Załącznik nr 3

Instrukcja
obsługi systemu informatycznego
przetwarzania danych osobowych

I. Pojęcia wstępne

1. Instrukcja określa sposób postępowania w zakresie przetwarzania i ochrony danych osobowych.
2. Przez użyte w Instrukcji pojęcia rozumie się:
   a) *dane osobowe* – każda informacja dotycząca osoby fizyczne pozwalająca określić jej tożsamość,
   b) *system informatyczny* – system sprzętowo - osobowy przetwarzający dane osobowe,
   c) *administrator danych* osobowych – dyrektor szkoły,
   d) *administrator bezpieczeństwa informacji* – osoba odpowiedzialna za bezpieczeństwo danych osobowych w systemie informatycznym,
   e) *administrator systemu* – osoba odpowiedzialna za sprawne funkcjonowanie systemu,
   f) *użytkownik* – osoba upoważniona do dostępu do danych osobowych,
   g) *naruszenie ochrony danych osobowych* – sytuacja lub stan w którym dokonano naruszenia bezpieczeństwa danych,
   h) *naruszenie zabezpieczenia systemu informatycznego* – jakiekolwiek naruszenie bezpieczeństwa dokonane przez osoby niepowołane lub nieumyślnie.
3. Obszarami do przetwarzania danych w Gimnazjum Nr 1 są gabinety i pokoje:
   a) dyrektora,
   b) wicedyrektora,
   c) głównego księgowego,
   d) sekretarza szkoły (sekretariat),
   e) przewodniczącego Komisji Socjalnej,
   f) pracowni nr 2, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 16, 17, 18 i 23 w części biurka i komputera nauczyciela,
   g) pokoju nauczycielskiego,
   h) bibloteki szkolnej w części biurka i komputara nauczyczyciela – bibliotekarza,
   i) kasy w części biurka i komputara kasjera,
   j) pedagoga szkolnego części biurka i komputera,
   k) lekarza szkolnego,
   l) archiwum,
   m) psychologa,
   n) intendenta.
4. Przebywanie wewnątrz obszaru, o którym mowa w ust.3, osób nieuprawnionych do dostępu do danych osobowych jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych i za zgodą administratora danych lub osoby przez niego upoważnionej.
5. Budynki lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp osób trzecich.
6. Zbiory danych osobowych w Gimnazjum Nr 1 stanowi załącznik nr 1 niniejszej instrukcji.

II. Procedura rejestrowania użytkowników i przydziału hasła

1. Utworzenie konta użytkownika umożliwiającego dostęp do aplikacji lub systemu następuje na ustny wniosek administratora danych.
2. Administrator systemu zakłada konto zabezpieczone hasłem.
3. Użytkownik nie może zmienić samodzielnie hasła.
4. Nazwa konta i hasło jest przekazywane użytkownikowi.
5. Konto użytkownika jest usunięte na wniosek administratora danych.
6. Zmiana hasła użytkownika następuje, co 30 dni.
7. W sytuacji podejrzeń o ujawnienie hasło jest zmieniane natychmiast.
8. Administrator systemu składa informacje o treści hasła do swojego konta dyrektorowi szkoły.

III. Procedura rozpoczynania i zakończenia pracy

1. Przed rozpoczęciem pracy użytkownik jest zobowiązany sprawdzić stan systemu informatycznego.
2. Rozpoczęcie pracy następuje przez podanie nazwy konta i hasła w sposób uniemożliwiający ich ujawnienie innym osobom.
3. Ustawienie monitora powinno uniemożliwiać podgląd osobom nieupoważnionym.
4. W przypadku opuszczenia pracy użytkownik jest zobowiązany zaktywizować wygaszacz ekranu.
5. Po zakończeniu pracy użytkownik powinien prawidłowo wylogować się z systemu, wyłączyć komputer i zabezpieczyć przed dostępem osób nieupoważnionych.

IV. Kopie bezpieczeństwa

1. Kopie bezpieczeństwa wykonuje się w każdy piątek i na koniec miesiąca.
2. Kopie bezpieczeństwa są opisane.
3. Kopie bezpieczeństwa nie mogą być przechowywane w tych samych pomieszczeniach, co odpowiednie aplikacje.
4. Kopie bezpieczeństwa przechowuje się w sejfie.
5. Kopie bezpieczeństwa należy okresowo sprawdzić na ich zdolność odtwarzania danych.
6. Nieużyteczne kopie bezpieczeństwa niszczy się w taki sposób, aby uniemożliwić ich odczytanie.

V. Ochrona antywirusowa

1. Ochrona antywirusowa jest realizowana przez oprogramowanie antywirusowe na każdej stacji roboczej i serwerze.
2. Oprogramowanie antywirusowe jest systematycznie aktualizowane.
3. Sprawdzenie nośników na obecność wirusów powinno odbywać się przynajmniej raz na miesiąc.
4. Za ochronę antywirusową odpowiada administrator bezpieczeństwa informacji.

VI. Sposób przechowywania nośników informacji i wydruków

1. Wydruki komputerowe z aplikacji przetwarzania danych osobowych wykonuje się jedynie w celach operacyjnych.
2. Wydruki ze zbiorów danych osobowych przechowywane są w odpowiednich szafach.
3. Nośniki z danymi osobowymi przechowywane są w odpowiednich szafach lub sejfach.
4. Likwidacja wydruków przeprowadza się za pomocą odpowiednich urządzeń.
5. Nośniki elektroniczne niszczy się zgodnie z odpowiednimi przepisami.

VII. Konserwacja systemu przetwarzania danych osobowych

1. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.
2. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, pozbawia się wcześniej zapisu tych danych.
3. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.
4. Naprawa lub konserwacja urządzeń przetwarzających dane osobowe może odbywać się jedynie za zgodą lub w obecności administratora bezpieczeństwa informacji.

VIII. Udostępnianie informacji posiadanych w zbiorze danych osobowych

1. Do udostępniania posiadanych w zbiorze danych osobowych upoważniony jest administrator danych osobowych lub pracownik posiadający wymagane prawem upoważnienie.

IX. Przepisy końcowe

1. Każda osoba upoważniona do przetwarzania danych osobowych obowiązana jest zapoznać się przed dopuszczeniem do pracy z niniejszą Instrukcją.
2. Za naruszenie obowiązków użytkownik może być pociągnięty do odpowiedzialności zgodnie z Regulaminem pracy i innymi przepisami.
3. W sprawach nie uregulowanych w Instrukcji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych o przepisy aktów wykonawczych wydanych na jej podstawie.