REGULAMIN WEWNĘTRZNYCH PROCEDUR

Reguluje postępowanie pracowników\użytkowników w celu pełnej kontroli oraz zapobieganiu możliwym zagrożeniom związanym z ochroną danych osobowych na podstawie **Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).**

Rozdzielnik:	Dokument do użytku wewnętrznego
Podmiot:	Zespół Szkół nr 2 im. H. Kołłątaja w Myszkowie
z dnia:	3 września 2018 r.
Zatwierdził(a):	Dyrektor Mgr inż. Jerzy Bryś *Podpis administratora danych*

SPIS TREŚCI:

DEFINICJE:

Administrator Danych Osobowych (AD) - [**pełna nazwa placówki**] zwanym/ą dalej [**skrót**] z reprezentacją w osobie AD [**Imię i nazwisko**].

Inspektor Ochrony danych (IOD) w osobie [**Imię i nazwisko**] jest to osoba wyznaczona przez Administratora Danych oraz zgłoszona w Urzędzie Ochrony Danych Osobowych w celu zapewnienia prawidłowości przetwarzanych danych w [skrót].

Pracownik\Użytkownik – osoba upoważniona lub użytkownik systemu; posiadająca upoważnienie do przetwarzania danych osobowych wydane przez Administratora.

ASI-Administrator Systemu Informatycznego / pracownik/użytkownik odpowiedzialny za system informatyczny w podmiocie-osoba wyznaczona przez AD. Odpowiedzialna w za prawidłowe działanie systemów informatycznych w [**skrót**].

System informatyczny - zespół współpracujących ze sobą urządzeń, programów, przetwarzania informacji i narzędzi programowych, zastosowanych w celu przetwarzania danych.

Zabezpieczenie systemu informatycznego – wdrożenie przez Administratora Danych Osobowych stosownych środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przetwarzanych w systemach informatycznych przed dostępem, modyfikacją ujawnieniem, pozyskaniem lub zniszczeniem przez osobę trzecią.

Przetwarzanie danych osobowych – wykonywanie operacji na danych osobowych, takich jak zbieranie, katalogowanie, utrwalanie, przechowywanie, opracowywanie, udostępnianie i usuwanie, w formie papierowej, a także w systemach informatycznych.

Naruszenie - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem; utracenia danych osobowych, zmodyfikowania danych osobowych, nieuprawnionego ujawnienia danych osobowych lub nieuprawnionego dostępu do danych osobowych.

Kodeks dobrych praktyk - zbiór zasad postępowania do którego, pracownicy zobowiązali się dostosować i przestrzegać zgodnie z obowiązującymi przepisami.

Zasada rozliczalności - AD jest odpowiedzialny za przestrzeganie przepisów o ochronie danych i musi być w stanie wykazać ich przestrzeganie.

Zasada integralności i poufności - przetwarzanie; w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Zasada minimalizacji - Dane osobowe powinny być przetwarzane przez administratora w sposób adekwatny w stosunku do celów, w jakich zostały zebrane. Każdy podmiot przetwarzający dane musi dokonać selekcji danych i wybrać tylko taką ich ilość oraz rodzaj, jakie są dla niego niezbędne.

CEL REGULAMINU:

Zachowując zasadę rozliczalności AD wskazuje zasady postępowania na stanowisku pracy, w sytuacji naruszeń, zgodnie z obowiązującymi przepisami o ochronie danych osobowych. Celem niniejszego dokumentu jest ustalenie działań w dziedzinie poprawnych praktyk ochrony danych oraz skatalogowanie możliwych naruszeń, oraz opisanie procedur działania w przypadku ich wystąpienia, jak i również ograniczenie ich powstania w przyszłości.

PROCEDURA KODEKSU DOBRYCH PRAKTYK NA STANOWISKU PRACY:

Uwzględniając zasadę poufności i integralności AD w Zespole Szkół nr 2 im. H. Kołłątaja w Myszkowie zobowiązuje pracowników/użytkowników do przestrzegania następujących praktyk ochrony danych na stanowisku pracy:

- Pracownik/Użytkownik zobowiązany jest do zachowania poufności w związku z przetwarzaniem danych, jakie powierza mu AD.
- Pracownik/Użytkownik na stanowisku pracy, zobowiązany jest do ustawienia monitora komputera, tak aby osoby nieuprawnione nie miały wglądu w zakres wykonywanych zadań.
- Pracownik/Użytkownik zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są pracownikowi niezbędne w danym momencie pracy do wykonania bieżących zadań.
- Na biurku nie mogą znajdować się napoje w pojemnikach grożących rozlaniem płynu.
- Po zakończonej pracy pracownik zobowiązany jest odłożyć wszystkie dokumenty na miejsce, gdzie będą odpowiednio zabezpieczone (np. w szafie zamykanej na klucz).
- Po zakończonej pracy pracownik zobowiązany jest wylogować się z systemu, pozostawić laptop w miejscu niedostępnym dla osób nieupoważnionych (np. w szafie zamykanej na klucz).
- Wiadomości mailowe zawierające dane szczególnych kategorii są wysyłane w sposób zabezpieczony, aby uniemożliwić osobom trzecim dostęp do tych danych.
- Zaleca się aby pracownik/użytkownik korespondował w kwestiach zawodowych jedynie z emaila służbowego.
- Pracownik/Użytkownik ma obowiązek pamiętać, aby podczas zbiorczego wysyłania maili, powinien korzystać z funkcji kopii ukrytych (poza głównym) bowiem ich upublicznienie, wiąże się z naruszeniem danych osobowych.
- Pracownik/Użytkownik nie przechowuje hasła dostępu do komputera w miejscu dostępnym dla osób nieuprawnionych (np.: pod klawiaturą).
- Pracownik/Użytkownik, chcąc zniszczyć niepotrzebne dokumenty, używa tylko niszczarki.
- Pracownik/Użytkownik bez zgody AD /IOD nie wynosi danych na zewnątrz (nie zgrywa danych na pendrive czy inne nośniki danych).

- Pracownik/Użytkownik nie udostępnia osobom postronnym, hasła dostępu do programu, którego jest upoważniony. W sytuacji nieobecności pracownika/użytkownika i konieczności skorzystania z danego programu zostaje wygenerowane hasło tymczasowe i na czas zastępstwa zostaje upoważniony inny pracownik/użytkownik.
- Pracownik/Użytkownik nie udostępnia danych telefonicznie, o ile nie wynika to z przepisów prawa.
- Pracownik/Użytkownik, chcąc pobrać dane do zrealizowania celu, zgodnie z zasadą minimalizacji, pobiera te dane, które są konieczne. Nie dopuszcza się kserowania dowodów, dane są spisywane.
- Pracownik/Użytkownik zobowiązany jest do nieingerowania w system informatyczny. O wszystkich programach instalowanych na służbowym sprzęcie decyduje AD/ASI. Wszelka dowolność pracownika w tym przypadku będzie powodowała wysokie ryzyko utraty kontroli nad danymi.
- Pracownik/Użytkownik posiadający służbowy laptop lub telefon, ma obowiązek stosować odpowiednie zabezpieczenie aby w sytuacji kradzieży, dostęp do danych przetwarzanych na nośniku był niemożliwy.

W Zespole Szkół nr 2 im. H. Kołłątaja w Myszkowie AD w celu podniesienia świadomości pracowników w dziedzinie poprawnych praktyk ochrony danych przeprowadza cykliczne szkolenia z zakresu ochrony danych, co określa ***załącznik nr 1*** (niniejszego Regulaminu).

NARUSZENIE OCHRONY DANYCH OSOBOWYCH:

W Zespole Szkół nr 2 im. H. Kołłątaja w Myszkowie naruszeniem danych określa się incydent bezpieczeństwa prowadzący do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub dostępu osoby nieupoważnionej do przetwarzanych danych osobowych. Każdy incydent bezpieczeństwa może nieść za sobą poważne konsekwencje dla praw i wolności osób, których dane dotyczą.

AD u którego doszło, do naruszenia ochrony przetwarzanych danych, powinien bezzwłocznie podjąć odpowiednie środki zaradcze. W niektórych sytuacjach konieczne będzie również zgłoszenie naruszenia bezpieczeństwa Prezesowi Urzędu Ochrony Danych Osobowych oraz poinformowanie osób, których dane naruszenie dotyczyło.

Wyróżnia się trzy zasadnicze grupy incydentów w ochronie danych osobowych:

Umyślne incydenty:

- kradzież danych i sprzętu,
- ujawnienie danych osobom nieupoważnionym,
- świadome zniszczenie danych,

- włamanie do systemu informatycznego lub pomieszczeń,
- dopuszczenie do przetwarzania danych osób nieposiadających upoważnienia.

Zdarzenia losowe wewnętrzne:

- awaria komputera/serwera/dysku twardego/oprogramowania,
- niewłaściwe zabezpieczenie dostępu do pomieszczeń, w których przetwarzane są dane,
- pomyłki informatyków,
- niewłaściwe zabezpieczenie sprzętu komputerowego.

Zdarzenia losowe zewnętrzne:

- pożar, zalanie wodą,
- utrata zasilania,
- klęski żywiołowe,
- utrata łączności.

PROCEDURA POSTĘPOWANIA PRACOWNIKA/UŻYTKOWNIKA NA WYPADEK WYSTĄPIENIA INCYDENTU BEZPIECZEŃSTWA

Każdy pracownik/użytkownik Zespołu Szkół nr 2 im. H. Kołłątaja w Myszkowie w przypadku stwierdzenia lub podejrzenia faktu o naruszeniu danych ma obowiązek:

- Bezzwłocznie powiadomić o tym fakcie IOD/ AD telefonicznie /email-em.
- Podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn, oraz skutków naruszenia.
- Udokumentować zdarzenie-***załącznik nr 2*** (niniejszego Regulaminu)

ASI jest zobowiązany do informowania IOD o wszelkich awariach i zmianach dotyczących systemu informatycznego, mogących być przyczyną lub skutkiem incydentu w zakresie danych osobowych.

REJESTR PRZYKŁADOWYCH INCYDENTÓW NARUSZEŃ DANYCH OSOBOWYCH

NR. INCYDENTU	**INCYDENTY; umyślne, losowe** ***(wewnętrzne i zewnętrzne)***	**POSTĘPOWANIE** ***(w przypadku stwierdzenia lub podejrzenia faktu o incydencie naruszenia danych)***
1.	Ślady wskazujące na próbę włamania (np.: zniszczenia na drzwiach, oknach, szafach wzbudzające podejrzenia).	Należy; podjąć czynności niezbędne do powstrzymania skutków naruszenia danych (np.; zabezpieczyć dane osobowe, sporządzić notatkę z zaistniałej sytuacji. IOD/AD po ocenie sytuacji wzywa policję, sporządza raport.
2.	Dokumentacja zawierająca dane osobowe została wyrzucona do kosza lub zniszczona w sposób umożliwiający odczyt (bez użycia niszczarki). Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/ urządzenia elektronicznego przed jego zbyciem przez administratora.	Należy; podjąć czynności niezbędne do powstrzymania skutków naruszenia danych (np.: zabezpieczyć dane osobowe), powiadomić IOD/AD sporządzić notatkę z zaistniałej sytuacji. IOD/AD sporządza raport.
3.	Udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, ustnej lub elektronicznej.	Należy; podjąć czynności niezbędne do powstrzymania skutków naruszenia danych (np.; przerwać rozmowę lub inną czynność prowadzącą do ujawnienia danych), powiadomić IOD/AD sporządzić notatkę z zaistniałej sytuacji. IOD/AD sporządza raport.
4.	Zgubienie służbowych nośników danych; laptop, telefon, pendrive.	Należy; podjąć czynności niezbędne do powstrzymania skutków naruszenia danych (np.; podjąć próbę odnalezienia i odtworzenia sytuacji, w jakich okolicznościach doszło do zgubienia), powiadomić IOD/AD sporządzić notatkę z danej sytuacji. IOD/AD sporządza raport.
5.	Próba kradzieży danych osobowych poprzez zewnętrzny nośnik danych.	Należy; podjąć czynności niezbędne do powstrzymania skutków naruszenia danych. IOD/ASI powinien zabezpieczyć nośnik danych i powiadomić AD. IOD/AD sporządza raport.
6.		Należy; podjąć czynności niezbędne do powstrzymania skutków naruszenia danych (np.; zabezpieczyć dane,

	Próba kradzieży danych osobowych w formie papierowej.	zabezpieczyć dowody) powiadomić IOD/AD zrobić notatkę z zaistniałej sytuacji. IOD/AD sporządza raport.
7.	Kradzież komputerów lub twardych dysków z danymi osobowymi.	Należy; wezwać policję, poinformować IOD/AD sporządzić notatkę z zaistniałej sytuacji. IOD/AD sporządza raport.
8.	Dane osobowe przechowywane są w pomieszczeniach, gdzie stwierdzono brak zabezpieczeń; otwarte szafy, biurka, regały, otwarte pomieszczenie archiwalne.	Należy; podjąć czynności niezbędne do powstrzymania skutków naruszenia danych (np.; uniemożliwić dostęp osób bez upoważnienia do pomieszczeń) oraz powiadomić AD/IOD. IOD/AD sporządza raport.
9.	Omyłkowe wysłanie maila z zawartością danych osobowych, do osoby nieuprawnionej.	Należy; podjąć czynności niezbędne do powstrzymania skutków naruszenia danych (np.; poinformować odbiorcę o natychmiastowym usunięciu maila) powiadomić IOD/AD sporządzić notatkę z zaistniałej sytuacji. IOD/AD sporządza raport.
10.	Działanie zewnętrznych aplikacji, wirusów, złośliwego oprogramowania.	Należy; podjąć czynności niezbędne do powstrzymania skutków naruszenia danych (np.; zabezpieczyć dane) powiadomić IOD/AD sporządzić notatkę z zaistniałej sytuacji. IOD/AD sporządza raport. Dla bezpieczeństwa zrobić audyt systemów zabezpieczeń, w szczególności systemów antywirusowych, firewall.
11	Brak aktywnego oprogramowania antywirusowego.	Należy; powiadomić IOD/AD. IOD/AD/ASI powinien zaktualizować lub nabyć oprogramowanie antywirusowe. IOD/AD sporządza raport.
12.	Stwierdzono próbę lub modyfikację danych, lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji).	Należy; podjąć czynności niezbędne do powstrzymania skutków naruszenia danych (np.; zabezpieczyć dane, zabezpieczyć dowody) powiadomić IOD/AD sporządzić notatkę z zaistniałej sytuacji. IOD/AD sprawdza stan uszkodzeń, sporządza raport.
13.	Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych i sieci.	Należy; podjąć czynności niezbędne do powstrzymania skutków naruszenia danych (np.; zabezpieczyć listę z hasłami) powiadomić IOD/AD sporządzić notatkę z zaistniałej sytuacji. IOD/AD sporządza raport.

14.	Uszkodzenie komputerów, nośników danych.	Należy; podjąć czynności niezbędne do powstrzymania skutków naruszenia danych (np.; zabezpieczyć dane, zabezpieczyć dowody) powiadomić IOD/AD zrobić notatkę z zaistniałej sytuacji. IOD/AD/ASI powinien, ocenić w wyniku czego, doszło do zniszczenia i przywrócić dane z kopii zapasowej. IOD/AD sporządza raport.
15.	Próba nieuprawnionej interwencji przy sprzęcie komputerowym.	Należy; podjąć czynności niezbędne do powstrzymania skutków naruszenia danych (np.; uniemożliwić dostęp osób do sprzętu komputerowego, zabezpieczyć dane) sporządzić notatkę z zaistniałej sytuacji, powiadomić IOD/AD.AD/IOD sporządza raport.
16.	Zdarzenia losowe.	Należy; podjąć czynności niezbędne do powstrzymania skutków naruszenia danych (np.; wezwać służby ratunkowe, zabezpieczyć dowody, podjąć próbę odzyskania dokumentacji i sprzętu) poinformować AD/IOD. AD/IOD szacuje powstałe straty. AD/IOD sporządza raport.
17.	Nieprawidłowa anonimizacja danych w dokumencie	Należy; podjąć czynności niezbędne do powstrzymania skutków naruszenia danych (np.; zabezpieczyć dane, zabezpieczyć dowody) powiadomić IOD/AD zrobić notatkę z zaistniałej sytuacji. IOD/AD sporządza raport.
18.	Niezamierzona publikacja	Należy; podjąć czynności niezbędne do powstrzymania skutków naruszenia danych(np.; zabezpieczyć dane, zabezpieczyć dowody) powiadomić IOD/AD zrobić notatkę z zaistniałej sytuacji. IOD/AD sporządza raport.
19.	Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji.	Należy; podjąć czynności niezbędne do powstrzymania skutków naruszenia danych (np.; zabezpieczyć dane, zabezpieczyć dowody) powiadomić IOD/AD zrobić notatkę z zaistniałej sytuacji. IOD/AD sporządza raport.

20.	Korespondencja papierowa została, utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy	Należy; podjąć czynności niezbędne do powstrzymania skutków naruszenia danych(np.; zabezpieczyć dane, zabezpieczyć dowody) powiadomić IOD/AD zrobić notatkę z zaistniałej sytuacji. IOD/AD sporządza raport.

PROCEDURA POSTĘPOWANIA IOD/AD PO PRZYJĘCIU ZGŁOSZENIA O INCYDENCIE NARUSZENIA DANYCH

W Zespole Szkół nr 2 im. H. Kołłątaja w Myszkowie AD/IOD po otrzymaniu zgłoszenia o incydencie naruszenia danych ma obowiązek podjąć następujące kroki:

- Zapoznać się z zaistniałą sytuacją, poprzez relację z powstałego naruszenia bezpieczeństwa danych złożoną (ustnie i na piśmie) przez osobę powiadamiającą, oraz każdą inną, która może mieć informacje w związku z zaistniałym naruszeniem.
- Ocenić sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości ciągłości pracy np.: zabezpieczyć dowody, zabezpieczyć dane osobowe, podjąć próbę przywrócenia stanu sprzed zaistnienia zagrożenia, wprowadzić procedury uniemożliwiające ponowne powstanie zagrożenia, powiadomić policję, jeśli jest taka konieczność, powiadomić o zaistniałej sytuacji AD.
- Udokumentować zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając raport-***załącznik nr 3*** (niniejszego Regulaminu).
- Wprowadzić działania naprawcze i zapobiegające ponownemu wystąpieniu naruszeń-***załącznik nr 4*** (niniejszego Regulaminu).

PROCEDURA ZGŁASZANIA NARUSZEŃ DO ORGANU NADZORCZEGO

W Zespole Szkół nr 2 im. H. Kołłątaja w Myszkowie AD po stwierdzeniu faktu, iż naruszone zostały dane osobowe i naruszenie to, skutkowało ryzykiem naruszenia praw wolności osób fizycznych, podejmuje następujące kroki:

- Zgłasza naruszenie do Prezesa Urzędu Ochrony Danych Osobowych (zgłoszenie dokonujemy elektronicznie za pomocą odpowiedniego formularza dostępnego na stronie Urzędu Ochrony Danych Osobowych https://uodo.gov.pl/data/filemanager_pl/770.docx).
- Nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.
- W sytuacji opóźnienia i zgłoszenia naruszenia danych po upływie 72 godzin dołącza wyjaśnienie przyczyn opóźnienia.

W zgłoszeniu ujmuje poniższe informacje:

- Dane kontaktowe IOD, (jeżeli jest powołany) lub AD dane osoby powiadamiającej o naruszeniu,
- Miejsce naruszenia,
- Czas naruszenia,
- Charakter naruszenia;
    - naruszenie poufności danych,
    - naruszenie integralności danych,
    - naruszenie dostępności danych.
- Konsekwencje naruszenia danych osobowych,
- Kategorie danych osobowych,
- Kategorie osób,
- Środki bezpieczeństwa zastosowane przed naruszeniem,
- Środki zastosowane lub proponowane przez AD w celu zaradzenia naruszenia ochrony danych osobowych, tym - w stosownych przypadkach-środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli powyższych informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

PROCEDURA ZAWIADAMIANIA OSOBY, KTÓREJ DANE DOTYCZĄ O NARUSZENIU DANYCH OSOBOWYCH

W Zespole Szkół nr 2 im. H. Kołłątaja w Myszkowie w sytuacji stwierdzenia przez AD , iż naruszenie może spowodować wysokiego ryzyko naruszeń praw lub wolności osób fizycznych AD bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą.

1. Zawiadomienie, o którym mowa musi zawierać; prostym, zrozumiałym językiem charakter naruszenia ochrony danych, oraz wszystkie informacje, które określone są w ***załączniku nr 5*** (niniejszego Regulaminu).

2. Zawiadomienie nie jest wymagane w następujących przypadkach:

- AD wdrożył odpowiednie środki ochrony (techniczne i organizacyjne) środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie (np. szyfrowanie uniemożliwiające odczyt osobom nieuprawnionym do tych danych osobowych).

- AD zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą.
- Wymagałoby ono niewspółmiernie dużego wysiłku; w takim przypadku zostaje wydany publiczny komunikat lub informacja zostaje przekazana w inny, ale również skuteczny sposób (np.; na stronie internetowej lub w BIP) - ***załącznik nr 6*** (niniejszego Regulaminu).

ODPOWIEDZIALNOŚĆ ZA NARUSZENIE OCHRONY DANYCH OSOBOWYCH

W Zespole Szkół nr 2 im. H. Kołłątaja w Myszkowie AD w sytuacji stwierdzania zaniechania działań ze strony pracownika/użytkownika, związanych ze zgłoszeniem naruszenia, oraz zaniedbań i niepodjęcia odpowiednich kroków określonych w niniejszym dokumencie wszczyna postępowanie dyscyplinarne.

Kara dyscyplinarna, wobec pracownika uchylającego 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.

Każdy pracownik/użytkownik zatrudniony w Zespole Szkół nr 2 im. H. Kołłątaja w Myszkowie ma obowiązek zapoznać się z niniejszym regulaminem i przestrzegać procedur w nim zawartych. Wykonanie powyższego zobowiązania pracownik/użytkownik potwierdza własnoręcznym podpisem- ***załącznik nr 7*** (niniejszego Regulaminu).

„REGULAMIN WEWNĘTRZNYCH PROCEDUR” Zapisy tego dokumentu wchodzą w życie z dniem **3 września 2018 r.**

Dyrektor

mgr inż. Jerzy Bryś

……..
(data i podpis Administratora Danych)

Wykaz załączników;

- **załącznik nr 1** - lista osób, które zostały przeszkolone z zakresu nowych przepisów RODO,
- **załącznik nr 2** - zgłoszenie o naruszeniu ochrony danych do IOD/AD
- **załącznik nr 3** - raport z naruszenia ochrony danych,

- **załącznik nr 4** - rejestr incydentów bezpieczeństwa, działań naprawczych i zapobiegawczych,
- **załącznik nr** 5 – zawiadomienie o naruszeniu danych osoby, której naruszenie dotyczy,
- **załącznik nr 6** - komunikat o naruszeniu ochrony danych,
- **załącznik nr 7** - lista pracowników\użytkowników zapoznanych z regulaminem.

LISTA OSÓB, KTÓRE ZOSTAŁY PRZESZKOLONE Z ZAKRESU NOWYCH PRZEPISÓW RODO

Załącznik nr 1

Lp.	NAZWISKO I IMIĘ	DATA OSTATNIEGO SZKOLENIA	CZYTELNY PODPIS

…….
(data i podpis Administratora Danych)

ZGŁOSZENIE Z NARUSZENIA OCHRONY DANYCH DO IOD/AD **Załącznik nr 2**

1. PEŁNA NAZWA PLACÓWKI: ……

2. DATA /GODZINA ZDARZENIA …….

3. DATA /GODZINA POINFORMOWANIA IOD/AD O ZDARZENIU ……..

4. OSOBA POWIADAMIAJĄCA O NARUSZENIU ORAZ INNE OSOBY ZAANGAŻOWANE W ZDARZENIE:

……
(imię, nazwisko, stanowisko służbowe)

……
(imię, nazwisko, stanowisko służbowe)

5. LOKALIZACJA ZDARZENIA (NAZWA POMIESZCZENIA, NR POKOJU, OKREŚLENIE KOMPUTEROWEGO STANOWISKA, ROBOCZEGO, NAZWA PROGRAMU LUB APLIKACJI ITP.):

……

……

……

6. PODJĘTE CZYNNOŚCI NIEZBĘDNE DO POWSTRZYMANIA SKUTKÓW NARUSZENIA DANYCH

……

……

7. RODZAJ NARUSZENIA I OKREŚLENIE OKOLICZNOŚCI TOWARZYSZĄCYCH NARUSZENIU:

……

……

…… ……

(data i podpis pracownika) (data i podpis AD)

RAPORT Z NARUSZENIA OCHRONY DANYCH **Załącznik nr 3**

1. PEŁNA NAZWA PLACÓWKI: ……..

2. DANE OSOBY SPORZĄDZAJĄCEJ RAPORT: ……

3. DATA/GODZINA ZDARZENIA : ……

4. DATA /GODZINA PRZYJĘCIA ZGŁOSZENIA PRZEZ IOD/AD: ……

5. OSOBA POWIADAMIAJĄCA O NARUSZENIU ORAZ INNE OSOBY ZAANGAŻOWANE W ZDARZENIE:

……
(imię, nazwisko, stanowisko służbowe)

……
(imię, nazwisko, stanowisko służbowe)

6. LOKALIZACJA ZDARZENIA (NAZWA POMIESZCZENIA, NR POKOJU, OKREŚLENIE KOMPUTEROWEGO STANOWISKA ROBOCZEGO, NAZWA PROGRAMU LUB APLIKACJI ITP.):

……

……

……

7. RODZAJ NARUSZENIA I OKREŚLENIE OKOLICZNOŚCI TOWARZYSZĄCYCH NARUSZENIU:

……

……

……

……

……

8. ZABEZPIECZONE DOWODY:

……

……

……

8. INFORMACJE O DANYCH, KTÓRE ZOSTAŁY LUB MOGŁY ZOSTAĆ UJAWNIONE:

……

……

……

……

9. PODJĘTE DZIAŁANIA NAPRAWCZE I ZAPOBIEGAWCZE:

……

……

……

……. ……

(data i podpis pracownika) (data i podpis Administratora Danych)

REJESTR INCYDENTÓW BEZPIECZEŃSTWA, DZIAŁAŃ NAPRAWCZYCH I ZAPOBIEGAWCZYCH **Załącznik nr 4**

Lp.	INCYDENT BEZPIECZEŃSTWA	ŹRÓDŁO ZGŁOSZENIA; (zawiadomienie, skarga, kontrola)	DATA I GODZINA ROZPOCZĘCIA	DATA I GODZINA ZAKOŃCZ -ENIA	ZGŁOSZENIE DO PUODO TAK/NIE	OSOBA ODPOWIEDZIALNA	PRZYCZYNA POWSTANIA INCYDENTU	DZIAŁANIE NAPRAWCZE/ ZAPOBIEGAWCZE (przywracające bezpieczeństwo)	SKUTKI DZIAŁAŃ NAPRAWCZYCH/ ZAPOBIEGAWCZYCH

ZAWIADOMIENIE O NARUSZENIU DANYCH OSOBOWYCH OSOBY, KTÓREJ NARUSZENIE DOTYCZY

Załącznik nr 5

1. PEŁNA NAZWA PLACÓWKI: …….

2. DANE OSOBY SPORZĄDZAJĄCEJ RAPORT IOD/AD: ……..

3. DATA / GODZINA ZDARZENIA: …….

4. DATA /GODZINA PRZYJĘCIA ZGŁOSZENIA PRZEZ IOD/AD: ……..

5. OSOBA POWIADAMIAJĄCA O NARUSZENIU ORAZ INNE OSOBY ZAANGAŻOWANE W ZDARZENIE:

……..
(imię, nazwisko, stanowisko służbowe)

……
(imię, nazwisko, stanowisko służbowe)

6. LOKALIZACJA ZDARZENIA (NAZWA POMIESZCZENIA, NR POKOJU, OKREŚLENIE KOMPUTEROWEGO STANOWISKA ROBOCZEGO, NAZWA PROGRAMU LUB APLIKACJI ITP.):

……

……

……

7. CHARAKTER NARUSZENIA OCHRONY DANYCH OSOBOWYCH: (NALEŻY WSKAZAĆ KATEGORIE I PRZYBLIŻONĄ LICZB OSÓB, KTÓRYCH DANE DOTYCZĄ, ORAZ KATEGORIE I PRZYBLIŻONĄ LICZBĘ WPISÓW DANYCH OSOBOWYCH, KTÓRYCH DOTYCZY NARUSZENIE):

……

……

……

……

……

8. PRZYCZYNY WYSTĄPIENIA NARUSZENIA I MOŻLIWE KONSEKWENCJE NARUSZENIA OCHRONY DANYCH OSOBOWYCH:

……

……

……

……

……

……

……

9. ŚRODKI ZASTOSOWANE LUB PROPONOWANE W CELU ZARADZENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH, W TYM – W STOSOWNYCH PRZYPADKACH – ŚRODKI W CELU ZMINIMALIZOWANIA JEGO EWENTUALNYCH NEGATYWNYCH SKUTKÓW:

……

……

……

……

……

(data i podpis Administratora Danych)

KOMUNIKAT O NARUSZENIU OCHRONY DANYCH **Załącznik nr 6**

Komunikat o naruszeniu ochrony danych z dnia ……

1.	CHARAKTER NARUSZENIA OCHRONY DANYCH:	
2.	KATEGORIA I PRZYBLIŻONA LICZBA OSÓB, KTÓRYCH DANE DOTYCZĄ:	
3.	LICZBA WPISÓW, KTÓRYCH DOTYCZY NARUSZENIE:	
4.	MOŻLIWE KONSEKWENCJE NARUSZENIA OCHRONY DANYCH:	
5.	ŚRODKI ZASTOSOWANE LUB PROPONOWANE W CELU ZARADZENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH, W TYM – W STOSOWNYCH PRZYPADKACH – ŚRODKI W CELU ZMINIMALIZOWANIA JEGO EWENTUALNYCH NEGATYWNYCH SKUTKÓW:	

…….
(data i podpis Administratora Danych)

LISTA PRACOWNIKÓW/UŻYTKOWNIKÓW ZAPOZNANYCH Z REGULAMINEM **Załącznik nr 7**

LP.	NAZWISKO I IMIĘ	DATA ZAPOZNANIA	CZYTELNY PODPIS
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			

…….

(data i podpis Administratora Danych)