Nazwa jednostki:		I Liceum Ogólnokształcące im. Wacława Nałkowskiego w Wołominie	
Tytuł standardu:		Polityka Bezpieczeństwa Teleinformatycznego	
Wersja dokumentu:	1.0		
Data utworzenia:	15.12.2020	Zakres dokumentu:	Lokalny

I LICEUM OGÓLNOKSZTAŁCĄCE IM. WACŁAWA NAŁKOWSKIEGO W WOŁOMINIE

POLITYKA BEZPIECZEŃSTWA TELEINFORMATYCZNEGO

Spis treści

1. WPROWADZENIE

Niniejsza instrukcja dotyczy zasad bezpieczeństwa podczas przetwarzania danych osobowych w systemach teleinformatycznych. Referencją do niniejszych wymagań są polskie normy PN-ISO/IEC 27001 oraz PN-ISO/IEC 27002.

2. CEL I ZAKRES OBOWIĄZYWANIA

Celem niniejszego dokumentu jest określenie zasad bezpiecznego przetwarzania danych osobowych z wykorzystaniem nowoczesnej technologii.

3. DOKUMENTY ZWIĄZANE

1. Polityka Bezpieczeństwa Danych Osobowych.
2. Wytyczne Urzędu Ochrony Danych Osobowych oraz Ministra Edukacji Narodowej dotyczące zdalnego nauczania.

4. DEFINICJE

Użyte w dokumencie skróty i definicje zostały zawarte w Polityce Bezpieczeństwa Danych Osobowych.

5. POLITYKA BEZPIECZEŃSTWA TELEINFORMATYCZNEGO

5.1. Zasady ogólne

1. Nie ma możliwości, aby ktokolwiek mógł mieć uprawnienia dostępu do jakiegokolwiek systemu informatycznego, w którym przetwarzane są dane osobowe bez uwierzytelnienia potwierdzającego tożsamości użytkownika.
2. Uwierzytelnianie użytkownika na poziomie systemu operacyjnego oraz programu/aplikacji może się odbywać na podstawie:
    a. indywidualnego identyfikatora/loginu oraz hasła;
    b. Indywidualnego certyfikatu zlokalizowanego w lokalnym systemie lub w zewnętrznym sprzętowym kluczu;
    c. Danych biometrycznych (odcisk palca, skan siatkówki kształt twarzy)[1].
3. Dostęp do sieci wewnętrznej (lokalnej) zabezpiecza się na styku z innymi sieciami (szczególne publicznymi) przed nieuprawnioną ingerencją.
4. Każdy komputer w szkole zabezpiecza się oprogramowaniem antywirusowym.
5. Każdy komputer w szkole zabezpiecza się lokalną zaporą sieciową w taki sposób, aby do stacji roboczej pracowników blokowany był ruch przychodzący inicjujący nowe połączenia sieciowe. Niniejsza zasada za zgodą ADO może nie być stosowana na komputerach wykorzystywanych do celów dydaktycznych.

[1] Uwaga! Ze względu na fakt, że dane biometryczne są szczególnie chronioną kategorią danych osobowych, użycie tych cech osobowych powinno być potwierdzone dodatkową zgodą użytkownika systemu.

6. Nie jest rekomendowanym udostępnianie plików na lokalnych stacjach roboczych. W tym celu zaleca się stosowanie zewnętrznego magazynu danych (plików) dla użytkowników. Niniejsza zasada za zgodą ADO może nie być stosowana na komputerach wykorzystywanych do celów dydaktycznych.
7. Nośniki danych w urządzeniach, na których przetwarzane są dane osobowe zabezpiecza się kryptograficznie. Niniejszą zasadę wprowadza się w stosunku do komputerów przenośnych.
8. Nośniki danych zabezpieczane są kryptograficznie przed wydaniem sprzętu użytkownikowi do eksploatacji lub na każde żądanie ADO.
9. Monitory sytuuje się w sposób uniemożliwiający skuteczny odczyt danych osobowych przez osoby nieupoważnione.
10. Komputery przenośne, na których przetwarzane są dane osobowe często w miejscach publicznych lub w miejscach, w których nie można zapewnić wcześniejszego wymagania powinny być zaopatrzone w filtry prywatyzujące.
11. Użytkownicy są zobowiązani do należytego zabezpieczenia danych osobowych przetwarzanych w systemie informatycznym, programie/aplikacji przed nieuprawnionym dostępem w trakcie wykonywania swoich obowiązków oraz do prawidłowego zamknięcia aplikacji oraz systemu operacyjnego kończąc pracę.

5.2. Zarządzanie uprawnieniami oraz zasady uwierzytelniania użytkowników

1. Nadawanie uprawnień w systemach informatycznych następuje wyłącznie po wcześniejszej akceptacji ADO lub na jego wniosek;
2. Przydzielenie dostępu do systemu lub aplikacji jest realizowane poprzez nadanie przez ASI unikalnego identyfikatora/loginu i hasła dla użytkownika oraz z uwzględnieniem poniższych zasad:
   a. Nadanie uprawnień, o których mowa w niniejszym podpunkcie następuje na wniosek zgłoszony elektronicznie lub pisemnie, chyba że ADO postanowi inaczej. Wnioski, o których mowa przekazuje przełożony pracownika do ADO w celu akceptacji. Zaakceptowany wniosek zostaje przekazany do ASI w celu realizacji. Wnioski mogą być przekazywane bezpośrednio przez ADO;
   b. Wnioski o nadanie zwiększonych uprawnień administratora w systemach muszą posiadać również akceptację IOD.
3. W procesie nadawania, zmiany, odbierania lub zawieszania uprawnień stosuje się następujące zasady:
   a. użytkownikowi standardowemu nie nadaje się uprawnień w zakresie administracji systemem informatycznym, programem/aplikacją, chyba że ADO wyrazi na to zgodę;
   b. każdy użytkownik otrzymuje hasło początkowe, które musi zostać zmienione przy pierwszym logowaniu, o ile ADO nie postanowi inaczej;
   c. odebranie uprawnień zatwierdza ADO, a realizuje to zadanie ASI. ADO podejmuje decyzję działając na wniosek przełożonego pracownika, osoby zainteresowanej (wnioskodawca) zaakceptowany przez ADO albo z własnej inicjatywy w przypadku konieczności zapewnienia bezpieczeństwa danych lub ciągłości działania systemu ochrony danych osobowych – w takim wypadku wnioskodawca powiadamia ADO o konieczności odebrania uprawnienia użytkownikowi;

d. odebranie uprawnień ze względów bezpieczeństwa (np. w wyniku zaistniałego incydentu) powinno być niezwłocznie zrealizowane przez ASI oraz zgłoszone do IOD;

e. kont w systemach informatycznych nie usuwa się, a jedynie blokuje, tak aby nie można było się nimi posłużyć;

f. Nie wolno używać ponownie tych samych identyfikatorów w systemach nawet dla tego samego użytkownika;

g. użytkownik ma prawo do wykonywania tylko tych czynności, do których uzyskał uprawnienie i ponosi odpowiedzialność za czynności wykonywane w systemie informatycznym przy użyciu jego identyfikatora oraz hasła;

h. użytkownik zobowiązany jest do bezterminowego zachowania w tajemnicy wszelkich nadanych mu identyfikatorów/loginów oraz haseł, także po ustaniu zatrudnienia lub współpracy; służby informatyczne poucza użytkownika o jego uprawnieniach i konsekwencjach, o których mowa powyżej;

i. ASI musi zostać poinformowany o każdej zmianie dotyczącej użytkowników mającej wpływ na zakres posiadanych przez niego uprawnień;

j. na wniosek ADO, IOD oraz ASI dokonują przeglądu kont użytkowników pod kątem posiadanych uprawnień. Wyniki takiego przeglądu powinny zostać udokumentowane;

k. do weryfikacji uprawnień w systemach uprawnieni są: ADO, IOD oraz inne wskazane na piśmie przez ADO osoby;

l. dostęp do systemu informatycznego z uprawnieniami administratora przyznawany jest wyłącznie za zgodą ADO;

m. w uzasadnionych przypadkach (np. konserwacja, nadzór autorski systemu informatycznego, programu, aplikacji, usunięcie błędu oprogramowania, naprawa baz/zasobów danych itp.) dostęp do systemu informatycznego mogą uzyskać osoby delegowane przez firmy zewnętrzne, z którymi ADO zawarł umowę współpracy z odpowiednią klauzulą poufności; dostęp do systemu informatycznego, w przypadku opisanym powyżej, odbywa się na warunkach i w zakresie określonym w umowie współpracy;

4. ASI jest odpowiedzialny za adekwatną konfigurację uprawnień użytkownika w systemie informatycznym (systemie operacyjnym oraz programach/aplikacjach) na podstawie wniosku.

5. Odwołanie upoważnienia do przetwarzania danych osobowych użytkownika wywołuje zablokowanie jego dostępów w systemach przetwarzających dane osobowe.

6. Raz przydzielony identyfikator (login) w systemach informatycznych nie może być przydzielony innemu użytkownikowi.

5.3. Metody i środki uwierzytelniania

1. W dostępach do systemów informatycznych należy stosować uwierzytelnianie co najmniej dwustopniowe tj. na poziomie dostępu do systemu operacyjnego oraz danego programu/aplikacji, w której przetwarzane są dane osobowe (jeżeli funkcjonalność programu/aplikacji na to pozwala).

2. W przypadku zastosowania mechanizmu SSO (Single Sign-On) na poziomie systemu operacyjnego oraz aplikacji do przetwarzania danych osobowych, powyższe wymaganie może nie być stosowane „jawnie”, ponieważ mechanizm SSO uwierzytelnia użytkownika w aplikacjach automatycznie.

3. Wprowadza się następujące zasady stosowania haseł w systemach zarządzanych przez ADO:
   a. hasła w systemach informatycznych nie mogą być krótsze niż 8 znaków.
   b. hasła zmienia się cyklicznie – **częstotliwość zmiany haseł ustalano na okres 90 dni**;
   c. **zabrania się używania tych samych haseł przez co najmniej trzy kolejne cykle zmiany hasła** oraz zlecania zmiany hasła innemu użytkownikowi lub osobie nieupoważnionej.
   d. hasła nie mogą być przekazywane użytkownikowi w postaci umożliwiającej zapoznanie się z ich treścią przez osoby nieupoważnione;
   e. użytkownik nie może udostępniać haseł innemu użytkownikowi, chyba że ADO na to zezwoli. Ujawnione w ten sposób hasło musi zostać zmienione niezwłocznie;
   f. hasła użytkownika powinny być skonstruowane w taki sposób, aby maksymalnie utrudnić jego odgadnięcie, ale również umożliwić jego możliwie szybkie zapamiętanie przez użytkownika. Hasła nie powinny zawierać informacji powiązanych z użytkownikiem, w szczególności:
      - wyrazów słownikowych;
      - imion, nazwisk, pseudonimów, inicjałów;
      - znaków, liter, cyfr następujących po sobie na klawiaturze;
      - dat, numerów rejestracyjnych pojazdów, nr telefonów, nazw programów/aplikacji; nazwy ulubionego zwierzaka;
      - powszechnie znanych skrótów i innych kombinacji znaków kojarzących się bezpośrednio z użytkownikiem lub ADO albo mogących w inny sposób doprowadzić do łatwego ich odgadnięcia przez osoby nieupoważnione;
   g. każdy użytkownik zobowiązany jest do zachowania w tajemnicy hasła, także po okresie jego używania,
   h. hasło podlega niezwłocznej zmianie w przypadku podejrzenia jego użycia przez osobę nieupoważnioną,
4. Pozyskując nowe systemy informatyczne, ADO dąży do zapewnienia właściwości systemu informatycznego, programu lub aplikacji polegającej na wymuszeniu okresowej zmiany haseł.
5. W przypadku, gdy użytkownik zapomni hasła, ASI na wniosek ADO przydziela hasło tymczasowe, które użytkownik ma obowiązek zmienić przy kolejnym uwierzytelnieniu. Przed wydaniem hasła tymczasowego ASI potwierdza tożsamość użytkownika.
6. Jeżeli w systemie informatycznym istnieje właściwość umożliwiająca zapamiętanie identyfikatora/loginu użytkownika i jego hasła nie należy z niej korzystać.
7. Hasła do kont o najwyższych uprawnieniach (administracyjnych) przechowuje się na odpowiednio zabezpieczonym nośniku lub w formie pisemnej, w zapieczętowanej, zaklejonej albo inaczej zabezpieczonej kopercie, w miejscu, do którego dostęp posiada wyłącznie ADO lub upoważniona przez niego osoba. Hasła te powinny podlegać zmianie natychmiast po ich wyodrębnieniu z koperty. ADO lub upoważniona przez niego osoba, w sytuacjach uzasadnionych nagłą potrzebą, w szczególności celem zapewnienia ciągłości działania systemu informatycznego, może udostępnić hasło administratorskie upoważnionej lub wskazanej osobie lub uprawnionemu podmiotowi zewnętrznemu. Udostępnienie hasła musi zostać udokumentowane na piśmie.

5.4. Procedura pracy przy stanowisku komputerowym

1. **Rozpoczęcie i zakończenie pracy przy stanowisku komputerowym**
   a. Użytkownik zwraca uwagę na stan komputera i urządzeń komputerowych oraz swojego stanowiska pracy przed przystąpieniem do pracy. W przypadku stwierdzenia nieprawidłowości, użytkownik powiadamia bezpośredniego przełożonego lub ADO;
   b. Nieprawidłowością nie można nazwać stanu systemu / komputera po zakończeniu prowadzonych prac ASI;
   c. Użytkownik ma obowiązek niezwłocznie zgłosić ASI każdy problem związany z niewłaściwym funkcjonowaniem systemu informatycznego, w którym przetwarzane są dane osobowe, jeżeli wymaga to jego interwencji. Użytkownik powinien posiadać minimalną wiedzę, aby rozwiązać podstawowe problemy wynikające z normalnej eksploatacji komputera, aplikacji czy urządzeń biurowych we własnym zakresie;
   d. Pracę na komputerze użytkownik rozpoczyna od zalogowania się w systemie operacyjnym. W celu zalogowania do programu/aplikacji użytkownik wykorzystuje przypisany mu identyfikator/login oraz dokonuje uwierzytelnienia za pomocą hasła lub innego składnika potwierdzającego jego tożsamość;
   e. Użytkownik kończy pracę wylogowując się w pierwszej kolejności z programów/aplikacji, następnie zamyka system operacyjny zgodnie z procedurą używania komputera. Procedura kończy się automatycznym wyłączeniem komputera.
2. **Zawieszenie i przerwanie pracy komputera**
   a. Użytkownik zobowiązany jest przed każdorazowym opuszczeniem stanowiska pracy zablokować stację roboczą;
   b. W razie wątpliwości lub problemów z wylogowaniem albo zablokowaniem systemu operacyjnego, użytkownik jest zobowiązany niezwłocznie poinformować o tym fakcie ASI. Do podjęcia działań przez ASI użytkownik nie może pozostawić swojej stacji roboczej bez rozwiązania problemu;
   c. Opuszczenie stanowiska komputerowego jest zabronione, jeżeli w pomieszczeniu przebywa osoba nieupoważniona, a nie przebywa żaden inny upoważniony przez ADO użytkownik;
3. **Blokowanie systemu**
   a. W celu wzmocnienia bezpieczeństwa ADO wprowadza, w miarę istniejących potrzeb i możliwości, wygaszacze ekranów uruchamiające się automatycznie po upływie **5 minut nieaktywności**, powodujące automatyczne zablokowanie systemu operacyjnego na danym stanowisku. Odblokowanie systemu następuje po ponownym wprowadzeniu hasła przez użytkownika;
   b. W miarę możliwości, ASI wprowadza mechanizm blokowaniu dostępu do systemu informatycznego po przekroczeniu liczby trzech prób logowania. Blokada może być czasowa, np. **na czas 10 minut**.
   c. Działania użytkowników w systemach informatycznych (dzienniki audytowe) powinny być rejestrowane.

5.5. Kopie zapasowe

1. Kopie zapasowe sporządza się regularnie, tak aby zapewnić maksymalne bezpieczeństwo danych osobowych i ciągłość pracy szkoły. Harmonogram wykonywania kopii bezpieczeństwa oraz zakres określa ADO lub ASI po wcześniejszym uzgodnieniu z ADO.

2. W przypadku wymiany komputerów, pliki znajdujące się w profilu użytkownika należy przenieść w sposób bezpieczny.
3. Gdy wcześniej używany komputer zostaje przekazany innemu użytkownikowi, należy usunąć profil wcześniejszego użytkownika wraz z jego danymi (uwzględniając zapis pkt. 2), usunąć aplikacje lub przywrócić komputer do ustawień fabrycznych np. poprzez odtworzenie „czystego" systemu (recovery).
4. W miarę możliwości technicznych i organizacyjnych należy przestrzegać następującej częstotliwości tworzenia kopii zapasowych:
   - kopie bezpieczeństwa baz danych zawierających dane osobowe lub inne wrażliwe dane dla ADO sporządza się w cyklu dziennym i tygodniowym;
   - kopie bezpieczeństwa plików systemowych (lub obrazów systemów) serwerów – sporządza się w cyklu miesięcznym lub po każdej istotnej zmianie;
   - kopie bezpieczeństwa wybranych plików użytkowników (dokumentów) – sporządza się w cyklu dziennym lub tygodniowym.
5. W nagłych sytuacjach ADO może zezwolić na udostępnienie kopii zapasowych osobie przez siebie wyznaczonej.
6. ADO może wyznaczyć osoby odpowiedzialne za tworzenie doraźnych kopii zapasowych na dysku lokalnym lub na innym wskazanym nośniku informacji, a użytkownicy są zobowiązani przestrzegać wyznaczonych mu terminów tworzenia takich kopii.
7. Kopie zapasowe, jeżeli są wykonywane na zewnętrznych nośnikach danych i zawierają zbiory danych osobowych, należy odpowiednio oznakować i przechowywać w należycie zabezpieczonych pomieszczeniach, innych niż te, w których znajdują się zbiory danych osobowych przetwarzane na bieżąco.

5.6. Ochrona przed szkodliwym oprogramowaniem

1. Komputery stacjonarne oraz przenośne powinny być zabezpieczone przed:
   - nieuprawnionym dostępem do danych osobowych;
   - próbą penetracji;
   - utratą danych spowodowaną działaniem złośliwego oprogramowania;
   - wpływem na aplikacje umożliwiającym dostęp danych osobowych w taki sposób, że przetwarzane dane osobowe ulegną odczytaniu, modyfikacji lub zniszczone;
   - przechwyceniem danych osobowych podczas transmisji w przypadku rozproszonego przetwarzania danych z wykorzystaniem ogólnodostępnej sieci Internet;
   - niedozwolonymi aplikacjami uruchamianymi przez użytkowników bez zgody ADO lub ASI;
2. Potencjalnymi źródłami przedostawania się programów szpiegujących oraz wirusów na stacje robocze są załączniki do poczty elektronicznej, przeglądane strony internetowe, pliki i aplikacje pochodzące z nośników wymiennych uruchamiane i odczytywane na komputerze.
3. Oprogramowanie antywirusowe powinno być aktualizowane na bieżąco po udostępnieniu aktualizacji przez jego producenta.
4. System antywirusowy powinien być skonfigurowany w następujący sposób:
   - powinien przez cały czas pracy komputera działać w tle;
   - skaner ruchu internetowego powinien być aktywny (łącznie z komunikacją szyfrowaną);
   - skaner poczty elektronicznej powinien być stale włączony.

- zabezpieczenie przez złośliwym oprogramowaniem typu ransomware powinno być stale włączone ze wskazaniem plików lub folderów, w których znajdują się chronione dane / dokumenty.
- blokada możliwości ingerencji użytkownika w ustawienia oprogramowania antywirusowego,
- możliwość centralnego zarządzania agentami antywirusowymi na stacjach roboczych oraz zbieranie zdarzeń z komputerów w jednym miejscu.

5. Korzystanie przez użytkownika z prywatnych nośników danych jest możliwe, o ile podłączenie takiego nośnika wiąże się z automatycznym jego skanowaniem pod kątem obecności złośliwego oprogramowania.
6. Niedopuszczalne jest otwieranie załączników poczty elektronicznej oraz innych plików bez sprawdzenia reputacji źródła.
7. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, ASI podejmuje działania zmierzające do usunięcia zagrożenia.
8. Przygotowywanie wymagań do zakupu systemu antywirusowego może być konsultowane z IOD.

5.7. Pozostałe środki bezpieczeństwa

1. ADO wprowadza środki ochrony kryptograficznej zabezpieczające przetwarzanie danych osobowych w komputerach przenośnych służących do przetwarzania danych osobowych.
2. Komputery przenośne służące do przetwarzania danych osobowych mogą być używane poza obszarem przetwarzania danych po ich odpowiednim zabezpieczeniu, o którym mowa w pkt. 1.
3. Obowiązuje bezwzględny zakaz samodzielnego instalowania oprogramowania na komputerach będących własnością ADO bez jego akceptacji. Za pisemną akceptację traktuje się również formę elektroniczną (wiadomość email lub SMS).
4. Wykaz dopuszczonego oprogramowania do eksploatacji na stacjach roboczych użytkowników stanowi załącznik nr 1 do niniejszej polityki.
5. Aktualizacje oprogramowania, które wymagają podwyższonych uprawnień w systemie muszą być wykonywane wyłącznie w asyście ASI lub innej osoby wskazanej przez ADO.
6. Należy odpowiednio obchodzić się ze sprzętem, w szczególności chronić go przed zagrożeniami środowiskowymi, aktami wandalizmu oraz kradzieżą.
7. Użytkownik korzystający ze sprzętu poza obszarem przetwarzania danych zachowuje szczególną ostrożność podczas transportu.
8. Nie można powierzyć sprzętu osobom nieupoważnionym ani pozostawić sprzętu bez dozoru, w szczególności w miejscu publicznym.
9. Dla systemu informatycznego służącego do przetwarzania danych osobowych zapewnia się właściwe zasilanie energetyczne, umożliwiające należyte działanie sprzętu komputerowego odpowiadające wymaganiom i rekomendacjom producentów. W miarę możliwości technicznych i bieżących potrzeb, sprzęt komputerowy należy chronić przed awariami zasilania i innymi zakłóceniami elektrycznymi.
10. W pomieszczeniach technicznych należy zapewnić odpowiednie warunki środowiskowe tj. wilgotność oraz temperaturę powietrza.

5.8. Przeglądy i konserwacja

1. Przeglądy oraz konserwacja urządzeń służących do przetwarzania danych powinny być wykonywane w terminach określonych przez producentów sprzętu oraz oprogramowania. Jeśli producent nie przewidział potrzeby dokonywania przeglądów lub konserwacji, bądź też nie określił ich częstotliwości, o dokonaniu czynności oraz sposobie jej przeprowadzenia decyduje ADO w uzgodnieniu z ASI.
2. ADO lub osoba przez niego wyznaczona może dokonywać przeglądów i konserwacji urządzeń wchodzących w skład systemu informatycznego, jeżeli dana czynność nie wymaga skorzystania z usług firmy zewnętrznej lub wykwalifikowanej w tym celu osoby i nie naruszy zasad wynikających z udzielonej gwarancji przez producenta sprzętu lub oprogramowania.
3. Administrator danych osobowych lub osoba przez niego wyznaczona sprawuje nadzór nad pracami, o których mowa powyżej i dba, aby przebiegały one w miarę możliwości bez dostępu do danych osobowych. Przed rozpoczęciem przez podmioty zewnętrzne prac, o których mowa powyżej konieczne jest potwierdzenie tożsamości serwisantów.
4. Przegląd systemów operacyjnych, programów/aplikacji i narzędzi programowych służących do przetwarzania danych osobowych przeprowadzany jest w celu sprawdzenia poprawności działania i wykonuje się go w następujących przypadkach:
   - zmiany wersji oprogramowania systemów operacyjnych, programów/aplikacji, na stanowisku komputerowym użytkownika;
   - zmiany systemu operacyjnego, na którym eksploatowany jest program/aplikacja, na stanowisku komputerowym użytkownika;
   - wykonania zmian w systemie operacyjnym, programie/aplikacji, spowodowanych koniecznością naprawy lub ich modyfikacją.
5. Konserwację oprogramowania przeprowadza się również po zgłoszeniu przez użytkownika potrzeby wprowadzenia zmian pozwalających dostosować funkcjonalność systemu operacyjnego, programu/aplikacji do bieżącej obsługi lub planowanych potrzeb.
6. ADO lub osoba przez niego wyznaczona prowadzą we własnym zakresie, w miarę potrzeb i możliwości, dzienniki systemu informatycznego z przeprowadzanych działań konserwacyjnych, awarii lub napraw lub w innym niezbędnym przedmiocie.

5.9. Postępowanie ze sprzętem przeznaczonym do likwidacji lub naprawy

1. Uszkodzone nośniki danych, z których przed awarią nie zostały w sposób kontrolowany usunięte dane osobowe nie podlegają naprawie.
2. Sprzęt komputerowy przeznaczony do likwidacji, na którego nośnikach mogą znajdować się dane osobowe pozbawia się wcześniej nośników danych lub pozbawia się danych przez co najmniej dwukrotne nadpisanie każdego z nośników dedykowanym oprogramowaniem. W przypadku, gdy programowe usunięcie danych nie jest to możliwe, uszkadza się nośniki w inny sposób uniemożliwiający odczytanie danych.
3. Nośniki zawierające znaczne ilości danych osobowych (dane z systemów kadrowych, płacowych, innych baz danych) mogą być niszczone tylko fizycznie. Alternatywnie, można skorzystać z usług firm specjalizujących się w usuwaniu danych z nośników magnetycznych i elektronicznych w sposób inny niż programowy.
4. Przed przekazaniem nośników do utylizacji należy sporządzić protokół zawierający modele i numery seryjne nośników. Protokół powinien zawierać nazwę podmiotu odpowiedzialnego za przeprowadzenie utylizacji oraz nr umowy, w ramach której takie działanie zostanie przeprowadzone.

5.10. Praca na odległość

1. Praca na odległość dotyczy sytuacji, gdy pracownicy łączą się z systemami wewnętrznymi szkoły lub korzystają z platform dostępnych w sieci Internet, w których przetwarzane są dane osobowe pracowników, współpracowników lub uczniów.
2. W przypadku nawiązywania połączenia z systemami wewnętrznymi szkoły, należy stosować bezpieczny tunel VPN.
3. Wprowadzenie rozwiązania umożliwiającego wykonywanie pracy na odległość wymaga wprowadzenia w szkole odpowiedniego regulaminu dla wszystkich pracowników. Regulamin ten powinien być współtworzony lub konsultowany z ASI oraz IOD.
4. Wykonywanie pracy na odległość z wykorzystaniem komputerów prywatnych pracowników jest możliwe. Szczegóły dotyczące zabezpieczeń technicznych oraz organizacyjnych w takim rozwiązaniu powinny zostać określone w regulaminie, o którym mowa w pkt. 1.
5. Wdrożenie rozwiązań technicznych do pracy zdalnej realizuje ASI pod warunkiem, że zostały przez ADO zapewnione odpowiednie do tego warunki.
6. Powyższe zapisy nie dotyczą nauczania na odległość, gdzie proces ten jest realizowany na podstawie aktów wykonawczych Ministra Edukacji Narodowej lub Rady Ministrów.

5.11. Nauczanie na odległość

1. Nauczanie na odległość jest możliwe pod warunkiem, że istnieje do tego podstawa prawna. W takiej sytuacji ADO powiadamia nauczycieli, rodziców i uczniów.
2. ADO decyduje z jakich platform oraz aplikacji kształcenia na odległość mogą korzystać nauczyciele kierując się m. in. rekomendacjami innych ADO czy ogólnodostępną reputacją tych platform. ADO powinien mieć pewność, że dostawcy usług zapewniają środki techniczne i organizacyjne do bezpiecznego przetwarzania powierzonych danych.
3. Nauczyciele nie powinni sami decydować o doborze narzędzi do komunikacji z prawnymi opiekunami oraz uczniami bez zgody ADO.
4. ADO powierzając dane osobowe dostawcom platform internetowym powinien zawrzeć umowę powierzenia danych. Jeżeli dostawcy usług w swoich regulaminach posiadają zapisy, które regulują zasady przetwarzania danych w wyniku ich powierzenia – ADO może odstąpić od zawierania dodatkowej umowy.
5. Korzystając z usług dostawców platform należy stosować zasadę minimalizacji ilości danych osobowych. Dane, które nie muszą być przetwarzane w ramach świadczenia usługi – nie powinny być w niej umieszczane. Jeżeli jest to możliwe, zaleca się stosowania pseudonimów zamiast rzeczywistych danych.
6. Jeżeli nauczyciel nie ma możliwości realizowania zdalnego nauczania poza szkołą, administrator danych osobowych powinien dać taką możliwość nauczycielowi w siedzibie szkoły.
7. Do kontaktów z prawnymi opiekunami uczniów oraz samymi uczniami nauczyciel powinien wykorzystywać służbową skrzynkę (adres e-mail). Jeżeli szkoła nie posiada takich skrzynek, nauczyciele muszą zadbać, aby komunikacja taka była bezpieczna.
8. Komunikacja z wieloma osobami za pośrednictwem jednej wiadomości poczty elektronicznej musi być tak realizowana, aby zapewnić prywatność adresatów poprzez np. umieszczania listy odbiorców w polu „ukryci odbiorcy wiadomości” – pole UDW (PL) lub BCC (EN) w zależności od wersji językowej aplikacji.
9. Za wyciek danych, gdy do zdalnego nauczania wykorzystywany jest prywatny komputer nauczyciela odpowiada ADO.

10. Na ogólnodostępnych portalach internetowych, które nie wymagają potwierdzania tożsamości użytkownika, nauczyciel może publikować materiały edukacyjne dla uczniów, ale nie może umieszczać danych osobowych opiekunów czy uczniów.
11. W celu monitorowania obecności ucznia podczas zajęć lekcyjnych przy zdalnym nauczaniu, nauczyciel nie może wykorzystywać narzędzi zbierających dane biometryczne, w szczególności systemów wykrywania twarzy.
12. Jeżeli zdalne nauczanie odbywa się za pośrednictwem platform, których nie utrzymuje ADO, opiekunowie oraz pełnoletni uczniowie powinni zostać poinformowani o tym fakcie w klauzuli informacyjnej.

6. WYJĄTKI

Wyjątki od powyższych reguł wymagają zgody ADO.

7. WEJŚCIE W ŻYCIE DOKUMENTU

1. Dokument polityki zostaje wprowadzony zarządzeniem dyrektora szkoły.
2. Dokument zastępuje „Instrukcję Zarządzania Systemem Informatycznym”..

Załącznik nr 1

LISTA OPROGRAMOWANIA DOPUSZCZONEGO DO UŻYTKOWANIA

Lista obejmuje oprogramowanie dopuszczone do eksploatacji na stacjach roboczych użytkowników. Lista nie uwzględnia oprogramowania serwerowego i specjalnego przeznaczenia oraz ilości licencji zakupionych do oprogramowania płatnego i stanowi jedynie informacje jakie aplikacje są dozwolone do zainstalowania na komputerach użytkowników.

Sale lekcyjne nie zostały objęte poniższymi wymaganiami, ponieważ nauczyciele dobierają środki dydaktyczne w taki sposób, aby zrealizować założony program. **Warunkiem jednak jest to, aby przyjęte rozwiązania uzyskało akceptację ADO. Rekomendowane jest, aby sale lekcyjne były logicznie odseparowane sieciowo od segmentu sieci biurowej.**

Oprogramowanie standardowe (dla użytkowników)

Typ oprogramowania	Producent	Nazwa
System operacyjny	Microsoft Corporation	Windows 8, 10 lub nowszy
System operacyjny	Open Source	Linux (w wersji wspieranej)
Oprogramowanie biurowe	Microsoft Corporation	Office (wersja w zależności od posiadanej licencji objęta wsparciem producenta w zakresie dystrybucji aktualizacji bezpieczeństwa)
Oprogramowanie biurowe	Community	LibreOffice lub zamiennie OpenOffice
Oprogramowanie biurowe	Adobe Systems Incorporated	Acrobat Reader (czytnik plików PDF)
Oprogramowanie biurowe	Foxit	Foxit Reader (czytnik plików PDF)
Przeglądarka internetowa	Microsoft Corporation	Internet Explorer, Microsoft Edge
Przeglądarka internetowa	Mozilla	Firefox, Firefox ESR
Przeglądarka internetowa	Google	Chrome lub Chromium
Aplikacja narzędziowa	Open Source	7Zip
Oprogramowanie biurowe	Microsoft Corporation	Edytor równań

Oraz inne oprogramowanie dziedzinowe do obsługi biblioteki, multimediów (materiały promocyjne) itp. Za zgodą ADO.

Oprogramowanie narzędziowe (specjalnego przeznaczenia)

Typ oprogramowania	Producent	Nazwa
Aplikacja narzędziowa	Open Source	VeraCrypt
Biblioteki dla aplikacji	Oracle	Java Runtime Environment (IRE)
System antywirusowy	Microsoft Corporation	Windows Defender
System antywirusowy	Dowolny, dostępny na rynku komercyjnym	W zależności od zakupionej licencji
Sterowniki urządzeń	*Każdy*	*Oficjalne sterowniki udostępnione przez producentów sprzętu.*

Oprogramowanie warunkowo dopuszczone do eksploatacji

Typ oprogramowania	Producent	Nazwa
System operacyjny	Microsoft Corporation	Windows 7 (brak wsparcia)
Plugin przeglądarki internetowej	Adobe Systems Incorporated	Flash Player (wiele podatności). Zakończenie wsparcia dla tej biblioteki to 31 grudnia 2020 r.