Liceum Ogólnokształcące Nr III im. Juliusza Słowackiego w Otwocku
ul. Słowackiego 4/10
05-400 Otwock

# Polityka ochrony danych osobowych w systemach informatycznych

# Liceum Ogólnokształcące Nr III im. Juliusza Słowackiego w Otwocku

**REJESTR ZMIAN W DOKUMENCIE:**

| Data [RRRR-MM-DD] | Autor | Wersja | Opis zmian |
|---|---|---|---|
| | Piotr Eisenmann<br>z upoważnienia<br>IOD Pawła Maliszewskiego<br>PERFECTINFO SP. Z O. O. | 1.0 | Wersja inicjalna dokumentu |

**AKCEPTACJA DOKUMENTU**

| Data [RRRR-MM-DD] | Osoba akceptująca | Zaakceptowana wersja |
|---|---|---|
| 2026.10.26 | DYREKTOR Liceum Ogólnokształcącego Nr III im. J. Słowackiego w Otwocku<br>mgr Barbara Laskus | |

Niniejszy dokument jest własnością **Liceum Ogólnokształcące Nr III im. Juliusza Słowackiego w Otwocku** i nie może być przedrukowywany ani kopiowany bez zgody **Dyrektora**. Dokument ten jest aktualny i podlega nadzorowi ADO i IOD.

## Spis treści


1. 4
2. 4
3. 4
4. 4
   4.1. 5
5. 5
6. 6
7. 7
   7.1. 7
   7.2. **Błąd! Nie zdefiniowano zakładki.**
   7.3. **Błąd! Nie zdefiniowano zakładki.**
   7.4. **Błąd! Nie zdefiniowano zakładki.**
8. 8
9. 9
10. 9
11. 11
12. 12
13. 12
14. 12
15. 13

## 1. Zakres stosowania dokumentu

Polityka Ochrony Danych Osobowych w Systemach Informatycznych (dalej jako „Polityka") określa zasady zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, a w szczególności: sposób rejestrowania i wyrejestrowania użytkownika, sposób przydzielania haseł i zasady korzystania z nich, procedury rozpoczęcia i zakończenia pracy, obowiązki użytkowników, metody i częstotliwość tworzenia kopii zapasowych, zasady sprawdzania obecności złośliwego oprogramowania oraz dokonywania przeglądów i konserwacji systemu.
Polityka przeznaczona jest dla informatyków i użytkowników systemów informatycznych zainstalowanych w Liceum Ogólnokształcącym Nr III im. Juliusza Słowackiego w Otwocku (dalej jako **„Liceum"**), którzy wykorzystują te systemy w ramach wykonywania swoich obowiązków służbowych.

## 2. Definicje i skróty

Zastosowane w niniejszej Polityce pojęcia i skróty należy interpretować zgodnie z ich definicjami zawartymi w Polityce Bezpieczeństwa Danych Osobowych.

## 3. Wymagania dotyczące sprzętu i oprogramowania

1. Sprzęt obsługujący procesy związane z przetwarzaniem danych osobowych składa się ze stacji roboczej o parametrach technicznych zapewniających sprawne i bezawaryjne przetwarzanie danych.
2. Oprogramowanie zainstalowane na stacjach roboczych przetwarzających dane osobowe jest użytkowane z zachowaniem praw autorskich i posiada aktualne licencje.
3. Oprogramowanie sprzętu obsługującego przetwarzanie danych osobowych jest instalowane wyłącznie przez upoważnione osoby.
4. Nadzór nad przestrzeganiem powyższych wymogów sprawuje Informatyk. Dokonuje on również okresowych kontroli.
5. Za konfigurację systemów operacyjnych i aplikacji służących do przetwarzania danych osobowych zapewniającą ochronę danych i stosowanie mechanizmów uwierzytelniania Użytkowników, odpowiada Informatyk.
6. Oprogramowanie zainstalowane na stacjach roboczych przetwarzających dane osobowe posiada zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.
7. Konieczne jest bieżące utrzymywanie oprogramowania, w tym systemów operacyjnych i aplikacji, w najnowszych wspieranych wersjach dostępnych aktualizacji. W miarę możliwości należy stosować mechanizmy automatycznej aktualizacji, w celu zapewnienia niezwłocznego eliminowania znanych podatności oraz podniesienia poziomu bezpieczeństwa systemów. W przypadku wdrożenia mechanizmów automatycznej aktualizacji, należy również wprowadzić testowanie aktualizacji przed zainstalowaniem jej w środowiskach produkcyjnych.

## 4. Procedury nadawania uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

Do przetwarzania danych osobowych zgromadzonych w Liceum Ogólnokształcącym Nr III im. Juliusza Słowackiego w Otwocku mogą być dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych wydane przez ADO.

Przydział uprawnień odbywa się zgodnie z zasadą minimalnych koniecznych uprawnień (least privilege principle), co oznacza, że Użytkownik otrzymuje dostęp tylko do tych danych i funkcji, które są niezbędne do wykonywania obowiązków służbowych.

### 4.1. Podstawowe wymagania stawiane Użytkownikom

1. Każdy Użytkownik systemu informatycznego przetwarzającego dane osobowe posiada umiejętność bezpiecznej obsługi danego systemu informatycznego i urządzenia oraz dobrą znajomość oprogramowania, z którego będzie korzystał.
2. W przypadku niewystarczających kwalifikacji określonych w pkt 1, przed dopuszczeniem do obsługi systemu informatycznego przetwarzającego dane osobowe, nowo zatrudnieni pracownicy lub powracający po długotrwałej nieobecności podlegają przeszkoleniu uzupełniającemu w zakresie:
   a. obsługi systemu informatycznego przetwarzającego dane osobowe, który będą wykorzystywali;
   b. bezpiecznej obsługi urządzeń i oprogramowania systemowego w zakresie niezbędnym do użytkowania systemu informatycznego przetwarzającego dane osobowe;
   c. przepisów o ochronie danych osobowych, zadań i obowiązków wynikających z tych przepisów oraz odpowiedzialności za ochronę danych osobowych.

## 5. Rejestrowanie i wyrejestrowanie Użytkowników

1. Nadanie, modyfikację lub cofnięcie uprawnień do pracy w systemie informatycznym realizuje Informatyk.
2. Liceum stosuje różne metody rejestrowania/wyrejestrowania Użytkowników. Podstawowe stosowane narzędzia to:
   a. przyznanie uprawnień w zakresie dostępu do systemu informatycznego polegające na wprowadzeniu do systemu dla każdego Użytkownika unikalnego identyfikatora, hasła oraz ustanowieniu zakresu dostępnych danych i operacji.
   b. uwierzytelnianie Użytkowników odbywające się na podstawie kont zaimplementowanych w systemie informatycznym — mogą to być konta lokalne lub konta zarządzane centralnie (np. poprzez Active Directory, LDAP lub usługę federacyjną). Konto użytkownika jest zakładane przez Informatyka zgodnie z dyspozycją ADO lub innej osoby upoważnionej. Po nadaniu unikalnego identyfikatora i przypisaniu odpowiednich uprawnień, Użytkownik otrzymuje hasło startowe (jeżeli dany system przewiduje jego stosowanie). Hasło to powinno być zmienione przez Użytkownika przy pierwszym logowaniu, o ile nie obowiązuje inny mechanizm inicjalizacji dostępu.
3. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło. W przypadku konta mailowego Informatyk może ustawić autoodpowiedź (autoresponder). Skrzynka mailowa jest dla Użytkownika w tym czasie blokowana – opcja uniemożliwiająca odbieranie i wysyłanie maili. W razie potrzeby Informatyk może ustawić przekierowanie na dowolne, wskazane według potrzeb adresy e-mail, które posiada Liceum.
4. Konta użytkowników, którzy utracili uprawnienia dostępu do systemu są blokowane przez Informatyka.
5. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych nie może zostać przydzielony innej osobie. Nie dotyczy to adresów mailowych typu biuro@, sekretariat@ itp.
6. W przypadku zagubienia identyfikatora lub hasła przez Użytkownika Informatyk resetuje stare hasło i podaje Użytkownikowi nowe.
7. Zmiana zakresu uprawnień Użytkowników do systemów informatycznych odbywa się analogicznie do procesu nadawania im uprawnień.

## 6. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Do uwierzytelniania się w systemie, Użytkownik wykorzystuje identyfikator i hasło. Dla zabezpieczenia mogą być również stosowane protokoły uwierzytelnienia federacyjnego (SSO), inteligentne karty kryptograficzne, tokeny lub certyfikaty oparte na standardzie X.509 (PKI).
2. Zaleca się stosowanie uwierzytelniania wieloskładnikowego (MFA) do wszystkich systemów przetwarzających dane osobowe, szczególnie tych dostępnych zdalnie.
3. Identyfikator nadany Użytkownikowi powinien być nie krótszy niż 6 znaków i nadawany według ustalonego wewnętrznie systemu pozwalającego na jednoznaczne połączenie Użytkownika z jego identyfikatorem wykorzystywanym w systemach.
4. Identyfikator użytkownika nie powinien być zmieniany, niedopuszczalne jest przydzielenie go innemu Użytkownikowi. *Nie dotyczy to funkcyjnych adresów mailowych, np.: sekretariat@lo3otwock.eu.*
5. Jeżeli system informatyczny posiada takie możliwości, zmiana pierwszego hasła (nadanego przez informatyka) powinna być wymuszona przez system przy pierwszym logowaniu Użytkownika.
6. Hasło używane przez Użytkownika do uwierzytelnienia się w systemie powinno składać się z co najmniej **12 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne**, lub posiadać równoważną siłę kryptograficzną.
7. Zasady użytkowania haseł:
   a. hasło użytkownika wprowadzane **podczas logowania do systemu jest maskowane** (niewidoczne na ekranie),
   b. Użytkownik ma obowiązek zmiany hasła przed upływem terminu ważności lub gdy system informatyczny żąda zmiany hasła,
   c. Użytkownik ma obowiązek stosować zasady bezpieczeństwa podczas logowania, jak i procesu aktualizacji haseł uniemożliwiające kompromitację jego haseł (poznanie hasła przez osobę bez upoważnienia),
   d. jeżeli Użytkownik ma podejrzenia co do odkrycia jego hasła przez osobę nieupoważnioną, niezwłocznie zmienia hasło **i informuje o tym fakcie ADO,**
   e. Użytkownik zobowiązany jest do zachowania w tajemnicy własnego hasła, również po upływie jego ważności,
   f. zabronione jest odnotowywanie haseł, jak również przechowywanie ich w formie zapisów tradycyjnych (papier), dopuszczalne jest przechowywanie haseł na stacji roboczej użytkownika z zastosowaniem programu szyfrującego do przechowywania haseł (np. KeePass),
   g. zabronione jest przekazywanie danych dotyczących logowania innym osobom.
8. Postępowanie z Użytkownikami uprzywilejowanymi
   a. Do Użytkowników Uprzywilejowanych zalicza się:
      i. Użytkowników posiadających w systemie informatycznym przetwarzającym dane osobowe uprawnienia administratora tego systemu,
      ii. Użytkowników posiadających uprawnienia administratora systemu operacyjnego, na którym działa system, w którym przetwarzane są dane osobowe,
      iii. Użytkowników posiadających uprawnienia administratora w urządzeniach infrastruktury technicznej, w ramach których pracują systemy informatyczne używane do przetwarzania danych osobowych

b. Hasła użytkowników uprzywilejowanych mogą być przechowywane w programie szyfrującym zainstalowanym na zdalnym pulpicie Administratora (na serwerze wewnętrznym) lub innym bezpiecznym miejscu. Hasło dostępowe do programu szyfrującego zna ADO.
c. Hasła użytkowników uprzywilejowanych przechowywane w postaci jawnej tzn. zapisane w formie papierowej podlegają szczególnej ochronie i powinny być przechowywane w postaci bezpiecznej w opieczętowanej kopercie (lub bezpiecznej kopercie), w miejscu wyznaczonym przez ADO np. w sejfie.
d. Hasła użytkowników uprzywilejowanych zmieniane są nie rzadziej niż raz w roku oraz każdorazowo w przypadku podejrzenia ich ujawnienia osobom nieupoważnionym lub częściej wedle bieżących potrzeb.

# 7. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla Użytkowników systemu

## 7.1. Rozpoczęcie pracy w systemie

1. Przed rozpoczęciem przetwarzania danych w systemie informatycznym, należy sprawdzić czy urządzenia służące do przetwarzania danych osobowych nie wskazują na ingerencję innych osób oraz czy stanowisko pracy zastano w takim stanie jak pozostawiono po zakończeniu pracy.
2. Wszelkie zauważone nieprawidłowości należy bezzwłocznie zgłaszać do ADO i Informatyka.
3. Rozpoczynając pracę na stacji roboczej Użytkownik loguje się do systemu informatycznego, w którym przetwarzane są dane osobowe posługując się swoim identyfikatorem i hasłem.
4. Użytkownik upoważniony przez ADO do przetwarzania danych osobowych zobowiązany jest do pracy zgodnie z przydzielonym mu identyfikatorem. Niedopuszczalne jest udostępnianie swojego identyfikatora do pracy innym Użytkownikom.
5. Użytkownik zobowiązany jest niezwłocznie zgłosić do ADO i Informatyka wszelkie odstępstwa od procedury logowania się i uwierzytelnienia, a w szczególności:
   a. zablokowanie dostępu do swojego konta pomimo wprowadzania poprawnego identyfikatora i hasła,
   b. stwierdzenia niekompletności lub niepoprawności zgromadzonych w bazie danych osobowych,
   c. stwierdzenia fizycznej ingerencji w system informatyczny służący do przetwarzania danych osobowych lub system operacyjny zainstalowany na stacji roboczej.
6. Użytkownik systemu informatycznego, przy którego stacji roboczej zainstalowano urządzenia zabezpieczające przed awarią zasilania lub zakłóceniami sieci energetycznej powinien stosować te urządzenia.

## 7.2. Zasady zabezpieczenia systemu przed dostępem osób nieuprawnionych

1. Użytkownik powinien dopilnować, aby w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, osoby nieupoważnione przebywały tylko za zgodą przełożonych i w obecności osób uprawnionych.
2. W sytuacji, gdy Użytkownik jest nieobecny, zastępująca go osoba, korzystając z jego stacji roboczej, loguje się do systemu za pomocą własnego identyfikatora i hasła.
3. Ekrany monitorów powinny być ustawione w taki sposób, aby uniemożliwić odczyt wyświetlanych informacji osobom nieupoważnionym.

4. Wydruki z systemu zawierające dane osobowe powinny być przechowywane w szafach do których dostęp mają tylko osoby upoważnione do przetwarzania danych osobowych, a wydruki błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru.
5. Dokumenty zdezaktualizowane i zbędne mogą być niszczone przez firmę zewnętrzną.
6. Przy przesyłaniu danych osobowych pocztą elektroniczną należy rozważyć konieczność ich zaszyfrowania i zabezpieczenia hasłem pliku załącznika. Hasło należy przekazać drogą telefoniczną lub za pomocą wiadomości SMS.
7. Obowiązuje zakaz używania przenośnych stacji roboczych przez osoby inne niż Użytkownicy, którym zostały one powierzone, w tym przez domowników i osoby bliskie Użytkownikowi.

### 7.3. Zawieszenie pracy

1. Podczas przerwy w pracy zarówno zaplanowanej, jak i niezaplanowanej, obowiązkiem Użytkownika jest zabezpieczenie stanowiska pracy, jak również stacji roboczych przed dostępem osób nieuprawnionych.
2. Podczas przerwy trwającej dłużej niż 5 minut, Użytkownik ma obowiązek wylogowania się z aplikacji oraz zabezpieczenia systemu operacyjnego poprzez wylogowanie się z sesji lub zablokowanie konta użytkownika.
3. We wszystkich systemach operacyjnych na kontach użytkownika przetwarzających dane osobowe zainicjowano blokadę - uruchamianą bezczynnością systemu.

### 7.4. Zakończenie pracy w systemie

1. Po zakończeniu pracy Użytkownik zobowiązany jest do prawidłowego zamknięcia pracy w systemie informatycznym, w szczególności poprzez zakończenie rozpoczętych operacji, wylogowanie i wyrejestrowanie się z systemów informatycznych oraz wylogowanie z systemu operacyjnego. Ostatnim krokiem powinno być wyłączenie stacji roboczej.
2. Po zakończeniu pracy Użytkownik zobowiązany jest do zabezpieczenia stanowiska pracy, a w szczególności wszelkiej dokumentacji oraz nośników danych informatycznych, na których znajdują się dane osobowe i umieszczenia ich w meblach biurowych zamykanych na klucz bądź innym dedykowanym miejscu do przechowywania danych na nośnikach zewnętrznych.

## 8. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Systemem kopii zapasowych objęte są wszystkie serwery i jednostanowiskowe stacje zawierające dane osobowe. Obejmuje on wykonywanie kopii zapasowych oraz kopii archiwalnych.
2. Kopie zapasowe wykonuje się w celu zabezpieczenia danych i oprogramowania na wypadek awarii. Kopia zapasowa powinna umożliwić odtworzenie zbioru danych osobowych przetwarzanego w systemie.
3. Częstotliwość i metodę kopii zapasowej dla poszczególnych systemów określa Informatyk.
4. Za prawidłowe sporządzanie kopii zapasowych, przestrzeganie terminów ich wykonywania, oznakowanie i warunki ich przechowywania oraz przeprowadzanie okresowych kontroli odczytu tych kopii odpowiedzialny jest Informatyk lub Użytkownik danej stacji roboczej.
5. Zbiory zapisywane na nośnikach zewnętrznych są odpowiednio oznakowane i przechowywane w wyznaczonych, odpowiednio zabezpieczonych pomieszczeniach.
6. Kopiowanie danych osobowych na nośniki informacji lub w formie wydruku w innych celach niż wymienione w pkt 2 jest zabronione, chyba że istnieje konieczność ich sporządzania, która wynika z nałożonych na Użytkownika obowiązków i dozwolona jest przepisami prawa.

7. Kopia zapasowa z systemu informatycznego może być sporządzana na tradycyjnym nośniku danych, jeśli nie ma innej możliwości (np. w postaci papierowych wydruków). Taka kopia musi być przechowywana zgodnie z zasadami ochrony danych osobowych oraz ich kopii.

## 9. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe

1. Kopie zapasowe danych zapisane na elektronicznych nośnikach są przechowywane w miejscu zabezpieczonym przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem. Zalecane jest przechowywanie ich w dwóch różnych lokalizacjach geograficznych (jeśli jest taka możliwość).
2. Pomieszczenia, w których przechowywane są nośniki kopii spełniają warunki bezpieczeństwa stosownie do wartości przechowywanych na tych nośnikach danych.
3. Osoba odpowiedzialna za wykonywanie kopii na bieżąco weryfikuje stan przydatności wykorzystywanych nośników oraz utworzonej kopii bezpieczeństwa. Minimum raz w roku Informatyk testuje uruchomienie bazy danych z kopii bezpieczeństwa.
4. Po wykonaniu zarówno kopii danych, jak i kopii systemu (jeżeli dotyczy) nośniki trafiają niezwłocznie do sejfu/szafy.
5. Informatyk prowadzi ewidencję wykorzystywanych nośników zewnętrznych.
6. Nośniki oraz kopie zapasowe, które uległy uszkodzeniu lub zostały wycofane z eksploatacji podlegają komisyjnemu zniszczeniu.
7. Po upływie wymaganego okresu przechowywania danych lub ustaniu ich użyteczności decyzję o likwidacji archiwalnych danych osobowych podejmuje Informatyk, wyznaczając jednocześnie skład komisji likwidacyjnej.
8. Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów archiwalnych, komisja sporządza protokół, który w szczególności zawiera następujące informacje:
   a. data dokonania likwidacji,
   b. przedmiot likwidacji (typ nośnika),
   c. przedział czasowy likwidowanego archiwum lub typy kopii zapasowych,
   d. sposób zniszczenia nośnika lub zapisu na nim,
   e. podpisy osób dokonujących i obecnych przy likwidacji nośników.
9. Zapisy danych z nośników magnetycznych należy usunąć w sposób uniemożliwiający ich odczytanie, a w przypadku, gdy usunięcie danych nie jest możliwe, nośniki podlegają zniszczeniu w stopniu uniemożliwiającym dostęp do zawartych na nich danych.

## 10. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest nieuprawniony dostęp do systemu informatycznego

1. Ochronie przed uzyskaniem nieuprawnionego dostępu do systemu podlegają systemy informatyczne przetwarzające dane osobowe, bazy danych, systemy operacyjne i stacje robocze.
2. Ochrona i bezpieczeństwo danych osobowych uwzględniane są już przy początkowej fazie projektów informatycznych w obszarze ochrony danych osobowych (zgodnie z zasadą „Privacy by design").
3. Sprawdzanie obecności złośliwego oprogramowania w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania zainstalowanego na serwerach, stacjach roboczych przez Informatyka.

4. Oprogramowanie, o którym mowa w ppkt 3, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.
5. Źródłami przedostania się szkodliwego oprogramowania do systemu mogą być między innymi:
   a. Internet;
   b. poczta elektroniczna i jej załączniki;
   c. zewnętrzne nośniki informacji (np. pamięć typu flash, CD-ROM, DVD, dyski zewnętrzne).
6. Przez oprogramowanie, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, rozumie się wszelkie narzędzia informatyczne lub ich komponenty, których działanie ma na celu naruszenie poufności, integralności, dostępności lub rozliczalności systemu informatycznego, danych lub usług IT, w tym między innymi:
   a. **złośliwe oprogramowanie (malware)** – w szczególności wirusy, robaki, konie trojańskie, ransomware, spyware, adware, rootkity, keyloggery oraz inne programy instalujące się bez świadomej zgody użytkownika lub działające w sposób ukryty;
   b. **narzędzia wykorzystujące podatności (eksploity)** – oprogramowanie, skrypty i frameworki atakujące znane lub nieznane luki w systemach operacyjnych, aplikacjach, protokołach komunikacyjnych i urządzeniach sieciowych w celu uzyskania nieautoryzowanego dostępu, eskalacji uprawnień, wykonania kodu lub unieruchomienia systemu;
   c. **narzędzia do rozpoznania i analizy (pre-attack tooling)** – w szczególności skanery sieci i portów, sniffery, programy do przechwytywania danych (packet capture), analizatory ruchu, narzędzia do fingerprintingu, mapowania infrastruktury oraz inne używane w celu przygotowania ataku;
   d. **nowo pojawiające się formy zagrożeń (emerging threats)** – takie jak ataki oparte na sztucznej inteligencji, malware bezplikowy (fileless malware), oprogramowanie wykorzystywane w atakach typu supply chain, narzędzia automatyzujące phishing, social engineering, deepfake itp.
7. W celu ochrony systemów informatycznych przed działaniem wyżej wymienionego oprogramowania zakłada się stosowanie następujących zabezpieczeń:
   a. stosowanie bezpiecznych konfiguracji systemu – zasady ogólne dla wszystkich elementów systemu:
      i. wyłączenie nieużywanych usług systemu informatycznego,
      ii. instalacja aktualnych poprawek bezpieczeństwa,
      iii. stosowanie indywidualnych identyfikatorów i haseł w celu uwierzytelniania użytkowników,
      iv. ograniczenie uprawnień użytkowników do niezbędnego minimum,
      v. uaktywnienie logów systemowych.
   b. zabezpieczenia sieci informatycznej – stosowanie zapór ogniowych (z ang. Firewall);
   c. ochrona antywirusowa – stosowanie oprogramowania antywirusowego na serwerach i stacjach roboczych użytkowników w sieci wewnętrznej;
   d. zabezpieczenia przenośnych stacji roboczych:
      i. stosowanie haseł na BIOS,
      ii. stosowanie oprogramowania do kryptograficznego zabezpieczenia plików lub dysków z danymi;
   e. bieżąca aktualizacja sygnatur wirusów oraz poprawek i uaktualnień oprogramowania antywirusowego wykonuje się niezwłocznie po ich otrzymaniu;
   f. okresowe kontrole w zakresie instalowania aktualnych wersji oprogramowania antywirusowego oraz sprawdzania systemu pod kątem obecności wirusów przez wyznaczonych pracowników lub użytkowników systemu;

g. zapewnienie systematycznego przeprowadzania kopii zapasowych wszelkich nośników informacji, zawierających dane wrażliwe oraz dane niezbędne dla organizacji oraz upewnienie się, że dane te można odzyskać z utworzonych kopii zapasowych.

8. Niezależnie od ciągłego nadzoru, o którym mowa w ppkt 3, Informatyk nie rzadziej niż raz na tydzień przeprowadza kontrolę obecności złośliwego oprogramowania w systemie oraz jego zasobach, jak również w serwerach i stacjach roboczych.
9. Użytkownik jest obowiązany zawiadomić Informatyka o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.

## 11. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

1. Do dokonywania bieżących przeglądów danych osobowych pod kątem ich kompletności i poprawności obowiązani są użytkownicy, zgodnie z indywidualnymi zakresami obowiązków.
2. Do wykonywania systematycznych przeglądów systemów zobowiązany jest administrator danego systemu lub osoba przez niego upoważniona.
3. Dla zapewnienia wymaganego poziomu bezpieczeństwa przetwarzania danych osobowych oraz w celu zapewnienia Użytkownikom ciągłej i bezawaryjnej pracy należy przeprowadzać regularne przeglądy i konserwacje sprzętu informatycznego, systemów oraz oprogramowania.
4. Zakres prac i częstotliwość ich wykonywania określa dokumentacja techniczna i użytkowa sprzętu informatycznego, systemów i oprogramowania. Zapisy te zaleca się weryfikować, co najmniej raz w roku na podstawie doświadczeń eksploatacyjnych i dokumentacji napraw.
5. Przeglądy, konserwacje i bieżące naprawy, niewymagające angażowania autoryzowanych podmiotów serwisowych, wykonywane są przez Informatyka.
6. Przeglądy, konserwacje i naprawy mogą być wykonywane przez podmioty zewnętrzne jedynie na mocy umów serwisowych. Jeżeli w wyniku tych prac zachodzi konieczność dostępu do baz danych osobowych, to pracownicy podmiotów zewnętrznych realizujących umowy serwisowe powinni posiadać upoważnienia do przetwarzania tych danych.
7. W przypadku przekazywania stacji roboczej z dyskiem lub innym nośnikiem danych osobowych do naprawy na zewnątrz struktur organizacyjnych Liceum Ogólnokształcącego Nr III im. Juliusza Słowackiego w Otwocku i poza outsourcowany dział IT, należy nośnik zdemontować, zabezpieczyć dostęp hasłem lub dokonać naprawy w obecności osoby upoważnionej przez ADO, w przypadku przekazania nośnika innemu podmiotowi należy dane nieodwracalnie skasować.
8. Do wydzielonej sieci energetycznej zasilającej system informatyczny nie wolno podłączać żadnych innych urządzeń (czajników elektrycznych, odkurzaczy, radioodbiorników).
9. Zabronione jest dokonywanie napraw sprzętu informatycznego samodzielnie przez pracowników.
10. Środki techniczne i organizacyjne mające zapewnić bezpieczeństwo przetwarzania są regularnie testowane i oceniane pod kątem skuteczności. Zalicza się do nich:
    a. prawidłowe zarządzanie uprawnieniami dostępu;
    b. funkcjonalność systemu, który nie pozwala, aby zbierać więcej danych niż to konieczne;
    c. funkcje systemu, które przyczyniają się do wykazania rozliczalności;
    d. alerty w przypadku wystąpienia incydentu;
    e. wszelkie wdrożone zabezpieczenia systemów informatycznych oraz;
    f. środki bezpieczeństwa wdrożone w odpowiedzi na przeprowadzoną wcześniej analizę ryzyka.
11. Testy i oceny powyższych środków powinny być wykonywane okresowo minimum raz na rok, a ich wyniki powinny być przechowywane w formie raportu.

## 12. Raporty i wydruki

1. Raporty i wydruki wykonywane są na drukarkach lokalnych bądź sieciowych.
2. W przypadku drukowania sieciowego Użytkownik zobowiązany jest do:
   a. niezwłocznego odbioru wydrukowanych dokumentów,
   b. sprawdzenia kompletności wydruku,
   c. sprawdzenia czy nie zabrał druków innego pracownika,
3. Niedopuszczalne jest pozostawianie w drukarce wydrukowanych dokumentów. W przypadku, gdy Użytkownik wykonujący druk nie odbiera go, każdy z pracowników jest zobowiązany do zniszczenia wydrukowanej dokumentacji w niszczarce.

## 13. Zasady korzystania z przenośnych stacji roboczych

1. Przenośne stacje robocze wykorzystywane są wyłącznie do celów służbowych. Pracownicy korzystają z nich w miejscu pracy bądź za zgodą ADO poza miejscem pracy.
2. Logowanie do systemu zawierającego dane osobowe odbywa się dwustopniowo, poprzez logowanie do systemu stacji roboczej (hasło), a następnie logowanie na serwerze (domena). Dane przetwarzane przez Użytkowników przechowywane są na wydzielonej partycji lub w folderze zabezpieczonym hasłem.

## 14. Poczta elektroniczna

1. Zabronione jest wysyłanie wiadomości zawierających Szczególne kategorie danych osobowych (np. dane o stanie zdrowia jak i dane typu PESEL, dane z dokumentu tożsamości, dane okołofinansowe pracownika) bez szyfrowania (np. Zip, 7Z, wbudowany mechanizm haseł w plikach pakietu narzędzi biurowych do przetworzenia dokumentacji). Hasło wysyłamy zawsze inną drogą komunikacyjną (telefon, sms). Hasło do zaszyfrowanego pliku należy przesłać inną drogą niż poczta elektroniczna np. SMS na telefon odbiorcy maila.
2. Nie wolno odbierać załączników niewiadomego pochodzenia (klikać w nie).
3. Nie wolno uruchamiać linków w treści maila od nieznanych nadawców (klikać w nie).
4. Przynajmniej raz w roku powinny, być przeprowadzane obowiązkowe szkolenia pracowników z zakresu ochrony danych osobowych w tym zaleca się dodatkowo szkolenia z phishingu oraz innych zagrożeń związanych z pocztą elektroniczną. Udział w szkoleniu powinien być dokumentowany.

## 15. Praca zdalna

1. Praca zdalna wymaga korzystania z bezpiecznych metod dostępu do systemów informatycznych, w szczególności z rozwiązań takich jak wirtualne sieci prywatne (VPN), uwierzytelnianie wieloskładnikowe (MFA) oraz szyfrowane połączenia transmisji danych.
2. Użytkownik wykonujący pracę zdalnie zobowiązany jest do korzystania wyłącznie ze sprzętu i oprogramowania które udostępnia Liceum, spełniającego wymagania bezpieczeństwa określone w Polityce.
3. Stacje robocze wykorzystywane do pracy zdalnej muszą posiadać aktualne oprogramowanie antywirusowe, system operacyjny oraz wszystkie aplikacje zabezpieczone i zaktualizowane do najnowszej wspieranej wersji.
4. Urządzenia używane do pracy zdalnej muszą być chronione silnymi hasłami oraz innymi mechanizmami kontroli dostępu, w tym blokadą ekranu aktywowaną po określonym czasie bezczynności.

5. Pracownik wykonujący pracę zdalną jest zobowiązany do zapewnienia poufności danych, w szczególności poprzez pracę w odosobnionym i zabezpieczonym środowisku, np. w zamkniętym pomieszczeniu, z ograniczonym dostępem osób trzecich.
6. Przesyłanie danych osobowych i innych informacji poufnych powinno odbywać się za pomocą bezpiecznych kanałów komunikacji, takich jak szyfrowana poczta elektroniczna lub dedykowane systemy.
7. Niedopuszczalne jest przetwarzanie i przechowywanie danych osobowych na urządzeniach prywatnych lub w usługach chmurowych bez wyraźnej zgody i kontroli ADO.
8. Każdy pracownik wykonujący pracę zdalną powinien przestrzegać wszystkich procedur i polityk bezpieczeństwa obowiązujących w organizacji, w tym zasad ochrony danych osobowych.
9. Pracownik wykonujący pracę zdalną ma obowiązek niezwłocznego zgłaszania wszelkich incydentów bezpieczeństwa, w szczególności utraty sprzętu, prób nieuprawnionego dostępu czy naruszenia poufności danych.
10. Praca zdalna wymaga stosowania się do zasad ochrony prywatności i przestrzegania poufności dokumentów, danych i wszelkich informacji przetwarzanych w związku z wykonywaniem obowiązków służbowych.
11. Liceum zastrzega sobie prawo do monitorowania przestrzegania zasad bezpieczeństwa pracy zdalnej w granicach obowiązujących przepisów prawa oraz z poszanowaniem prywatności pracowników.
12. W uzasadnionych przypadkach mogą być przeprowadzane audyty oraz kontrole urządzeń i środowisk wykorzystywanych do pracy zdalnej w celu weryfikacji zgodności z zasadami bezpieczeństwa.

## 16. Obowiązki i odpowiedzialność Użytkownika

1. Użytkownik systemu jest zobowiązany zapoznać się z treścią niniejszej Polityki i potwierdzić to stosownym oświadczeniem.
2. Naruszenie przez pracownika niniejszej Polityki może zostać potraktowane jako naruszenie obowiązków pracowniczych i powodować określoną przepisami Kodeksu pracy odpowiedzialność pracownika.
3. Treść niniejszej Polityki ma charakter poufny, chroniony tajemnicą pracodawcy na zasadzie art. 100 § 2 pkt. 4 Kodeksu Pracy.
4. Nadzór i kontrolę nad realizacją niniejszej Polityki sprawuje ADO.
5. Osoby sprawujące nadzór i kontrolę nad poszczególnymi zapisami niniejszej Polityki zobowiązane są do dokonywania regularnych okresowych sprawdzeń przestrzegania jej zapisów i procedur przez nią wskazanych.
6. Każdy Użytkownik jest zobowiązany niezwłocznie zgłosić każde naruszenie ochrony danych osobowych Inspektorowi Ochrony Danych (IOD).