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 ZAPEWNIENIA PRAWIDŁOWEGO PRZETWARZANIA DANYCH PRZY KORZYSTANIU ZE SPRZĘTU IT I SYSTEMÓW U ADMINISTRATORA

1. ZAKRES OBOWIĄZYWANIA PROCEDURY

1.1. Niniejsza procedura dotyczy:

1.1.1. określenia sposobów zapewnienia prawidłowego przetwarzania danych osobowych w systemach i przy korzystaniu ze sprzętu IT.

1.2. Czynności określone w niniejszej procedurze są wykonywane przez Administratora.

1.3. Administrator korzysta z pomocy odpowiednich działów i Administratora Systemów Informatycznych, a w razie jego niewyznaczenia – z pomocy osoby pełniącej funkcję informatyka u Administratora. 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 (w tym systemy operacyjne, programy antywirusowe, programy biurowe, inne oprogramowanie), aplikacje, programy komputerowe, pocztę elektroniczną, chmury obliczeniowe oraz inne narzędzia udostępniane przez Administratora lub dla Administratora przez organy administracji, organy ścigania czy organy władzy sądowniczej,

1.4.3. przez użytkownika rozumie się każdą z następujących osób:

1.4.3.1. osoby zatrudnione u Administratora,

1.4.3.2. osoby współpracujące z Administratorem na podstawie umów cywilnoprawnych,

1.4.3.3. stażystów, praktykantów i wolontariuszy,

która – z uwagi na zakres obowiązków wynikających z jej umowy z Administratorem lub na podstawie wiążących poleceń Administratora – na podstawie zgody udzielonej przez Administratora korzysta ze sprzętu IT lub systemów.

2. PODSTAWOWE ZASADY

2.1. Do przetwarzania danych należy wykorzystywać wyłącznie sprzęt IT i systemy udostępniane przez Administratora (systemy informatyczne dostarczane przez podmioty, z którymi zawarte są umowy powierzenia) lub udostępnione Administratorowi 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.

2.3. Administrator dąży do tego, aby stosowany przez niego sprzęt IT i systemy były na bieżąco aktualizowane, posiadały wsparcie (support) i były objęte gwarancją producenta i zapewniały

możliwość przetwarzania danych osobowych zgodnie z RODO, a w szczególności umożliwiały Administratorowi zapewnienie rozliczalności.

3. ZABEZPIECZENIA SYSTEMÓW

3.1. Administrator zabezpiecza systemy i sprzęt IT służące do przetwarzania danych osobowych.

3.2. Zabezpieczenia systemów i sprzętu IT powinny w szczególności zapewniać ochronę przed:

3.2.1. działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemów, co najmniej poprzez:

3.2.1.1. zainstalowanie na każdym sprzęcie IT, na którym jest to możliwe, programu antywirusowego,

3.2.1.2. zainstalowanie na każdym sprzęcie IT, na którym jest to możliwe, firewall (zapory sieciowej),

3.2.1.3. zapewnienie automatycznego i cyklicznego skanowania za pomocą programu antywirusowego każdego sprzętu IT, na którym takie oprogramowanie jest zainstalowane,

3.2.1.4. zapewnienie skanowania za pomocą programu antywirusowego każdego sprzętu IT, na którym takie oprogramowanie nie jest zainstalowane – za każdym razem, gdy sprzęt IT jest podłączany lub używany na sprzęcie IT, na którym jest zainstalowane oprogramowanie antywirusowe,

3.2.1.5. zapewnienie automatycznego skanowania za pomocą programu antywirusowego zawartości poczty elektronicznej użytkowników,

3.2.1.6. wprowadzenie filtrów antyspamowych na kontach poczty elektronicznej użytkowników.

3.2.2. utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej, w szczególności poprzez zastosowanie:

3.2.2.1. urządzenia chroniącego system informatyczny przed skutkami awarii zasilania typu UPS,

3.2.2.2. generatora prądu,

3.2.2.3. wydzielonej sieci elektroenergetycznej.

3.3. Niedopuszczalne jest umożliwienie użytkownikom dostępu do sieci Internet bez aktywnej ochrony antywirusowej oraz zabezpieczenia przed dostępem szkodliwego oprogramowania.

3.4. Należy instalować zalecane przez producentów oprogramowania poprawki i uaktualnienia systemów celem wyeliminowania błędów w działaniu lub poprawienia wydajności działania.

4. PRZEGLĄDY I KONSERWACJA SYSTEMÓW

4.1. W celu zapewnienia kontroli nad wykorzystywanym sprzętem IT i systemami, Administrator prowadzi następujące rejestry:

4.1.1. Rejestr sprzętu IT (Załącznik nr 1 do niniejszej Procedury),

4.1.2. Rejestr systemów (Załącznik nr 2 do niniejszej Procedury).

4.2. Przeglądy i konserwacje sprzętu IT oraz systemów przeprowadzane są przez Administratora Systemów Informatycznych w przypadku jego wyznaczenia lub innej osoby wyznaczonej przez Administratora.

4.3. W przypadku przekazywania do naprawy sprzętu IT z zainstalowanym systemem, sprzęt IT powinien zostać pozbawiony danych osobowych przez fizyczne wymontowanie dysku lub skasowanie danych. W innym przypadku musi być zawarta umowa powierzenia danych osobowych z podmiotem, który dokonuje naprawy sprzętu IT.

4.4. Przeglądy techniczne i konserwacje sprzętu IT oraz przeglądy systemów wykonywane muszą być nie rzadziej niż raz w roku.

5. POCZTA ELEKTRONICZNA

5.1. Administrator zapewnia, że wszystkie konta poczty elektronicznej, z jakich korzystają użytkownicy spełniają następujące wymogi:

5.1.1. konta poczty elektronicznej są założone w domenie, do której nazwy prawa przysługują Administratorowi, a gdy nie jest to możliwe – w innej domenie, z zapewnieniem spełnienia co najmniej wymogów określonych w pkt. 5.1.2. – 5.1.6,

5.1.2. dane są przechowywane na serwerze, którego właścicielem jest Administrator lub są przechowywane na serwerze podmiotu, z którym Administrator zawarł umowę powierzenia przetwarzania danych,

5.1.3. dane nie są przesyłane do państw trzecich,

5.1.4. konta poczty elektronicznej wymuszają okresową zmianę haseł lub Administrator zobowiązuje użytkowników do okresowej zmiany haseł,

5.1.5. konta poczty elektronicznej zawierają filtry antyspamowe lub umożliwiają ich aktywowanie przez Administratora,

5.1.6. podmiot dostarczający usługę poczty elektronicznej nie przetwarza danych w celach marketingowych, ani nie profiluje osób, dla których zostało założone konto pocztowe.

6. ARCHIWIZACJA

6.1. Osobą odpowiedzialną u Administratora za wykonywanie obowiązków związanych z archiwizacją danych przetwarzanych na sprzęcie IT i w systemach jest Administrator Systemów Informatycznych, a w przypadku jego niewyznaczenia – osoba pełniąca funkcję informatyka u Administratora. Jeśli takich osób nie ma, za archiwizację odpowiada Administrator.

6.2. Osoba określona zgodnie z pkt. 6.1 prowadzi weryfikację dokumentów i wpisów na sprzęcie IT i w systemach względem terminów dopuszczalności ich przetwarzania w oparciu o:

6.2.1. dane wskazane w rejestrze czynności przetwarzania,

6.2.2. treść obowiązków informacyjnych oraz innych dokumentów określających czas przetwarzania danych przez Administratora,

6.2.3. przepisy prawa,

6.2.4. instrukcje kancelaryjne,

6.2.5. zasadność dalszego ich przetwarzania.

Przed podjęciem decyzji Administrator może się skonsultować z Inspektorem Ochrony Danych.

6.3. Weryfikacja przeprowadzana jest cyklicznie, nie rzadziej niż 1 raz na rok. Z przeprowadzonej weryfikacji osoba określona zgodnie z pkt. 6.1 sporządza notatkę służbową. W przypadku stwierdzenia konieczności usunięcia danych lub braku potrzeby ich dalszego przetwarzania, należy dokonać archiwizacji tych danych.

6.4. Archiwizację przeprowadza się w następujący sposób:

6.4.1. osoba określona zgodnie z pkt. 6.1 tworzy kopię zapasową danych osobowych przetwarzanych w formie elektronicznej, a następnie usuwa dane osobowe z systemów; jeśli nie posiada odpowiednich uprawnień do systemów, korzysta z pomocy wyznaczonej przez Administratora osoby posiadającej takie uprawnienia,

6.4.2. osoba określona zgodnie z pkt. 6.1 przekazuje do wszystkich osób w jednostce uprawnionych do przetwarzania danych polecenie usunięcia wskazanych danych osobowych z wszelkich materiałów w formie pisemnej lub elektronicznej, w tym z notatek, dokumentów, sprzętu IT.

7. TWORZENIE KOPII ZAPASOWYCH

7.1. Osobą odpowiedzialną u Administratora za wykonywanie obowiązków związanych z wykonywaniem kopii zapasowych jest Administrator Systemów Informatycznych, a w przypadku jego niewyznaczenia – osoba pełniąca funkcję informatyka u Administratora. Jeśli takich osób nie ma, za wykonywanie kopii zapasowych odpowiada Administrator.

7.2. Kopie zapasowe wykonywane są z częstotliwością zależną od rodzaju danych i co do zasady nie rzadziej niż zgodnie z poniższymi zasadami:

7.2.1. kopia zapasowa danych zapisywanych na sprzęcie IT niepodłączonym do sieci i/lub zapisywanych poza dyskami wspólnymi lub serwerem tworzona jest nie rzadziej niż 1 raz na 2 tygodnie,

7.2.2. kopia zapasowa danych zapisywanych na dyskach wspólnych lub serwerze tworzona jest nie rzadziej niż 1 raz dziennie, a kopia zapasowa serwera – nie rzadziej niż 1 raz na 2 tygodnie,

7.2.3. kopia zapasowa danych z monitoringu tworzona jest nie rzadziej niż 1 raz dziennie, chyba że dane są nadpisywane i kopie zapasowe nie są tworzone,

7.2.4. kopie zapasowe wykonywane są także przed dokonaniem istotnej zmiany w konfiguracji lub zasadach zapisu danych w systemach i na sprzęcie IT.

7.3. Kopie zapasowe podlegają testom pod kątem ich prawidłowości oraz przydatności zgodnie z poniższymi zasadami:

7.3.1. testy należy przeprowadzać nie rzadziej niż 1 raz na kwartał,

7.3.2. wykonanie testów należy potwierdzić notatką służbową,

7.3.3. test polega na próbnym odtworzeniu zawartości kopii zapasowej na urządzeniu testowym,

7.3.4. w przypadku stwierdzenia jakiejkolwiek nieprawidłowości, osoba wykonująca test kopii zapasowej niezwłocznie kontaktuje się z Administratorem Systemów Informatycznych oraz Inspektorem Ochrony Danych.

7.4. Odzyskiwanie danych i systemów z kopii zapasowych wykonuje się wtedy, gdy jest to niezbędne, szczególności z uwagi na utratę części lub całości danych, utratę integralności danych, awarię lub atak uniemożliwiającą korzystanie z danych. Przed odzyskaniem danych z kopii zapasowych należy wykonać test kopii zapasowych pod kątem ich prawidłowości oraz zakresu danych, jakie mogą być z nich odtworzone. Po przywróceniu danych z kopii zapasowej należy wykonać kolejny test. W zakresie, w jakim przywrócenie danych nie było możliwe, należy odtworzyć dokumenty i wprowadzić brakujące dane. Każdy z użytkowników odpowiada za ponowne przygotowanie dokumentów i wprowadzenie danych, których nie udało się odtworzyć z kopii zapasowej.

7.5. Sprzęt IT, w tym kopie zapasowe zawierające dane osobowe lub kopie systemów, są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.

7.6. Kopie zapasowe:

7.6.1. przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pomieszczeniu zamkniętym;

7.6.2. usuwa się niezwłocznie po ustaniu ich użyteczności.

7.7. W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemów informatycznych służących do przetwarzania danych osobowych należy przed ich likwidacją usunąć dane osobowe lub uszkodzić je w sposób uniemożliwiający odczyt danych osobowych.

Zatwierdzam i nakazuję stosować.

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

data i podpis Administratora