Załącznik nr 2 do
Zarządzenia nr 14/2011/2012 Dyrektora
Zespołu Szkół nr 1
w Wejherowie
z dnia 30.12.2011

Instrukcja zarządzania systemem informatycznym w Szkole Podstawowej nr 6 w Wejherowie

I. Postanowienia ogólne

§ 1

Ilekroć w niniejszej Instrukcji mowa o:

1) Instrukcji – należy przez to rozumieć Instrukcję bezpieczeństwa i zarządzania systemem informatycznym, obowiązującą w Szkole Podstawowej nr 6 w Wejherowie
2) dyrektorze – należy przez to rozumieć osobę powołaną do kierowania Szkołą, o której mowa w pkt 1;
3) głównym księgowym – należy przez to rozumieć osobę, która pełni funkcję głównego księgowego w Szkole;
4) administratorze danych – należy przez to rozumieć dyrektora Szkoły,
5) administratorze bezpieczeństwa informacji – należy przez to rozumieć osobę wyznaczoną przez dyrektora,
6) administratorze sieci informatycznej – należy przez to rozumieć pracownika zatrudnionego na stanowisku administratora sieci internetowej,
7) użytkowniku systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym, która jest pracownikiem Szkoły,
8) sieci lokalnej – należy przez to rozumieć połączenie systemów informatycznych Szkoły wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych,
9) sieci rozległej – należy przez to rozumieć sieć publiczną w rozumieniu ustawy z dnia 21 lipca 2000 r. – Prawo komunikacyjne.

§ 2

Do przetwarzania danych osobowych używane są komputery klasy PC, połączone w sieć lokalną, z dostępem do sieci rozległej.

§ 3

1. W Szkole są tworzone i przetwarzane zbiory danych osobowych pracowników zatrudnionych w Szkole i uczniów Szkoły.
2. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych jest obowiązany zapoznać się z:
   1) niniejszą Instrukcją,
   2) Polityką bezpieczeństwa,
   3) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,
   4) pozostałymi aktami prawnymi wymienionymi w § 15 Instrukcji.
3. Potwierdzenie zapoznania się z Instrukcją i aktami prawnymi wymienionymi w § 15 Instrukcji dokonuje się w formie podpisania przez użytkownika odpowiedniego oświadczenia.[…]
4. Użytkownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.

5. Wszelkie przekroczenia lub próby przekroczenia uprawnień będą traktowane jako naruszenie obowiązków pracowniczych.
6. Systemy komputerowe i sieć telekomunikacyjna, znajdujące się w Szkole, mogą być używane wyłącznie do celów służbowych.

§ 5

0. Sprzęt komputerowy znajduje się w odpowiednio zabezpieczonych pomieszczeniach, zamkniętych na klucz, jeżeli nikt z pracowników Szkoły w nich nie przebywa.
1. Przed rozpoczęciem pracy klucze do pomieszczeń pobierane są z pokoju nauczycielskiego Szkoły, a po zakończeniu pracy klucze pozostawiane są w pokoju nauczycielskim.
2. Monitory powinny być ustawione w sposób uniemożliwiający oglądanie ich ekranów przez okna, drzwi i z miejsc ogólnodostępnych.
3. W pomieszczeniach, w których znajduje się sprzęt komputerowy, obowiązuje zakaz używania otwartego ognia i palenia tytoniu.
4. Sprzęt komputerowy wyposażony jest w odpowiednie zasilacze awaryjne na wypadek zaniku napięcia.
5. Jednostki centralne, monitory i drukarki muszą być oznaczone celem ich identyfikacji.
6. Użytkownik nie może samodzielnie dokonywać zmiany akcesoriów ani przyłączać akcesoriów prywatnych.
7. Sprzęt komputerowy nie może być wynoszony ze Szkoły bez zgody administratora danych.
8. Sprzęt komputerowy nie może być przenoszony w inne miejsce bez zgody administratora danych i administratora sieci informatycznej.
9. W Szkole może być wykorzystywane wyłącznie oprogramowanie legalne i używane zgodnie z prawami licencji.

II. Zasady rejestrowania i wyrejestrowywania użytkowników

§ 6

1. Osobą odpowiedzialną za rejestrowanie i wyrejestrowanie użytkowników w Szkole jest administrator sieci informatycznej.
2. Podstawą do zarejestrowania użytkownika do danego systemu przetwarzania danych jest zakres czynności pracownika, w którym musi być wskazane, że zadaniem danej osoby jest praca przy przetwarzaniu danych danego systemu w podanym zakresie.
3. Podstawą do wyrejestrowania użytkownika z danego systemu przetwarzania danych jest nowy zakres czynności pracownika lub rozwiązanie stosunku pracy z pracownikiem.
4. Administrator sieci informatycznej rejestruje oraz wyrejestrowuje użytkownika, prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych, archiwizując identyfikator oraz imię i nazwisko użytkownika
5. Identyfikatory osób, które utraciły uprawnienia dostępu do danych, należy wyrejestrować z systemu, unieważniając ich hasło. Identyfikator po wyrejestrowaniu użytkownika nie jest przydzielany innej osobie.
6. Osoby dopuszczone do przetwarzania danych zobowiązane są do zachowania tajemnicy dostępu do danych i ich merytorycznej treści. Obowiązek ten istnieje również po ustaniu zatrudnienia.

III. Zarządzanie systemami haseł

§ 7

1. Osobą odpowiedzialną za przydział haseł dla użytkowników oraz częstotliwość ich zmiany jest administrator sieci informatycznej.
2. Każdy użytkownik systemu informatycznego ma przydzielony jednorazowy, niepowtarzalny identyfikator (login) oraz okresowo zmieniane hasło dostępu.
3. Pierwsze hasło dla użytkownika zakładane jest przez administratora sieci informatycznej podczas wprowadzania jego identyfikatora do systemu.
4. Przekazywanie haseł odbywa się w sposób poufny, w formie ustnej, hasło nie może być zapisywane w miejscu pozwalającym na dostęp osób nieuprawnionych.
5. Użytkownik jest zobowiązany do zmiany przydzielonego hasła […].
6. Dostęp do zasobów systemu może odbywać się tylko w oparciu o system haseł przydzielanych indywidualnie pracownikom - użytkownikom systemu.
7. Zapewnione jest generowanie haseł w cyklu miesięcznym. Użytkownicy mają obowiązek zmieniać swoje hasło nie rzadziej niż co 30 dni.
8. Użytkownik nie może udostępniać swego hasła innym osobom.
9. W przypadku utraty hasła lub podejrzenia naruszenia systemu haseł przez osoby nieuprawnione, dotychczasowy zestaw haseł musi być niezwłocznie unieważniony i zastąpiony nowym.

IV. Procedury rozpoczęcia, zawieszenia i zakończenia pracy

§ 8

1. Użytkownicy przed przystąpieniem do pracy przy przetwarzaniu danych powinni zwrócić uwagę, czy nie istnieją przesłanki świadczące o naruszeniu danych. Jeżeli istnieje takie podejrzenie, należy postępować zgodnie z zasadami określonymi w niniejszej Instrukcji.
2. Dostęp do konkretnych zasobów danych jest możliwy dopiero po podaniu właściwego identyfikatora i hasła dostępu.
3. Hasło użytkownika należy podawać do systemu w sposób dyskretny […].
4. W sytuacji tymczasowego zaprzestania pracy wskutek opuszczenia stanowiska pracy należy wylogować się z systemu i zamknąć pomieszczenie (jeśli inny pracownik Szkoły nie przebywa w pomieszczeniu), natomiast w celu zabezpieczenia danych, w okolicznościach kiedy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba, należy niezwłocznie wyłączyć monitor.
5. Ekrany monitorów są automatycznie wygaszane w przypadku dłuższej nieaktywności użytkownika. Wygaszacz jest chroniony hasłem.
6. Użytkownik ma obowiązek zamykania programu komputerowego i systemu po zakończeniu pracy. Stanowisko komputerowe z uruchomionym systemem nie może pozostawać bez kontroli pracującego na nim użytkownika.

V. Obsługa kopii bezpieczeństwa, nośników informacji oraz wydruków

§ 9

1. Wydruki z systemów informatycznych oraz inne nośniki informacji muszą być zabezpieczone w sposób uniemożliwiający do nich dostęp osobom nieupoważnionym w każdym momencie przetwarzania, a po upływie czasu ich przydatności są niszczone lub archiwizowane w zależności od kategorii archiwalnej.
2. Wydruki i nośniki zawierające dane osobowe (urządzenia, dyskietki, dyski optyczne itp.) oraz inne dokumenty przeznaczone do likwidacji, muszą być pozbawione zapisów, lub w

przypadku gdy jest to możliwe, muszą być trwale uszkodzone w sposób uniemożliwiający odczytanie z nich informacji.

3. Kopie bezpieczeństwa (zapasowe) wykonywane są w systemie dziennym, w dni robocze, na dysku twardym oraz na nośniku zewnętrznym.
4. Nośniki z kopiami bezpieczeństwa, po uprzednim zaplombowaniu, przechowywane są w szafie metalowej znajdującej się w pomieszczeniu administratora sieci informatycznej.
5. Administrator sieci informatycznej wykonuje również raz w miesiącu kopie archiwalne, które przechowuje się przez okres jednego roku w sejfie znajdującym się w pomieszczeniu kadrowym Szkoły, w zaplombowanym przez administratora sieci informatycznej pojemniku.
6. Czas użytkowania dysków optycznych wielokrotnego zapisu wynosi nie dłużej niż rok kalendarzowy. Po tym czasie, po uprzednim pozbawieniu zapisu danych, dyski są fizycznie niszczone (pocięcie na wiele kawałków) przez administratora sieci informatycznych w niszczarce specjalnie przeznaczonej do tego celu.
7. W przypadku wykonywania wydruków ze zbiorów danych osobowych, pracownik jest zobowiązany do zachowania wszelkich niezbędnych środków ostrożności w celu niedopuszczenia do ich utraty lub nieuprawnionego ujawnienia.

VI. Ochrona danych przed ich utratą z systemów informatycznych

§ 10

1. Urządzenia i systemy informatyczne zasilane energią elektryczną powinny być zabezpieczone przed utratą danych, spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej (czyli posiadać zasilacze awaryjne UPS).
2. Pomieszczenia komputerowe powinny być zabezpieczone przed pożarem.
3. Instalacja oprogramowania może odbywać się tylko przez administratora sieci informatycznej lub pod jego nadzorem.
4. Potencjalnym źródłem przedostania się szkodliwego oprogramowania do systemu są: nośniki zewnętrzne (np. dyskietka, pamięć flash, dyski optyczne, zewnętrzne dyski twarde), sieć lokalna i rozległa.
5. W celu ochrony przed wirusami komputerowymi, każde stanowisko pracy wyposażone jest w program antywirusowy typu AVG, który aktualizuje się automatycznie co 2 godziny.
6. Osobą odpowiedzialną za zarządzanie oprogramowaniem antywirusowym jest administrator sieci informatycznej.
7. W przypadku stwierdzenia obecności wirusów komputerowych w systemie, należy zastosować się do zaleceń programu antywirusowego.
8. Jeżeli realizacja zaleceń programu nie powoduje usunięcia wirusów, należy niezwłocznie zawiadomić administratora sieci informatycznej.

VII. Sposób komunikacji w zakresie sieci komputerowej

§ 11

1. Dopuszcza się łączenie z siecią Internet i używanie poczty elektronicznej tylko w celach służbowych z zachowaniem szczególnych środków ostrożności.
2. Przesyłanie danych osobowych na nośnikach zewnętrznych (np. dyskietki, dyski optyczne, wydruki), na zewnątrz może odbywać się tylko w formie przesyłki poleconej, zgodnie z obowiązującymi przepisami.

3. Zabrania się przekazywania danych osobowych w jawnej formie za pośrednictwem Internetu (poczty elektronicznej).
4. Zabrania się:
   1) korzystania z portali społecznościowych,
   2) przeglądania stron zawierających treści nieetyczne oraz obrażające uczucia innych,
   3) pobierania plików niewiadomego pochodzenia,
   4) wykonywania czynności naruszających prawa autorskie w tym przeglądania, pobierania i przesyłania plików oraz stron naruszających te prawa,
   5) działania na szkodę innych użytkowników Internetu.

VIII. Przeglądy i konserwacja systemów i zbiorów danych

§ 12

1. Przeglądów i konserwacji systemów przetwarzania danych dokonuje administrator sieci informatycznej co najmniej raz w miesiącu.
2. Ocenie podlegają: stan techniczny urządzeń (komputery, serwery, UPS, itp.), stan okablowania budynku (sieć logiczna), spójność bazy danych, stan zabezpieczeń fizycznych (zamki, karty), stan rejestrów systemu serwera lokalnej sieci komputerowej.
3. Urządzenia, dyski i inne elektroniczne nośniki danych zawierające dane osobowe, przeznaczone do naprawy, winny być trwale pozbawione zawartości przez wymazanie tej zawartości specjalistycznym oprogramowaniem.
4. Naprawa urządzeń zawierających dane osobowe, jeżeli nie można danych usunąć, winna być wykonana pod nadzorem osoby upoważnionej przez administratora danych.

IX. Postępowanie w sytuacjach naruszenia zasad ochrony systemów informatycznych

§ 13

1. Przesłanki lub fakty wskazujące na naruszenie bezpieczeństwa systemu, a zwłaszcza stan różny od ustalonego w systemie informatycznym, w tym:
   1) stan urządzeń (np. brak zasilania, problemy z uruchomieniem),
   2) stan systemu zabezpieczeń obiektu,
   3) stan aktywnych urządzeń sieciowych i pozostałej infrastruktury informatycznej,
   4) zawartość zbioru danych (np. brak lub nadmiar danych),
   5) stwierdzenie korzystania z komputera przez osobę nieuprawnioną,
   6) sposób działania programu (np. komunikat informujący o błędach, brak dostępu do funkcji programu, nieprawidłowości w wykonywanych operacjach),
   7) przebywanie osób nieuprawnionych w obszarze przetwarzania danych,
   8) inne zdarzenia mogące mieć wpływ na naruszenie systemu informatycznego (np. obecność wirusów komputerowych)

stanowią dla osoby uprawnionej do przetwarzania danych podstawę do natychmiastowego działania.

2. Sposób postępowania:
   1) o każdej sytuacji odbiegającej od normy, a w szczególności o przesłankach naruszenia ochrony danych w systemie informatycznym opisanych ust. 1, należy natychmiast informować administratora sieci informatycznej,
   2) niezwłocznie taką sytuację należy opisać w notatce służbowej skierowanej do administratora danych.

3. Stwierdzone przez administratora sieci informatycznej naruszenie zasad ochrony danych osobowych wymaga:

1) usunięcia uchybień (np. wymiana niesprawnego zasilacza awaryjnego, usunięcie wirusów komputerowych z systemu, itp.),
2) zastosowania dodatkowych środków zabezpieczających zgromadzone dane,
3) wstrzymania przetwarzania danych do czasu usunięcia awarii systemu informatycznego.

4. Osoba stwierdzająca naruszenie przepisów lub stan mogący mieć wpływ na bezpieczeństwo danych zobowiązana jest do możliwie pełnego udokumentowania zdarzenia, celem precyzyjnego określenia przyczyny i ewentualnych skutków naruszenia obowiązujących zasad.

X. Zasady instalacji oprogramowania

§ 14

1. Instalacji oprogramowania lub aktualizacji dokonuje administrator sieci informatycznej.
2. Na wszystkich komputerach Zespołu dopuszcza się instalację tylko legalnego i licencjonowanego oprogramowania.
3. Zabrania się instalowania oprogramowania bez zgody administratora bezpieczeństwa informacji lub administratora sieci informatycznej

XI. Postanowienia końcowe

§ 15

W sprawach nieuregulowanych w niniejszej Instrukcji mają zastosowanie:

1) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),
2) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024),
3) Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565 z późn. zm.),
4) Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204 z późn. zm.),
5) Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450 z późn. zm.),
6) Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz. U. Nr 212, poz. 1766),
7) Rozporządzenie Prezesa Rady Ministrów z dnia 29 września 2005 r. w sprawie warunków organizacyjno-technicznych doręczania dokumentów elektronicznych podmiotom publicznym (Dz. U. Nr 200, poz. 1651),
8) inne regulaminy i instrukcje wewnętrzne.