Liceum Ogólnokształcące
im. Polskiej Macierzy Szkolnej
ul. Piękna 7A, 05-300 Mińsk Mazowiecki
tel./fax 25-758-51-02
NIP 822-10-96-528

Zarządzenie Nr 19/2020/2021
Dyrektora Liceum Ogólnokształcącego im. Polskiej Macierzy Szkolnej w Mińsku Mazowieckim

z dnia 1 marca 2021 r. w sprawie wprowadzeniu Instrukcji postępowania w przypadku naruszenia bezpieczeństwa danych

Na podstawie art. 33 ust. 5 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zarządzam co następuje:

§1

Wprowadzam w Liceum Ogólnokształcącym im. Polskiej Macierzy Szkolnej w Mińsku Mazowieckim Instrukcję postępowania w przypadku naruszenia bezpieczeństwa danych, która stanowi załącznik do zarządzenia.

§2

Zobowiązuję pracowników pedagogicznych oraz administracyjnych do zapoznania się z treścią w/w instrukcji. Wersja papierowa instrukcji jest dostępna w sekretariacie szkoły. Wersja elektroniczna dokumentu zostanie przesłana do pracowników drogą elektroniczną przez dziennik Librus lub pocztę mailową.

§3

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
LICEUM OGÓLNOKSZTAŁCĄCEGO
im. Polskiej Macierzy Szkolnej
mgr inż. Joanna Papińska

Liceum Ogólnokształcące
im. Polskiej Macierzy Szkolnej
ul. Piękna 7A, 05-300 Mińsk Mazowiecki
tel./fax 25-758-51-02
NIP 822-10-96-528

załącznik
do Zarządzenia Dyrektora Nr 19/2020/2021
z dnia 1 marca 2021 r.

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych przetwarzanych w Liceum Ogólnokształcącym im. Polskiej Macierzy Szkolnej w Mińsku Mazowieckim

Spis treści:

Rozdział 1
Cel wydania instrukcji i jej zakres przedmiotowy

§ 1. 1. Instrukcja określa zasady postępowania wszystkich osób upoważnionych do przetwarzania danych osobowych zatrudnionych przy przetwarzaniu danych osobowych przez administratora tj. Liceum Ogólnokształcące im. Polskiej Macierzy Szkolnej w Mińsku Mazowieckim w przypadku naruszenia ich bezpieczeństwa.

2. Naruszeniem zabezpieczenia danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia lub usunięcia, a w szczególności:

1) nieautoryzowany dostęp do danych;
2) nieautoryzowane modyfikacje lub zniszczenie danych;
3) udostępnienie danych nieautoryzowanym podmiotom;
4) nielegalne ujawnienie danych.

3. Postanowienia Instrukcji mają zastosowanie do wewnętrznych komórek organizacyjnych szkoły, a także do samodzielnych stanowisk w szkole.

4. Wobec osoby, która w przypadku naruszenia danych osobowych nie podjęła działania określonego w niniejszej Instrukcji, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne lub porządkowe. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z aktualnie obowiązującym przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

Rozdział 2
Rodzaje incydentów świadczących o możliwości naruszenia bezpieczeństwa danych

§ 2. 1. „Naruszenie ochrony danych osobowych" oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

2. Wyróżnia się następujące rodzaje naruszeń:

1) „naruszenie poufności", które polega na ujawnieniu lub udostępnieniu danych osobie nieuprawnionej;
2) „naruszenie integralności", które sprowadza się do zmiany treści danych osobowych, czyli ich modyfikowania, w sposób nieautoryzowany;

3) „naruszenie dostępności", które wiąże się z trwałą utratą dostępu do danych lub ich zniszczeniem.

3. O możliwości wystąpienia naruszenia bezpieczeństwa danych osobowych mogą świadczyć:

1) nadmierne w stosunku do wykonywanych zadań (zakresu upoważnienia), uprawnienia użytkownika do zasobów danych;
2) niestabilna praca systemu teleinformatycznego;
3) korzystanie z zasobów danych poza miejscem przetwarzania/godzinami pracy (bez zgody przełożonego);
4) nowe „podejrzane" (nieznane) konta użytkowników w systemie;
5) wysoka aktywność kont, które długo pozostawały niewykorzystane;
6) zanotowanie w krótkim czasie dużej liczby nieudanych prób logowania;
7) anomalie w pracy systemu lub programu (świadczące np. o obecności wirusa komputerowego);
8) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach, w których następuje przetwarzanie danych osobowych (uszkodzone zamki, okna, drzwi, naruszone plomby, itp.).

4. Prawdopodobne incydenty naruszenia bezpieczeństwa danych zostały określone w wykazie naruszeń, stanowiącym załącznik 1 do instrukcji.

Rozdział 3
Postępowanie w przypadku podejrzenia naruszenia bezpieczeństwa danych

§ 3. 1. Każdy pracownik, który stwierdzi lub podejrzewa fakt naruszenia danych osobowych, jest zobowiązany niezwłocznie zgłosić to swojemu bezpośredniemu przełożonemu – wzór zgłoszenia stanowi załącznik nr 2. Przełożony zgłasza fakt Inspektorowi Ochrony Danych.

2. Sytuacje, które wymagają zgłoszenia to:

1) fizyczna obecność w budynku szkoły osób zachowujących się podejrzanie;
2) ślady na drzwiach, oknach i szafach wskazują na próbę włamania;
3) niszczenie dokumentów bez użycia niszczarki;
4) otwarte drzwi do pomieszczeń, szaf, w których przechowywane są dane osobowe w formie papierowej oraz na nośnikach elektronicznych;
5) niewylogowanie się przed opuszczeniem stanowiska pracy;
6) pozostawienie danych w drukarce, na ksero;
7) niezamknięcie pomieszczenia z komputerem;
8) niewykonanie w określonym terminie kopii zapasowych;
9) prace z danymi osobowymi w celach prywatnych;
10) ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe;

11) wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz placówki bez upoważnienia;

12) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej;

13) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);

14) telefoniczne próby wyłudzenia danych osobowych;

15) kradzież komputerów lub twardych dysków z danymi osobowymi;

16) utrata kontroli nad kopią danych osobowych;

17) maile zachęcające do ujawnienia identyfikatora i/lub hasła;

18) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;

19) istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki";

20) pozostawianie niezabezpieczonych haseł w pobliżu komputera.

§ 4. Każdy pracownik, który stwierdzi fakt naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia.

§ 5. W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia administratora sieci lub innej osoby upoważnionej przez Administratora Danych.

§ 6. Administrator danych lub upoważniona przez niego osoba dokonuje wstępnej identyfikacji zaistniałego zdarzenia i na podstawie dostępnych informacji oraz analizy okoliczności kwalifikuje zdarzenie (lub serię zdarzeń) jako:

1) zdarzenie niemające cech naruszenia bezpieczeństwa, np. zaplanowana przerwa technologiczna;

2) błąd w działaniu elementu systemu teleinformatycznego, infrastruktury teleinformatycznej lub infrastruktury biurowej;

3) awaria techniczna czasowo blokująca dostępność informacji;

4) zdarzenie niskiej kategorii – związane z naruszeniem bezpieczeństwa ochrony danych, a szczególnie jej integralności i poufności, nie generujące kar finansowych, jednak powodujący pośrednio lub bezpośrednio utrudnienia w realizacji jakiegokolwiek procesu przetwarzania;

5) zdarzenie średniej kategorii – związane z naruszeniem bezpieczeństwa ochrony danych skutkujące pośrednio lub bezpośrednio zatrzymaniem realizacji jakiegokolwiek procesu ustawowego i/lub stratami finansowymi oraz możliwością konsekwencji prawnych i/lub utraty wizerunku;

6) zdarzenie wysokiej kategorii – związane z naruszeniem bezpieczeństwa ochrony danych, którego skutkiem jest destrukcja (zniszczenie, utrata) kluczowych zasobów i przerwanie funkcjonowania procesów funkcjonowania placówki.

§ 7. Przy analizie naruszeń, o których mowa w § 4 należy wziąć pod uwagę:

1) charakter zdarzenia i jego znaczenie związane z naruszeniem bezpieczeństwa ochrony danych osobowych;
2) miejsce wystąpienia zdarzenia - identyfikacja punktu, w którym nastąpiło zdarzenie (lokalizacja pomieszczenia, serwer, stacja robocza itp.);
3) zakres zasobów dotkniętych naruszeniem;
4) identyfikację zasobów potrzebnych przy dalszych działaniach w ramach postępowania ze zdarzeniem związanym z naruszeniem bezpieczeństwa ochrony danych;
5) możliwości rozszerzania się naruszenia i sposoby jego ograniczania;
6) rodzaj ujawnionej informacji (jeśli ma zastosowanie - np. dane osobowe);
7) szacunkowy czas, po którym skutki naruszenia zostaną zlikwidowane, jeżeli nie ma możliwości natychmiastowego usunięcia stanu naruszenia bezpieczeństwa ochrony danych;
8) skutki organizacyjne i prawne (wstępny szacunek).

§ 8. W przypadku, gdy zasięg i szacunkowy czas trwania powoduje zakwalifikowanie naruszenia do wysokiej kategorii, administrator powiadamia niezwłocznie Prezesa Urzędu Ochrony Danych Osobowych (PUODO), a następnie przeprowadza dochodzenie wyjaśniające.

§ 9. W przypadku, gdy rodzaj i zasięg incydentu, zidentyfikowany na którymkolwiek z etapów postępowania, uzasadnia potrzebę powiadomienia organów ścigania, to decyzję o sposobie i terminie powiadomienia podejmuje administrator.

§ 10. 1. Administrator danych osobowych o każdym incydencie naruszenia bezpieczeństwa danych osobowych informuje Inspektora ochrony danych osobowych oraz sporządza raport, zgodnie ze wzorem raportu, który stanowi załącznik nr 3 do Instrukcji.

§ 11. 1. Inspektor Ochrony Danych podejmuje następujące kroki:

1) zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy;
2) odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem;
3) nawiązuje kontakt ze specjalistami zewnętrznymi (jeśli zachodzi taka potrzeba).

2. Inspektor Ochrony Danych zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych) - załącznik nr 4 - Rejestr incydentów i działań korygujących i zapobiegawczych.

Rozdział 4
Ograniczanie skutków naruszeń

§ 12. 1. Dokumentacja naruszenia podlega rygorom ochrony przez tworzenie autoryzowanych kopii tych elementów, które mają zastosowanie przy postępowaniu z naruszeniem, w tym: rejestry urządzeń, systemów operacyjnych i aplikacji, kopie zapasowe, pliki konfiguracyjne i systemowe, bezpieczne przechowywanie tych kopii, przyjęcia dokumentacji oraz jej wszystkich części.

2. IODO przeprowadza bieżące działania zmierzające do ograniczenia skutków naruszenia i zidentyfikowania jego źródła. W tym celu może spowodować zablokowanie części systemu lub dostępnych usług.

3. W przypadku, gdy działania opisane w ust. 2 obejmują wyłączenie lub ograniczenie funkcjonowania zasobów niezbędnych do realizowania celów ustawowych bądź statutowych placówki, IODO przedstawia decyzję do akceptacji Administratora danych.

Rozdział 5
Odtwarzanie systemu

§ 13. 1. Administrator sieci / informatyk lub osoba upoważniona przez administratora przystępuje do odtworzenia systemu po zidentyfikowaniu i usunięciu lub zablokowaniu źródła naruszenia.

2. Odtwarzanie systemu odnosi się do punktu odtworzenia, co do którego administrator sieci ma uzasadnioną pewność, że nie zawiera źródła naruszenia.

3. Zasoby w postaci oprogramowania oraz danych są odtwarzane z oryginalnych źródeł dystrybucji oprogramowania oraz kopii zapasowych.

4. Administrator danych, po zasięgnięciu opinii IODO, może podjąć decyzję o podjęciu przetwarzania danych mimo braku pewności usunięcia źródła naruszenia, jeśli szacowane negatywne skutki braku przetwarzania przewyższają potencjalne ryzyko podjęcia działania.

Rozdział 6
Zgłaszanie naruszenia ochrony danych do UODO

§ 14. 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 Osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

2. Zgłoszenie, o którym mowa w ust. 1, musi zawierać co najmniej:

1) 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;

2) zawierać imię i nazwisko oraz dane kontaktowe Inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

4) opisywać środki zastosowane lub proponowane przez Administratora w celu zapobiegania naruszeniu ochrony danych osobowych, w tym w stosownych 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.

5. Zgłoszenia można dokonać za pomocą formularza dostępnego na stronie www.uodo.gov.pl na 4 sposoby:

1) elektronicznie poprzez wypełnienie dedykowanego formularza dostępnego bezpośrednio na platformie www.biznes.gov.pl;

2) elektronicznie poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP: UODO/SkrytkaESP;

3) elektronicznie poprzez wysłanie wypełnionego formularza za pomocą pisma ogólnego dostępnego na platformie www.biznes.gov.pl;

4) tradycyjną pocztą, wysyłając wypełniony formularz na adres Urzędu.

Rozdział 7
Zawiadamianie osób o naruszeniu ochrony ich danych osobowych

§ 15. 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. 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.

3. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d). RODO.

4. Nie dokonuje się zawiadomienia osób w następujących przypadkach, gdy:

1) 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;

2) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;

3) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Załączniki:

1) Tabela naruszeń bezpieczeństwa danych osobowych – załącznik 1.
2) Wzór zgłoszenia incydentu przez pracownika – załącznik 2.
3) Raport z naruszenia bezpieczeństwa danych – załącznik 3a i 3b.
4) Rejestr naruszeń ochrony danych oraz podjęte środki zaradcze i naprawcze – załącznik 4.

Mińsk Mazowiecki, dnia 1 marca 2021 r.

DYREKTOR
LICEUM OGÓLNOKSZTAŁCĄCEGO
im. Polskiej Macierzy Szkolnej
mgr inż. Joanna Papińska

Załącznik nr 1

Tabela naruszeń bezpieczeństwa danych osobowych

Symbol	Formy naruszeń	Sposób postępowania
P	Formy naruszenia bezpieczeństwa danych przez pracownika	
P/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.
P/2	Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej, stosowanych zabezpieczeniach	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić Administratora Bezpieczeństwa Informacji.
P/3	Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych	Niezwłocznie zakończyć działanie aplikacji. Sporządzić raport.
P/4	Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez inne osoby niż osoba, która została upoważniona.	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Pouczyć osobę, która dopuściła do takiej sytuacji o naruszaniu porządki pracy. Sporządzić raport.
P/5	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 Administratora Bezpieczeństwa Informacji. W trybie natychmiastowym dokonać zmiany hasła. Sporządzić raport.
P/6	Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych przez osoby nie będące pracownikami, w szczególności w pracy zdalnej.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działające programy. Niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji. Sporządzić raport.
P/7	Samodzielne instalowanie jakiegokolwiek oprogramowania.	Pouczyć osobę popełniającą wymieniona czynność, aby jej zaniechała. Wezwać służby informatyczne w celu odinstalowania programów. Sporządzić raport.

P/8	Modyfikowanie parametrów systemu i aplikacji.	Wezwać osobę popełniającą wymieniona czynność, aby jej zaniechała. Zainstalować z modyfikowane programy pliku źródłowego. Sporządzić raport.
P/9	Odczytywanie dyskietek i innych nośników przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę popełniającą wymienioną czynność o stosowaniu polityki bezpieczeństwa. Wezwać służby informatyczne w celu wykonania kontroli antywirusowej. Sporządzić raport.
P/10	Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru	Zabezpieczyć dokumenty. Sporządzić raport.
P/11	Przechowywanie dokumentów zabezpieczonych w niedostatecznym stopniu przed dostępem osób niepowołanych	Powiadomić przełożonych. Spowodować poprawienie zabezpieczeń. Sporządzić raport.
P/12	Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie, z pominięciem niszczenia niszczarką.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić przełożonych. Sporządzić raport.
P/13	Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią, w tym umożliwienie uzyskania kopii z ksero	Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonych. Sporządzić raport.
P/14	Dopuszczanie, aby osoby postronne odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. W przypadku ujawnienia ważnych danych sporządzić raport.
P/15	Sporządzanie kopii danych na nośnikach danych bez uzasadnienia oraz braku obowiązku takiego kopiowania.	Spowodować zaprzestanie kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić Administratora Bezpieczeństwa Informacji. Sporządzić raport
P/16	Opuszczanie i pozostawianie bez dozoru niezamkniętego 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.

P/17	Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym.	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość. Powiadomić przełożonych i Administratora Bezpieczeństwa Informacji. Sporządzić raport.
P/18	Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakikolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i przewodów kablowych lub dokonywały jakichkolwiek zmian.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i Administratora Bezpieczeństwa Informacji. Sporządzić raport.
P/19	Wynoszenie dokumentacji papierowej lub dokumentacji w formie elektronicznej poza teren szkoły bez zgody dyrektora.	Powiadomić przełożonych i Administratora Bezpieczeństwa Informacji. Sporządzić raport.
P/20	Logowanie się do systemów w okresie choroby w miejscu przebywania w czasie trwania L4 bez upoważnienia dyrektora lub przełożonego.	Powiadomić przełożonych i Administratora Bezpieczeństwa Informacji. Sporządzić raport.
P/21	Nieterminowe dokonywanie zmiany haseł i longinów.	Powiadomić przełożonych i Administratora Bezpieczeństwa Informacji. Sporządzić raport.
P/22	Nieaktualizowanie programów użytkowych	Powiadomić przełożonych i Administratora Bezpieczeństwa Informacji. Sporządzić raport.
P/23	Nieaktualizowanie programów antywirusowych	Powiadomić przełożonych i Administratora Bezpieczeństwa Informacji. Sporządzić raport.
P/24	Otwieranie załączników niewiadomego nadawcy	Powiadomić przełożonych i Administratora Bezpieczeństwa Informacji. Sporządzić raport
N	**Zjawiska świadczące o możliwości naruszenia bezpieczeństwa danych**	
N/1	Ślady manipulacji przy układach sieci komputerowej lub komputerach	Powiadomić niezwłocznie Administratora Bezpieczeństwa Informacji oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.

N/2	Obecność nowych kabli o nieznanym przeznaczeniu.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
N/3	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.
N/4	Nie dające się wyjaśnić, zmiany zawartości bazy danych.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
N/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.
N/6	Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe	Postępować zgodnie z właściwymi przepisami. Powiadomić niezwłocznie Administratora Bezpieczeństwa Informacji. Sporządzić raport.
Z	**Ingerencja zewnętrzna**	
Z/1	Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej	Powiadomić Administratora Bezpieczeństwa Informacji. Sporządzić raport.
Z/2	Zablokowanie dostępu	Powiadomić Administratora Bezpieczeństwa Informacji. Sporządzić raport.
Z/3	Wirusy, konie trojańskie	Powiadomić Administratora Bezpieczeństwa Informacji. Sporządzić raport.
Z/4	Telefoniczne próby wyłudzenia haseł dostępu lub danych osobowych	Powiadomić Administratora Bezpieczeństwa Informacji. Sporządzić raport.
Z/4	Maile zachęcające do ujawnienia identyfikatora i/lub hasła;	Powiadomić Administratora Bezpieczeństwa Informacji. Sporządzić raport.

Załącznik nr 2

Wzór zgłoszenie incydentu naruszenia bezpieczeństwa danych przez pracownika

Miejscowość, data .....

1. **Dane zgłaszającego:**

   Imię i nazwisko: .....

   Stanowisko: .....

   Komórka lub jednostka organizacyjna: .....

   Telefon kontaktowy: .....

   e - mail: .....

2. **Wskazanie, w którym miejscu wystąpiło naruszenie:**

   Sieci: .....

   System teleinformatyczny: .....

   Dokumentacja papierowa, zbiór danych: .....

3. **Data i godzina stwierdzenia naruszenia**: .....
4. **Charakterystyka naruszenia:**

Opisać szczegółowo na czym polegało naruszenie ochrony danych osobowych, w tym:

- opis zdarzenia ze wskazaniem np. faktu zniszczenia, utraty, nieuprawnionej modyfikacji danych, ujawnienia danych, nieuprawnionego dostępu do danych wraz z okolicznościami tego zdarzenia:

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

Na czym polegało naruszenie? / można podać kategorię z tabeli – załącznik 1:

☐ Zgubienie, kradzież nośnika/urządzenia

☐ Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji

☐ Korespondencja papierowa utracona przez operatora pocztowego/pocztę resortową lub otwarta przed zwróceniem jej do nadawcy

☐ Nieuprawnione uzyskanie dostępu do informacji/systemu

☐ Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń

☐ Złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych

☐ Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy

☐ Nieprawidłowa anonimizacja danych osobowych w dokumencie

☐ Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora

☐ Niezamierzona publikacja

☐ Dane osobowe wysłane do niewłaściwego odbiorcy

☐ Ujawnienie danych niewłaściwej osoby

☐ Ustne ujawnienie danych osobowych

☐ Inne.....

.....

.....

Przyczyna naruszenia:

☐ Wewnętrzne działanie niezamierzone

☐ Wewnętrzne działanie zamierzone

☐ Zewnętrzne działanie niezamierzone

☐ Zewnętrzne działanie zamierzone

Opisać możliwe konsekwencje naruszenia ochrony danych osobowych:

Naruszenie ma wpływ na:

☐ poufność (nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych)

☐ integralność (wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania)

☐ dostępność (brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną)

Kategorie danych osobowych, których dotyczy naruszenie:

☐ nazwiska i imiona

☐ nazwa użytkownika i/lub hasło

☐ imiona rodziców

☐ dane dot. zarobków i/lub posiadanego majątku

☐ data urodzenia

☐ nazwisko rodowe matki

☐ nr rachunku bankowego

☐ seria i numer dowodu osobistego

☐ adres zamieszkaniu lub pobytu

☐ numer telefonu

☐ numer ewidencyjny PESEL

☐ wizerunek

☐ adres e-mail

☐ inne.....

- przybliżona liczba osób, których mogło dotyczyć naruszenie.....
- przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie.....

Dane szczególnej kategorii przetwarzania:

☐ dane o pochodzeniu rasowym lub etnicznym
☐ dane o poglądach politycznych
☐ dane o przekonaniach religijnych lub światopoglądowych
☐ dane o przynależności do związków zawodowych
☐ dane dotyczące seksualności lub orientacji seksualnej
☐ dane dotyczące zdrowia
☐ dane genetyczne
☐ dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej

MOŻLIWE KONSEKWENCJE

Opisać konsekwencje dla osoby, której dane dotyczą:

☐ utrata kontroli nad własnymi danymi osobowymi
☐ ograniczenie możliwości realizowania praw z art. 15-22 RODO
☐ ograniczenie możliwości realizowania praw
☐ dyskryminacja
☐ kradzież lub sfałszowanie tożsamości
☐ strata finansowa
☐ naruszenie dobrego imienia
☐ utrata poufności danych osobowych chronionych tajemnicą zawodową
☐ nieuprawnione odwrócenie pseudonimizacji
☐ inne: .....

Czy naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych:

☐ NIE
☐ TAK (art. 33 ust.1 RODO)
☐ niskie ☐ średnie ☐ wysokie

.....

podpis osoby zgłaszającej

☐ Zarejestrowano w rejestrze naruszeń ochrony danych osobowych

w dniu .....godz. ..... poz. rejestru .....

Załącznik nr 3a

Raport z naruszenia ochrony danych

1. Data ..... Godzina ..... nr zgłoszenia: .....

2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub wysłuchane w związku z naruszeniem:

.....

(imię, nazwisko, stanowisko służbowe,):

3. Lokalizacja zdarzenia

.....

(nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):

4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:

.....

.....

5. Wstępna ocena przyczyn wystąpienia naruszenia:

.....

.....

6. Postępowanie wyjaśniające:

.....

.....

7. Działania podjęte w związku z wystąpieniem naruszenia - środki zaradcze i naprawcze:

1) Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa dotychczas stosowanych:

.....

2) Środki bezpieczeństwa zastosowane lub proponowane w celu zminimalizowania ryzyka ponownego wystąpienia naruszenia:

.....

4) Środki zastosowane lub proponowane w celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osób, których dane dotyczą:

5) .....

.....
(podpis pracownika)

.....
(data i podpis Inspektora Ochrony Danych)

Załącznik nr 3b

Wzór raportu końcowego sporządzanego przez administratora bezpieczeństwa informacji po zażegnaniu sytuacji naruszającej bezpieczeństwo danych osobowych

1. Sporządzający raport:

Imię i nazwisko:

.....

stanowisko (funkcja)

Dział, pokój, nr telefonu

.....

2. Kod formy naruszenia ochrony danych ..... (wg tabeli)

3. Miejsce, dokładny czas i data naruszenia ochrony danych osobowych (piętro, nr pokoju, godzina, itp.):

.....

.....

4. Osoby powodujące naruszenie (które swoim działaniem lub zaniechaniem przyczyniły się do naruszenia ochrony danych osobowych):

.....

.....

5. Osoby, które uczestniczyły w zdarzeniu związanym z naruszeniem ochrony danych osobowych:

.....

.....

6. Informacje o danych, które zostały lub mogły zostać ujawnione:

.....

.....

7. Zabezpieczone materiały lub inne dowody związane z wydarzeniem:

.....

.....

8. Krótki opis wydarzenia związanego z naruszeniem ochrony danych osobowych (przebieg zdarzenia, opis zachowania uczestników, podjęte działania):

.....

.....

9. Wnioski:

.....

.....

....

Załącznik nr 4

Rejestr naruszeń ochrony danych oraz środki zaradcze i naprawcze w przypadku naruszenia bezpieczeństwa danych

L.p.	Informacja o wystąpieniu i stwierdzenie naruszeń			Okoliczności naruszenia			Skutki naruszenia	Środki zaradcze i naprawcze	Data zgłoszenia do UODO (jeśli nie, przyczyna niedokonania zgłoszenia)	Czy poinformowano osoby, których dane osobowe zostały naruszone
	Data zdarzenia	Źródło informacji	Data poinformowania o zdarzeniu	Charakter naruszenia	Kategoria osób	Liczba rekordów	Opis konsekwencji naruszenia			