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w sytuacji, jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w tym, jeżeli zajdą ku temu odpowiednie przesłanki, konsultację z organem nadzorczym,
n) nadawanie upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
o) wyrażanie zgody na udostępnienie informacji zgodnie z przepisami prawa,
p) nadzoruje działania IOD oraz ABI oraz wydaje im zalecenia, co do sposobu wykonywania obowiązków wynikających z Polityki Bezpieczeństwa.

1.2. Inspektor Ochrony Danych

1. Funkcję IDO pełni osoba powołana przez Administratora Danych.
2. Wzór dokumentu powołania IOD stanowi załącznik nr 2 do Polityki oraz odwołania załącznik 2a do Polityki
4. Do zadań IOD należy:
   a) informowanie o obowiązkach wynikających z RODO oraz innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych oraz doradzanie w tym zakresie,
   b) monitorowanie przestrzegania RODO oraz innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych,
   c) monitorowanie przestrzegania wdrożonych procedur ochrony danych osobowych,
   d) działania zwiększające świadomość pracowników Administratora Danych w zakresie obowiązków wynikających z RODO lub przyjętych procedur,
   e) przeprowadzanie audytów w zakresie przestrzegania RODO i wdrożonych procedur ochrony danych osobowych,
   f) udzielanie na żądanie zaleceń, co do oceny skutków dla ochrony danych osobowych oraz monitorowanie jej wykonania,
   g) realizuje procedury dotyczące: sprostowania, uzupełnienia, usuwania danych osobowych, przenoszenia oraz sprzeciwu w zakresie przetwarzania danych osobowych.

1.3. Administrator Bezpieczeństwa Informacji

1. Wyznaczenie ABI nie jest obowiązkiem, ale prawem Administratora Danych Osobowych. Decyzja o jego wyznaczeniu zostaje potwierdzona stosownym dokumentem załącznik nr 3 do Polityki lub o odwołaniu - załącznik nr 3a do Polityki.
2. W przypadku niepowołania ABI zadania określone w art. 36a ust. 2 pkt 1, z wyłączeniem obowiązku sporządzania sprawozdania, o którym mowa w art. 36a ust. 2 pkt 1 lit.a, wykonuje Administrator Danych Osobowych – oświadczenie załącznik nr 3b.
3. Do zadań ABI należy:
   a) nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
   b) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,
   c) identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych,
   d) sprawowanie nadzoru nad kopiami zapasowymi;

e) inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych,
f) podejmowanie innych czynności w zakresie zabezpieczenia przetwarzania danych w systemach informatycznych,
g) dokonywanie cyklicznych przeglądów aktualności i stosowania procedur z zakresu przetwarzania danych w systemach informatycznych, na podstawie opracowanego planu przeglądów,
h) ścisła współpraca z IOD w zakresie bezpieczeństwa i zasad przetwarzania danych osobowych w systemach informatycznych.

1.4. **Osoby upoważnione do przetwarzania danych osobowych**

1. Do przetwarzania danych w Zespole Szkolno – Przedszkolnym w Lisewie mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez ADO, do zadań tych osób należy m.in:
a) przestrzeganie przepisów prawa powszechnie obowiązującego i regulacji dotyczących ochrony danych osobowych,
b) przetwarzania danych zgodnie z zakresem upoważnienia,
c) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia,
d) niezwłoczne zgłaszanie incydentów dotyczących bezpieczeństwa danych osobowych.

C. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. **Ogólne zasady przetwarzania danych osobowych**

1. Przetwarzanie danych osobowych w strukturze Administratora Danych odbywa się zgodnie z ogólnymi zasadami przetwarzania danych osobowych określonymi w art. 5 RODO. Oznacza to, że dane osobowe przetwarza się:
   a) zgodnie z prawem, w sposób rzetelny przy uwzględnieniu interesów i rozsądnych oczekiwań osób, których dane dotyczą,
   b) w sposób przejrzysty dla osób, których dane dotyczą,
   c) w konkretnych, wyraźnych i prawnie uzasadnionych celach,
   d) w zakresie adekwatnym, stosownym oraz niezbędnym dla celów, w których są przetwarzane,
   e) przy uwzględnieniu ich prawidłowości i ewentualnego uaktualniania,
   f) przez okres nie dłuższy, niż jest to niezbędne dla celów, w których są przetwarzane,
   g) w sposób zapewniający odpowiednie bezpieczeństwo.
2. Administrator Danych gwarantuje, że określone decyzje odnoszące się do procesów przetwarzania danych osobowych zostały przeanalizowane z punktu widzenia zgodności z ogólnymi zasadami przetwarzania danych, a przede wszystkim, że są z nimi zgodne.

3. W przypadku przetwarzania danych osobowych na podstawie zgody osoby, której dane dotyczą, należy stosować oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych, którego wzór stanowi załącznik nr 4 do niniejszej Polityki, natomiast załącznik nr 4a stanowi wzór oświadczenia o cofnięciu zgody na przetwarzanie danych osobowych.
4. Każdej osobie przysługuje prawo do kontroli przetwarzanych danych, które jej dotyczą zawartych w zbiorach danych, a w szczególności:
   a) prawo dostępu do danych (art. 15 RODO),
   b) prawo do sprostowania danych (art. 16 RODO),
   c) prawo do usunięcia danych („prawo do bycia zapomnianym") (art. 17 RODO),
   d) prawo do ograniczenia przetwarzania danych (art. 18 RODO),
   e) prawo do przenoszenia danych (art. 20 RODO),
   f) prawo do sprzeciwu (art. 21 RODO).

2. Obowiązek informacyjny przy przetwarzaniu danych

1. Obowiązek informacyjny spoczywa na Administratorze w myśl art. 13 RODO, realizowany jest poprzez przekazanie osobie, której dane dotyczą informacji dotyczącej pozyskania danych osobowych, a także ich dalszego przetwarzania - wzór klauzuli informacyjnej stanowi załącznik nr 5 do niniejszej Polityki, osoby korzystające z finansowania z Zakładowego Funduszu Świadczeń Socjalnych otrzymują klauzulę załącznik nr 5a
2. Powyższy obowiązek należy spełniać w momencie zbierania danych.
3. Administrator realizuje obowiązek informacyjny w sposób uznany za najbardziej dogodny, poprzez wykorzystanie odpowiednich środków, które umożliwiają w zwięzłej, przejrzystej i łatwo dostępnej formie udzielenie osobie, której dane dotyczą wszelkich informacji. Pracownik otrzymanie klauzuli informacyjnej potwierdza własnoręcznym podpisem w załączniku nr 5b do niniejszej Polityki.

3. Upoważnienie do przetwarzania danych osobowych

1. Administrator Danych Osobowych nadaje upoważnienie do przetwarzania danych osobowych. Upoważnienie jest dokumentem dającym określonym osobom prawo do przetwarzania ściśle określonych danych osobowych - wzór stanowi załączniki nr 6 do Polityki, natomiast osoby będące w komisji Zakładowego Funduszu Świadczeń Socjalnych otrzymują upoważnienie załącznik nr 6a.
2. Administrator Danych Osobowych odwołuje nadane upoważnienia załącznik nr 6b.
3. Upoważnienie nadawane jest wyłącznie w formie pisemnej.
4. W upoważnieniu określony jest zbiór danych osobowych, które pracownik będzie mógł przetwarzać.
5. Administrator Danych Osobowych wpisuje upoważnienia do ewidencji – załącznik nr 6c.
6. Ewidencja upoważnień prowadzona jest w wersji papierowej i musi odzwierciedlać aktualny stan nadanych upoważnień.
7. Ewidencja zawiera następujące dane:
   a) imię i nazwisko pracownika,
   b) datę nadania upoważnienia,
   c) datę odebrania upoważnienia,
   d) nazwy zbiorów objętych zakresem upoważnienia.

4. Umowy powierzenia przetwarzania danych osobowych

1. Administrator Danych Osobowych w uzasadnionych przypadkach wynikających z realizacji zadań może zawrzeć umowę powierzenia z podmiotom zewnętrznym w celu wykonania określonych zadań - załącznik nr 7 do Polityki.
2. Umowa musi być zawarta w formie papierowej, zawierać nazwę podmiotu, zakres i cel przetwarzania danych, określać czas na jaki zostaje zawarta, formę przekazywania danych do przetwarzania, klauzule dotyczącą rozwiązania umowy.
3. Administrator prowadzi rejestr zawartych umów powierzenia według wzoru stanowiącego załącznik 7a do Polityki.

5. Przekazywanie danych do państw trzecich

Administrator nie będzie przekazywał danych do państwa trzeciego, poza sytuacjami w których następuje to na wniosek podmiotów takich jak sądy, urzędy, organy ścigania lub osoby, której dane dotyczą.

6. Zakres przetwarzania danych osobowych

1. Polityka ma zastosowanie w stosunku do wszystkich danych osobowych przetwarzanych przez Administratora Danych, niezależnie od formy ich przetwarzania (elektroniczna lub papierowa) oraz tego, czy są to dane przetwarzane w zbiorach danych, w zestawach czy stanowią one pojedyncze informacje osobowe.
2. Administrator Danych prowadzi:
    1. rejestr czynności przetwarzania danych osobowych, których jest administratorem załącznik nr 8 do Polityki,
    2. rejestr kategorii czynności przetwarzania dokonywanych w imieniu administratorów, którzy powierzyli mu przetwarzanie danych załącznik nr 9 do Polityki.
4. Rejestr czynności przetwarzania zawiera następujące informacje:
    a) nazwę oraz dane kontaktowe Administratora Danych,
    b) gdy ma to zastosowanie imię, nazwisko lub nazwę oraz dane kontaktowe swojego przedstawiciela,
    c) imię i nazwisko oraz dane kontaktowe IOD,
    d) cele przetwarzania,
    e) opis kategorii osób, których dane dotyczą,
    f) opis kategorii danych osobowych,
    g) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
    h) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,
    i) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
    j) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

5. Rejestr kategorii czynności zawiera następujące informacje:
   a) nazwę oraz dane kontaktowe Administratora Danych Osobowych,
   b) imię i nazwisko lub nazwę oraz dane kontaktowe każdego administratora, w imieniu którego działa Administrator Danych Osobowych,
   c) gdy ma to zastosowanie, imię, nazwisko lub nazwę oraz dane kontaktowe przedstawiciela każdego administratora, w imieniu którego działa ADO,
   d) gdy ma to zastosowanie, imię i nazwisko oraz dane kontaktowe IOD każdego administratora, w imieniu którego działa Administrator Danych,
   e) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów,
   f) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,
   g) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

7. Ogólne zasady bezpieczeństwa obowiązujące przy przetwarzaniu danych osobowych

1. Podmiotem odpowiedzialnym za przetwarzanie danych osobowych i ich bezpieczeństwo jest Administrator Danych Osobowych. Zważywszy jednakże na ilość osób upoważnionych do przetwarzania danych osobowych i związane z tym ryzyko niebezpieczeństwa udostępnienia danych osobowych podmiotom nieupoważnionym ustala się następujące ogólne zasady bezpieczeństwa przy przetwarzaniu danych osobowych.
2. Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze, indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.
3. Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
4. Każda osoba, która uzyskała pisemne upoważnienie do przetwarzania danych osobowych, zobowiązana jest do zachowania w poufności wszelkich informacji - wzór oświadczenia o zachowaniu poufności załącznika nr 10 do niniejszej Polityki natomiast załącznik 10a wykaz osób, które otrzymały oświadczenie.
5. Osoba upoważniona powinna przetwarzać dane osobowe w sposób zgodny z przepisami RODO, Ustawy oraz postanowieniami Polityki w Zespole Szkolno - Przedszkolnym w Lisewie oraz zabezpieczać dane przed ich udostępnieniem osobom nieupoważnionym, w sposób:
   a. stosownie zasady „czystego biurka” – w trakcie pracy użytkownik powinien mieć na biurku tylko te materiały, które są niezbędne do wykonywania obowiązków służbowych. W przypadku opuszczenia stanowiska pracy materiały zawierające dane, wymagające szczególnej ochrony powinny być zabezpieczone przed dostępem osób nieuprawnionych. Po zakończeniu dnia pracy każdy użytkownik zobowiązany jest do zabezpieczenia wszelkich dokumentów i nośników zawierających istotne dane, w celu uniemożliwienia dostępu do nich osób nieupoważnionych,
   b. stosowanie zasady „czystego ekranu” – w przypadku czasowego opuszczenia stanowiska pracy użytkownik zobowiązany jest do każdorazowego wylogowania się z sytemu bądź zablokowania dostępu do pulpitu stacji roboczej w celu uniemożliwienia dostępu do systemu operacyjnego lub aplikacji przez osoby niepowołane. Ponadto w trakcie pracy użytkownik

powinien mieć otwarte tylko te aplikacje, które są niezbędne do wykonania obowiązków służbowych,

c. bieżące niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarki oraz przechowywanie pozostałej dokumentacji papierowej w szafach zamykanych na klucz,
d. zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. korytarzach, na kserokopiarkach, drukarkach.
e. zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucenia ich na zewnątrz budynku,
f. niepozostawiania osób postronnych w pomieszczeniach, w których przetwarzane są dane osobowe, bez obecności osoby upoważnionej.

6. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.
7. Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia.
8. Pracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy, jak i po jej zakończeniu, a klucze nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem.
9. Nikomu nie należy udostępniać indywidualnych haseł i identyfikatorów do systemów informatycznych.
10. Po zakończeniu pracy w systemie informatycznym, w którym przechowywane są dane osobowe, należy wylogować się z sytemu.
11. Osoba użytkująca komputer przenośny zawierający dane osobowe zobowiązana jest do zachowania szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe.
12. Na pracowniku pracującym zdalnie spoczywa obowiązek odpowiedniego zabezpieczenia danych tak, aby osoby trzecie nie miały dostępu do danych osobowych.
13. Dane osobowe przesyłane elektronicznie powinny być zabezpieczone hasłem. Hasło to powinno być wysłane oddzielnym kanałem telekomunikacyjnym.
14. Użytkownik odpowiada za niezwłoczne poinformowanie ADO o wszelkich naruszeniach w zakresie bezpieczeństwa ochrony danych osobowych.
15. Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy skutkuje poniesieniem odpowiedzialności karnej na podstawie przepisów Ustawy oraz stanowi ciężkie naruszenie obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy w trybie art. 52 Ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy bądź rozwiązania stosunku cywilnoprawnego.
16. Wszelkie przekroczenia lub jakiekolwiek próby przekroczenia uprawnień, traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.
17. W uzasadnionych sytuacjach ADO może odebrać uprawnienia Użytkownikowi sytemu z podaniem daty oraz przyczyny odebrania uprawnień. W takiej sytuacji należy sporządzić notatkę służbową.

D. NARUSZENIE OCHRONY DANYCH OSOBOWYCH

1. Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

1. W przypadku zaistnienia sytuacji, w której doszło do naruszenia ochrony danych osobowych, odpowiedzialność ponosi Administrator Danych Osobowych. Na nim ciąży obowiązek należytego wykonania wskazanych procedur zabezpieczających.
2. Typowe sytuacje, które mogą świadczyć o fakcie naruszenia danych osobowych:
   a) ślady na drzwiach, oknach i szafach wskazujące na próbę włamania,
   b) otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe, stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały),
   c) fizyczna obecność w budynku szkoły lub pomieszczeniach osób zachowujących się podejrzanie,
   d) dokumentacja jest niszczona bez użycia niszczarki,
   e) niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na kserze, nie zamkniecie pomieszczenia z komputerem,
   f) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej,
   g) telefoniczne próby wyłudzenia danych osobowych,
   h) maile zachęcające do ujawnienia identyfikatora lub hasła,
   i) przechowywanie haseł do systemów w pobliżu komputera.
3. Każda osoba, która poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych osobowych, jest zobowiązana fakt ten niezwłocznie zgłosić Administratorowi Danych Osobowych.
4. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych ADO osoba powiadamiająca powinna:
   a) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny, lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,
   b) zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
   c) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia.
5. Po przybyciu na miejsce naruszenia Administrator Danych Osobowych lub osoba przez niego wyznaczona podejmuje następujące kroki:
   a) wysłuchuje relacji osoby zgłaszającej zaistniałe naruszenie, jak również relacji każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
   b) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metod dalszego postępowania,
   c) fizyczne odłączenie urządzeń, które mogłyby umożliwić dostęp do bazy danych osoby nieupoważnionej,
   d) nawiązuje kontakt ze specjalistami zewnętrznymi (jeśli zachodzi taka potrzeba),
6. Administrator Danych Osobowych lub osoba przez niego wyznaczona dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych i sporządza raport naruszenia załącznik nr 11, który wpisuje do rejestru naruszeń załącznik 11a.
7. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu, Administrator Danych Osobowych lub osoba przez niego wyznaczona, zasięga niezbędnych opinii i proponuje postępowanie naprawcze, (w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych).

2. Zgłoszenie naruszenia ochrony danych do Urzędu Ochrony Danych Osobowych

1. W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Urzędowi Ochrony Danych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych – zgłoszenia naruszenia załącznik 11b
2. Zgłoszenie musi:
   a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
   b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
   c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
   d) opisywać środki zastosowane lub proponowane przez Administratora w celu zapobiegania naruszeniu ochrony danych osobowych, w tym w stosowanych przypadkach – środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
3. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
4. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

3. Zawiadomienie osoby której dane dotyczą, o naruszeniu ochrony danych osobowych

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu
2. Zawiadomienie, załącznik nr 11c, o którym mowa opisuje charakter naruszenia ochrony danych osobowych oraz zawiera informacje o podjętych środkach zaradczych.
3. Zawiadomienie nie jest wymagane, w następujących przypadkach:
   a) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,
   b) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
   c) wymagałoby ono niewspółmiernie dużego wysiłku.

   W tych trzech przypadkach wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w skuteczny sposób.

E. ŚRODKI TECHNICZNE I ORGANIZACYJNE ZAPEWNIAJĄCE BEZPIECZEŃSTWO PRZETWARZANYCH DANYCH OSOBOWYCH

1. Administrator, działając w oparciu o art. 24 ust. 1 i art. 32 ust. 1 RODO, uwzględniając stan wiedzy technicznej, koszt wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.
2. W przypadku stosowania przez Administratora monitoringu wizyjnego zobowiązany jest on do poinformowania pracowników o tym fakcie, w sposób u niego przyjęty, np. poprzez obwieszczenie lub oświadczenie indywidualne, nie później niż 2 tygodnie przed jego uruchomieniem. Administrator, przed wprowadzeniem monitoringu, zobowiązany jest w sposób widoczny i czytelny, za pomocą odpowiednich znaków oznaczyć monitorowany teren. W Zespole Szkolno – Przedszkolnym w Lisewie obowiązuje regulamin funkcjonowania monitoringu wizyjnego.
3. Administrator nie może przechowywać danych z monitoringu wizyjnego przez okres dłuższy, niż 3 miesiące od momentu dokonania nagrania, chyba że istnieje potrzeba przedłużenia tego okresu do czasu zakończenia prawomocnego postępowania, jeżeli nagrania mogą stanowić dowód w postępowaniu. Administrator wykorzystuje nagrania z monitoringu jedynie w celu: zapewnienia bezpieczeństwa pracowników, ochrony mienia, kontroli jakościowego i ilościowego świadczenia pracy oraz zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić Administratora na szkodę.
4. Obszar przetwarzania danych jest zabezpieczony przed dostępem osób nieupoważnionych poprzez zastosowanie drzwi z zamkami, w biurach zainstalowano alarm.
5. Administrator wyznaczył osoby, które upoważnione są do otwierania drzwi wejściowych oraz do rozkodowywania systemu alarmowego przed rozpoczęciem pracy jednostki załącznik nr 12, natomiast załącznik nr 12a stanowi odwołanie upoważnienia do posiadania kluczy. Administrator prowadzi rejestr upoważnień odbioru kluczy załącznik 12b. Osoby, którym zostały powierzone klucze oraz kod cyfrowy do systemu alarmowego zobowiązani są do nieudostępniania kluczy oraz kodu cyfrowego do systemu alarmowego osobom trzecim.
6. Klucze do poszczególnych pomieszczeń pracownicy pobierają i zdają po zakończonym dniu pracy do pokoju nauczycielskiego. Od momentu pobrania kluczy do momentu ich zdania na użytkownikach spoczywa pełna odpowiedzialność za ich zabezpieczenie.
   Po otwarciu pomieszczeń biurowych, przed przystąpieniem do pracy, użytkownicy sprawdzają stan zastosowanych zabezpieczeń. W przypadku stwierdzenia nieprawidłowości należy postępować zgodnie z procedurą naruszeń.
7. Zabrania się pozostawiania kluczy do pomieszczeń obszaru przetwarzania danych w drzwiach lub w miejscach ogólnie dostępnych, pomieszczenia zamyka się na czas nieobecności wszystkich użytkowników w sposób uniemożliwiający dostęp osobom nieupoważnionym.
8. Użytkownicy po godzinach pracy jednostki mogą w nim przebywać jedynie za zgodą Administratora.
9. W przypadku przebywania pracowników w pomieszczeniach obszaru przetwarzania danych po wyznaczonych godzinach pracy, godzinach pełnienia obowiązków, wykonywania zadań na rzecz Administratora należy upewnić się czy zamknięto drzwi wejściowe do obszaru przetwarzania danych osobowych. Dodatkowo opuszczając obszar przetwarzania danych należy sprawdzić czy zamknięto wszystkie okna oraz drzwi wejściowe do pomieszczeń.
10. Szczegółowe skatalogowanie środków technicznych opisane jest w załączniku nr 12c.

F. SZKOLENIA Z ZAKRESU OCHRONY DANYCH OSOBOWYCH

1. Administrator Danych Osobowych przeprowadza wewnętrzne szkolenia z zakresu ochrony danych osobowych dla osób mających dostęp do danych.
2. Szkolenie wewnętrzne powinno być przeprowadzone w przypadku każdej istotnej zmiany zasad lub przepisów dotyczących ochrony danych osobowych wzór karty szkolenia stanowi załącznik nr 13
3. W przypadku przeprowadzenia szkolenia wskazane jest jego udokumentowanie i potwierdzenie uczestnictwa przez osoby biorące w nim udział – załącznik nr 13a.

G. KONTROLA PRZETWARZANIA I STANU ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Nadzór i kontrolę nad ochroną przetwarzanych danych osobowych sprawuje Administrator Danych Osobowych.
2. Jeżeli został ustanowiony Inspektor Ochrony Danych przejmuje on ww. obowiązki w zakresie ochrony i nadzoru wskazanych danych osobowych.
3. Jeżeli został ustanowiony Administrator Systemów Informatycznych sprawuje on nadzór i kontrolę w odniesieniu do danych osobowych przetwarzanych w systemach informatycznych służących do przetwarzania danych osobowych.
4. Z czynności kontrolnych sporządzany jest protokół, którego wzór stanowi załącznik nr 14 do niniejszej Polityki.
5. W protokole zamieszcza się dokładny opis zakresu kontroli i przeprowadzonych czynności.
6. Protokół podpisywany jest przez osoby wykonujące czynności kontrolne. Dołącza się go do dokumentacji przechowywanej u Administratora Danych Osobowych (w przypadku ustanowienia u Inspektora Ochrony Danych, a w zakresie systemów informatycznych u Administratora Systemów Informatycznych).

H. UPRAWNIENIAMIA UŻYTKOWNIKÓW W SYSTEMACH INFORMATYCZNYCH

1. Instrukcja zarządzania uprawnieniami użytkowników w systemach informatycznych

1. Obsługa informatyczna dokonuje modyfikacji, zmiany lub wyrejestrowania uprawnień użytkowników systemów informatycznych na podstawie wniosku otrzymanego od bezpośredniego przełożonego.
2. Obsługa informatyczna jednostki przeprowadza okresową kontrolę uprawnień i kont użytkowników, w celu weryfikacji czy użytkownicy posiadają uprawnienia adekwatne do wykonywanej pracy w systemach informatycznych.
3. Z przeprowadzonej kontroli ww. osoba sporządza notatkę służbową.

2. Procedura dostępu do systemów informatycznych

1. W przypadku dostępu użytkowników do systemów informatycznych (dziedzinowych i operacyjnych) należy stosować metodę uwierzytelniania poprzez wpisanie indywidualnego identyfikatora / loginu oraz hasła.
2. Identyfikator jest przydzielany wg zasady przyjętej w jednostce (np. pierwsza litera imienia i nazwisko). W identyfikatorze należy pomijać polskie znaki diakrytyczne.
3. W przypadku dublowania się identyfikatorów powinien być on rozszerzany o kolejne litery lub cyfry.

4. Hasło powinno składać się z unikalnego zestawu znaków, zawierających małe i wielkie litery, cyfry oraz znaki specjalne.
5. Hasło nie może być identyczne z identyfikatorem użytkownika ani z jego imieniem lub nazwiskiem.
6. Hasła powinny być regularnie zmieniane przez użytkowników oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione osobie nieuprawnionej.
7. Użytkownik zobowiązany jest do zachowania hasła w poufności i niezapisywania haseł w sposób jawny.
8. Hasła administracyjne do urządzeń i systemów informatycznych, w tym baz danych winny być przechowywane w miejscu wskazanym przez Administratora.

3. Obowiązki związane z rozpoczęciem i zakończeniem pracy w systemie informatycznym

1. Przed uruchomieniem komputera użytkownik winien sprawdzić, czy nie zostało do niego podłączone żadne niezidentyfikowane urządzenie.
2. Przed przystąpieniem do pracy w systemie informatycznym, użytkownik winien upewnić się, że spełnione są podstawowe warunki bezpieczeństwa wymagane przy przetwarzaniu danych w systemie informatycznym, a w szczególności ustawienie urządzenia odtwarzającego obraz ze stacji roboczej (np. monitora) w sposób uniemożliwiający osobom trzecim wgląd w dane.
3. Po uruchomieniu komputera użytkownik dokonuje uwierzytelnienia się przy pomocy Identyfikatora oraz Hasła.
4. Przy każdorazowym opuszczeniu stanowiska komputerowego użytkownik powinien dopilnować, aby na ekranie nie były wyświetlane dane.
5. Wychodząc z pomieszczenia, w którym przetwarzane są dane z systemu informatycznego użytkownik powinien sprawdzić czy zamknięte są okna i wejście do pomieszczenia.
6. Przy opuszczaniu stanowiska komputerowego na czas dłuższy niż 5 minut użytkownik zobowiązany jest ustawić wygaszacz ekranu.
7. Na każdym komputerze w ramach sieci lokalnej wygaszacz ekranu uruchamia się po 10 minutach braku aktywności.
8. Po zakończeniu pracy w systemie informatycznym użytkownik obowiązany jest wylogować się z tego systemu.

4. Procedura wykonywania kopii bezpieczeństwa

1. W celu zwiększenia poziomu bezpieczeństwa oraz zapewnienia ciągłości działania jednostki tworzy się kopie zapasowe danych.
2. Za sporządzenie kopi zapasowej odpowiedzialna jest obsługa informatyczna jednostki.
3. Użytkownicy we własnym zakresie odpowiadają za sporządzanie kopii zapasowych dokumentów znajdujących się na lokalnych dyskach twardych.
4. Po wykonaniu kopii zapasowej zaleca się ich weryfikację poprzez dokonanie próby odtworzeniowej.

5. Procedura zarządzania sprzętem elektronicznym i oprogramowaniem

1. Użytkownik zobowiązany jest korzystać ze sprzętu elektronicznego w sposób zgodny z jego przeznaczeniem i chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem.
2. Użytkownik ma obowiązek niezwłocznie zgłosić utratę lub zniszczenie powierzonego sprzętu Administratorowi.
3. Użytkownik nie może bez zgody Administratora instalować dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączać niezatwierdzonych urządzeń do systemu informatycznego.
4. Użytkownik nie może bez zgody Administratora korzystać z prywatnego sprzętu elektronicznego (np. laptopów, telefonów, aparatów fotograficznych, nośników typu pendrive) do wykonywania zadań służbowych.
5. Użytkownik zobowiązany jest do korzystania wyłącznie z oprogramowania dopuszczonego do stosowania w jednostce.
6. Użytkownik nie może instalować ani używać oprogramowania innego, niż przekazane lub udostępnione przez Administratora.

6. Procedura korzystania z poczty elektronicznej

1. Użytkownik jest zobowiązany do korzystania z przyznanego mu adresu mailowego wyłącznie w celu prowadzenia korespondencji służbowej.
2. Użytkownik nie może używać służbowego adresu mailowego do celów prywatnych, w szczególności do rejestracji na portalach społecznościowych, dokonywania zakupów w sklepach internetowych.
3. Użytkownik nie może używać służbowego adresu mailowego w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
4. Użytkownik powinien zachować szczególną ostrożność przy wpisywaniu adresu odbiorcy wiadomości.
5. Użytkownik podczas wysyłania maili do wielu adresatów jednocześnie, powinien użyć metody „Ukryte do wiadomości - UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości".
6. Użytkownik podczas przesyłania danych osobowych pocztą elektroniczną powinien zawrzeć prośbę o potwierdzenie zapoznania się z informacją przez adresata.
7. Użytkownik powinien zastosować zabezpieczenia kryptograficzne przy przesyłaniu załączników do wiadomości. Zabezpieczenie kryptograficzne mogą polegać na przesyłaniu zahasłowanych plików w formie załącznika, niemniej hasło powinno być przekazane adresatowi sms, bądź podczas rozmowy telefonicznej po uprzednim zweryfikowaniu tożsamości adresata.
8. Użytkownik powinien zachować szczególną ostrożność podczas odbierania poczty elektronicznej, a w szczególności nie powinien otwierać plików i linków w niej zawartych, ani otwierać załączników jeżeli nie ma pewności co do autentyczności adresata wiadomości. Tego typu maile większości przypadków mogą zawierać załączniki ze szkodliwym kodem, które po „kliknięciu" infekują komputer użytkownika oraz może istnieć realne ryzyko zaimplementowania kodu w pozostałych komputerach sieci wewnętrznej jednostki.
9. Użytkownik powinien regularnie usuwać niepotrzebne wiadomości pocztowe (tj. spam, oferty handlowe) i opróżniać folder elementów usuniętych.
10. Administrator, jako pracodawca w świetle art. 22^3 § 1 ustawy z dnia 26 czerwca 1974 r. – Kodeks Pracy może wprowadzić kontrolę służbowej poczty elektronicznej pracownika, jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych użytkownikowi narzędzi pracy.
11. W przypadku rozwiązania stosunku pracy z użytkownikiem, osoba wyznaczona przez Administratora zobowiązana jest zablokować konto poczty i usunąć dane.

7. Procedura korzystania z Internetu

1. Użytkownik powinien korzystać z dostępu do sieci Internetu wyłącznie w celach niezbędnych do wykonywania zadań służbowych.
2. Użytkownik nie powinien otwierać stron zawierających treści nie związanych bezpośrednio z merytoryką pracy, ze względu na możliwość przypadkowego pobrania złośliwego kodu, który może automatycznie zainfekować system operacyjny komputera.
3. Użytkownik nie może pobierać aplikacji z sieci Internet bez wcześniejszej zgody Administratora.
4. Użytkownik ponosi pełną odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
5. Użytkownik nie może korzystać ze stron, na których prezentowane są treści o charakterze przestępczym, hackerskim, pornograficznym lub innym zakazanym przez prawo (na większości stron tego typu może być zaimplementowany złośliwy kod, który może automatycznie zainfekować system operacyjny komputera w sposób niewidoczny dla użytkownika).
6. Użytkownik w przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, powinien zwrócić uwagę na pojawienie się odpowiedniej ikony (kłódka) oraz adresu WWW rozpoczynającego się frazą „https:". Dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
7. Użytkownik powinien zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet.

8. Procedura korzystania z bankowości elektronicznej

1. Użytkownik, który wykonuje przelewy bankowe zobowiązany jest do regularnej zmiany hasła oraz nieprzechowywania go w formie pisemnej wraz z loginem.
2. Użytkownik nie może opuścić stanowiska pracy bez wylogowania się i zamknięcia przeglądarki.
3. Użytkownik logujący się do bankowości elektronicznej nie powinien korzystać z nieznanych sieci bezprzewodowych.
4. W celu zalogowania się do systemu bankowości elektronicznej użytkownik nie powinien wchodzić na stronę internetową banku za pośrednictwem linków znajdujących się w korespondencji elektronicznej.

9. Procedura pracy na odległość i mobilnego przetwarzania danych

Administrator dopuszcza możliwość pracy zdalnej pod warunkiem stosowania się do poniższych zasad bezpieczeństwa.

1. Komunikacja z zewnątrz powinna być realizowana tylko poprzez mechanizmy zapewniające odpowiednie bezpieczeństwo (np. VPN, Team Viewer). W przypadku firm zewnętrznych dokonujących czynności serwisowych (np. aktualizacja oprogramowania dziedzinowego) dostęp taki jest nadzorowany przez obsługę informatyczną oraz każdorazowo powinien być poprzedzony autoryzacją (np. podaniem hasła do Team Viewer, które wygasa po skończonej sesji).
2. Administrator dopuszcza możliwość pracy z urządzeń mobilnych wyłącznie z urządzeń przeznaczonych do użytku służbowego.
3. Administrator wprowadza obowiązek logowania połączeń wykonywanych za pomocą sieci bezprzewodowej w celu rejestracji działań użytkowników w sieci i zmniejszenia ryzyka użytkowania sieci niezgodnie z przeznaczeniem.

4. Komunikację należy prowadzić tylko za pomocą bezpiecznych metod transmisji, w tym włączenie transmisji szyfrowanej lub przeniesienie usług sieciowych na serwer posiadających taką możliwość.
5. Urządzenie mobilne służące do łączenia się z systemami i sieciami zarządzanymi przez Administratora muszą być zgłoszone do obsługi informatycznej, celem zabezpieczenia ich odpowiednimi środkami uwierzytelniania, takimi jak np. PIN-y, do zainstalowania odpowiedniego oprogramowania antywirusowego, zaszyfrowania.
6. Obsługa informatyczna prowadzi ewidencję udostępnionych urządzeń mobilnych.
7. Administrator zabrania wykorzystywania służbowych urządzeń mobilnych do celów prywatnych oraz udostępniania ich osobom trzecim, jak również instalowania aplikacji, które nie są niezbędne do wykonywania obowiązków danego pracownika.
8. Administrator zabrania korzystania z publicznych sieci Wi-Fi oraz pozostawiać urządzenia bez nadzoru pracownika, w szczególności w miejscach ogólnodostępnych dla szerokiego grona osób trzecich.
9. Jeżeli użytkownicy korzystają ze służbowych urządzeń mobilnych poza miejscem pracy, zobowiązani są do przestrzegania poniższych zasad bezpiecznego korzystania z urządzeń mobilnych:
   a) nie wolno pozostawiać urządzenia bez opieki i nigdy nie wolno go pożyczać osobie trzeciej,
   b) należy używać kodu blokady, otrzymanego od Administratora, znanego wyłącznie osobie, która dysponuje urządzeniem,
   c) należy na bieżąco (lub z ustalonym przez obsługę informatyczną harmonogramem) zgłaszać się do obsługi informatycznej w celu wykonania aktualizacji systemu oraz aplikacji zainstalowanych w urządzeniu,
   d) jeżeli urządzenie posiada Wi-Fi lub Bluetooth, należy je wyłączać, jeśli nie są w danym czasie wykorzystywane,
   e) nie wolno łączyć się z nieznanymi sieciami bezprzewodowymi,
   f) nie wolno otwierać nieznanych linków lub załączników i nie należy akceptować nieoczekiwanych instalacji aplikacji i/lub wtyczek – o fakcie zaistnienia takich okoliczności należy każdorazowo poinformować Informatyka,
   g) potrzebne do pracy aplikacje należy pobierać tylko ze znanych i zaufanych źródeł,
   h) z siecią firmową należy łączyć się tylko za pośrednictwem urządzeń zaakceptowanych przez Administratora,
   i) należy zawsze używać rozwiązań posiadających silne mechanizmy szyfrowania transmisji i ochrony danych.

10. Procedura postępowania z dokumentami papierowymi zawierającymi dane osobowe

1. W stosunku do dokumentów papierowych stanowiących wydruki z systemu obowiązują następujące środki ostrożności:
   a) wydruki i dokumentacja powinny być niedostępne dla osób postronnych,
   b) nie mogą być pozostawione w drukarce ogólnodostępnej,
   c) wydruki niepotrzebne i nieprzydatne powinny być na bieżąco niszczone za pomocą niszczarki,
   d) dokumenty, których nie można zniszczyć z przyczyn technicznych lub formalnych, powinny być składowane w miejscu z ograniczonym dostępem, systematycznie weryfikowane, a następnie archiwizowane zgodnie z obowiązującymi w tym zakresie przepisami.

11. Procedura zabezpieczania sprzętu elektronicznego i systemu informatycznego

1. Komputery stacjonarne i przenośne powinny być zabezpieczone programem antywirusowym, który sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu.
2. Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie powinno odbywać się przy wykorzystaniu ww. oprogramowania zainstalowanego na stacjach roboczych oraz komputerach przenośnych.
3. Obowiązkiem obsługi informatycznej jest nadzór nad aktualizacją oprogramowania antywirusowego.
4. Użytkownik jest obowiązany każdorazowo zawiadomić obsługę informatyczną o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem – wirusa lub w przypadku sygnalizowanych problemów z działaniem oprogramowania antywirusowego.
5. Użytkownik, który posiada dostęp do systemów informatycznych powinien mieć zablokowaną możliwość instalowania nieautoryzowanego oprogramowania.

12. Procedura korzystania z elektronicznych nośników danych oraz komputerów przenośnych

1. Użytkownik może korzystać wyłącznie z elektronicznych nośników danych w szczególności pendrive'ów, dysków zewnętrznych, CD-R, DVD, oraz komputerów przenośnych przeznaczonych do użytku służbowego.
2. Użytkownik korzystający z elektronicznych nośników danych oraz komputerów przenośnych jest w całym okresie użytkowania odpowiedzialny za bezpieczeństwo danych i oprogramowania na nim zainstalowanego.
3. Użytkownik korzystający z ww. urządzeń zobowiązany jest do:
   a) przechowywania danych na dysku szyfrowanym zabezpieczonym hasłem,
   b) transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia oraz stosownego zabezpieczenia komputera przed uszkodzeniem,
   c) zdecydowanego i skutecznego uniemożliwienia korzystania z komputera osobom nieuprawnionym (np. rodzinie, dzieciom, znajomym).
3. Obsługa informatyczna jest odpowiedzialna za prowadzenie inwentaryzacji sprzętu elektronicznego i oprogramowania oraz utrzymywanie jej w aktualności.

13. Procedura wykonywania przeglądów i konserwacji sprzętu elektronicznego i nośników danych

1. Obsługa informatyczna dokonuje przeglądu i konserwacji sprzętu elektronicznego i nośników danych.
2. Użytkownik nie może samodzielnie dokonywać napraw sprzętu elektronicznego, wymiany jego podzespołów oraz wykonywać innych czynności nie związanych bezpośrednio z jego eksploatacją lub niedopuszczonych do wykonywania przez producenta sprzętu w instrukcji obsługi.
3. Użytkownik ma obowiązek niezwłocznie powiadomić obsługę informatyczną o wszelkich nieprawidłowościach i awariach sprzętu informatycznego, mogących prowadzić do próby naruszenia lub naruszenia bezpieczeństwa danych osobowych.
4. W przypadku awarii systemu informatycznego i utraty informacji lub w przypadku zaistnienia możliwości uszkodzenia informacji, obsługa informatyczna jest zobowiązana do:

a) przetestowania sieci informatycznej, systemu informatycznego oraz aplikacji służącej do przetwarzania danych,
b) ocenić zasadność odtworzenia danych przy wykorzystaniu aktualnej kopii zapasowej lub kilku kopii zapasowych, a w przypadku uzasadnionej konieczności odtworzyć dane przy wykorzystaniu aktualnej kopii zapasowej lub kilku kopii zapasowych.

14. Procedura utylizacji i serwisu sprzętu elektronicznego

1. W przypadku wycofania sprzętu elektronicznego z użycia, dane osobowe na nim zapisane powinny być kasowane przy użyciu dedykowanego oprogramowania do bezpiecznego usuwania danych, najlepiej za pomocą certyfikowanego urządzenia np. de magnetyzera.
2. W przypadku braku możliwości programowego usunięcia danych ze sprzętu elektronicznego podlega on fizycznemu zniszczeniu.
3. Zniszczenie sprzętu elektronicznego powinno być potwierdzone protokołem zniszczenia.
4. W przypadku przekazywania stacji roboczej z dyskiem albo innych nośników danych do naprawy, dysk lub nośnik powinien zostać zdemontowany lub pozbawiony danych. Naprawa powinna być dokonywana w obecności osoby upoważnionej przez Administratora lub powinna zostać zawarta umowa powierzenia przetwarzania danych.

I. PROCEDURA ZARZĄDZANIA RYZYKIEM

1. Administrator analizuje możliwe sytuacje i naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
2. Administrator przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii.
3. Analiza ryzyka powinna zapewniać:

a) zidentyfikowanie ryzyka,
b) oszacowanie ryzyka z punktu widzenia następstw dla działalności oraz prawdopodobieństwa wystąpienia,
c) informowanie o prawdopodobieństwie i następstwach ryzyka oraz zrozumienie tych informacji,
d) ustanowienie priorytetów postępowania z ryzykiem,
e) regularne monitorowanie i przegląd różnych typów ryzyka oraz procesu zarządzania ryzykiem,
f) zbieranie informacji w celu doskonalenia podejścia do zarządzania ryzykiem.

4. Administrator dokumentuje wykonaną analizę ryzyka.
5. Administrator dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka, ryzyko naruszenia praw i wolności osób jest wysokie.

J. PRZEPISY KOŃCOWE

W sprawach nieuregulowanych w niniejszej Instrukcji mają zastosowanie przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej: RODO), ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa

K. WYKAZ ZAŁĄCZNIKÓW:

1. Wykaz osób zapoznanych z Polityką Ochrony Danych Osobowych
2. Powołanie Inspektora Ochrony Danych
2a. Odwołanie Inspektora Ochrony Danych
3. Powołanie Administratora Bezpieczeństwa Informacji
3a. Odwołanie Administratora Bezpieczeństwa Informacji
3b. Oświadczenie Administratora Danych Osobowych
4. Oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych
4a. Oświadczenie o cofnięciu zgody na przetwarzanie danych osobowych
5. Obowiązek informacyjny art. 13 RODO
5a. Obowiązek informacyjny art. 13 RODO na potrzeby świadczeń socjalnych
5b. Wykaz osób, które otrzymały obowiązek informacyjny art. 13 RODO
6. Upoważnienie do przetwarzania danych osobowych
6a. Upoważnienie do przetwarzania danych osobowych dla członka komisji socjalnej
6b. Odwołanie upoważnienia do przetwarzania danych osobowych
6c. Ewidencja osób upoważnionych do przetwarzania danych osobowych
7. Umowa powierzenia danych osobowych
7a. Rejestr zawartych umów powierzenia
8. Rejestr czynności przetwarzania
9. Rejestr kategorii przetwarzania danych
10. Oświadczenie o zachowaniu w poufności danych
10a. Wykaz osób, które otrzymały oświadczenie o zachowaniu poufności danych
11. Raport naruszenia ochrony danych osobowych
11a. Rejestr naruszeń ochrony danych osobowych
11b. Zgłoszenie o naruszeniu ochrony danych osobowych organowi nadzorczemu
11c. Zawiadomienie o naruszeniu ochrony danych osoby, której dane zostały naruszone
12. Upoważnienie do posiadania kluczy wejściowych
12a. Odwołanie upoważnienia do posiadania kluczy wejściowych
12b. Ewidencja przydziału kluczy wejściowych
12c. Opis środków technicznych stosowanych do zabezpieczenia danych
13. Karta szkolenia z zakresu ochrony danych osobowych, w tym z zakresu przepisów RODO
13a. Potwierdzenie uczestnictwa w szkoleniu z zakresu ochrony danych osobowych
14. Protokół z kontroli przetwarzania i stanu zabezpieczenia danych osobowych

ZESPÓŁ SZKOLNO-PRZEDSZKOLNY
w Lisewie
86-230 Lisewo, ul. Toruńska 17
tel./fax 56 676 79 16
NIP: 875-14-97-933

Dyrektor Zespołu
Szkolno-Przedszkolnego w Lisewie
mgr Grzegorz Zalewski

Lisewo, 17 maja 2018 r.