DOKUMENTACJA OCHRONY DANYCH OSOBOWYCH
w III LICEUM OGÓLNOKSZTAŁCĄCYM
IM. MIKOŁAJA KOPERNIKA
w Kaliszu

Administrator Danych Osobowych:

III Liceum Ogólnokształcące im. Mikołaja Kopernika

ul. Kościuszki 10, 62-800 Kalisz

SPIS TREŚCI:

1. WPROWADZENIE

Tworzy się dokumentację ochrony danych osobowych celem opisu sposobu przetwarzania danych osobowych oraz opisu środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

Jednym z głównych celów dokumentacji jest przekazanie pracownikom III Liceum Ogólnokształcącego im. Mikołaja Kopernika w Kaliszu podstawowej wiedzy z zakresu ochrony danych osobowych oraz zasad i procedur zwiększając świadomość pracowników o wartości posiadanych i przetwarzanych danych osobowych m.in. poprzez:

- wyjaśnienie zagadnienia i opisanie podstaw prawnych;
- scharakteryzowanie podstawowych zagrożeń bezpieczeństwa oraz sposób postępowania w przypadku ich wykrycia;
- opis zastosowanej polityki bezpieczeństwa;
- szczegółowy opis procedur pracy w systemach informatycznych;
- wykaz rejestru czynności ochrony danych osobowych;
- ocenę ryzyka w zakresie przetwarzania danych osobowych;
- zasady organizacji pracy przy zbiorach osobowych przetwarzanych metodami tradycyjnymi.

Stosując zasady zawarte w niniejszej dokumentacji, ryzyko wystąpienia negatywnych konsekwencji wynikających z zagrożeń przetwarzania danych osobowych takich jak:

- naruszenie interesów lub praw osoby fizycznej, której dane osobowe dotyczą;
- naruszenia danych osobowych rozumianych jako dobro prywatne powierzone III LO;
- naruszenie przepisów prawa;
- utraty lub obniżenia reputacji III LO mogącej mieć wpływ na jej wartość;
- strat finansowych ponoszonych w wyniku nałożonych kar lub utraty wiarygodności;
- zakłócenie czynności spowodowanych nieprawidłowym działaniem systemów informatycznych

jest zminimalizowane.

III Liceum Ogólnokształcące im. Mikołaja Kopernika w Kaliszu realizuje zadania w zakresie edukacji, określone w ustawie z dnia 14 grudnia 2016 r. - Prawo oświatowe ze zmianami oraz z dnia 26 stycznia 1982 r. - Karta Nauczyciela ze zmianami.

2. PODSTAWA PRAWNA

Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016.

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

3. DEFINICJE

W dokumencie przyjmuje się następującą terminologię:

III LO – III Liceum Ogólnokształcące im. Mikołaja Kopernika w Kaliszu

RODO - Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r.

Ustawa - ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych ze zmianami.

Dane osobowe - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Przetwarzania – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Dane wrażliwe - dane o pochodzeniu rasowym lub etnicznym, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniowa, partyjna lub związkowa, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Administrator danych (ADO) – III Liceum Ogólnokształcące im. Mikołaja Kopernika z siedzibą w Kaliszu, ul. Kościuszki 10.

Inspektor ochrony danych (IOD) – osoba fizyczna wspierająca administratora danych w realizacji obowiązków dotyczących ochrony danych osobowych oraz nadzorująca stosowanie środków technicznych i organizacyjnych przetwarzanych danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną. Osoba powołana przez ADO.

Administrator systemu informatycznego (ASI) – osoba odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych przetwarzających dane osobowe. Osoba powołana przez ADO.

Zbiór danych - uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Zabezpieczenie danych w systemie informatycznym - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

Zgoda osoby, której dane dotyczą – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

Rozliczalność - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

Integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

Niezawodność – właściwość zapewniająca, że zamierzone zachowania i skutki są spójne.

Poufność danych – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.

Dokumentacja – dokumentacja przetwarzania danych osobowych opisująca sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, określoną w przepisach prawnych.

4. WPROWADZENIE DO OCHRONY DANYCH OSOBOWYCH

Poniżej przedstawiono wyciąg najważniejszych informacji odnośnie ochrony danych osobowych.

4.1. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:

- osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
- przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

4.2. W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o:

- swojej tożsamości i danych kontaktowych oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe inspektora ochrony danych;
- celu przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;
- prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
- informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
- inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania takie jak: okres, przez który dane osobowe będą przechowywane, prawa osoby fizycznej, czy podanie danych jest konieczne j jakie są ewentualnie konsekwencje niepodania danych, informacje o zautomatyzowanym podejmowaniu decyzji.

Informacje powyższe przekazuje się również w przypadku zbierania danych osobowych w sposób inny niż od osoby, której dane dotyczą, wraz z podaniem źródła pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych.

Powyższych zasad nie stosuje się, jeżeli przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania lub osoba, której dane dotyczą, posiada już te informacje.

4.3. Przetwarzanie danych jest zabronione w przypadku:

- przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Przetwarzanie powyższych danych, jest jednak dopuszczalne, jeżeli m.in.:

- osoba, której dane dotyczą, wyrazi na to zgodę na piśmie;
- przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą;

- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
- przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym;
- przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy;
- przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych.

4.5. Zasady dotyczące przetwarzania danych osobowych:

Aby przetwarzać dane osobowe muszą one być:

- przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
- zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
- adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
- prawidłowe i w razie potrzeby uaktualniane;
- przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;
- przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem;

Administrator danych jest odpowiedzialny za przestrzeganie powyższych zasad.

4.5. Prawa osoby, której dane dotyczą:

Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do m.in.:

- dostępu do danych i ich poprawiania, przenoszenia danych;
- cofnięcia zgody na przetwarzanie danych;
- ograniczenia przetwarzania danych, sprzeciwu przetwarzania;
- usunięcia danych („prawo do bycia zapomnianym”);
- niepodlegania zautomatyzowanemu podejmowaniu decyzji, profilowaniu;
- wniesienia skargi do organu nadzorczego - Prezesa Urzędu Ochrony Danych Osobowych.

4.6. Prezes Urzędu Ochrony Danych Osobowych

Organem nadzorczym do spraw ochrony danych osobowych w Polsce jest Urząd Ochrony Danych Osobowych (Prezes Urzędu Ochrony Danych Osobowych).

Do zadań Prezesa Urzędu Ochrony Danych Osobowych w szczególności należy m.in.:

- monitorowanie i egzekwowanie stosowania przepisów o ochronie danych osobowych;
- współpraca innymi organami nadzorczymi;
- wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych;
- inicjowanie i podejmowanie przedsięwzięć oraz doradzanie w zakresie upowszechniania i doskonalenia wiedzy z zakresu ochrony danych osobowych.

4.7. Obowiązki Administratora Danych Osobowych

Administrator Danych Osobowych (ADO) zobowiązany jest do zapewnienia zgodności przetwarzania danych osobowych z przepisami prawa, ochrony przetwarzania danych osobowych przed ich

udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieupoważnioną, zbieraniem i przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Ponadto ADO zobowiązany jest zapewnić kontrolę i rozliczalność nad tym, jakie dane osobowe, kiedy i przez kogo są przetwarzane oraz komu są przekazywane.

W tym celu ADO prowadzi dokumentację oraz wszelkie potrzebne ewidencje i upoważnienia.

ADO, w przypadku podmiotów publicznych, obowiązany jest powołać Inspektora Ochrony Danych (IOD) oraz może powołać Administratora Systemu Informatycznego (ASI). Szczegółowe zadania IOD i ASI wykazane są w dalszej części dokumentacji.

5. ZAGROŻENIA BEZPIECZEŃSTWA

Charakterystyka możliwych zagrożeń:

Zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), których występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, a ciągłość systemu zostaje zakłócona, lecz nie dochodzi do naruszenia poufności danych.

Zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora systemu, awarie sprzętowe, błędy oprogramowania), przy których może dojść do zniszczenia danych, a ciągłość pracy systemu może zostać zakłócona oraz może nastąpić naruszenie poufności danych.

Zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, gdzie występuje naruszenia poufności danych (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy). Zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

Poniżej przedstawiono przykładowe sytuacje świadczące o naruszeniu zasad bezpieczeństwa. W przypadku zaistnienia lub stwierdzenia podejrzenia wystąpienia któregokolwiek z zagrożeń należy niezwłocznie powiadomić ADO lub IOD:

Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, włamanie, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.

Sytuacje przypadkowe - pozostawienie niezamkniętych drzwi lub okien w pomieszczeniach gdzie przetwarza się dane osobowe w przypadku gdy w pomieszczeniu nie ma osób uprawnionych.

Niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych.

Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu oraz sam fakt pozostawienia serwisantów bez nadzoru.

Pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu.

Jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie.

Naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie.

Próba lub modyfikacja danych oraz zmiana w strukturze danych bez odpowiedniego upoważnienia (uwierzytelnienia).

Niedopuszczalna manipulacja danymi osobowymi w systemie.

Ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu.

Praca w systemie informatycznym wykazująca nieprzypadkowe odstępstwa od założonego rytmu pracy oraz wskazująca na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.

Podmiana lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony, kasowania lub kopiowanie danych.

Rażące naruszenia dyscypliny pracy w systemie informatycznym w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

Zapisywanie danych osobowych na niezabezpieczonych nośnikach zewnętrznych oraz wynoszenie ich poza obszar przetwarzania lub przesyłanie niezabezpieczonych danych przez internet.

Rażące naruszenia dyscypliny przetwarzania danych papierowych w zakresie przestrzegania procedur bezpieczeństwa informacji (pozostawienie danych na biurkach, pólkach, pozostawienie otwartych szaf, przechowywanie dokumentów w miejscach do tego nieprzeznaczonych, wyrzucanie dokumentów z danymi osobowymi bez uprzedniego zniszczenia, pozostawienie danych osobowych w drukarce, na ksero, itp).

Nieuprawnione instalowanie jakiegokolwiek oprogramowania, obecność podejrzanego oprogramowania.

Awarie sprzętu i oprogramowania, w tym zasilaczy awaryjnych podtrzymujących zasilanie.

Nieoczekiwane, niewyjaśnione i niezapowiedziane zmiany w działaniu, wyglądzie oprogramowania, urządzenia, kabli.

Nieuzasadnione przeglądanie danych w ramach konsultacji lub pomocy technicznej.

Pozostawienie nośników danych, wydruków, kserokopii, pism i innych dokumentów zawierających dane osobowe w miejscach narażonych na łatwy dostęp osób trzecich.

Nieuzgodnione, nieoczekiwane, nagłe wizyty osób próbujących ingerować w system celem naprawy, konfiguracji lub kontroli.

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W III LICEUM OGÓLNOKSZTAŁCĄCYM IM. MIKOŁAJA KOPERNIKA W KALISZU

Polityka bezpieczeństwa to zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz III LO. Jest ona częścią dokumentacji danych osobowych, z której wstępem należy się zapoznać przed przeczytaniem niniejszego dokumentu.

Dokument ten odnosi się całościowo do problemu zabezpieczenia danych osobowych w III LO tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych. Wskazuje działania, jakie należy wykonać oraz ustanawia zasady i reguły postępowania, które należy stosować, aby właściwie zabezpieczyć dane osobowe.

1. OŚWIADCZENIE O INTENCJACH KIEROWNICTWA

W celu realizacji postanowień dokumentacji ochrony danych osobowych Dyrektor III LO dołoży wszelkich starań i zapewni:

- niezbędne środki finansowe, prawidłowe wyposażenie i zabezpieczenie stanowisk i narzędzi pracy;
- odpowiedni poziom procedur, konieczne szkolenia pracowników, uświadamianie w dziedzinie bezpieczeństwa informacji;
- odpowiednie zabezpieczenia pomieszczeń i systemu informatycznego.

Zasady i standardy określone w dokumentacji muszą być stosowane przez wszystkich pracowników III LO (również osoby nie mające bezpośredniego dostępu do danych jak np. osoby pilnujące porządku, sprzątające), dlatego każdy pracownik zobligowany jest do zapoznania się z dokumentacją i bezwzględne przestrzeganie zasad w niej zawartych.

Mając świadomość, iż żadne zabezpieczenie techniczne nie gwarantuje 100%-towej szczelności systemu konieczne jest, aby każdy pracownik był pełen świadomej odpowiedzialności, postępował zgodnie z przyjętymi zasadami i minimalizował zagrożenia wynikające z błędów ludzkich.

W przypadku naruszenia bezpieczeństwa informacji stosuje się procedury postępowania stworzone dla takiej sytuacji, a pracownicy ponoszą odpowiedzialność dyscyplinarną i prawną wynikającą z przepisów prawa, Kodeksu Cywilnego oraz Kodeksu Pracy.

2. ANALIZY, REJESTRY I EWIDENCJE PROWADZONE PRZEZ ADO

W celu odpowiedniego zabezpieczenia i rozliczalności ochrony danych osobowych prowadzi się w formie papierowej lub elektronicznej:

- rejestr czynności przetwarzania danych osobowych oraz analizę ryzyka;
- rejestr naruszeń ochrony danych osobowych;
- ewidencję osób upoważnionych do przetwarzania danych osobowych;
- ewidencję zapoznania się z niniejszą dokumentacją;
- ewidencję dostępów do systemów informatycznych;
- ewidencję podmiotów przetwarzających powierzone dane osobowe.

ADO może wyznaczyć osobę odpowiedzialną za prowadzenie poszczególnych rejestrów i ewidencji.

ADO na bieżąco analizuje ocenę skutków dla ochrony danych, ocenę ryzyka naruszenia praw i wolności osoby fizycznej oraz zabezpieczenia związane z ochroną danych osobowych zbiorów tradycyjnych i systemów informatycznych.

3. OKREŚLENIE ŚRODKÓW ORGANIZACYJNYCH

W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych, wprowadza się następujące środki organizacyjne:

- urządzenia w systemie informatycznym III LO są połączone do sieci publicznej, w związku z tym ADO stosuje środki bezpieczeństwa na poziomie wysokim;
- przetwarzanie danych osobowych może odbywać się wyłącznie w ramach wykonywania zadań służbowych;
- zakres uprawnień do przetwarzania danych osobowych wynika z zakresu zadań służbowych;
- do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie, natomiast osoby przebywające w pomieszczeniach gdzie przetwarzane są dane osobowe, powinny mieć na to zgodę; podpisane upoważnienie lub zgoda dołączane jest do akt osobowych; wzór upoważnienia i zgody stanowią załączniki nr 1 i 2 do niniejszej dokumentacji; wydanie nowego upoważnienia/zgody unieważnia automatycznie poprzednio wydane;
- każdy pracownik podpisuje oświadczenie o zobowiązaniu się do zachowania poufności; wzór oświadczenia stanowi załącznik nr 3 do niniejszej dokumentacji;
- prowadzona jest ewidencja osób upoważnionych do przetwarzania danych oraz mających zgodę na przybywanie w miejscu przetwarzania danych;
- prowadzona jest ewidencja zapoznania się osób upoważnionych z niniejszą dokumentacją;
- obszar przetwarzania danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych; klucze do pomieszczeń przechowywane i wydawane są zgodnie z instrukcją przechowywania i wydawania kluczy;
- przebywanie osób nieuprawnionych w w/w obszarze jest dopuszczalne za zgodą ADO lub w obecności osoby upoważnionej do przetwarzania danych osobowych;
- przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach;
- pomieszczenia w których przetwarza się dane osobowe zamykane są na klucz;
- zabrania się gromadzenia lub tworzenia odrębnych zbiorów danych osobowych poza zbiorami zgodnie z prowadzonym rejestrem czynności przetwarzania - w szczególności w podręcznej dokumentacji;
- wszelkie podręczne wydruki lub zestawienia, w których występują dane osobowe powinny być zminimalizowane do niezbędnych informacji, a po użyciu trwale zniszczone lub zanonimizowane (usunięte dane osobowe jak np. pesel, adres);
- niepotrzebne dokumenty lub dokumenty po ustaniu ich przydatności zawierające dane osobowe powinny być niszczone w sposób uniemożliwiający ich odczytanie;
- monitory komputerów, na których przetwarzane są dane osobowe powinny być ustawione w sposób uniemożliwiający odczytanie tych danych osobom trzecim;
- wszelki dostęp do danych osobowych zapisanych elektronicznie oraz dostęp do systemów komputerowych powinien odbywać się poprzez logowanie z użyciem osobistych loginów i haseł;
- zbiory danych osobowych przechowywane elektronicznie powinny być zabezpieczone poprzez regularne wykonywanie kopii bezpieczeństwa;
- wszelkie dokumenty elektroniczne zawierające dane osobowe, które są wynoszone lub przesyłane poza obszar przetwarzania danych powinny być zabezpieczone hasłem odczytu lub zaszyfrowane;
- szczegółowe zasady postępowania ze zbiorami przetwarzanymi elektronicznie określa Instrukcja Zarządzania Systemem Informatycznym, która jest częścią dokumentacji;
- zasady korzystania z komputerów służbowych oraz z zasobów informatycznych, w tym sieci internet określa odrębny regulamin korzystania z zasobów informatycznych III LO;

4. OKREŚLENIE ŚRODKÓW TECHNICZNYCH

Środki techniczne niezbędne dla zapewnienia poufności, bezpieczeństwa, integralności, rozliczalności i niezawodności przetwarzanych danych:

- budynek III LO zabezpieczony jest alarmem oraz monitoringiem wizyjnym; całodobowy dozór ochrony pełni zewnętrzna firma ochroniarska;
- budynek wyposażony jest w wolnostojące gaśnice przeciwpożarowe, które powinny być w miejscach ogólnie dostępnych, w szczególności w miejscach w których przechowywane są dane osobowe;
- obszary przechowywania i przetwarzania danych zabezpiecza się przed fizycznym dostępem poprzez zamki w drzwiach, a także przestrzeganie procedur spraw porządkowych oraz postępowania z kluczami;s
- komputery na których przetwarza się dane osobowe zaopatrzone są w licencjonowane programy i okresowo sprawdzane pod kątem poprawności ich instalacji i aktualizacji;
- system informatyczny zabezpieczony jest poprzez nadanie haseł uprawnionym użytkownikom a także poprzez sporządzanie kopii bezpieczeństwa danych na nośnikach magnetycznych i optycznych oraz wydrukach komputerowych;
- zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego;
- wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbiorów danych osobowych;
- system informatyczny zabezpieczony jest oprogramowaniem antywirusowym zarządzanym centralnie, umożliwiającym w łatwy sposób diagnozowanie poprawności aktualizacji oraz występujących problemów;
- zastosowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe;
- komputery, które służą do przechowywania i przetwarzania danych osobowych, za wyjątkiem komputerów służących przede wszystkim do odczytu powinny być zabezpieczone w urządzenia podtrzymujące napięcie na wypadek braku zasilania;
- dostęp z sieci publicznej do sieci wewnętrznej zabezpieczony jest systemem typu firewall na głównym urządzeniu dostępowym z sieci publicznej w celu ochrony zagrożeń z zewnątrz, próby nieuprawnionego dostępu są logowane;
- dostęp z sieci do komputerów lokalnych zabezpieczony jest oprogramowaniem typu firewall;
- zbiory danych w postaci tradycyjnej umieszczane są w szafach zamykanych na klucz;
- zbiory danych w postaci tradycyjnej, zawierające dane osobowe mające istotne znaczenie dla ochrony danych osoby fizycznej umieszczane są w szafach metalowych lub sejfach;
- archiwalne bazy danych znajdują się w składnicy akt szkoły; klucze do składnicy akt posiadają uprawnieni pracownicy.

5. POLITYKA PRYWATNOŚCI NA STRONIE INTERNETOWEJ III LO

W celu zapewnienia bezpieczeństwa danych osobowych osób korzystających z serwisów internetowych III LO, stworzona została polityka prywatności.

Polityka prywatności jest zamieszczona na stronach www placówki.

6. ZASADY POSTĘPOWANIA PRZY PRZETWARZANIU DANYCH OSOBOWYCH

Każdy pracownik działający z upoważnienia administratora i mający dostęp do danych osobowych przetwarza je wyłącznie na polecenie administratora i w zakresie jaki został wskazany w upoważnieniu.

Osoby upoważnione zobowiązane są do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczeń. Obowiązek ten istnieje również po ustaniu stosunku pracy.

Każdy pracownik, który dokonuje czynności związane z przetwarzaniem danych osobowych zobligowany jest stosować się do niniejszej dokumentacji oraz ponosi odpowiedzialność za bezpieczeństwo przetwarzania danych osobowych.

Wynoszenie poza placówkę dokumentów zawierających dane osobowe w formie papierowej oraz cyfrowej jest surowo zabronione z wykluczeniem sytuacji związanych z wykonywaniem czynności służbowych oraz zastosowaniem odpowiednich zabezpieczeń.

Pracownik korzystający z systemu informatycznego zobowiązany jest do przestrzegania Instrukcji Zarządzania Systemem Informatycznym, która jest częścią niniejszej dokumentacji oraz wskazówek zawartych w instrukcji obsługi urządzeń, oprogramowania i nośników.

7. PROCEDURY PRZEKAZYWANIA DANYCH PODMIOTOM TRZECIM

Administrator Danych może przekazywać w szczególnych przypadkach przetwarzanie danych osobowych zewnętrznym podmiotom, instytucjom, organizacjom, placówkom tylko i wyłącznie w konkretnym i sprecyzowanym celu oraz na podstawie przepisów prawa, które umożliwia przetwarzanie danych osobowych w tym celu.

ADO może korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi przepisów prawa i chroniło prawa osób, których dane dotyczą.

Powierzenie danych musi być potwierdzone umową powierzenia, która zawiera cel przekazania, zakres danych, kategorię osób oraz czas planowanego przetwarzania danych przez podmiot przetwarzający.

ADO prowadzi rejestr podmiotów, którym powierzył przetwarzanie danych.

8. ZAPEWNIENIE DOKUMENTACJI I CIĄGŁOŚCI DOSKONALENIA ZABEZPIECZEŃ

Mając na uwadze złożoność problemu stosowania zabezpieczeń ADO dołoży wszelkich starań aby należycie wykonać zadania związane z ochroną danych osobowych.

Najważniejsze czynniki wpływające na złożoność problemu to:

- asymetria działań mających na celu zabezpieczenie systemu - polega ona tym, że aby skutecznie zabezpieczyć system należy usunąć wszystkie słabości, podczas gdy wystarczy znaleźć jedną, aby skutecznie system został zaatakowany;
- zależność od otoczenia - wpływ całego otoczenia systemu i środowiska informatycznego na bezpieczeństwo, w którym dany system/program przetwarzania danych funkcjonuje;
- ciągłość działania - wymóg permanentnego monitorowania i aktualizowania zastosowanych środków bezpieczeństwa. Jakakolwiek zmiana struktury systemu czy też dodanie nowych usług każdorazowo wymaga jego weryfikacji pod względem zagrożeń i ryzyka, na jakie przetwarzane dane mogą być narażone i tym samym - weryfikacji zastosowanych środków bezpieczeństwa.

9. ZADANIA INSPEKTORA OCHRONY DANYCH

Zgodnie z przepisami prawa ADO powinien powołać Inspektora Ochrony Danych. Do głównych zadań IOD należy:

- informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów prawa oraz wewnętrznych procedur;
- doradzanie i szkolenia pracowników w zakresie upowszechniania i doskonalenia wiedzy z zakresu ochrony danych osobowych;
- monitorowanie przestrzegania przepisów prawa oraz wewnętrznych procedur w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
- współpraca z organem nadzorczym;
- nadzorowanie opracowania i aktualizowania dokumentacji ochrony danych;
- pomoc w prowadzeniu rejestru czynności przetwarzania danych osobowych oraz innych rejestrów i ewidencji;
- monitorowanie działań i skuteczności zabezpieczeń wdrożonych w celu ochrony danych osobowych.

10. ZADANIA ADMINISTRATORA SYSTEMU INFORMATYCZEGO

ADO może powołać Administratora Systemu Informatycznego. W takim przypadku do jego głównych zadań należy m.in.:

- zarządzanie systemem informatycznym przetwarzającym dane;
- opracowywanie wykazu użytkowanego oprogramowania, jego konserwacja oraz uaktualnianie;
- prowadzenie monitoringu przetwarzania danych osobowych;
- nadawanie uprawnień użytkowników i prowadzenie aktualnego rejestru;
- kontrola mechanizmów uwierzytelnienia użytkowników;
- kontrola wykonywania kopii bezpieczeństwa;
- kontrola systemu antywirusowego i firewall;
- informowanie Administratora danych o wszelkich próbach złamania zabezpieczeń, awariach programów czy niewłaściwego wykorzystania sprzętu.

W przypadku niepowołania Administratora Systemu Informatycznego, powyższe zadania odwołują się do Administratora Danych Osobowych.

11. POSTĘPOWANIE W PRZYPADKU NARUSZENIA ZASAD BEZPIECZEŃSTWA

Użytkownik zobowiązany jest do niezwłocznego powiadamiania bezpośredniego przełożonego, ASI, ADO lub IOD o wszelkich wykrytych lub podejrzewanych słabościach systemu, zagrożeniach z nimi związanych oraz o wszelkich innych incydentach, a w szczególności:

- stwierdzenia włamania i/lub kradzieży sprzętu lub nośników zawierających dane;
- stwierdzenia zaginięcia nośnika zawierającego dane (wydruku, kopii bezpieczeństwa, itp.);
- stwierdzenia lub podejrzenia nieuprawnionego dostępu do pomieszczeń, gdzie są przetwarzane dane lub do systemu informatycznego;

- stwierdzenia nieuzasadnionej modyfikacji, utraty danych lub niezgodności w danych (np. utraty plików na dysku komputera, braku lub nadmiaru danych);
- znalezienia poza pomieszczeniami przetwarzania wszelkich dokumentów, wydruków, dyskietek i innych nośników danych;
- przesłania danych lub informacji dotyczących danych lub polityki bezpieczeństwa do niewłaściwego miejsca lub adresata;
- wszelkich awarii systemu informatycznego (sprzętu lub oprogramowania);
- nietypowego działania systemu informatycznego, np. braku połączenia szyfrowanego przy uwierzytelnianiu się przez przeglądarkę internetową;
- nietypowych komunikatów wyświetlanych na ekranie monitora;
- obecności podejrzanych plików w poczcie elektronicznej;
- obecności podejrzanych urządzeń w pobliżu komputera, np. kamer, mikrofonów, urządzeń wpiętych w porty usb;
- wykrycia wirusa w systemie.

Po stwierdzeniu wystąpienia lub podejrzeniu wystąpienia incydentu naruszenia bezpieczeństwa informacji użytkownik powinien:

- niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców;
- rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia;
- zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę;
- powstrzymać się od wszelkich czynności w pomieszczeniu przetwarzania mogących zatrzeć ślady naruszenia bezpieczeństwa informacji;
- zastosować się do poleceń ADO, IOD lub ASI;
- zwrócić uwagę, aby nie porzucać, wyrzucać do śmieci, niszczyć lub sprawdzać zawartości znalezionych nośników danych;
- sporządzić notatkę o zdarzeniu i przekazać ją ASO lub IOD.

Użytkownik posiadający tylko informacje mogące mieć wpływ na bezpieczeństwo danych osobowych również zobowiązany jest niezwłocznie zgłosić ten fakt ADO lub IOD.

ADO wraz z IOD po zgłoszeniu naruszenia zasad bezpieczeństwa lub incydentu dokonuje:

- analizy sytuacji oraz konsekwencji naruszenia dóbr osobistych osób fizycznych, których dotyczy naruszenie;
- podejmuje odpowiednie kroki zabezpieczające dane osobowe oraz minimalizujące negatywne skutki naruszenia dóbr osobistych osób fizycznych, których dotyczy naruszenie;
- w przypadku poważnego naruszenia dokonuje oceny konieczności powiadomienia osób fizycznych których dane dotyczą oraz Prezesa Urzędu Ochrony Danych o fakcie i zakresie naruszenia przepisów;
- udokumentowuje zaistniały przypadek i sporządza raport.

Po sporządzeniu raportu IOD przygotowuje dokument procesów naprawczych, określa możliwości techniczne związane z ewentualnym odtworzeniem danych z kopii zapasowych, jak również zarządza w jakim terminie nastąpi wznowienie procesu przetwarzania danych.

Za incydentalne naruszenie przepisów o ochronie danych osobowych uznaje się pojedyncze zdarzenie lub serię niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań placówki i zagrażają bezpieczeństwu informacji, czyli:

- nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł itd.);
- niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;

- nieodpowiednie zabezpieczenie sprzętu IT czy oprogramowania przed wyciekiem lub utratą danych osobowych.

Za wysokie naruszenie przepisów o ochronie danych osobowych uznaje się takie naruszenie, które ma związek z naruszeniem dóbr osobistych, które są pod ochroną prawa cywilnego, w szczególności: zdrowie, wolność, swoboda sumienia, dane personalne, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska oraz dotyczy wielu osób.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W III LICEUM OGÓLNOKSZTAŁCĄCYM IM. MIKOŁAJA KOPERNIKA 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 III 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 III 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 III 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.

DYREKTOR
mgr Anna Narewska
Podpis dyrektora

……..
(pieczątka podmiotu)

Kalisz, dn……..

Upoważnienie Nr……...
w zakresie przetwarzania danych osobowych
w III Liceum Ogólnokształcącym im. Mikołaja Kopernika w Kaliszu

Na podstawie Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27.04.2016 r

upoważniam Panią/Pana ……..……..
do przetwarzania danych osobowych gromadzonych i przetwarzanych w III Liceum Ogólnokształcącym im. Mikołaja Kopernika w Kaliszu w zakresie Pani/Pana obowiązków i uprawnień, tj:

Czynności objęte zakresem upoważnienia:

……..……..……

Równocześnie zobowiązuję Panią/Pana do zapoznania się z wewnętrzną dokumentacją ochrony danych osobowych oraz zachowania w tajemnicy wszelkich informacji dotyczących przetwarzania danych osobowych oraz sposobu ich zabezpieczenia.

Informuję, że w przypadku naruszenia bezpieczeństwa informacji stosuje się procedury postępowania stworzone dla takiej sytuacji, a pracownicy ponoszą odpowiedzialność dyscyplinarną i prawną zgodnie z przepisami prawa o ochronie danych osobowych oraz Kodeksem Cywilnym.

Upoważnienie jest ważne od dnia …….. do odwołania.

Upoważnienie wygasa natychmiast z chwilą rozwiązania umowy o pracę.

Zachowanie tajemnicy obowiązuje również po ustaniu stosunku pracy.

…….
(data i podpis upoważnionego)

……..…
(data i podpis administratora danych)

…….. Kalisz, dn.: ……
(pieczątka podmiotu)

Zgoda Nr ….
na przebywanie w obszarze przetwarzania/przechowywania danych w III Liceum Ogólnokształcącym im. Mikołaja Kopernika w Kaliszu

Na podstawie Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27.04.2016r

upoważniam Pana/Panią **……..……** do przebywania w pomieszczeniach, w których przetwarzane i/lub przechowywane są dane osobowe w III Liceum Ogólnokształcącym im. Mikołaja Kopernika w Kaliszu w zakresie Pana/Pani obowiązków i uprawnień.

Równocześnie zobowiązuję Panią/Pana do zapoznania się z wewnętrzną dokumentacją ochrony danych osobowych oraz zachowania w tajemnicy wszelkich informacji dotyczących przetwarzania danych osobowych oraz sposobu ich zabezpieczenia.

Informuję, że w przypadku naruszenia bezpieczeństwa informacji stosuje się procedury postępowania stworzone dla takiej sytuacji, a pracownicy ponoszą odpowiedzialność dyscyplinarną i prawną zgodnie z przepisami prawa o ochronie danych osobowych oraz Kodeksem Cywilnym.

Zgoda jest ważne od dnia …….. do odwołania.

Zgoda wygasa natychmiast z chwilą rozwiązania umowy o pracę.

Zachowanie tajemnicy obowiązuje również po ustaniu stosunku pracy.

…… ……..…
(data i podpis upoważnionego) (data i podpis administratora danych)

Kalisz, dn……..

Oświadczenie pracownika o zobowiązaniu się do zachowania poufności

Ja niżej podpisana/y ……

zatrudniona/y na stanowisku ……..……

zobowiązuję się zachować w tajemnicy informacje uzyskane w związku z powierzonymi mi obowiązkami. Uzyskane informacje zachowam w poufności zarówno w trakcie zatrudnienia, jak i po jego ustaniu.

Świadoma/y jestem obowiązku ochrony danych osobowych na zajmowanym stanowisku i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu zatrudnienia.

……..……..
Podpis