INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W I LICEUM OGÓLNOKSZTAŁCĄCYM IM. ADAMA ASNYKA W KALISZU

1. WSTĘP, CHARAKTERYSTYKA, OGÓLNE ZASADY

Niniejsza instrukcja stanowi podstawę do określenia sposobu zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz innych prawnie chronionych w I LO. Jest ona częścią dokumentacji danych osobowych, z którą należy się zapoznać przed przeczytaniem niniejszej instrukcji.

Na system informatyczny składa się:

- lokalna sieć informatyczna wraz z urządzeniami sieciowymi;
- serwery oraz wszystkie stacje robocze (komputery);
- wszystkie urządzenia peryferyjne podłączane do komputerów;
- podłączenie sieci lokalnej do sieci publicznej poprzez usługodawcę internetowego.

Wprowadza się zasady ogólne:

- wszystkie komputery i serwery zabezpieczone są oprogramowaniem antywirusowym i firewall;
- każde oprogramowanie jest licencjonowane oraz uaktualniane w razie potrzeby; oprogramowanie systemowe oraz wszelkie przeglądarki powinny być uaktualniane w możliwie najkrótszym czasie od wydania poprawki przez producenta;
- dostęp do systemu i programów odbywa się poprzez autoryzację użytkownika w systemie na podstawie loginu i hasła;
- dostęp do zbiorów danych zabezpieczony jest mechanizmami kontroli dostępu oraz ochrony poufności, dostępności i integralności informacji;
- komputery i serwery, na których przechowywane są zbiory danych osobowych zabezpieczone są zasilaczami awaryjnymi oraz wykonywane są odpowiednie kopie zapasowe danych oraz aplikacji;
- sieć lokalna zabezpieczona jest oprogramowaniem typu Firewall przed nieuprawnionym dostępem z zewnątrz;
- do przesyłania danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej stosuje się środki kryptograficznej ochrony; te same środki stosuje się do przesyłania danych osobowych na zewnątrz.

Użytkownikom zabrania się:

- samowolnego wyłączania zabezpieczeń, instalowania dodatkowych programów, zmian w oprogramowaniu, konfiguracji sprzętu;
- udostępniania stanowisk komputerowych osobom nieuprawnionym;
- udostępniania haseł dostępu osobom trzecim;
- wykorzystywania stanowisk komputerowych w celach innych niż wyznaczonych przez ADO;
- jakichkolwiek zmian w systemie umożliwiających dostęp do zasobów zarówno z sieci lokalnej jak i z publicznej;
- podejmowania prób testowania, modyfikacji lub naruszenia zabezpieczeń lub jakichkolwiek działań noszących takie znamiona;
- wykonywania jakichkolwiek działań niezgodnych z ustawą o ochronie praw autorskich.

2. PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH

Do przetwarzania danych osobowych i korzystania z systemu informatycznego wymagane jest upoważnienie. Upoważnienia są imienne i udzielane w formie pisemnej na czas określony lub na czas nieokreślony – do odwołania udzielonego upoważnienia.

Każde upoważnienie jest rejestrowane.

Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych wraz z informacją o przyznanym loginie do danego programu komputerowego.

ASI określa loginy oraz hasła początkowe użytkowników komputerów oraz programów do przetwarzania danych osobowych.

Uprawnienia do pracy w systemie informatycznym są odbierane w przypadku ustania stosunku pracy lub na prośbę ADO. Usuwanie uprawnień polega na dezaktywacji loginów pozostawiając historię ich aktywności. Usuwanie loginów stosowane jest wyłącznie w uzasadnionych przypadkach.

Osoby upoważnione do pracy w systemie informatycznym są zobowiązane zachować loginy, hasła oraz metody zabezpieczeń w tajemnicy nawet po ustaniu stosunku pracy.

3. STOSOWANE METODY I ŚRODKI UWIERZYTELNIANIA

Każdy użytkownik systemu informatycznego posiada osobiste identyfikatory (loginy) oraz hasła dostępu do swojego osobistego i wyłącznego użytku. Hasła stanowią tajemnicę służbową i znane są wyłącznie temu użytkownikowi. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła dostępu oraz jego przechowywanie.

Identyfikatory użytkowników powinny być niepowtarzalne, nie powinny być zmieniane, a w przypadku utraty uprawnień przez użytkownika niezwłocznie blokowane.

Uwierzytelnianie się do systemu informatycznego polega przede wszystkim na zalogowaniu się do systemu Windows poprzez przyznany login i hasło oraz automatyczne zarejestrowanie tego faktu w logach systemowych.

Korzystanie ze zbiorów danych osobowych wymaga kolejnego uwierzytelnienia się poprzez zalogowanie do danego programu osobnym loginem i hasłem oraz zarejestrowanie tego faktu w logach systemowych.

Hasło do systemu lub programu przechowującego dane osobowe musi być okresowo zmieniane, zgodnie z wymaganiami dla danego systemu informatycznego, musi składać się co najmniej z 8 znaków i być kombinacją liter (dużych i małych) i cyfr.

Hasło nie powinno być zbyt łatwe, tzn. nie powinno zawierać prostych słów lub imion, nie powinno być ciągiem tych samych lub kolejnych znaków z klawiatury, nie może być datą urodzenia, nie może się powtarzać itp. Hasło nie może być zapisywane i przechowywane przez użytkownika

W przypadku podejrzenia, że hasło może znać inna osoba należy je niezwłocznie zmienić lub zgłosić ten fakt do ASI lub IOD.

ASI ma obowiązek uruchomić w systemach tam gdzie jest to możliwe automatyczne sprawdzanie stopnia skomplikowania hasła oraz narzucanie okresowej zmiany zgodnie z wymaganiami dla danego systemu informatycznego. Jeżeli system nie ma możliwości narzucenia zmiany hasła obowiązek zmiany hasła spoczywa na użytkowniku.

ASI powinien uruchomić, o ile to możliwe, niedopuszczenie do logowania tego samego użytkownika na więcej niż jednej stacji roboczej oraz wymusić logowanie tylko w określonych porach dnia.

Hasła administracyjne przechowywane są przez ASI w zamkniętej kopercie w sejfie.

4. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY W SYSTEMACH

Przed przystąpieniem do pracy z systemem informatycznym, użytkownik zobowiązany jest dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.

Na stanowiskach, na których przetwarzane są dane osobowe ekrany monitorów powinny być tak ustawione, aby osoby nieupoważnione nie miały dostępu do informacji na nich wyświetlanych.

Po uruchomieniu komputera należy wprowadzić odpowiedni login i hasło do systemu upewniając się, że osoby nieupoważnione nie mają możliwości podglądu.

W przypadku wprowadzania danych uwierzytelniających poprzez sieć publiczną (przez przeglądarkę internetową) należy upewnić się, że połączenie jest szyfrowane.

W razie przerwania pracy należy zastosować wygaszacz ekranu dezaktywujący się po ponownym wprowadzeniu hasła.

Przy zakończeniu pracy należy upewnić się czy dane zostały zarejestrowane, aby uniknąć utraty danych z powodu awarii i poprawnie wylogować się z programu lub systemu. Niedopuszczalne jest wyłączanie komputera włącznikiem bez uprzedniego wylogowania się.

Osoba przetwarzająca dane w przypadku konieczności opuszczenia pomieszczenia, obowiązana jest do zastosowania odpowiednich środków bezpieczeństwa tj. wylogowanie się z programu, wygaszacz ekranu, wyłączenie komputera.

ASI i IOD monitoruje poprawne działania użytkowników.

5. UŻYWANIE KOMPUTERÓW PRZENOŚNYCH

Osoba używająca komputer przenośny zawierający dane osobowe zobowiązana jest zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych.

Osoba używająca komputer przenośny w szczególności powinna:

- stosować ochronę kryptograficzną wobec przetwarzanych danych osobowych;
- zabezpieczyć dostęp do na poziomie systemu operacyjnego poprzez silne hasło;
- nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych;
- nie wykorzystywać komputera do przetwarzania danych osobowych w obszarach użyteczności publicznej;
- zachować szczególną ostrożność przy podłączaniu do sieci publicznych poza obszarem przetwarzania danych osobowych.

Za wszelkie działania wykonywane na komputerze przenośnym odpowiada jego formalny użytkownik.

W przypadku ustania – rozwiązania umowy o pracę, pracownik (użytkownik) komputera przenośnego lub innego urządzenia mobilnego jest zobowiązany do natychmiastowego zdania powierzonych mu urządzeń.

6. INNE METODY I ŚRODKI TECHNICZNE ZABEZPIECZAJĄCE SYSTEM INFORMATYCZNY

Programy zainstalowane na komputerach powinny być użytkowane z zachowaniem praw autorskich i posiadać licencje

Oprogramowanie typu freeware, shareware lub inne dostarczane bez opłat jest unzawane jako nieautoryzowane, jeżeli nie otrzyma stosownej aprobaty ASI.

Przed zainstalowaniem nowego oprogramowania ASI lub inna osoba upoważniona zobowiązany jest sprawdzić jego działanie pod kątem bezpieczeństwa całego systemu.

Sieć teleinformatyczna powinna mieć zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu informatycznego.

Infrastruktura techniczna (rozdzielnie elektryczne, urządzenia sieciowe, skrzynki bezpieczników, punkty dostępu) powinna być zabezpieczona przed dostępem osób nieuprawnionych.

Zdalne uruchamianie komend systemowych ze stacji roboczych znajdujących się w lokalizacjach nie należących do I LO jest możliwe, po prawidłowym logowaniu się użytkownika i zastosowaniu silnego uwierzytelnienia.

7. PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH

Kopie informatyczne zbiorów danych osobowych oraz aplikacji wykonuje się w miarę potrzeb w częstotliwości, która zapewnia krótki czas przywrócenia zbiorów danych.

ASI odpowiedzialny jest za przygotowanie, wdrożenie i nadzorowanie zasad i mechanizmów tworzenia kopii zapasowych.

Kopie mogą być sporządzane automatycznie lub ręcznie z wykorzystaniem specjalistycznych programów lub za pomocą standardowych mechanizmów systemów operacyjnych.

Nośniki, na których przechowywane są kopie powinny być czytelnie oznaczone oraz odpowiednio przechowywane w zabezpieczonych miejscach.

Tworzenie wydruków danych z systemów informatycznych powinno być ściśle uzgadniane z ADO i tworzone wyłącznie w zakresie i ilości niezbędnej dla konkretnego celu.

8. SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW I KOPII ZAPASOWYCH

Decyzję o likwidacji zbiorów danych osobowych, przetwarzanych w systemach informatycznych podejmują właściciele zasobów danych osobowych.

Kopie zapasowe przechowuje się na oznaczonych nośnikach elektronicznych w zamkniętych szafach lub na dyskach zabezpieczając je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem. Kopie okresowo sprawdza się pod kątem przydatności, a po ustaniu ich użyteczności niezwłocznie zostają usunięte.

Nośniki z kopiami zapasowymi są przechowywane w innej lokalizacji, niż miejsce przechowywania zarchiwizowanych na nich zbiorów danych osobowych.

Kopie zapasowe, które są już nieprzydatne lub uległy uszkodzeniu powinny podlegać natychmiastowemu zniszczeniu.

W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopie zapasowe należy przed ich likwidacją usunąć wszelkie dane lub uszkodzić je w sposób uniemożliwiający ich odczyt.

Wydruki, które nie są przeznaczone do udostępniania, przechowuje się w zamykanej szafie, do której dostęp mają tylko osoby uprawnione.

Komputery przenośne, nośniki wymienne i inne urządzenia zawierające dane osobowe, które są wynoszone poza obszar przetwarzania danych, powinny być odpowiednio zabezpieczone - zaszyfrowane. Nośniki zewnętrzne powinny być przed użyciem skanowane.

Wszelkie wydruki zawierające dane osobowe powinny być przechowywane w miejscu uniemożliwiającym ich odczyt przez osoby nieupoważnione, zaś po upływie czasu ich przydatności – niszczone w niszczarkach dokumentów.

Zabrania się gromadzenia i przechowywania danych osobowych w innych miejscach niż wskazane w dokumentacji.

9. SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED WIRUSAMI

System informatyczny zabezpieczony jest programem antywirusowym na każdym urządzeniu, w szczególności zabezpieczona jest każda stacja robocza i każdy komputer przenośny.

ASI jest odpowiedzialny za aktualność i poprawność programu antywirusowego oraz za skuteczne usunięcie występujących zdarzeń i zagrożeń.

Program antywirusowy musi być skonfigurowany na automatyczne wykrywanie wirusów i wszelkich innych zagrożeń oraz na automatyczne aktualizacje do najnowszych baz zagrożeń.

W przypadku stwierdzenia wykrycia wirusa lub niepoprawności działania programu antywirusowego użytkownik jest zobowiązany natychmiast zgłosić ten fakt ASI, IOD lub ADO.

Użytkownik ma obowiązek skanowania antywirusowego każdego zewnętrznego nośnika danych przed jego użyciem.

10. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMU

Przeglądy i konserwacje systemu informatycznego oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby, które złożyły pisemnie oświadczenie do zachowania w tajemnicy wszelkich pozyskanych informacji oraz posiadające upoważnienie bądź umowę na powierzenie przetwarzania danych wydane przez Administratora Danych Osobowych. Przed rozpoczęciem prac należy dokonać potwierdzenia tożsamości tych osób. Przeglądy w miejscu użytkowania systemu wymagają obecności ASI lub osoby upoważnionej.

Dyski lub inne nośniki danych przed likwidacją lub przekazaniem podmiotowi nieuprawnionemu pozbawia się wcześniej zapisanych danych lub trwale niszczy.

W przypadku konieczności przeprowadzenia prac serwisowych lub przeglądu poza I LO, dane osobowe znajdujące się w naprawianym urządzeniu muszą zostać w sposób trwały usunięte lub odpowiednio zabezpieczone programami kryptograficznymi.

Przed dokonaniem zmian w systemie informatycznym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych na testowej bazie danych. Sprawdzenie powinno obejmować poprawność działania aplikacji oraz poprawność funkcjonalną systemu.

ASI dokonuje okresowych przeglądów systemu informatycznego oraz nośników danych i na bieżąco wraz z ADO eliminuje te, które nie zapewniają odpowiedniego poziomu bezpieczeństwa.

11. PROCEDURY PRZESYŁANIA DANYCH POZA OBSZAR PRZETWARZANIA

Dane mogą być przekazane podmiotom trzecim tylko i wyłącznie na podstawie stosownych przepisów.

Nośniki danych lub urządzenia zawierające dane osobowe przekazywane poza obszar przetwarzania muszą być zabezpieczone poprzez zastosowanie ochrony kryptograficznej.

W przypadku przesyłania danych osobowych w postaci elektronicznej lub wprowadzania ich ręcznie do innych systemów za pomocą sieci publicznej połączenie musi być szyfrowane.

mgr Urszula Jarczar
DYREKTOR
I Liceum Ogólnokształcącego
im. Adama Asnyka w Kaliszu

.....
Podpis dyrektora