PROCEDURY POSTĘPOWANIA Z INFORMACJAMI W SZKOLE PODSTAWOWEJ IM. MARII KONOPNICKIEJ W MROKOWIE

DEFINICJA

§ 1

1. Procedury postepowania z informacjami to zbiór spójnych, precyzyjnych oraz zgodnych z obecnym stanem prawnym reguł i procedur, zgodnie z którymi jednostka zarządza bezpieczeństwem zbiorów danych, informacji i bezpieczeństwem systemów, w których zbiory danych i informacje są lub mogą być przetwarzane.
2. Procedury są aktem wewnętrznego stosowania. Z dokumentem powinny zapoznać się oraz przestrzegać jego postanowień wszystkie osoby mające dostęp do przetwarzanych informacji.
3. Procedury mają na celu osiągnięcie takiego poziomu organizacyjnego i technicznego systemu zarządzania bezpieczeństwem informacji, które:
   a) będą gwarantem pełnej ochrony informacji oraz ciągłości procesu ich przetwarzania;
   b) zapewnią zachowanie poufności informacji chronionych, integralności i dostępności informacji chronionych oraz jawnych;
   c) zagwarantują odpowiedni poziom bezpieczeństwa informacji, bez względu na jej postać, we wszystkich systemach, w których jest przetwarzana;
   d) ograniczą występowanie zagrożeń dla bezpieczeństwa informacji;
   e) zapewnią poprawne i bezpieczne funkcjonowanie wszystkich systemów przetwarzania informacji;
   f) zapewnią gotowość do podjęcia działań w sytuacjach kryzysowych.
4. Powyższe cele realizowane są poprzez:
   a) ustalenie struktury organizacyjnej zapewniającej optymalny podział i koordynację zadań oraz odpowiedzialności związanych z zapewnieniem bezpieczeństwa informacji;
   b) zobowiązanie do stosowania przez wszystkie osoby zatrudnione i wykonujące pracę;
   c) wdrożenie i utrzymanie niezbędnych zabezpieczeń organizacyjnych i technicznych;
   d) przegląd i aktualizację polityk, procedur, instrukcji oraz innych regulacji wewnętrznych dotyczących bezpieczeństwa informacji dokonywane przez odpowiedzialne osoby w celu jak najlepszej reakcji na zagrożenia i incydenty;
   e) podnoszenie świadomości i kwalifikacji pracowników w obszarze bezpieczeństwa informacji.

§ 2

Polityka bezpieczeństwem informacji zapewnia następujące reguły:

a) poufności - zapewnienie dostępu do informacji wyłącznie podmiotom upoważnionym;
b) integralności - zapewnienia dokładności i kompletności danych i informacji oraz określenie metod ich przetwarzania;
c) dostępności informacji - zapewnienia, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów tylko wtedy, gdy zachodzi taka potrzeba;

§ 3

Cele, o których mowa w § 1 ust. 4 realizowane są w oparciu o zasady:

a) minimalizacji uprawnień, tzn. każdy pracownik powinien posiadać tylko takie uprawnienia jakie są wymagane do realizacji jego obowiązków;
b) wielowarstwowych zabezpieczeń, tzn. system informatyczny podlega ochronie równolegle na wielu poziomach;
c) ograniczania dostępu, tzw. domyślnym uprawnieniem w systemach informatycznych jest „zabroniony dostęp". Dopiero w przypadku zaistnienia odpowiedniej potrzeby, przyznawane są stosowne uprawnienia.

ZAKRES PROCEDUR

§ 4

1. Procedury postępowania z informacjami mają zastosowanie do całego mechanizmu informacyjnego panującego w Szkole Podstawowej w Nowej Iwicznej i obejmują:
   a) wszystkie istniejące, wdrażane obecnie lub w przyszłości systemy informatyczne oraz tradycyjne (papierowe), w których przetwarzane są lub będą informacje;
   b) informacje będące własnością jednostki;
   c) informacje będące własnością kontrahentów, które zostały przekazane na podstawie zawartych umów;
   d) wszystkie typy nośników, na których są lub będą znajdować się informacje;
   e) wszystkie budynki i pomieszczenia, w których są lub będą przetwarzane informacje;
   f) wszystkich pracowników w rozumieniu Kodeksu Pracy i innych osób mających dostęp do informacji, na zasadach określonych w niniejszej polityce bezpieczeństwa.
2. Dane i informacje mogą być przetwarzane wyłącznie w miejscu i systemach, które spełniają warunki opisane w niniejszej procedurze.

OBOWIĄZKI I ODPOWIEDZIALNOŚĆ

§ 5

1. Odpowiedzialność za bezpieczeństwo informacji w jednostce ponoszą wszyscy pracownicy zgodnie z posiadanym zakresem obowiązków. Administrator Danych — Dyrektor, jest odpowiedzialny za zapewnienie zasobów niezbędnych do funkcjonowania, utrzymania i doskonalenia procedur zarządzania bezpieczeństwem informacji.
2. Zadania zarządzania systemem informatycznym pełni Administrator Systemu Informatycznego (ASI) — osoba wyznaczona przez Dyrektora.
3. Proces zarządzania bezpieczeństwem jest działaniem ciągłym i realizowanym przy współpracy użytkowników systemów informatycznych z Administratorem Danych Osobowych oraz ASI.
4. Zapewnienie ochrony danych osobowych zostało uregulowane w osobnym dokumencie: „Polityka Bezpieczeństwa Przetwarzania Danych Osobowych w Szkole Podstawowej w Mrokowie"

OZNACZENIE I KLASYFIKACJA ZASOBÓW INFORMACYJNYCH

§ 6

Informacje gromadzone i przetwarzane podlegają klasyfikacji według następujących kategorii:

1. informacje jawne — informacje publicznie dostępne;
2. informacje wewnętrzne informacje, których przetwarzanie i udostępnianie podlega restrykcjom ze względu na szczególne znaczenie:
   a) informacje wewnętrzne — dostępne dla wszystkich pracowników;
   b) informacje wewnętrzne wrażliwe — dostępne dla grupy pracowników upoważnionych ze względu na stanowisko, funkcję lub na wykonywany zakres obowiązków służbowych;
3. informacje niejawne — informacje, do których stosuje się przepisy o ochronie informacji niejawnych lub o ochronie danych osobowych lub innych tajemnic prawnie chronionych.
4. informacje podlegające szczególnej ochronie oznaczają:
   a) informacje o realizowanych kontraktach (zarówno planowane, bieżące jak i historyczne);
   b) informacje finansowe;
   c) informacje organizacyjne;
   d) dane dostępowe do systemów IT;
   e) dane osobowe;
   f) inne informacje oznaczone jako „informacje wrażliwe" lub „dane wrażliwe".

§ 7

Informacje gromadzone i przetwarzane w sposób o którym mowa w 7 posiadają trzystopniową skalę bezpieczeństwa:

1. Wrażliwość „W" - ze względu na rozmiar szkód, które mogłoby wywołać ich ujawnienie nieuprawnionym osobom lub instytucjom:
   a) W1 (poziom niski) — dotyczy informacji, które mogą być publicznie znane lub, których ujawnienie nie powoduje lub powoduje niewielkie konsekwencje natury prawnej lub finansowej;
   b) W2 (poziom średni) — dotyczy informacji, których ujawnienie może wiązać się z poważnymi konsekwencjami natury prawnej lub finansowej. Do tej grupy zaliczymy również dane osobowe;
   c) W3 (poziom wysoki) informacje krytyczne których ujawnienie mogłoby zagrozić funkcjonowaniu jednostki lub spowodować bardzo poważne szkody natury prawnej lub finansowej. Do tej grupy zaliczamy również dane sensytywne.
2. Integralność „I" - ze względu na rozmiar szkód, które mogłoby wywołać ich nieautoryzowana zmiana:
   a) I1 (poziom niski) — informacje, których nieautoryzowana zmiana nie powoduje lub powoduje niewielkie konsekwencje natury prawnej lub finansowej;
   b) I2 (poziom średni) — informacje, których nieautoryzowana zmiana może wiązać się z poważnymi konsekwencjami natury finansowej lub prawnej. Do tej grupy zaliczamy dane osobowe;
   c) I3 (poziom wysoki) — informacje, których nieautoryzowana zmiana mogłaby zagrozić funkcjonowaniu jednostki lub spowodować bardzo poważne szkody natury prawnej lub finansowej.
3. Dostępność „D" - ze względu na maksymalny akceptowalny okres niedostępności do informacji lub konsekwencje ich utraty:
   a) D1 (poziom niski) — długotrwały brak dostępu do tych informacji nie odbija się (negatywnie) w istotny sposób na funkcjonowaniu oraz nie pociąga za sobą konsekwencji prawnych lub finansowych;
   b) D2 (poziom średni) — informacje dla których brak dostępu krótszy niż jeden dzień nie odbija się (negatywnie) w istotny sposób na funkcjonowaniu oraz nie pociąga za sobą konsekwencji prawnych lub finansowych;

c) D3 (poziom wysoki) — informacje dla których brak dostępu dłuższy niż cztery godziny w istotny sposób odbije się na funkcjonowaniu lub może pociągać za sobą poważne konsekwencje natury prawnej lub finansowej.

DOSTĘP I ZABEZPIECZENIE

§ 8

Zapewnienie bezpieczeństwa informacji oraz danych przechowywanych i przetwarzanych w jednostce polega na:

a) wydzieleniu obszarów przeznaczonych do przetwarzania i przechowywania zbiorów danych, od obszarów ogólnie dostępnych i zapewnieniu odpowiednich barier fizycznych przeciwdziałających nieuprawnionemu dostępowi;
b) zarządzaniu uprawnieniami poszczególnych użytkowników, z zastosowaniem zasady „minimalnych uprawnień", to znaczy przydzielania dostępu wyłącznie do danych związanych z realizacją obowiązków służbowych;
c) stosowaniu zasady ograniczonego dostępu, gdzie domyślnymi uprawnieniami jest zabronienie dostępu. Stosowne uprawnienia są nadawane przez ASI w przypadku zaistnienia uzasadnionej potrzeby;
d) stosowaniu wielowarstwowych zabezpieczeń systemów przetwarzania informacji;
e) monitorowania adekwatności i skuteczności stosowanych środków kontroli dostępu do informacji.

§ 9

1. Szkoła współpracuje z kontrahentami na podstawie zawartych umów, które zawierają deklarację o zachowaniu poufności oraz zobowiązanie do przestrzegania zasad bhp i ppoż, w przypadku umów, na mocy których kontrahent wykonuje zlecenie na terenie jednostki.
2. Pomieszczenie jednostki (sekretariat szkoły) zajmujący się przetwarzaniem danych chronionych wyposażony jest w barierę fizyczną (lada) umożliwiającą obsługę klientów przy jednoczesnym odseparowaniu od zasobów informacyjnych.
3. Pomieszczenia, w których znajdują się urządzenia przetwarzające zasoby informacyjne są zabezpieczone fizycznie.
4. Ciągi komunikacyjne pozostają pod nadzorem systemu monitoringu wizyjnego i alarmowego.
5. W jednostce obowiązuje „Instrukcja Zarządzania Systemem Informatycznym" załącznik nr 1 do PBDO.

§ 10

1. Jednostka, w procesie zarządzania ciągłością działania systemu dba o zapewnienie usług związanych z przetwarzaniem danych, poprzez przewidywanie możliwości wystąpienia krytycznych zdarzeń i przeciwdziałanie awariom i przerwom w działaniu systemów i urządzeń.
2. Jednostka, w miarę potrzeb zapewnia cykliczną edukację pracowników w zakresie bezpieczeństwa informacji. Pracownicy w zależności od zajmowanego stanowiska mogą uczestniczyć w szkoleniach z zakresu ochrony danych osobowych i szczegółowych aspektów bezpieczeństwa.

§ 11

1. Pracownikom szkoły zabrania się:
   a) przenoszenia niezabezpieczonych danych poufnych poza teren, w szczególności zabrania się przenoszenia danych poufnych na nośnikach elektronicznych, bez uprzedniej zgody Administratora Danych;
   b) zabrania się korzystania z firmowej infrastruktury IT w celach prywatnych.
2. W przypadku rozwiązania umowy o pracę z pracownikiem, dezaktywowane są wszystkie jego dostępy w systemach IT.
3. Wszelkie podejrzenia naruszenia Procedur bezpieczeństwa należy zgłaszać do Administratora Danych i/lub ASI oraz ADO.
4. Każdy incydent jest odnotowywany w stosownej bazie danych. AD w porozumieniu z ADO i/lub ASI podejmuje właściwe kroki zaradcze.

ŚRODKI OCHRONY

§ 12

1. W razie potrzeby kierownicy jednostek organizacyjnych dokonują oceny ryzyka dla poszczególnych systemów.
2. Analiza ryzyka dotyczy:
   a) identyfikacji występujących zagrożeń dla systemów, zbiorów i baz danych;
   b) oceny dotychczas stosowanej ochrony przetwarzania danych osobowych;
   c) określenia skali ryzyka, tj. prawdopodobieństwa wystąpienia określonego zagrożenia;
   d) identyfikacji obszarów wymagających szczególnych zabezpieczeń.

§ 13

1. AD jest zobowiązany do zastosowania środków ochrony, tj. środki fizyczne, osobowe i techniczne, które zapewnią poufność, integralność i rozliczalność przetwarzanych informacji.
2. Środki ochrony fizycznej obejmują:
   a) lokalizację miejsc przetwarzania danych osobowych w pomieszczeniach o ograniczonym i kontrolowanym dostępie;
   b) ustalenie zasad kontroli dostępu do obiektów, pomieszczeń i szaf;
   c) wyposażenia pomieszczeń, w których przetwarzane są dane osobowe we właściwe, w tym antywłamaniowe zabezpieczenia tj. wzmocnione drzwi, odpowiednio zabezpieczone okna i meble oraz niezbędne zabezpieczenia alarmowe;
   d) przechowywanie danych wrażliwych oraz nośników wymiennych i nośników kopii zapasowych w odpowiednio zabezpieczonych miejscach;
   e) odpowiednie wyposażenie i zabezpieczenie pomieszczeń serwerowni.
3. Środki ochrony osobowej obejmują:
   a) dopuszczenie do przetwarzania danych osobowych i informacji wrażliwych wyłącznie osób posiadających upoważnienie;
   b) zapewnienie osobom, o których mowa w ust. I odpowiedniego przygotowania zgodnie z zasadami i obsługą systemu przetwarzania danych osobowych;
   c) prowadzenie dokumentacji zawierającej stosowne zobowiązania i oświadczenia tj. do zachowania w tajemnicy danych i sposobów ich zabezpieczania czy oświadczenia o zapoznaniu się z treścią przepisów określających zasady postępowania przy przetwarzaniu danych osobowych.
4. Środki ochrony technicznej obejmują:
   a) mechanizmy kontroli dostępu do wybranych pomieszczeń;
   b) zastosowanie i aktualizowanie narzędzi ochrony (programy antywirusowe) systemów i baz danych;
   c) regularne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych;
   d) zastosowanie ochrony zasilania.

POSTĘPOWANIE W SYTUACJACH NARUSZENIA ZASAD BEZPIECZEŃSTWA

§ 14

1. Za naruszenie zabezpieczenia systemu bądź urządzenia, w którym są przetwarzane dane wrażliwe, przyjmuje się każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu osobom nie upoważnionym, zabrania danych przez osobę nieupoważnioną lub uszkodzenie jakiegokolwiek elementu systemu.
2. W przypadku zaistnienia zdarzeń, które mogą wskazywań na naruszenie lub stwierdzenia naruszenia zabezpieczenia systemu oraz wykryte słabości systemów informatycznych należy zgłosić niezwłocznie do ASI.
3. W przypadku zaistnienia zdarzeń, które mogą wskazywań na naruszenie lub stwierdzenia naruszenia/ujawnienia danych osobowych należy niezwłocznie zgłosić do ADO.

§ 15

1. Zgłoszenie zdarzenia, o którym mowa w 15 niniejszego paragrafu powinno zawierać:
   a) dane osoby zgłaszającej: imię, nazwisko, stanowisko, nazwę komórki organizacyjnej, tel. kontaktowy;
   b) opis oznak naruszenia procedur ochrony danych osobowych;
   c) określenie sytuacji i czasu wystąpienia zdarzenia;
   d) identyfikację rodzaju zaistniałego zdarzenia, w tym określenie skali zniszczeń, metody dostępu dokonania nieupoważnionego dostępu;
   e) przedstawienie wszystkich istotnych informacji i dokumentów (raportów) wskazujących na przyczynę zdarzenia;
   f) wskazanie możliwości zabezpieczenia systemu oraz wszelkich działań podjętych po ujawnieniu zdarzenia w celu uniemożliwienia lub ograniczenia nieuprawnionego dostępu, minimalizacji szkód i sposobów zabezpieczenia śladów naruszenia ochrony danych.
2. Zgłoszenia, o których mowa w 15 ust. 2 oraz ust. 3 podlegają rejestracji w rejestrze incydentów bezpieczeństwa informacji, dostępnym w sekretariacie szkoły.

§ 16

1. AD w porozumieniu z ASI i/lub ADO podejmuje wszelkie działania mające na celu:
   a) minimalizację negatywnych skutków zdarzenia; 2) wyjaśnienie przyczyn i okoliczności zdarzenia;
   b) zabezpieczenie dowodów zdarzenia;

c) zapewnienie możliwości dalszego bezpiecznego przetwarzania danych.

2. W celu realizacji działań, o których mowa w ust. I ma prawo do:
   a) żądania wyjaśnień od pracowników;
   b) korzystania z pomocy konsultantów;
   c) wnioskowania do ADO o wydanie zakazu wykonywania prac w zakresie przetwarzania danych osobowych do czasu przywrócenia możliwości przestrzegania procedur bezpieczeństwa.

§ 17

Odmowa udzielania wyjaśnień lub współpracy z AD w obszarze ochrony danych osobowych traktowana będzie, jako naruszenie obowiązków pracowniczych.

ZARZĄDZANIE RYZYKIEM

§ 18

1. Każde zidentyfikowane ryzyko podlega analizie w zakresie jego wpływu na bezpieczeństwo informacji oraz prawdopodobieństwa wystąpienia tego ryzyka.
2. Ustala się trzystopniową skalę oceny wpływu ryzyka na bezpieczeństwo informacji oraz trzystopniową miarę prawdopodobieństwa wystąpienia ryzyka. Miara istotności ryzyka bierze pod uwagę obydwa te czynniki, to jest miarę wpływu ryzyka oraz miarę prawdopodobieństwa wystąpienia ryzyka. Ustala się ją jako iloczyn tych dwóch miar.
3. Podczas oceny wpływu ryzyka i prawdopodobieństwa jego wystąpienia należy wziąć pod uwagę klasyfikację informacji na które wpływ może mieć zidentyfikowane ryzyko. Poniżej zdefiniowano miarę wpływu ryzyka, miarę prawdopodobieństwa jego wystąpienia oraz miarę istotności ryzyka:
4. Miara wpływu ryzyka na bezpieczeństwo informacji:
   a) W1 (niski, 2 punkty) — zdarzenie objęte ryzykiem powoduje niewielką stratę finansową, zakłócenie lub opóźnienie w wykonywaniu zadań; nie wpływa na reputację; skutki zdarzenia można łatwo usunąć;
   b) W2 (średni, 4 punkty) — zdarzenie objęte ryzykiem powoduje znaczną stratę posiadanych zasobów, ma negatywny wpływ na efektywność działania, jakość wykonywanych zadań, reputację; z wystąpieniem zdarzenia może wiązać się trudny proces przywracania stanu poprzedniego;
   c) W3 (duży, 6 punktów) — zdarzenie objęte ryzykiem powoduje uszczerbek mający krytyczny lub bardzo duży wpływ na realizację kluczowych zadań albo osiągania

założonych celów poważny uszczerbek w zakresie jakości wykonywanych zadań, poważna strata finansowa lub na reputacji.

5. Miara wpływu ryzyka związanego z aktywami informacyjnymi wyznaczana jest na podstawie klasyfikacji danych aktywów informacyjnych. Należy przyjąć, że dla aktywów informacyjnych, których klasyfikacje są na poziomie niskim (Cl, I1, A1) miara wpływu ryzyka wynosi W1. Dla ryzyka związanego z aktywami informacyjnymi dla których, dowolna z klasyfikacji jest na poziomie średnim (C2, I2, A2) miara wpływu ryzyka wynosi W2. Dla ryzyka związanego z aktywami informacyjnymi dla których, dowolna z klasyfikacji jest na poziomie wysokim (C3, I3, A3) miara wpływu ryzyka wynosi W3.
6. Miara prawdopodobieństwa wystąpienia ryzyka:
   a) P1 (niskie, 2 punkty) — istnieją uzasadnione powody by sądzić, że zdarzenie objęte ryzykiem zdarzy się raz w ciąg roku lub nie zdarzy się wcale (w ciągu roku);
   b) P2 (średnie, 4 punkty) — istnieją uzasadnione powody by sądzić, że zdarzenie objęte ryzykiem zdarzy się kilkakrotnie w ciągu roku;
   c) P3 (duże, 6 punktów) — istnieją uzasadnione powody by sądzić, że zdarzenie objęte ryzykiem zdarzy się wielokrotnie w ciągu roku.
7. Miara istotności ryzyka:
   a) IR1 (niska) — iloczyn wpływu ryzyka i prawdopodobieństwa ryzyka znajduje się w przedziale od 4 do 8 punktów;
   b) IR2 (średnia) — iloczyn wpływu ryzyka i prawdopodobieństwa ryzyka znajduje się w przedziale od 12 do 16 punktów;
   c) IR3 (duża) — iloczyn wpływu ryzyka i prawdopodobieństwa ryzyka znajduje się w przedziale od 24 do 36 punktów.
8. W zależności od zidentyfikowanego poziomu ryzyka określa się zasady postępowania z ryzykiem:
   a) ryzyko o niskiej istotności należy traktować jako akceptowalne. Zaakceptowanie ryzyka nie wyklucza możliwości jego monitorowania oraz podejmowania działań zaradczych;
   b) ryzyko oznaczone jako średnie wymaga rozważenia potrzeby wdrożenia działań zaradczych. W sytuacji, gdy zostanie podjęta decyzja o tolerowaniu ryzyka oznaczonego jako średnie, dokonać powtórnej oceny istotności ryzyka nie później niż po 6 miesiącach od daty decyzji o tolerowaniu ryzyka. W sytuacji gdy poziom istotności dla takiego ryzyka nie ulegnie zmianie, postępujemy tak, jak w przypadku ryzyka o wysokim poziomie istotności;

c) ryzyko oznaczone jako duże wymaga wprowadzenia działań zaradczych (reakcji na ryzyko), w tym modyfikacji lub uzupełnienia mechanizmów kontroli, które ograniczają możliwości wystąpienia ryzyka;

d) decyzję o akceptacji dużego ryzyka może podjąć Dyrektor Szkoły

9. Ustala się następujące sposoby ograniczania ryzyka:
   a) przeniesienie ryzyka (np. ubezpieczenie);
   b) akceptację ryzyka (trudności w przeciwdziałaniu lub gdy koszty podjętych działań mogą przekroczyć przewidywane korzyści);
   c) przeciwdziałanie (np. wzmocnienie mechanizmów kontrolnych, podjęcie działań zmniejszających prawdopodobieństwo wystąpienia niepożądanych sytuacji);
   d) przesunięcie w czasie (np. się z realizacji zadania, gdy jego realizacja wiąże się z pojawieniem się dużego ryzyka).
10. Proces zarządzania ryzykiem związanym z bezpieczeństwem informacji musi zostać udokumentowany w postaci dokumentu w postaci tradycyjnej (papierowej) lub elektronicznej, który zawiera:
    a) obszar ryzyka;
    b) jednoznaczne określenie ryzyka;
    c) zidentyfikowane podatności;
    d) działania ograniczające ryzyko z określeniem terminów realizacji tych działań i osób odpowiedzialnych.
11. Akceptacja Ryzyka wymaga sporządzenia Dokumentu Akceptacji Ryzyka zawierającego co najmniej :
    a) opis ryzyka;
    b) klasyfikację istotności ryzyka;
    c) opis stanu dotychczasowego;
    d) zastosowane środki ograniczające ryzyko;
    e) końcową ocenę poziomu ryzyka (niskie, średnie lub duże);
    f) datę ważności akceptacji (dopuszcza się ważność bezterminową dla ryzyka ocenionego jako niskie.
12. Dokument Akceptacji Ryzyka, w przypadku ryzyk o istotności niskiej i średniej dokonuje ASI i/lub ADO, a w przypadku ryzyk o istotności dużej akceptacji dokonuje Administrator Danych.

DYREKTOR
Szkoły Podstawowej im. Marii Konopnickiej
w Mokowie
mgr Małgorzata Perzyna