„ZATWIERDZAM”

POLITYKA BEZPIECZEŃSTWA INFORMACJI
I REGULAMIN
OCHRONY DANYCH OSOBOWYCH

w Zespole Szkół Nr 2 z Oddziałami Integracyjnymi w Hajnówce

Administrator
Bezpieczeństwa Informacji

Hajnówka**2013**

**SPIS** TREŚCI

1. POLITYKA BEZPIECZEŃSTWA 4

Pojęcia podstawowe 4

Cele 5

1. [ADMINISTRACJA I ORGANIZACJA BEZPIECZEŃSTWA 6](#bookmark1)

Informacje ogólne 6

Administrator Bezpieczeństwa Informacji 6

Użytkownik systemu 7

Bezpieczeństwo przetwarzania danych osobowych 7

1. WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM

PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH 8

1. SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI

SYSTEMAMI 8

Komunikacja 8

1. OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI

I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH 8

1. [UDOSTĘPNIANIE POSIADANYCH W ZBIORZE DANYCH OSOBOWYCH](#bookmark4) 9
2. [BEZPIECZEŃSTWO PERSONELU](#bookmark5) 9

Informacje ogólne 9

Użytkownicy systemu 9

1. [BEZPIECZEŃSTWO FIZYCZNE 1](#bookmark6)0

Informacje ogólne 10

Pomieszczenia lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe - obszar systemu - 10

Ochrona serwera, stacji roboczych i nośników 10

Zasady kontroli sprzętu 10

1. [BEZPIECZEŃSTWO SPRZĘTU I OPROGRAMOWANIA 1](#bookmark7)1

Informacje ogólne 11

Bezpieczeństwo Sprzętowe 11

Bezpieczeństwo Oprogramowania 11

1. KONSERWACJE I NAPRAWY 11

Konserwacja sprzętu 11

Konserwacja oprogramowania 11

Naprawa sprzętu 11

1. [PLANY AWARYJNE I ZAPOBIEGAWCZE 1](#bookmark8)2

Zasilanie 12

Kopie zapasowe 12

1. [POLITYKA ANTYWIRUSOWA 1](#bookmark9)2
2. [UDOSTĘPNIANIE DANYCH OSOBOWYCH 1](#bookmark10)2
3. POSTANOWIENIA KOŃCOWE 12
4. [LISTA ZAŁĄCZNIKÓW 1](#bookmark11)3

POJĘCIA PODSTAWOWE

1. Polityka Bezpieczeństwa została utworzona w związku z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926, ze zm.) oraz rozporządzeniu 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 Dz. U. z 2004 r. Nr 100, poz. 1024 i rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla systemów teleinformatycznych Dz. U. z 16 maja 2012 r., poz. 526. Opracowany dokument jest zgodny z dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osób oraz ochrony prywatności w sektorze komunikacji elektronicznej.
2. Regulamin niniejszy określa tryb i zasady ochrony danych osobowych przetwarzanych w Zespole Szkół nr 2 z Oddziałami Integracyjnymi w Hajnówce, zwanym dalej Jednostką.
3. Ilekroć w regulaminie jest mowa o:
4. Jednostce - rozumie się przez to **w Zespole Szkół Nr 2 z Oddziałami Integracyjnymi w Hajnówce**
5. zbiorze danych osobowych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
6. danych osobowych - rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
7. przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
8. systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
9. systemie tradycyjnym - rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;
10. zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
11. usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
12. administratorze danych osobowych - w świetle art. 3 i 7 pkt 4 ustawy o ochronie danych osobowych rozumie się przez to Dyrektora Jednostki, który decyduje o celach i środkach przetwarzania danych osobowych;
13. administratorze bezpieczeństwa informacji - rozumie się przez to osobę wyznaczoną przez Dyrektora Jednostki, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem oraz upoważnioną do realizacji zadań związanych z zarządzaniem systemem informatycznym;
14. użytkowniku systemu informatycznego - rozumie się przez to upoważnionego przez Dyrektora Jednostki, wyznaczonego do przetwarzania danych osobowych w systemie informatycznym pracownika, który odbył stosowne szkolenie w zakresie ochrony tych danych;
15. zgodzie osoby, której te 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.

CELE

Celem opracowania polityki bezpieczeństwa jest ochrona przed niepowołanym dostępem do:

1. systemu informatycznego oraz informacji udostępnianych z jego wykorzystaniem;
2. informacji zgromadzonych, przetwarzanych w formie tradycyjnej.

Niniejsze opracowanie określa politykę bezpieczeństwa w zakresie przetwarzania danych osobowych przez pracowników Jednostki, a w szczególności Administratora Danych Osobowych oraz Administratora Bezpieczeństwa Informacji.

Dane osobowe w Jednostce są gromadzone, przechowywane, edytowane, archiwizowane w kartotekach, skorowidzach, księgach, wykazach, zestawieniach oraz w innych zestawach i zbiorach ewidencyjnych poszczególnych komórek organizacyjnych Jednostki na dokumentach papierowych, jak również w systemach informatycznych na elektronicznych nośnikach informacji.

Powyższy dokument wprowadza regulacje w zakresie zasad organizacji procesu przetwarzania i odnosi się swoją treścią do informacji:

1. w formie papierowej - przetwarzanej w ramach SYSTEMU

TRADYCYJNEGO;

1. w formie elektronicznej - przetwarzanej w ramach SYSTEMU

INFORMATYCZNEGO;

Bezpośredni nadzór nad przetwarzaniem danych osobowych sprawują Administratorzy Danych Osobowych.

Z zapisanymi w polityce bezpieczeństwa obowiązkowo są zapoznawani wszyscy użytkownicy systemów informatycznych i tradycyjnych.

Do informacji przechowywanych w systemach informatycznych jak i dokumentów tradycyjnych mają dostęp jedynie upoważnieni pracownicy Jednostki oraz osoby mające imienne zarejestrowane upoważnienie. Wszyscy pracownicy zobowiązani są do zachowania tych danych w tajemnicy. Dopuszczalny sposób i zakres przetwarzania danych osobowych regulują zapisy ustaw kompetencyjnych, szczegółowych właściwych dla komórek organizacyjnych Jednostki.

Dane osobowe są chronione zgodnie z polskim prawem oraz procedurami obowiązującymi w instytucjach samorządowych dotyczącymi bezpieczeństwa i poufności przetwarzanych danych. Systemy informatyczne oraz tradycyjne, które przechowują dane osobowe, są chronione odpowiednimi środkami technicznymi. Opracowane procedury określają obowiązki użytkownika zbiorów tradycyjnych oraz zasady korzystania z systemów informatycznych. Każdy użytkownik systemu informatycznego zobowiązany jest zapamiętać swoją nazwę użytkownika oraz hasło i nie udostępniać go innym osobom. Użytkownik systemu informatycznego powinien pamiętać o wylogowaniu się po zakończeniu korzystania z usług systemów informatycznych.

1. ADMINISTRACJA I ORGANIZACJA BEZPIECZEŃSTWA

INFORMACJE OGÓLNE

Za bezpieczeństwo danych osobowych przetwarzanych w systemach przetwarzania danych osobowych odpowiada Administrator Danych Osobowych. Administrator Danych Osobowych obowiązany jest zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinni zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą utratą uszkodzeniem lub zniszczeniem.

Administrator Danych Osobowych wyznacza Administratora Bezpieczeństwa Informacji, nadzorującego przestrzeganie zasad ochrony. Imienne upoważnienie udzielane jest w formie pisemnej i stanowi załącznik nr 3 do niniejszego regulaminu.

Administrator Danych Osobowych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych. Prowadzi również ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać:

1. imię, nazwisko i stanowisko osoby upoważnionej
2. datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych/ nazwę użytkowanego programu (aplikacji)

Upoważnienie do przetwarzania danych osobowych wydawane przez Administratora Danych Osobowych pracownikom Jednostki stanowi załącznik nr 2, a ewidencję osób upoważnionych do przetwarzania danych osobowych stanowi załącznik nr 1 do niniejszego regulaminu.

Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia. Oświadczenie o zapewnieniu ochrony danych osobowych stanowi załącznik nr 4 do niniejszego regulaminu.

ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

Administrator Bezpieczeństwa Informacji wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemami informatycznymi i tradycyjnymi.

Administrator Bezpieczeństwa Informacji jest zobowiązany do zapewnienia, poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, iż wyłącznie autoryzowany personel ma dostęp do systemów informatycznych i tradycyjnych. Ponadto, w uzgodnieniu z Administratorem Danych Osobowych, przydziela użytkownikom systemu informatycznego konta i hasła oraz określa warunki i sposób ich przydzielania. Administrator Bezpieczeństwa Informacji posiada bieżącą listę osób upoważnionych do przetwarzania danych osobowych.

Szczegółowy zakres odpowiedzialności i obowiązków Administratora Bezpieczeństwa Informacji jest następujący:

1. nadzoruje bezpieczeństwo systemów informatycznych i tradycyjnych;
2. zapewnia aktualizację oprogramowania i dokumentacji technicznej systemu w tym opis struktur zbiorów i ich zależności
3. nadzoruje przestrzeganie przez wszystkich użytkowników stosowanie obowiązujących procedur;
4. weryfikuje listę autoryzowanych użytkowników systemów informatycznych;
5. doradza użytkownikom w zakresie bezpieczeństwa;
6. zapewnia, aby cały personel posiadający dostęp do systemu posiadał stosowne zezwolenia oraz był przeszkolony w zakresie obowiązujących regulacji bezpieczeństwa;
7. przygotowuje i prowadzi „Ewidencja osób biorących udział w przetwarzaniu danych osobowych";
8. prowadzi kontrole w zakresie bezpieczeństwa;
9. przygotowuje wnioski pokontrolne.

UŻYTKOWNIK SYSTEMU

Użytkownik systemu wykonuje wszystkie prace niezbędne do efektywnej oraz bezpiecznej pracy na stanowisku pracy również z wykorzystaniem stacji roboczej. Jest odpowiedzialny przed Administratorem Bezpieczeństwa Informacji za nadzór, implementację i utrzymanie niezbędnych warunków bezpieczeństwa w szczególności do przestrzegania procedur dostępu do systemu i ochrony danych osobowych.

BEZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH

1. Bezpieczeństwo w przetwarzaniu danych osobowych w formie tradycyjnej

Pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych pozostają zawsze pod bezpośrednim nadzorem upoważnionego do ich przetwarzania pracownika. Opuszczenie pomieszczenia, w których znajdują się zbiory danych osobowych musi być poprzedzone przeniesieniem zbioru danych do odpowiednio zabezpieczonego miejsca. Przy planowanej dłuższej nieobecności pracownika pomieszczenie winno być zamknięte na klucz.

Klucze do szaf, w których przechowywane są dane osobowe maj ą jedynie pracownicy upoważnieni do przetwarzania danych osobowych w zakresie zgodnym z kategorią danych. Dostęp do pokoi jest kontrolowany za pomocą monitoringu wizyjnego.

Korzystanie ze zbiorów danych osobowych przez osoby niezatrudnione w Jednostce powinno odbywać się po uzyskaniu upoważnienia lub skonsultowane z ABI w przypadku osób upoważnionych do przetwarzania tych danych na podstawie ogólnie obowiązujących przepisów.

1. Bezpieczeństwo w przetwarzaniu danych osobowych w systemach informatycznych

Zasady bezpiecznego użytkowania systemu informatycznego zawarte są w Instrukcji Zarządzania Systemem Informatycznym, obligatoryjnej do zapoznania się i stosowania przez wszystkich użytkowników systemu informatycznego szkoły.

1. WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

Dane osobowe są gromadzone, przechowywane i przetwarzane w kartotekach, skorowidzach, księgach, wykazach oraz w innych zbiorach ewidencyjnych poszczególnych komórek organizacyjnych Jednostki w postaci dokumentów papierowych.

Do przetwarzania zbiorów danych osobowych w systemie informatycznym Jednostki, stosowane są pakiety biurowe lub specjalizowane aplikacje (programy).

Zestawienie programów oraz zbiorów danych stanowi załącznik nr 5 i 6 do niniejszego regulaminu.

1. SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

**KOMUNIKACJA.**

Obieg dokumentów zawierających dane osobowe, pomiędzy komórkami

organizacyjnymi Jednostki, winien odbywać w sposób zapewniający pełną ochronę przed ujawnieniem zawartych w tych dokumentach danych (informacji).

Przekazywanie informacji (danych) w systemie informatycznym poza sieć lokalną Jednostki, w miarę możliwości, powinno odbywać się w sposób szyfrowany.

1. OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

Dostęp do danych wprowadzonych przez użytkowników systemów informatycznych mają jedynie Administrator Danych Osobowych, upoważnieni pracownicy oraz Administrator Bezpieczeństwa Informacji zapewniający jego prawidłową eksploatację. Wszyscy pracownicy, będący użytkownikami systemu zobowiązani są do zachowania tych danych w tajemnicy.

1. Ochronie podlegają dane osobowe gromadzone i przetwarzane w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych oraz w urządzeniach i systemie informatycznym Jednostki;
2. Pomieszczenia, w których przetwarza się dane osobowe powinny być fizycznie zabezpieczone przed dostępem osób nieuprawnionych, to znaczy posiadać odpowiednie zamki do drzwi, zabezpieczenia w oknach (w szczególności na parterze) oraz być wyposażone w środki ochrony ppoż. (gaśnice);
3. Dokumenty i nośniki informacji, zawierające dane osobowe powinny być zabezpieczone przed dostępem osób nieupoważnionych do przetwarzania danych. Jeśli nie są aktualnie używane powinny być przechowywane w szafach lub w innych przeznaczonych do tego celu urządzeniach biurowych, posiadających odpowiednie zabezpieczenia :

Zasady zabezpieczania danych:

1. zbiory kartotekowe winny znajdować się w zamkniętych pomieszczeniach zabezpieczonych przed dostępem osób nieupoważnionych;
2. zbiory w systemach informatycznych winny być zabezpieczone hasłem dostępu znanym użytkownikowi zbioru
3. UDOSTĘPNIANIE POSIADANYCH W ZBIORZE DANYCH OSOBOWYCH
4. Do udostępniania posiadanych w zbiorze danych osobowych upoważniony jest Administrator Danych Osobowych lub pracownik posiadający wymagane prawem upoważnienie.
5. W przypadku udostępniania danych osobowych w celach innych niż włączenie do zbioru, Administrator Danych Osobowych udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
6. BEZPIECZEŃSTWO PERSONELU

INFORMACJE OGÓLNE

Należy mieć świadomość, że każdy, kto ma dostęp do pomieszczenia, w którym zainstalowano sprzęt systemu informatycznego może spowodować jego uszkodzenie lub może mieć dostęp do informacji wyświetlanych na monitorze lub wydruków.

Zagrożenia w stosunku do systemu mogą pochodzić również od każdej innej osoby np. personelu pomocniczego, technicznego, konsultanta itp., posiadającej wystarczające umiejętności i wiedzę, aby uzyskać dostęp do sieci.

UŻYTKOWNICY SYSTEMU

Wszyscy użytkownicy systemu muszą stosować się do obowiązujących procedur bezpieczeństwa.

Hasło podlega szczególnej ochronie. Użytkownik ma obowiązek tworzenia haseł o długości min. 8 znaków, nie trywialnych lub słownikowych, tzn. nie może używać imion, danych identyfikujących użytkownika oraz jego najbliższych, oraz nie może tworzyć haseł przez kombinację tych nazw lub ich zmianę uporządkowania np. od tyłu. Jest wprowadzony wymóg zabraniający dokonywana zapisów haseł przez użytkowników. W przypadku, gdy użytkownik zapomni swoje hasło, może on uzyskać nowe hasło od Administratora Bezpieczeństwa Informacji zgodnie z obowiązująca procedurą.

VIM. BEZPIECZEŃSTWO FIZYCZNE

INFORMACJE OGÓLNE

Informacja przetwarzana i przechowywana w systemie musi być zabezpieczona w szczególny sposób.

Środki bezpieczeństwa fizycznego są konieczne dla zapobiegania niepowołanemu dostępowi do informacji, nieautoryzowanym operacjom w systemie, kontroli dostępu do zasobów oraz w celu zabezpieczenia sprzętu teleinformatycznego.

POMIESZCZENIA LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE - OBSZAR SYSTEMU -

Obszarem do przetwarzania danych osobowych z użyciem sprzętu komputerowego są:

1. sekretariat,
2. gabinet dyrektora,
3. gabinet wicedyrektora
4. gabinet pedagoga i psychologa szkolnego,
5. biblioteka szkolna,
6. pokój nauczycielski ,
7. pokój księgowości,
8. wszystkie sale lekcyjne wyposażone na stanowiskach nauczycielskich w komputery

Pomieszczenia te zabezpieczone są w następujący sposób:, zamki, szkolny monitoring.

OCHRONA SERWERA, STACJI ROBOCZYCH I NOŚNIKÓW

Pomieszczenia, w których znajdują się stanowiska komputerowe są:

1. zamknięte, jeśli nikt w nich nie przebywa;
2. wyposażone w zamykane szafy umożliwiające przechowywanie dokumentów.

Szkolny serwer znajduje się w zamkniętym osobnym pomieszczeniu, do którego dostęp ma tylko ADO i ABI..

ZASADY KONTROLI SPRZĘTU

Instalacja urządzeń systemu i sieci teleinformatycznej odbywa się za wiedzą i pod kontrolą Administratora Danych Osobowych, który jest również odpowiedzialny za warunki wprowadzania do użycia, przechowywania, eksploatacji oraz wycofywania z użycia każdego urządzenia.

IX. BEZPIECZEŃSTWO SPRZĘTU I OPROGRAMOWANIA

INFORMACJE OGÓLNE

Sprzęt i oprogramowanie, indywidualnie lub łącznie mają ścisły związek z bezpieczeństwem systemu i sieci teleinformatycznej. Dlatego, powinny być ściśle przestrzegane procedury bezpieczeństwa odnoszące się do tych elementów.

BEZPIECZEŃSTWO SPRZĘTOWE

Sieć teleinformatyczna jest organizacyjnym i technicznym połączeniem systemów teleinformatycznych wraz z łączącymi je urządzeniami i liniami telekomunikacyjnymi. Niedopuszczalne jest samowolne przemieszczanie lub zmiana konfiguracji stacji roboczej bez wiedzy Administratora Bezpieczeństwa Informacji.

BEZPIECZEŃSTWO OPROGRAMOWANIA

Nie zezwala się na korzystanie z jakiegokolwiek nowego oprogramowania bez zgody Administratora Bezpieczeństwa Informacji. Dodatkowe oprogramowanie może być instalowane wyłącznie przez Administratora Bezpieczeństwa Informacji. Kopie

oprogramowania operacyjnego, aplikacyjnego i użytkowego przechowuje się w szafie pancernej w serwerowni.

Używanie oprogramowania prywatnego w sieci jest kategorycznie zabronione. Na stacjach roboczych powinno być zainstalowane jedynie niezbędne oprogramowanie.

KONSERWACJA SPRZĘTU

Każde urządzenie użytkowane w systemie informatycznym, powinno podlegać rutynowym czynnościom kons erwacyjnym oraz przeglądom wykonywanym przez uprawnione osoby.

KONSERWACJA OPROGRAMOWANIA

Za konserwację oprogramowania systemowego oraz aplikacyjnego serwera systemu informatycznego odpowiedzialny jest Administrator Bezpieczeństwa Informacji. Konserwacja ww. oprogramowania obejmuje także jego aktualizację.

Za konserwację oprogramowania stanowisk roboczych odpowiedzialny jest Administrator Danych Osobowych. Wszelkie aktualizacje oprogramowania powinny być uzgadniane z Administratorem Bezpieczeństwa Informacji.

NAPRAWA SPRZĘTU

Administrator Bezpieczeństwa Informacji przed rozpoczęciem naprawy urządzenia przez zewnętrzne firmy sprawdza, czy spełnione są następujące wymagania:

1. w przypadku awarii serwera i konieczności oddania sprzętu do serwisu, nośniki magnetyczne zawierające dane osobowe powinny być wymontowane i do czasu naprawy serwera przechowywane w szafie metalowej znajdującej się w strefie o ograniczonym dostępie;
2. w przypadku uszkodzenia nośnika magnetycznego zawierającego dane osobowe należy komisyjnie dokonać jego zniszczenia.
3. PLANY AWARYJNE I ZAPOBIEGAWCZE

ZASILANIE

Serwer systemu oraz poszczególne stacje robocze (opcjonalnie) powinny być zabezpieczone urządzeniami podtrzymującymi zasilanie (UPS), co umożliwi funkcjonowanie systemu w przypadku awarii zasilania.

KOPIE ZAPASOWE

W celu zabezpieczenia ciągłości pracy, informacja przechowywana i przetwarzana w systemie podlega codziennej, przyrostowej archiwizacji (opcjonalnie) oraz pełnej archiwizacji przeprowadzanej nie rzadziej niż raz na miesiąc. Kopie archiwalne danych są wykonywane na nośnikach magnetooptycznych, i przechowywane są przez Administratora Bezpieczeństwa Informacji. Użycie kopii zapasowych następuje na polecenie Administratora Bezpieczeństwa Informacji w przypadku odtwarzania systemu po awarii.

1. POLITYKA ANTYWIRUSOWA

W zakresie ochrony antywirusowej wprowadza się następujące zalecenia:

1. nie należy używać oprogramowania na stacji roboczej innego niż zaleca Administrator Bezpieczeństwa Informacji
2. nie wolno instalować oprogramowania typu freeware czy shareware;
3. regularnie uaktualniać bazę wirusów zainstalowanego oprogramowania antywirusowego;
4. przed użyciem nośnika danych sprawdzić czy nie jest zainfekowany wirusem komputerowym.
5. UDOSTĘPNIANIE DANYCH OSOBOWYCH

Każda osoba, której dane osobowe są przetwarzane w systemie informatycznym, ma prawo uzyskać na piśmie, w powszechnie zrozumiałej formie, treść tych danych oraz następujące informacje:

1. datę pierwszego wprowadzenia danych tej osoby,
2. źródło pochodzenia danych,
3. identyfikator użytkownika wprowadzającego dane,
4. jakim uprawnionym podmiotom, kiedy i w jakim zakresie dane zostały udostępnione
5. W sprawach nieobjętych niniejszym regulaminem maja zastosowanie przepisy ustawy o ochronie danych osobowych.
6. Regulamin wchodzi w życie z dniem ogłoszenia.

XV. LISTA ZAŁĄCZNIKÓW

1. Ewidencja osób upoważnionych do przetwarzaniu danych osobowych - wzór
2. Upoważnienie do przetwarzania danych osobowych - wzór
3. Upoważnienie do wykonywania zadań Administratora Bezpieczeństwa Informacji - wzór
4. Oświadczenie o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych - wzór
5. Lista zbiorów danych osobowych
6. Lista oprogramowania wykorzystywanego do przetwarzania danych osobowych
7. „6 Zasad” bezpiecznej pracy przy przetwarzaniu wszelkiego rodzaju informacji, w tym danych osobowych.
8. Przypadki zakwalifikowane jako naruszenie bezpieczeństwa informacji.
9. Katalog form naruszeń i incydentów w zakresie danych osobowych.
10. Raport z naruszenia ochrony danych osobowych - wzór

Załącznik Nr 1 do Polityki Bezpieczeństwa Informacji i Regulaminu Ochrony Danych Osobowych

Lista osób upoważnionych do przetwarzaniu danych osobowych w Zespole Szkół Nr2 z Oddziałami Integracyjnymi w Hajnówce

1. Administrator Danych Osobowych -

Data nadania uprawnień , data ustania uprawnień ………….

2. Administrator Bezpieczeństwa Informacji -

Data nadania uprawnień , data ustania uprawnień ………….

3. Administrator Bezpieczeństwa Informacji -

Data nadania uprawnień , data ustania uprawnień ………….

5. Użytkownik -

Data nadania uprawnień , data ustania uprawnień …………

Zakres upoważnienia

6. Użytkownik -

Data nadania uprawnień , data ustania uprawnień …………

Zakres upoważnienia

7. Użytkownik -

Data nadania uprawnień , data ustania uprawnień …………

Zakres upoważnienia

8. Użytkownik -

Data nadania uprawnień , data ustania uprawnień …………

Zakres upoważnienia

9. Użytkownik -

Data nadania uprawnień , data ustania uprawnień …………

Zakres upoważnienia

(pieczęć administratora danych) Hajnówka, dnia roku

Załącznik Nr 2 do **Polityki Bezpieczeństwa Informacji i Regulaminu Ochrony Danych Osobowych**

Upoważnienie do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 roku nr 101, poz. 926 z późn. zm.) upoważniam

Panią/Pana

(imię i nazwisko, stanowisko)

do przetwarzania danych osobowych w zbiorze danych/zbiorach

danych\*

w następującym zakresie:

1.
2.
3.

wyłącznie w związku z wykonywaniem obowiązków pracowniczych.

Upoważnienie nie obejmuje przetwarzania danych osobowych w zakresie:

1.
2.
3.

Upoważnienie udzielane jest na czas trwania zatrudnienia/do odwołania/od

do

(podpis osoby reprezentującej administratora danych)

Wnoszę/nie wnoszę\* o nadanie identyfikatora użytkownika i przyznanie hasła

(podpis działu kadr)

**Pouczenie**: osoba upoważniona do przetwarzania danych zgodnie z art. 39 ust. 2 ustawy o ochronie danych osobowych obowiązana jest zachować w tajemnicy dane osobowe oraz sposoby ich zabezpieczenia, w tym także po ustaniu zatrudnienia/odwołaniu upoważnienia/upływie jego ważności. Ponadto podlega odpowiedzialności karnej wynikającej z art. 51-52 ustawy o ochronie danych osobowych, a także art. 266 kodeksu karnego.

Załącznik Nr 3 do **Polityki Bezpieczeństwa Informacji i Regulaminu Ochrony Danych Osobowych**

 Hajnówka, dn

pieczątka szkoły

UPOWAŻNIENIE

Na podstawie rozporządzenia 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 (Dz. U. nr 100, poz. 1024)

upoważniam Pana/Panią:

do wykonywania zadań Administratora Bezpieczeństwa Informacji w Zespole Szkół nr 2 z Oddziałami Integracyjnymi w Hajnówce wynikających z przepisów ustawy z 29.08.1997 r.

1. ochronie danych osobowych (Dz. U. nr 101, poz. 926, z 2002 r.) oraz aktów wykonawczych wydanych na jej podstawie.

Jednocześnie upoważniam Pana/Panią do dostępu do zbiorów danych osobowych prowadzonych w Zespole Szkół nr 2 z Oddziałami Integracyjnymi w Hajnówce, ich przetwarzania i kontrolowania pracowników zatrudnionych przy jego przetwarzaniu, a także do ich przetwarzania w zakresie niezbędnym do realizacji przydzielonych obowiązków służbowych.

Upoważnienie jest ważne przez czas zatrudnienia w Zespole Szkół nr 2 z Oddziałami Integracyjnymi w Hajnówce.

(imienna pieczątka i podpis dyrektora)

Podstawa prawna: art. 39 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (D. U. z 2002 r. nr 101, poz. 926 ze zm.)

Załącznik Nr 4 do **Polityki Bezpieczeństwa Informacji i Regulaminu Ochrony Danych Osobowych**

(imię i nazwisko pracownika)

**OŚWIADCZENIE**

Ja niżej podpisany(a), oświadczam, że zapoznałem(am) się z przepisami dotyczącymi ochrony danych osobowych i zobowiązuję się do przestrzegania:

1. ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. nr 101, poz. 926 z późn. zm.),
2. rozporządzenia 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 (Dz. U. nr 100, poz. 1024),
3. rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. 229, poz. 1536),
4. Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Zespole Szkół nr 2 z Oddziałami Integracyjnymi w Hajnówce,
5. Polityki Bezpieczeństwa i Regulaminu Przetwarzania Danych Osobowych w w Zespole Szkół nr 2 z Oddziałami Integracyjnymi w Hajnówce.

Jednocześnie zobowiązuj ę się do:

1. zapewnienia ochrony danych osobowych przetwarzanych w zbiorach Zespołu Szkół nr 2 z Oddziałami Integracyjnymi w Hajnówce, a w szczególności zapewnienia ich bezpieczeństwa przed udostępnieniem osobom nieupoważnionym, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem
2. zachowania w tajemnicy, także po ustaniu stosunku pracy, wszelkich informacji dotyczących przetwarzania danych osobowych w zbiorach szkoły, w tym hasła dostępu do systemu informatycznego;
3. natychmiastowego zgłoszenia przełożonemu i Administratorowi Bezpieczeństwa Informacji stwierdzenia próby lub faktu naruszenia zabezpieczenia pomieszczenia oraz bezpieczeństwa systemu informatycznego, w którym przetwarzane są dane osobowe.

Równocześnie oświadczam, że zapoznałem/am się z Instrukcji postępowania w przypadku naruszenia bezpieczeństwa danych osobowych oraz zostałem(am) poinformowany(a) o odpowiedzialności służbowej i karnej związanej z ochroną danych osobowych.

*Hajnówka, dnia……………. (podpis pracownika*)

Załącznik Nr 5 do **Polityki Bezpieczeństwa Informacji i Regulaminu Ochrony Danych Osobowych**

**W Zespole Szkół nr 2 z Oddziałami Integracyjnymi w Hajnówce tworzy się następujące zbiory danych osobowych:**

Zbiór nr 1 - Akta osobowe pracowników

Zbiór nr 2 - Ewidencja zasobów szkoły - SIO

Zbiór nr 3 - Ewidencja zwolnień lekarskich pracowników

Zbiór nr 4 - Dokumentacja zdrowotna uczniów

Zbiór nr 5 - Protokoły Rady Pedagogicznej, Księga Uchwał

Zbiór nr 6 - Ewidencja urlopów pracowników niepedagogicznych

Zbiór nr 7 - Ewidencja legitymacji pracowniczych

Zbiór nr 8 - Rejestr delegacji służbowych

Zbiór nr 9 - Ewidencja osób korzystających z księgozbioru bibliotecznego

Zbiór nr 10 - Listy płac pracowników

Zbiór nr 11 - Księgi ewidencji uczniów

Zbiór nr 12 - Dzienniki lekcyjne (elektroniczne) i pozalekcyjne

Zbiór nr 13 - Dziennik pedagoga i psychologa szkolnego

Zbiór nr 14 - Arkusze ocen wszystkich uczniów wraz z protokołami egzaminów klasyfikacyjnych i poprawkowych

Zbiór nr 15 - Karty zgłoszeń uczniów, podania o przyjęcie do szkoły;

Zbiór nr 16 - Ewidencja wydanych legitymacji szkolnych

 Zbiór nr 17 - Ewidencja wydanych świadectw ukończenia szkoły

 Zbiór nr 18 - Rejestr wypadków uczniów

Zbiór nr 19 - Kartoteki wydanej odzieży ochronnej i środków ochrony indywidualnej

Zbiór nr 20 - Arkusz organizacji roku szkolnego

Zbiór nr 21 - Zbiór upoważnień

Zbiór nr 22 - Ewidencja osób ubezpieczonych

Załącznik Nr 6 do **Polityki Bezpieczeństwa Informacji i Regulaminu Ochrony Danych Osobowych**

**W Zespole Szkół nr 2 z Oddziałami Integracyjnymi w Hajnówce.**

**do przetwarzania danych osobowych wykorzystuje się następujące oprogramowanie:**

1. MS OFFICE 2010
2. System Kontroli Frekwencji i Postępów w Nauce - LIBRUS
3. Sekretariat - LIBRUS
4. SIO
5. Świadectwa - LIBRUS
6. Płatnik
7. sQola Płace
8. sQola Księgowośc
9. e=Pefron
10. Arkusz - Optivum
11. Plan Lekcji - librus
12. Biblioteka – Moll

Załącznik Nr 7 do **Polityki Bezpieczeństwa Informacji i Regulaminu Ochrony Danych Osobowych**

.

 **„6 Zasad”**

 **bezpiecznej pracy przy przetwarzaniu**

 **wszelkiego rodzaju informacji, w tym danych osobowych:**

1. Dokumenty papierowe i nośniki komputerowe, kiedy nie są używane, przechowuje się w specjalnych segregatorach, teczkach, szafach, szczególnie poza godzinami pracy, pracownik jest zobowiązany do przechowywania wszystkich dokumentów w zamkniętych szafach i biurkach **(zasada czystego biurka)**.
2. W przypadku opuszczania stanowiska pracy, należy zablokować stację roboczą. O ile możliwe, monitor powinien być ustawiony w taki sposób, aby osoby postronne nie miały możliwości wglądu do przetwarzanych aktualnie informacji, wygaszacze ekranu w stacjach roboczych zostały ustawione na 15 minut **(zasada czystego ekranu)**.
3. Wszystkie wydruki zawierające dane osobowe klientów, pracowników, informacje o filmie zabierane są natychmiast z drukarki po zakończeniu drukowania **(zasada natychmiastowego odbioru wydruków z drukarki)**.
4. Ostatni pracownik opuszczający pomieszczenie zobowiązany jest do zamknięcia okien i drzwi zewnętrznych na klucz. Bezwzględnie zabrania się pozostawiania kluczy w zamku po zewnętrznej stronie drzwi **(zasada zamykania pomieszczeń)**.
5. W przypadku rozmów (również telefonicznych) dotyczących zadań związanych z realizacja zadań Zespołu Szkół nr 2, prowadzonych zarówno w siedzibie jednostki jak i poza jej obszarem należy zadbać, aby rozmowy nie były prowadzone w obecności osób nieupoważnionych do tych informacji **(zasada poufności rozmów)**.
6. Klienci/goście przyjmowani są w pomieszczeniach jednostki tylko i wyłącznie pod nadzorem pracowników jednostki. Pracownik opiekujący się osobą trzecią zobowiązany jest do nie pozostawiania jej bez nadzoru w przypadku, gdy istnieje możliwość spowodowania przez nią incydentu bezpieczeństwa np. nieuprawnionego dostępu do informacji **(zasada nadzorowania klientów/gości)**.

 ........................................................................................................................ /*data, podpis Administratora Bezpieczeństwa Informacji/*

Załącznik Nr 8 do **Polityki Bezpieczeństwa Informacji i Regulaminu Ochrony Danych Osobowych**

  **Przypadki zakwalifikowane jako naruszenie bezpieczeństwa informacji**

|  |  |
| --- | --- |
| **L p** | **Poniżej wymieniono najczęstsze zdarzenia, które mogą być uznane za naruszenie lub uzasadnione podejrzenie naruszenia bezpieczeństwa informacji lub systemu w którym przetwarzane są dane osobowe:** |
| 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 | Niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych. |
| 3 | Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru. |
| 4 | Pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu. |
| 5 | Jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie. |
| 6 | Nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie. |
| 7 | Stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji). |
| 8 | Nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie. |
| 9 | Ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy zabezpieczeń. |
| 10 | Praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazuje na przełamanie lub zaniechanie ochrony danych osobowych np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp. |
| 11 | Ujawniono istnienie nieautoryzowanych kont dostępu do danych, tzw. „bocznej furtki”, itp. |
| 12 | Podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub kopiowano dane osobowe. |
| 13 | Rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp. |
| 14 | Nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych, w tym także osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej, itp. |

Załącznik Nr 9 do **Polityki Bezpieczeństwa Informacji i Regulaminu Ochrony Danych Osobowych**

 **Katalog form naruszeń i incydentów w zakresie danych osobowych**

|  |  |
| --- | --- |
| **Nr kodu****naruszeń** | **Forma naruszenia ochrony danych osobowych przez pracownika zatrudnionego przy przetwarzaniu danych** |

|  |  |  |
| --- | --- | --- |
| **A** | **Formy naruszeń** | **Sposoby postępowania** |
| **A1** | **W zakresie wiedzy:** |  |
| **A.1.1.** | Ujawnianie sposobu działania aplikacji i systemu jej zabezpieczeń osobom niepowołanym | Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić Administratora Bezpieczeństwa Informacji (ABI). |
| **A.1.2.** | Ujawnienie informacji o sprzęcie i pozostałej infrastrukturze informatycznej | Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić ABI. |
| **A.1.3.** | Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać, np. z obserwacji lub dokumentacji | Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić ABI. |
| **A.2** | **W zakresie sprzętu i oprogramowania:** |  |
| **A.2.1.** | Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych | Natychmiast zakończyć działanie aplikacji. Sporządzić raport. |
| **A.2.2.** | Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony. | Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Pouczyć osobę, która dopuściła do takiej sytuacji |
| **A.2.3.** | Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych i sieci | Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Niezwłocznie powiadomić ABI. Sporządzić raport. |
| **A.2.4.** | Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych przez osoby nie będące pracownikami. | Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić jakie czynności zostały przez osoby nieuprawnione wykonane. Niezwłocznie powiadomić ABI. Sporządzić raport. |
| **A.2.5.** | Samodzielne instalowanie jakiegokolwiek oprogramowania. | Pouczyć osobę popełniającą wymienione czynności, aby je zaniechała. Wezwać służby informatyczne w celu odinstalowania programów. Sporządzić raport. |
| **A.2.6.** | Modyfikowanie parametrów systemu i aplikacji. | Wezwać osobę popełniająca wymienioną czynność, aby jej zaniechała. Sporządzić raport. |
| **A.2.7.** | Odczytywanie dyskietek i innych nośników przed sprawdzeniem ich programem antywirusowym. | Pouczyć osobę popełniającą wymienioną czynność, aby zaczęła się stosować do wymogów bezpieczeństwa pracy. Wezwać służby informatyczne w celu wykonania kontroli antywirusowej. Sporządzić raport |
| **A.3** | **W zakresie dokumentów i obrazów zawierających dane osobowe:** |  |
| **A.3.1.** | Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru. | Zabezpieczyć dokumenty. Sporządzić raport. |
| **A.3.2.** | Przechowywanie dokumentów zabezpieczonych w niedostatecznym stopniu przed dostępem osób niepowołanych | Powiadomić przełożonych. Spowodować poprawienie zabezpieczeń. Sporządzić raport. |
| **A.3.3.** | Wyrzucanie dokumentów w stopniu zniszczenia umożliwiających ich odczytanie. | Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić przełożonych. Sporządzić raport. |
| **A.3.4.** | Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią. | Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. |
| **A.3.5.** | Dopuszczanie aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe. | Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały ważne dane – sporządzić raport. |
| **A.3.6.** | Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą. | Spowodować zaprzestanie kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić ABI. Sporządzić raport |
| **A.3.7.** | Utrata kontroli nad kopią danych osobowych. | Podjąć próbę odzyskania kopii. Powiadomić ABI. Sporządzić raport. |
| **A.4.** | **W zakresie pomieszczeń i infrastruktury służących do przetwarzania danych osobowych:** |  |
| **A.4.1** | Opuszczenie i pozostawienie bez dozoru nie zamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych. | Zabezpieczyć (zamknąć) pomieszczenie. Powiadomić przełożonych. Sporządzić raport. |
| **A.4.2.** | Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do nich kontaktu ze sprzętem komputerowym. | Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia. Próbować ustalić ich tożsamość. Powiadomić przełożonych i ABI. Sporządzić raport. |
| **A.4.3.** | Dopuszczanie, aby osoby spoza służ informatycznych i telekomunikacyjnych podłączały jakiekolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji. | Wezwać osoby dokonujące czynności do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i ABI. Sporządzić raport. |
| **A.5.** | **W zakresie pomieszczeń, w których znajdują się komputery centralne i urządzenia sieci:** |  |
| A.5.1. | Dopuszczenie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakichkolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (hole, korytarze, itp.). | Wezwać osoby dokonujące czynności do ich zaprzestania i opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i ABI. Sporządzić raport. |
| A.5.2. | Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służ informatycznych i telekomunikacyjnych lub ignorowania tego faktu. | Wezwać osoby dokonujące czynności do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i ABI. Sporządzić raport. |
| **B** | **Zjawiska świadczące o możliwości naruszenia ochrony danych osobowych:** |  |
| B.1. | Ślady manipulacji przy układach sieci komputerowej lub komputerach. | Powiadomić niezwłocznie ABI oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport. |
| B.2. | Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu. | Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport. |
| B.3. | Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych. | Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport. |
| B.4. | Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych. | Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport. |
| B.5. | Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania. | Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport. |
| B.6. | Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe. | Postępować zgodnie z właściwymi przepisami. Powiadomić niezwłocznie Administratora Bezpieczeństwa Informacji (ABI). |

Załącznik Nr 10 do **Polityki Bezpieczeństwa Informacji i Regulaminu Ochrony Danych Osobowych**

WZÓR

**R a p o r t**

**z naruszenia ochrony danych osobowych**

**w Zespole Szkół nr 2 z Oddziałami Integracyjnymi w Hajnówce**

1. Data: ........................................................................ Godzina: ........................................

 *(dzień, miesiąc, rok) (00:00)*

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

....................................................................................................................................................

*(Imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje) )*

3. Lokalizacja zdarzenia:

.....................................................................................................................................................

*(np. nr pokoju, nazwa pomieszczenia)*

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

............................................................................................................................................................................................................................................................................................................

5. Podjęte działania:

........................................................................................................................................................................................................................................................................................................

6. Przyczyny wystąpienia zdarzenia:

........................................................................................................................................................................................................................................................................................................

7. Postępowanie wyjaśniające:

.............................................................................................................................................................................................................................................................................................................

 .............................................................................................................................

 /*data, podpis Administratora Bezpieczeństwa Informacji/*