SZKOŁA PODSTAWOWA Nr 2
im. Ks. Jana Twardowskiego
ul. Boh. Monte Cassino 25
15-873 Białystok
tel. 85 742 03 04
Reg. 000735227, NIP 542-20-73-403

Pieczęć Administratora

PROCEDURA KORZYSTANIA ZE SPRZĘTU IT I SYSTEMÓW

U ADMINISTRATORA

1. ZAKRES OBOWIĄZYWANIA PROCEDURY

1.1. Niniejsza procedura dotyczy:

1.1.1. określenia podstawowych zasad, jakimi kieruje się Administrator w zakresie przetwarzania danych osobowych w systemach i przy korzystaniu ze sprzętu IT,

1.1.2. nadawania uprawnień do korzystania ze sprzętu IT i systemów,

1.1.3. metod i zasad uwierzytelniania użytkowników korzystających ze sprzętu IT i systemów,

1.1.4. zasady korzystania ze sprzętu IT, systemów, Internetu i poczty elektronicznej.

1.2. Niniejsza procedura jest stosowana przez:

1.2.1. osoby zatrudnione u Administratora,

1.2.2. osoby współpracujące z Administratorem na podstawie umów cywilnoprawnych,

1.2.3. stażystów, praktykantów i wolontariuszy,

1.2.4. dział kadr lub osoby prowadzące sprawy kadrowe lub administracyjne u Administratora,

1.2.5. Administratora Systemów Informatycznych (jeżeli został wyznaczony) lub osoby zajmującej się sprawami informatycznymi u Administratora.

1.3. W sytuacjach wątpliwych Administrator zasięga opinii Inspektora Ochrony Danych.

1.4. W ramach niniejszej procedury przyjmuje się następujące definicje:

1.4.1. przez sprzęt IT rozumie się w szczególności laptopy, telefony, smartfony, tablety, komputery, monitory, drukarki, skanery, kserokopiarki, aparaty cyfrowe, nośniki pamięci (np. pendrive'y, płyty CD, karty pamięci, dyski zewnętrzne),

1.4.2. przez systemy rozumie się w szczególności systemy informatyczne, aplikacje, programy komputerowe, pocztę elektroniczną, chmury obliczeniowe oraz inne narzędzia udostępniane przez Administratora lub udostępnione Administratorowi przez organy administracji, organy ścigania czy organy władzy sądowniczej,

1.4.3. przez użytkownika rozumie się każdą z osób wskazanych w pkt. 1.2.1., 1.2.2. i 1.2.3. powyżej, wobec której – z uwagi na zakres obowiązków wynikających z jej umowy z Administratorem lub na podstawie wiążących poleceń Administratora – powstaje lub istnieje konieczność wyrażenia zgody na korzystanie ze sprzętu IT lub systemów.

2. PODSTAWOWE ZASADY

2.1. Do przetwarzania danych osobowych należy korzystać wyłącznie ze sprzętu IT i systemów udostępnianych przez Administratora (systemy informatyczne dostarczane przez podmioty, z którymi zawarte są umowy powierzenia) lub dla Administratora przez organy administracji, organy ścigania czy organy władzy sądowniczej.

2.2. Administrator zapewnia sprzęt IT i nadaje dostępy do systemów w taki sposób, aby każdy użytkownik miał możliwość wykonywania swoich obowiązków wynikających z umowy łączącej go z Administratorem lub poleceń Administratora zgodnie z zasadami wynikającymi z niniejszej procedury, przepisami prawa oraz zasadami ochrony danych osobowych wprowadzonymi przez Administratora.

3. NADAWANIE UPRAWNIEŃ DO KORZYSTANIA ZE SPRZĘTU IT

3.1. Przed przystąpieniem użytkownika do korzystania ze sprzętu IT, Administrator udziela mu stosownych zgód oraz upoważnia go do przetwarzania danych osobowych.

3.2. Zgody są udzielane zgodnie z wzorami stanowiącymi załączniki do niniejszej procedury, a następnie ewidencjonowane przez Administratora we właściwych rejestrach stanowiących załączniki do niniejszej procedury.

3.3. W przypadku, gdy zakres obowiązków lub polecenie Administratora tego wymagają, Administrator wyraża indywidualną **zgodę na korzystanie ze sprzętu IT (Załącznik nr 1 do niniejszej Procedury)**. Następnie Administrator ewidencjonuje udzieloną zgodę w **rejestrze zgód na korzystanie ze sprzętu IT (Załącznik nr 2 do niniejszej Procedury)**, a jeśli sprzęt IT został wydany użytkownikowi do wyłącznego korzystania – również w **rejestrze wydanego sprzętu IT (Załącznik nr 3 do niniejszej Procedury)**.

3.4. Zgodnie z zasadami przyjętymi przez Administratora, zabronione jest wynoszenie sprzętu IT poza przydzielone przez Administratora miejsce pracy lub wykonywania obowiązków lub poleceń, w szczególności poza pomieszczenia lub budynki Administratora. Wyjątkiem od powyższego zakazu jest sytuacja, gdy Administrator wyrazi na to konkretnemu użytkownikowi indywidualną **zgodę na wynoszenie sprzętu IT poza miejsce pracy (Załącznik nr 4 do niniejszej Procedury)**. Administrator prowadzi **rejestr zgód na wynoszenie sprzętu IT poza miejsce pracy (Załącznik nr 5 do niniejszej Procedury)**, w którym odnotowuje fakt udzielenia zgody użytkownikowi.

3.5. W przypadku uzyskania zgody na wynoszenie sprzętu IT, użytkownik zobowiązany jest złożyć oświadczenie, że dysponuje środkami organizacyjnymi gwarantującymi przetwarzanie danych osobowych zgodnie z przepisami prawa i zasadami ochrony danych osobowych wprowadzonymi przez Administratora, w szczególności w sposób chroniący prawa osób, których dane dotyczą. Oświadczenie takie składa się na dokumencie zgody, opatrując je datą i podpisem danej osoby.

3.6. Środki organizacyjne, o których mowa powyżej są zapewnione, jeśli co najmniej:

3.6.1. jedyną osobą mającą dostęp do sprzętu IT, którego dotyczy udzielona zgoda, jest użytkownik, który tę zgodę uzyskał,

3.6.2. sprzęt IT nie będzie podłączany do publicznych (w szczególności niezabezpieczonych) sieci WI-FI,

3.6.3. w przypadku konieczności połączenia z siecią internetową, sprzęt IT będzie podłączony do prywatnych, zabezpieczonych hasłem sieci WI-FI, a gdy tylko jest to możliwe, sprzęt IT będzie podłączony przez VPN (wirtualna sieć prywatna szyfrująca dane przesyłane przez sieć internetową),

3.6.4. sprzęt IT nie będzie pozostawiany bez nadzoru, w szczególności w pojazdach prywatnych, środkach komunikacji publicznej, na konferencjach itd.,

3.6.5. na czas wynoszenia sprzętu IT, znajdować się na nim mogą wyłącznie te dane osobowe i dokumenty, które są niezbędne do wykonania tych konkretnych obowiązków lub poleceń Administratora, w wykonaniu których użytkownik wynosi sprzęt IT,

3.6.6. w przypadku każdej przerwy w korzystaniu ze sprzętu IT niewymagającej wyłączenia sprzętu IT, użytkownik stosuje blokady ekranu lub wylogowuje się w taki sposób, aby nie było możliwe skorzystanie ze sprzętu przez inną osobę,

3.6.7. korzysta ze sprzętu IT w sposób uniemożliwiający osobom trzecim podejrzenie zawartości sprzętu IT i danych osobowych,

3.6.8. podejmuje wszelkie inne środki mające na celu zabezpieczenie sprzętu IT i przetwarzanych danych osobowych, które w danej sytuacji powinny zostać podjęte.

3.7. W przypadku, gdy Administrator ma wątpliwości co do zapewnienia przez użytkownika, którego dotyczy lub ma dotyczyć zgoda, środków organizacyjnych, o których mowa powyżej, Administrator może zażądać przedstawienia dowodu zapewnienia wyżej wskazanych środków. W

szczególności, Administrator może zażądać przedstawienia sprzętu IT w celu jego weryfikacji przez wyznaczoną przez Administratora osobę.

4. NADAWANIE UPRAWNIEŃ DO KORZYSTANIA Z PRYWATNEGO SPRZĘTU IT

4.1. Korzystanie z prywatnego sprzętu IT jest zabronione, z wyłączeniem sytuacji, gdy Administrator wyrazi w tym celu indywidualną zgodę konkretnemu użytkownikowi.

4.2. W przypadku, gdy zakres obowiązków lub polecenie Administratora tego wymagają, Administrator może wyrazić indywidualną **zgodę na korzystanie z prywatnego sprzętu IT (Załącznik nr 6 do niniejszej Procedury)**. Administrator ewidencjonuje udzielone zgody w **rejestrze zgód na korzystanie z prywatnego sprzętu IT (Załącznik nr 7 do niniejszej Procedury)**.

4.3. W przypadku uzyskania zgody na korzystanie z prywatnego sprzętu IT, użytkownik zobowiązany jest złożyć oświadczenie, że dysponuje środkami technicznymi i organizacyjnymi gwarantującymi przetwarzanie danych osobowych zgodnie z przepisami prawa i zasadami ochrony danych osobowych wprowadzonymi przez Administratora, w szczególności w sposób chroniący prawa osób, których dane dotyczą. Oświadczenie takie składa się na dokumencie zgody, opatrując je datą i podpisem danej osoby.

4.4. Środki techniczne, o których mowa powyżej są zapewnione, jeśli co najmniej:

4.4.1. prywatny sprzęt IT jest zabezpieczony hasłem, PIN-em, kodem lub inną formą kontroli dostępu, w szczególności biometryczną,

4.4.2. prywatny sprzęt IT zabezpieczony jest za pomocą oprogramowania antywirusowego i firewall (zapory sieciowej),

4.4.3. prywatny sprzęt IT jest na bieżąco aktualizowany, co najmniej w zakresie systemu operacyjnego, ochrony antywirusowej i firewall (zapory sieciowej),

4.4.4. prywatny nośnik pamięci będący nośnikiem pamięci nieposiadających innych funkcji jest szyfrowany lub pliki na nim zapisane są szyfrowane/zabezpieczane hasłem.

4.5. Środki organizacyjne, o których mowa powyżej są zapewnione, jeśli co najmniej:

4.5.1. jedyną osobą korzystającą z prywatnego sprzętu IT, którego dotyczy udzielona zgoda, jest użytkownik, który tę zgodę uzyskał,

4.5.2. prywatny sprzęt IT nie jest podłączony do publicznych (w szczególności niezabezpieczonych) sieci WI-FI, co najmniej w czasie, w którym znajdują się na nim dane osobowe pochodzące od Administratora,

4.5.3. w przypadku konieczności połączenia z siecią internetową w czasie, w którym znajdują się na nim dane osobowe pochodzące od Administratora, prywatny sprzęt IT jest podłączony do prywatnych, zabezpieczonych hasłem sieci WI-FI, a gdy tylko jest to możliwe, stosuje się połączenia przez VPN (wirtualna sieć prywatna szyfrująca dane przesyłane przez sieć internetową),

4.5.4. prywatny sprzęt IT nie jest pozostawiany bez nadzoru, co najmniej w czasie, w którym znajdują się na nim dane osobowe pochodzące od Administratora,

4.5.5. dane osobowe są zapisywane na prywatnym sprzęcie IT wyłącznie na czas, w którym jest to niezbędne, a następnie są one przenoszone, przesyłane lub w inny sposób przekazywane na sprzęt IT Administratora i usuwane – z zachowaniem zasad określonych w niniejszej Procedurze oraz zgodnie z obowiązującymi przepisami prawa i zasadami ochrony danych osobowych wprowadzonymi przez Administratora,

4.5.6. dane osobowe nie są wprowadzane do żadnych prywatnych systemów, w szczególności systemów poczty elektronicznej, chmury obliczeniowej, itd.

4.6. W przypadku, gdy Administrator ma wątpliwości co do zapewnienia przez użytkownika, którego dotyczy lub ma dotyczyć zgoda, w prywatnym sprzęcie IT środków technicznych lub organizacyjnych, o których mowa powyżej, Administrator może zażądać przedstawienia dowodu zapewnienia wyżej wskazanych środków. W szczególności, Administrator może zażądać

przedstawienia prywatnego sprzętu IT w celu jego weryfikacji przez wyznaczoną przez Administratora osobę.

4.7. Niezwłocznie, nie później niż w terminie 2 dni od wygaśnięcia lub odwołania zgody, użytkownik usuwa z prywatnego sprzętu IT wszelkie dane osobowe, ich kopie i kopie zapasowe, jakie nie zostały jeszcze przez niego usunięte z prywatnego sprzętu IT, a także informuje Administratora o wykonaniu tego obowiązku. Administrator może zażądać przedstawienia dowodu usunięcia wszelkich danych osobowych z prywatnego sprzętu IT. W szczególności, Administrator może zażądać przedstawienia prywatnego sprzętu IT w celu jego weryfikacji przez wyznaczoną przez Administratora osobę.

5. NADAWANIE UPRAWNIEŃ DO KORZYSTANIA Z SYSTEMÓW

5.1. W przypadku, gdy zakres obowiązków lub polecenie Administratora tego wymagają, Administrator może wyrazić indywidualną zgodę na korzystanie z systemów do przetwarzania danych osobowych.

5.2. Przed przystąpieniem użytkownika do korzystania z systemów, Administrator udziela mu **zgody na korzystanie z systemów (Załącznik nr 8 do niniejszej Procedury)** oraz upoważnia go do przetwarzania danych osobowych. Zgody są ewidencjonowane przez Administratora w **rejestrze zgód na korzystanie z systemów (Załącznik nr 9 do niniejszej Procedury)**.

5.3. Administrator zakłada indywidualne konto poczty elektronicznej dla każdego użytkownika, którego zakres obowiązków wynikający z umowy z Administratorem lub poleceń otrzymanych od Administratora wymaga korzystania z poczty elektronicznej.

5.4. Użytkownicy nie są uprawnieni do wykorzystywania do przetwarzania danych Administratora prywatnych systemów, w szczególności prywatnej poczty elektronicznej.

6. METODY I ŚRODKI UWIERZYTELNIANIA

6.1. Administrator zapewnia nadanie każdemu użytkownikowi przetwarzającemu dane osobowe przy wykorzystaniu systemów, indywidualne identyfikatory i hasła do tych systemów. Administrator odnotowuje nadany użytkownikowi identyfikator w treści zgody na korzystanie z systemów (Załącznik nr 8 do niniejszej Procedury).

6.2. Hasła wykorzystywane w celu zabezpieczenia dostępu do systemów powinny spełniać następujące kryteria:

6.2.1. hasło nie może składać się z danych personalnych, takich jak imię, nazwisko, adres zamieszkania lub ich fragmentów,

6.2.2. hasło nie może składać się z danych dotyczących jednostki, wydziału, nazwy systemu lub ich fragmentów,

6.2.3. hasło składa się z co najmniej 8 znaków, zawiera wielkie i małe litery oraz cyfry i znaki specjalne,

6.2.4. hasło nie może składać się z identycznych ciągów znaków lub ciągu znaków z klawiatury,

6.2.5. hasło nie może być jednakowe z identyfikatorem użytkownika, nie może również zawierać w sobie identyfikatora użytkownika,

6.2.6. hasło musi być unikalne, tj. takie, które nie było nigdzie i nigdy wcześniej stosowane przez użytkownika,

6.2.7. hasło musi się różnić od innych haseł oraz poprzednich haseł stosowanych przez użytkownika co najmniej czterema znakami.

6.3. W przypadku braku systemowego wymuszania zmiany haseł, Administrator zapewnia okresową zmianę haseł użytkowników, której dokonuje upoważniony do tego celu pracownik. Okres częstotliwości, z jaką zmieniane są hasła określa Administrator, jednak zastrzeżeniem, że nie może być on krótszy niż raz na kwartał.

6.4. Niedopuszczalną praktyką jest ujawnianie haseł osobom trzecim, a także zapisywanie haseł na kartkach, w notesach, przechowywanie w szufladach, na biurku, ukrywanie ich w otoczeniu sprzętu IT, którego hasła dotyczą. Użytkownicy obowiązani są do zachowania haseł w tajemnicy również po ich wygaśnięciu. O każdym przypadku złamania poufności hasła, także hasła, które już zostało zmienione, użytkownik zobowiązany jest poinformować Administratora zgodnie z zasadami wynikającymi z Procedury zgłaszania i oceny naruszeń.

6.5. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego służącego do przetwarzania danych osobowych nie może on zostać przydzielony innej osobie.

6.6. Identyfikator użytkownika, który stracił uprawnienia do przetwarzania danych lub dostęp do systemu informatycznego, należy niezwłocznie w danym systemie zablokować, a przypisane do niego hasło unieważnić. Dostęp do konta takiego użytkownika musi pozostać zapewniony dla Administratora, Administratora Systemów Informatycznych i innych osób upoważnionych przez Administratora.

7. ZASADY PRACY PRZY UŻYCIU SYSTEMÓW

7.1. Przed włączeniem sprzętu IT i systemów użytkownik powinien sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń. W przypadku wykrycia naruszenia, użytkownik zobowiązany jest niezwłocznie poinformować o tym fakcie Administratora zgodnie z zasadami wynikającymi z Procedury zgłaszania i oceny naruszeń.

7.2. Przystępując do pracy w systemie informatycznym, użytkownik zobowiązany jest wprowadzić nadany mu identyfikator oraz przypisane do niego hasło. Niedopuszczalne jest korzystanie z identyfikatorów i haseł nadanych innym użytkownikom.

7.3. W przypadku czasowego opuszczenia stanowiska pracy, użytkownik zobowiązany jest do zablokowania dostępu do komputera poprzez wprowadzenie kombinacji klawiszy (np. „windows" + L) lub skorzystania z opcji w Menu Start.

7.4. Zakończenie pracy w systemie informatycznym powinno zostać poprzedzone zabezpieczeniem sprzętu IT, na którym znajdują się dane osobowe, przed nieuprawnionym dostępem. Zakończenie pracy w systemie informatycznym następuje poprzez wylogowanie się z tego systemu i prawidłowe wyłączenie sprzętu IT.

8. KORZYSTANIE ZE SPRZĘTU IT I SYSTEMÓW

8.1. Użytkownik zobowiązany jest do korzystania ze sprzętu IT i systemów wyłącznie w celach służbowych.

8.2. Użytkownik zobowiązany jest do korzystania ze sprzętu IT i systemów zgodnie z prawem, zasadami przyjętymi u Administratora, udzielonymi zgodami i nadanymi upoważnieniami, a także zgodnie z instrukcjami korzystania ze sprzętu IT i systemów wydanymi przez ich producentów.

8.3. W przypadku zaistnienia problemów ze sprzętem IT lub systemem powodujących brak możliwości lub utrudnienia w korzystaniu z nich, użytkownik nie jest uprawniony do ich samodzielnego rozwiązywania. Użytkownik jest zobowiązany do poinformowania o zaistniałych problemach Administratora lub osobę przez niego wyznaczoną.

8.4. Użytkownik jest zobowiązany do zapisywania danych na sprzęcie IT i systemach wyłącznie w sposób zgodny z aktualnymi wytycznymi Administratora w tym zakresie. W szczególności, Administrator może wskazać użytkownikom miejsce zapisu plików i danych osobowych, zasady nazewnictwa folderów i plików, a także gdzie i w jaki sposób należy tworzyć kopie zapasowe.

8.5. Sprzęt IT zawierający dane osobowe lub kopie systemów są użytkowane i przechowywane przez użytkowników w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.

9. KORZYSTANIE Z INTERNETU

9.1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.

9.2. Zabrania się zgrywania na sprzęt IT oraz uruchamia na nim jakichkolwiek programów nielegalnych, plików pobranych z niewiadomego źródła lub niezatwierdzonych uprzednio przez Administratora.

9.3. Wszelkie pliki, aplikacje lub programy mogą być pobierane na sprzęt IT tylko za każdorazową zgodą Administratora Systemów Informatycznych (a w przypadku jego niewyznaczenia osoby upoważnionej do administrowania infrastrukturą IT) i tylko w uzasadnionych przypadkach.

9.4. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.

9.5. Nie należy korzystać ze stron i serwisów internetowych, na których prezentowane są informacje i treści o charakterze przestępczym, hackerskim, pornograficznym lub innym zabronionym przez prawo.

9.6. Przy korzystaniu z Internetu należy zachować szczególną ostrożność z uwagi na ryzyko zainfekowania sprzętu IT szkodliwym oprogramowaniem. W szczególności należy stosować następujące zasady:

9.6.1. nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł,

9.6.2. jeżeli jest to możliwe należy korzystać z szyfrowanego połączenia przez przeglądarkę, co należy każdorazowo po wejściu na stronę internetową zweryfikować poprzez sprawdzenie, czy w pasku adresu pojawia się odpowiednia ikonka (kłódka), a adres www rozpoczyna się frazą "https:",

9.6.3. dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel,

9.6.4. w przypadku, gdy adres www nie rozpoczyna się frazą "https:" należy ręcznie wprowadzić tę frazę na początku adresu,

9.6.5. ze stron niezabezpieczonych należy korzystać tylko wyjątkowo, jednakże nie należy przez takie strony internetowe podawać jakichkolwiek danych osobowych,

9.6.6. należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank,

9.6.7. należy skanować programem antywirusowym każdy dokument, zbiór danych, wiadomość e-mail przed ich otwarciem,

9.6.8. należy stosować filtry antyspamowe na kontach poczty elektronicznej,

9.6.9. niedopuszczalne jest korzystanie z sieci Internet bez aktywnej ochrony antywirusowej oraz zabezpieczenia przed dostępem szkodliwego oprogramowania.

10. KORZYSTANIE Z POCZTY ELEKTRONICZNEJ

10.1. Użytkownik jest uprawniony do korzystania wyłącznie z indywidualnie przydzielonego mu przez Administratora adresu poczty elektronicznej.

10.2. Użytkownik nie jest uprawniony do korzystania z prywatnej poczty elektronicznej do wykonywania obowiązków i poleceń Administratora.

10.3. Przesyłanie danych osobowych z użyciem poczty elektronicznej poza organizację może odbywać się tylko przez osoby posiadające zgodę na korzystanie z systemu – poczty elektronicznej.

10.4. W przypadku przesyłania danych osobowych poza organizację zaleca się wykorzystywanie mechanizmów kryptograficznych [szyfrowanie transmisji, hasłowanie wysyłanych dokumentów lub plików zzipowanych, korzystanie z podpisu kwalifikowanego (elektronicznego) lub za pomocą profilu zaufanego ePUAP].

10.5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych pocztą elektroniczną zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.

10.6. Przy korzystaniu z poczty elektronicznej należy zwracać szczególną uwagę na bezpieczeństwo, a w szczególności należy stosować się do poniższych zasad:

10.6.1. nie należy otwierać załączników (plików) w mailach nawet od rzekomo znanych nadawców bez weryfikacji tego nadawcy – wiadomości mailowe mogą zawierać załączniki ze szkodliwymi programami, które po „kliknięciu" infekują komputer użytkownika oraz często pozostałe komputery w sieci, co może doprowadzić do poważnych naruszeń bezpieczeństwa, łącznie z pełną utratą danych osobowych lub zaszyfrowanie wszystkich danych na sprzęcie IT podłączonym do sieci przez kryptowirusy,

10.6.2. bez weryfikacji wiarygodności nadawcy nie należy „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych - „klikając" na taki hiperlink użytkownik bezwiednie infekuje swój komputer oraz często pozostałe komputery w sieci, co może doprowadzić do poważnych naruszeń bezpieczeństwa, łącznie z pełną utratą danych osobowych lub zaszyfrowanie wszystkich danych na sprzęcie IT podłączonym do sieci przez kryptowirusy,

10.6.3. należy zgłaszać przypadki podejrzanych e-maili Administratorowi zgodnie z zasadami wynikającymi z Procedury zgłaszania i oceny naruszeń,

10.6.4. podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW", zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości - DW",

10.6.5. należy zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu,

10.6.6. przy korzystaniu z poczty elektronicznej, użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego,

10.6.7. użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.

11. KRAJOWE RAMY INTEROPERACYJNOŚCI

11.1. Niezależnie od zasad wprowadzonych niniejszą Procedurą, Administrator zapewnia zgodność przetwarzania i ochrony danych z Rozporządzeniem Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

11.2. W celu realizacji obowiązków wynikających z rozporządzenia, o którym mowa w pkt. 11.1, Administrator może zasięgnąć opinii Inspektora Ochrony Danych.

11.3. W zakresie, w jakim niniejsza Procedura wprowadza zasady ochrony danych osobowych w stopniu mniej rygorystycznym niż wynikające z rozporządzenia, o którym mowa w pkt. 11.1, Administrator stosuje zasady wynikające z ww. rozporządzenia.

Zatwierdzam i nakazuję stosować.

Dyrektor
Szkoły Podstawowej Nr 2
im. Ks. Jana Twardowskiego
w Białymstoku
mgr Halina Puchalska

data i podpis Administratora