

## **Instrukcja zarządzania systemami informatycznymi w Publicznej Szkole Podstawowej im. Marszałka Józefa Piłsudskiego w Laskach**

### **Informacje podstawowe**

Instrukcja zarządzania systemami informatycznymi (IZSI) ma na celu ustanowienie zasad zarządzania systemem informatycznym, w którym przetwarzane są dane osobowe, jak również warunków organizacyjnych i technicznych, jakie spełniać powinny, wchodzące w jego skład urządzenia, biorąc pod uwagę skalę zagrożeń i kategorie danych objęte ochroną.

Przestrzeganie zasad instrukcji ma na celu zapewnienie bezpieczeństwa przetwarzanych danych osobowych i innej informacji w Publicznej Szkole Podstawowej im. Marszałka Józefa Piłsudskiego w Laskach, rozumianego jako zapewnienie: poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie.

### **Definicje**

Ilekroć w Instrukcji jest mowa o:

1. szkole – należy przez to rozumieć Publiczną Szkołę Podstawową im. Marszałka Józefa Piłsudskiego w Laskach;
2. dyrektorze szkoły – należy przez to rozumieć dyrektora w Publicznej Szkole Podstawowej
3. im. Marszałka Józefa Piłsudskiego w Laskach;
4. systemie informatycznym - należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
5. danych osobowych – rozumie się przez to 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;
6. administratorze systemów informatycznych (ASI) – rozumie się przez to osobę wyznaczoną przez dyrektora szkoły, która odpowiada za zapewnienie sprawności, należytej konserwacji i wdrażania technicznych zabezpieczeń systemów informatycznych, w których przetwarzane są dane osobowe i inne informacje wytworzone przez szkołę.

### **Organizacja zarządzania**

#### **1. Administrator Systemów Informatycznych (ASI)**

- 1.1. ASI sprawuje nadzór nad funkcjonowaniem infrastruktury sieciowej, maszyn i urządzeń informatycznych, urządzeń peryferyjnych oraz oprogramowania. ASI dba, aby zasoby te:

- 1) były używane zgodnie z przeznaczeniem,
- 2) były sprawne,
- 3) były używane przez osoby uprawnione,
- 4) spełniały wymagania określone w przepisach,
- 5) spełniały wymagania licencyjne,
- 6) miały zapewnione wsparcie techniczne,
- 7) były na bieżąco aktualizowane,
- 8) były umieszczone w ewidencjach,
- 9) były jak najmniej podatne na zagrożenia integralności, poufności i dostępności przetwarzanej informacji.

1.2. ASI podpisuje oświadczenie o zachowaniu poufności informacji obejmujące ponadstandardowy zakres zobowiązań. W szczególności ASI zobowiązuje się do zachowania w tajemnicy przed osobami nieuprawnionymi:

- 1) wiedzy o stosowanych zabezpieczeniach,
- 2) wiedzy o odnotowanych incydentach, zagrożeniach i podatnościach,
- 3) haseł, kluczy, identyfikatorów, w szczególności identyfikatorów i haseł systemowych i administracyjnych,
- 4) planów zmian w zakresie bezpieczeństwa informacji.

1.3. ASI regularnie wykonuje lub zleca testy i audyty w celu potwierdzenia skuteczności istniejących zabezpieczeń. Testy i audyty są planowane z wyprzedzeniem i nie mogą zakłócać podstawowych procesów w szkole. Informacje o testach i audytach, plany, wyniki, stosowane narzędzia są ściśle chronione przed nieautoryzowanym dostępem.

1.4. ASI zdaje dyrektorowi szkoły sprawozdanie ze swoich bieżących działań a co najmniej raz na rok przedkłada pisemny raport o stanie urządzeń i systemów. Raport obejmuje między innymi:

- 1) wyniki przeprowadzonych audytów wewnętrznych,
- 2) stan realizacji zaleceń wynikających z wcześniejszych analiz, kontroli i audytów, własnych, wewnętrznych i zewnętrznych, w tym prowadzonych i nadzorowanych przez siebie działań naprawczych i zapobiegawczych,
- 3) wnioski z prowadzonych analiz podatności zasobów informatycznych na zagrożenia,

1.5. ASI prowadzi dziennik administratora zgodnie z **załącznikiem nr 1** do niniejszej Instrukcji.

1.6. ASI jest powoływany przez dyrektora szkoły.

1.7. Obowiązki ASI mogą być rozdzielone pomiędzy różne osoby. Można określić odrębnych ASI dla odrębnych systemów teleinformatycznych w ramach szkoły.

## **2. Ewidencja sprzętu i oprogramowania**

2.1. ASI prowadzi ewidencję sprzętu i oprogramowania zgodnie z **załącznikiem nr 2** do niniejszej Instrukcji.

- 2.2. Ewidencja jest chroniona przed nieautoryzowanym dostępem.
- 2.3. Ewidencja jest tworzona wykazy środków trwałych.

### **Zabezpieczenia organizacyjne**

### **3. Zatrudnienie, rotacja pracowników**

#### ***Warunki zatrudnienia***

- 3.1. Warunki zatrudnienia powinny odzwierciedlać politykę bezpieczeństwa szkoły oraz zawierać dodatkowe wymagania:
  - 1) określone prawa i odpowiedzialność pracownika, wykonawcy i użytkownika w świetle zasad ochrony bezpieczeństwa informacji w szkole oraz obowiązującego ustawodawstwa (np. praw autorskich),
  - 2) tam, gdzie to konieczne, stwierdzenie, że odpowiedzialność ta jest rozciągnięta także poza siedzibę szkoły i poza normalne godziny pracy, np. w przypadku pracy w domu,
  - 3) tam, gdzie to konieczne, odpowiedzialność ta powinna trwać przez określony czas po zakończeniu czasu zatrudnienia,
  - 4) zasady odpowiedzialności za klasyfikowanie i zarządzanie danymi należącymi do pracodawcy,
  - 5) zasady odpowiedzialności pracowników, wykonawców i użytkowników pochodzących spoza instytucji za utrzymanie informacji pochodzących z innych instytucji lub strony trzeciej,
  - 6) wskazanie działań, które mają być podjęte w przypadku zlekceważenia przez pracownika wymagań bezpieczeństwa,
  - 7) odpowiedzialność szkoły za informacje osobowe pracownika – w tym informacje powstałe
  - 8) w efekcie albo w trakcie zatrudnienia.

#### ***Szkolenia***

- 3.2. Każda osoba przed dopuszczeniem do pracy wymagającej dostępu do informacji winna być poddana przeszkoleniu lub zapoznana z:
  - 1) zasadami bezpieczeństwa informacji zawartych w Polityce Bezpieczeństwa Informacji i niniejszej Instrukcji,
  - 2) zasadami ujętymi w Regulaminie ochrony danych osobowych i Polityce ochrony danych osobowych,
  - 3) zasadami związanymi z bezpieczeństwem informatycznym,
  - 4) obszarami szczególnego ryzyka w szkole.
- 3.3. Za przeprowadzenie szkolenia lub zapoznanie z zasadami bezpieczeństwa informacji odpowiada Dyrektor szkoły.
- 3.4. Forma szkoleń jest dostosowana do okoliczności.
- 3.5. Treść szkoleń jest dostosowana do charakteru pracy (zakresu obowiązków) osób szkolonych.

- 3.6. Uczestnik szkolenia potwierdza swój udział podpisem na liście obecności.
- 3.7. Udział w szkoleniu obejmującym swoim zakresem zasady bezpieczeństwa informacji w szkole jest warunkiem wydania upoważnienia do przetwarzania informacji.

### ***Poufność***

- 3.8. Każdy z pracowników lub zleceniobiorców zobowiązany jest do podpisania Oświadczenia o poufności zgodnie z załącznikiem nr 3 do niniejszej Instrukcji.
- 3.9. Podpisane oświadczenia poufności są archiwizowane w aktach osobowych pracownika.
- 3.10. Oświadczenie poufności stanowi podstawę do nadania upoważnienia do przetwarzania informacji.

### ***Nadawanie uprawnień***

- 3.11. Przyznanie, anulowanie upoważnienia do przetwarzania informacji w systemie informatycznym lub w zbiorze papierowym wraz z uprawnieniami do przetwarzania tych danych w systemie informatycznym realizowane jest przez dyrektora szkoły. W tym przypadku obowiązuje wzór upoważnienia do przetwarzania danych osobowych (załącznik do Polityki Ochrony Danych Osobowych), chyba, że upoważnienie dotyczy innych niż dane osobowe informacji, wtedy upoważnienie należy nadać zgodnie ze wzorem stanowiącym załącznik nr 4 do niniejszej Instrukcji.
- 3.12. Przed nadaniem upoważnienia, dyrektor zobowiązany jest do sprawdzenia, czy osoba upoważniona:
  - 1) odbyła szkolenie z zakresu przestrzegania zasad bezpieczeństwa informacji lub została zapoznana z regulacjami wewnętrznymi dotyczącymi bezpieczeństwa informacji,
  - 2) podpisała oświadczenie o zachowaniu poufności,
  - 3) będzie przetwarzać informację w zakresie i celu określonym upoważnieniem.
- 3.13. Po nadaniu upoważnienia, dyrektor lub wyznaczona przez niego osoba przekazuje je ASI celem nadania identyfikatorów oraz uprawnień użytkownika w systemach informatycznych i aplikacjach.
- 3.14. Każdy użytkownik musi posiadać swój własny indywidualny identyfikator (login) w danym systemie informatycznym lub aplikacji.
- 3.15. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego lub aplikacji nie może być przydzielany innej osobie.
- 3.16. Pracownik Sekretariatu odpowiada za przechowywanie wszystkich upoważnień.
- 3.17. 3.16. Pracownik Sekretariatu opowiada za prowadzenie Ewidencji osób upoważnionych do przetwarzania informacji zgodnie z załącznikiem nr 6, osobnej ewidencji podlegają upoważnienia do przetwarzania danych osobowych. Ewidencja podlega regularnym przeglądom pod kątem jej adekwatności do rzeczywistych potrzeb i wymagań.

### ***Zwalnianie***

- 3.18. Podczas zwalniania pracownika przeprowadza się przegląd uprawnień do dostępu do aktywów i związanych systemów informatycznych i usług.

3.19. Zwalnianie pracownika wymaga:

- 1) wycofania wszystkich upoważnień pracownika do przetwarzania informacji,
- 2) odebrania od niego sprzętu,
- 3) cofnięcia dostępu do pomieszczeń.

3.20. Prawa dostępu powinny być usunięte z uwzględnieniem fizycznego i logicznego dostępu, kluczy, kart dostępu, dowodów tożsamości, urządzeń przetwarzania informacji (telefony, nośniki, komputery, urządzenia przenośne), prenumerat i usunięcia jakiegokolwiek dokumentacji identyfikującej byłego pracowników jako obecnego pracownika szkoły.

3.21. Zwalnianie pracownika wymaga powiadomienia ASI, który odpowiada za wycofanie wszystkich uprawnień pracownika do dostępu do systemów informatycznych (dezaktywacja identyfikatorów).

3.22. Jeśli zwalniany pracownik, wykonawca lub osoba trzecia znał aktywne hasła do kont, te powinny być zmienione po wygaśnięciu umowy. Prawa dostępu do aktywów i urządzeń przetwarzania informacji powinny być zredukowane zanim zatrudnienie wygaśnie albo ulegnie zmianie.

3.23. Wszystkie zasady opisane wyżej mają także zastosowanie do:

- 1) zmian charakteru zatrudnienia, pełnionej funkcji, zakresu obowiązków,
- 2) długotrwałych zwolnień lekarskich, urlopów.

#### ***Odpowiedzialność dyscyplinarna***

3.24. Postępowanie dyscyplinarne nie powinno być rozpoczęte bez wcześniejszej weryfikacji, czy nastąpiło naruszenie przepisów bezpieczeństwa. Formalny proces dyscyplinarny powinien zapewniać poprawne i uczciwe traktowanie pracowników podejrzanych o naruszenie bezpieczeństwa.

3.25. W poważnych przypadkach niewłaściwego postępowania, proces powinien uwzględniać natychmiastowe zawieszenie w obowiązkach, utratę dostępu i przywilejów.

#### **4. Podmioty zewnętrzne**

4.1. Dyrektor szkoły odpowiada za identyfikację podmiotów zewnętrznych, którym udostępnia się dane lub aktywa oraz podmioty, którym powierzono przetwarzanie danych (w tym danych osobowych) w formie usługi zewnętrznej.

4.2. Pracownik Sekretariatu prowadzi ewidencję tych podmiotów – zgodnie z załącznikiem do Instrukcji.

4.3. Podmioty te współpracują w oparciu o pisemne umowy (aneksy do istniejących umów), które powinny zawierać:

- 1) zakres świadczonych usług,
- 2) poziom świadczonych usług
- 3) cel i zakres przetwarzanych danych,
- 4) zobowiązanie do zachowania poufności informacji przekazywanych przez szkołę,

- 5) zobowiązanie do zachowania poufności danych osobowych,
- 6) zobowiązanie do przetwarzania danych wyłącznie w celu realizacji umowy,
- 7) zasady upoważniania pracowników podmiotu zewnętrznego do przetwarzania danych (upoważnienia nadaje podmiot zewnętrzny lub PZBI).

- 4.4. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych osobowych na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zobowiązany jest do stosowania zabezpieczeń z art. 36-39a, ogólnego rozporządzenia o ochronie danych.
- 4.5. W przypadku integracji systemu informatycznego z systemem podmiotu zewnętrznego stosuje się zasady wdrażania nowego oprogramowania oraz procedury.
- 4.6. Wszystkie zidentyfikowane wymagania bezpieczeństwa powinny być wprowadzone przed przyznaniem podmiotom zewnętrznym dostępu do informacji lub aktywów należących do szkoły.
- 4.7. Pracownik Sekretariatu dokonuje okresowego przeglądu umów ze stronami trzecimi.
- 4.8. Jeżeli podmiot zewnętrzny uczestniczy w rozwoju oprogramowania, należy w umowie uwzględnić precyzyjnie zasady dostępu tego podmiotu do zasobów, środowiska testowego i zawrzeć przepisy określające jasno odpowiedzialność tego podmiotu za przetwarzanie informacji związanej z rozwijaniem oprogramowaniem. Należy też wymagać posiadania odpowiednich zabezpieczeń, nie mniejszych niż stosowane w szkole.

### **Zabezpieczenia fizyczne**

#### **5. Obszary bezpieczne i obszary podwyższonego bezpieczeństwa**

- 5.1. Wszelka informacja jest na terenie szkoły przetwarzana w obrębie obszarów bezpiecznych. Obszary te są określone w wykazie budynków i pomieszczeń stanowiących obszary bezpieczne, który stanowi załącznik do Instrukcji. Wykaz obejmuje wyraźne oznaczenie granic obszarów oraz zabezpieczenia fizyczne przed nieautoryzowanym dostępem bądź skutkami zdarzeń losowych.
- 5.2. W obrębie obszarów bezpiecznych ustanawia się **obszary podwyższonego bezpieczeństwa (OPB)**, w których znajdują się komponenty szczególnie istotne z punktu widzenia bezpieczeństwa informacji.
- 5.3. OPB musi zapewnić systemowi teleinformatycznemu zabezpieczenie przed:
  - 1) nieautoryzowanym dostępem osób trzecich,
  - 2) uszkodzeniami,
  - 3) zakłóceniami w pracy.
- 5.4. Dostęp do obszarów bezpiecznych mają tylko upoważnieni pracownicy. Pracownicy podmiotów zewnętrznych fizyczny dostęp do obszarów bezpiecznych uzyskują tylko, gdy jest to konieczne, a pracę wykonują w obecności pracownika, chyba, że z umowy pomiędzy podmiotami wynika, że po spełnieniu odpowiednich wymagań mogą zostać indywidualnie upoważnieni w zakresie wymaganym do prowadzenia tych

prac. Osoba odpowiedzialna za pomieszczenie jest zobowiązana zadbać, aby podczas wykonywania prac wszelkie zasoby informacyjne i urządzenia do ich przetwarzania były odpowiednio zabezpieczone i chronione przed dostępem.

- 5.5. Wnoszenie i wynoszenie zasobów informatycznych do/ze obszarów bezpiecznych odbywa się za zgodą dyrektora szkoły i jest rejestrowane.

## **6. Polityka gospodarki kluczami**

- 6.1. W szkole funkcjonuje Polityka dotycząca zasad gospodarki kluczami.
- 6.2. Polityka określa zasady przechowywania i wydawania kluczy do budynku jak i pomieszczeń szkoły.
- 6.3. Z Polityką obowiązani są zapoznać się wszyscy pracownicy szkoły.

## **7. Ochrona poza siedzibą szkoły (obszarami bezpiecznymi)**

- 7.1. Wszelkie nośniki wynoszone poza obszary bezpieczne należy odpowiednio zabezpieczyć.

## **Zabezpieczenia informatyczne**

## **8. Polityka dostępu do systemów**

### **Polityka haseł**

- 8.1. Hasło pierwszego logowania (startowe) zostaje przekazane użytkownikowi w sposób bezpieczny, uniemożliwiający jego przechwycenie przez osoby nieuprawnione.
- 8.2. Hasło pierwszego logowania musi być za każdym razem – o ile system to umożliwia - wygenerowane losowo. Podczas użycia hasła startowego każdy system wymusza jego zmianę.
- 8.3. Hasła użytkowników do systemów podlegają następującym zasadom:
- 1) Hasło składa się z minimum 8 znaków.
  - 2) Hasło musi spełniać warunek złożoności polegający na występowaniu w nim: co najmniej jednej wielkiej i co najmniej jednej małej litery oraz co najmniej jednej cyfry lub znaku specjalnego (np. !@#).
  - 3) Hasło jest zmieniane minimum co 30 dni przez użytkownika.
  - 4) Kolejne hasła muszą być różne. Powtórzenie hasła może nastąpić najwcześniej po 15 jego zmianach.
  - 5) Hasła należy przechowywać w sposób gwarantujący ich poufność.
  - 6) Zabrania się udostępniania swoich haseł innym osobom.
  - 7) Zabrania się tworzenia haseł na podstawie:
    - cech i numerów osobistych (np. dat urodzenia, imion itp.),
    - sekwencji klawiszy klawiatury (np. qwerty, 12qwaszx),
    - identyfikatora użytkownika,
    - dodania znaku do używanego wcześniej hasła skomplikowanego,
    - popularnych wyrażen językowych.

- 8.4. Jeżeli system dopuszcza możliwość blokowania konta ze względu na źle podane hasło, należy korzystać z tej funkcjonalności przy konfiguracji systemu. System może automatycznie odblokować konto po określonym czasie.
- 8.5. Każdy system musi umożliwiać resetowanie hasła przez użytkownika. Do resetowania hasła stosuje się zasady ustanawiania nowego hasła, począwszy od przekazania hasła startowego.
- 8.6. ASI zobowiązany jest do analizowania logowań w systemie pod kątem kont nie używanych ponad 30 dni. Konta nie używane należy wyłączać oraz ustalić powód braku logowań.

### **Dostęp administracyjny**

- 8.7. ASI obowiązują wszystkie zasady opisane w Polityce haseł.
- 8.8. Nazwy kont administracyjnych domyślnie wbudowanych w system są wyłączone zawsze, jeżeli system to umożliwia.
- 8.9. Uruchamianie usług bądź aplikacji w systemach należy wykonywać logując się na konto z uprawnieniami użytkownika, stosując do wykonania zadania narzędzia tymczasowo podnoszące poziom uprawnień.
- 8.10. Hasła kont administracyjnych systemów powinny być deponowane w Rejestrze haseł, który jest zabezpieczony przed dostępem osób nieuprawnionych. Rejestr haseł jest zamknięty w kasie w sekretariacie szkoły.
- 8.11. Po każdej zmianie hasła w systemie administrator wpisuje w Rejestrze nowe hasło..
- 8.12. Otwieranie Rejestru haseł z hasłami administracyjnymi powinno odbywać się tylko w uzasadnionych przypadkach, w razie nieobecności ASI. Użycie hasła administracyjnego systemu może się odbyć tylko za zgodą przełożonego właściciela hasła.

### **9. Zabezpieczenia sieci**

- 9.1. Urządzenia sieciowe, korzystają z zasilania zabezpieczonego UPS.
- 9.2. Dostęp do urządzeń sieciowych posiadają wyłącznie dyrektor i ASI w trybie dostępu administracyjnego.
- 9.3. Zdalny dostęp do portów konfiguracyjnych i diagnostycznych jest możliwy tylko z lokalnej podsieci administracyjnej przez specjalnie upoważnionych administratorów.
- 9.4. Dostęp publiczny do Internetu jest dopuszczony tylko i wyłącznie przez sieć szkolną OSE (m.in. korytarze).
- 9.5. Przed nieautoryzowanym dostępem do środowiska sieciowego chronią:

- 1) stosowanie Polityki haseł
- 2) ograniczenie dostępu z sieci publicznej do niezbędnych zasobów, tylko w zakresie wybranych adresów, portów i protokołów. W tym celu stosuje się firewall skonfigurowany na routerze.
- 3) kontrola nad używaniem zewnętrznych nośników (np. USB, CD)

- 9.6. Przed złośliwym oprogramowaniem w sieci chronią:



- 1) stosowanie na serwerach DNS, oprogramowania antywirusowego G DATA i jego regularna aktualizacja
- 2) zabezpieczenie sieci programem antywirusowym w celu zabezpieczenia przed atakami.

9.7. W przypadku wykrycia wirusa lub innego złośliwego oprogramowania administrator zleca:

- 1) zawiadomienie użytkowników systemu, wydanie instrukcji postępowania
- 2) wyłączenie zainfekowanego systemu
- 3) dokonanie gruntownego sprawdzenia wszystkich systemów
- 4) odseparowanie zainfekowanych systemów
- 5) usunięcie wirusów i złośliwego oprogramowania
- 6) ponowne gruntowne sprawdzenie wszystkich systemów

9.8. Procedury powyższe stosuje się także do złośliwego kodu mobilnego.

9.9. ASI prowadzi dokumentację sieci, uwzględniającą strukturę fizyczną i logiczną, przepływy informacji i zabezpieczenia. Dokumentacja jest chroniona przed nieautoryzowanym dostępem.

## **10. Zabezpieczenia urządzeń**

10.1. Wszystkie urządzenia służące do przetwarzania informacji są umieszczane w obszarach bezpiecznych.

10.2. Wszystkie urządzenia służące do konfiguracji sieci (routery, przełączniki) oraz oferujące usługi w sieci lokalnej i rozległej (serwery) są umieszczane w obszarach podwyższonego bezpieczeństwa (OPB) i korzystają z zasilania zabezpieczonego urządzeniami UPS.

10.3. Komputery osobiste, na których odbywa się przetwarzanie informacji są:

- 1) umieszczone w taki sposób, aby ekrany monitorów i klawiatury były niewidoczne dla osób postronnych,
- 2) zabezpieczone hasłami.

10.4. Pamięci masowe serwerów i macierze dyskowe są skonfigurowane w sposób zapobiegający utracie danych wskutek awarii dysków za pomocą dysków zewnętrznych.

10.5. Urządzenie peryferyjne służące do pracy z informacją papierową (drukarki, skanery, kopiarki) są rozlokowane w taki sposób, aby nie dopuścić do sytuacji, w której osoby pracujące w pomieszczeniu, w którym znajduje się urządzenie nie mają upoważnienia do przetwarzania informacji, która byłaby przetwarzana na tym urządzeniu przez innego użytkownika.

10.6. Każdy nowo instalowany sprzęt służący przetwarzaniu informacji podlega sprawdzeniu w środowisku testowym pod kątem wykrycia ew. wad oraz zgodności z zamówieniem. Sprawdzony sprzęt jest dopuszczany do użytku przez ASI. Dowodem na dopuszczenie sprzętu do użytku jest wprowadzenie go do ewidencji.

- 10.7. Wszelkie okablowanie jest umieszczone w sposób uniemożliwiający dostęp ze strony osób nieupoważnionych, zabezpieczone przed przypadkowym lub celowym uszkodzeniem oraz chronione przed próbami podsłuchu.
- 10.8. Wszelki sprzęt podlega regularnym przeglądom i konserwacjom.
- 10.9. Przy naprawach i konserwacjach sprzętu dokonywanych przez podmioty trzecie poza obszarem bezpiecznym stosuje się przepisy właściwe dla nośników przenośnych, w szczególności istnieje obowiązek szyfrowania informacji zgromadzonej w pamięci masowej naprawianych urządzeń.

## **11. Zabezpieczenia systemów operacyjnych**

- 11.1. System operacyjny każdego urządzenia musi być skonfigurowany w sposób wymuszający podanie hasła użytkownika w celu rozpoczęcia pracy.
- 11.2. Użytkownicy komputerów osobistych posługują się standardowymi kontami użytkownika i nie znają danych logowania kont administracyjnych. Te drugie są znane wyłącznie administratorom wyznaczonym do administracji komputerami osobistymi użytkowników.
- 11.3. Do haseł użytkowników i haseł administracyjnych stosuje się Politykę haseł.
- 11.4. Użytkownicy komputerów osobistych, na których przetwarzana jest informacja muszą mieć uaktywnioną funkcję wygaszania ekranu po maksymalnie 2 minutach braku aktywności, z włączoną opcją wymuszania ponownego uwierzytelnienia użytkownika przy odblokowaniu.
- 11.5. Administratorzy dbają o bieżącą aktualizację systemów operacyjnych poszczególnych urządzeń, zgodnie z polityką wprowadzania zmian.
- 11.6. W każdym systemie operacyjnym obowiązkowo musi być zainstalowane i aktywne oprogramowanie antywirusowe. ASI decyduje, jakie oprogramowanie będzie stosowane. Administratorzy dbają o to by oprogramowanie antywirusowe było aktualne oraz by to oprogramowanie posługiwało się aktualnymi bazami sygnatur wirusów i innego złośliwego oprogramowania.

## **12. Zabezpieczenia aplikacji**

- 12.1. Aplikacja przetwarzająca informację musi wymuszać podanie identyfikatora i hasła użytkownika w celu rozpoczęcia pracy. Wszelkie aplikacje stosowane do przetwarzania informacji muszą spełniać zasady opisane w Polityce haseł.
- 12.2. Aplikacje są instalowane wyłącznie przez administratorów wyznaczonych przez ASI. Zabrania się użytkownikom samodzielnej instalacji jakiegokolwiek oprogramowania na komputerach szkolnych.
- 12.3. Instalacja, aktualizacja i ustawienie parametrów aplikacji są dokonywane zgodnie z politykami konfiguracji i aktualizacji.
- 12.4. Przy instalacji aplikacji wielostanowiskowych na serwerach administratorzy uwzględniają strukturę sieciową pod kątem jej podziału na podsieci i wzajemnego dostępu pomiędzy jej segmentami.
- 12.5. Każda aplikacja przetwarzająca dane (system informatyczny) musi:

- 1) zapewniać unikatowość stosowanych identyfikatorów,

- 2) jeżeli przetwarza dane osobowe – automatycznie rejestrować fakt utworzenia każdego rekordu danych, z zachowaniem daty i czasu utworzenia oraz identyfikatora użytkownika wykonującego tę akcję,
- 3) umożliwiać administratorom przypisanie każdemu użytkownikowi uprawnień do określonych operacji na określonych danych
- 4) zamykać nieaktywne sesje po określonym czasie, maksymalnie 5 minut.

### **13. Zabezpieczenia baz danych**

- 13.1. Przez bazy danych niniejsza Instrukcja rozumie niezależne od innych komponentów oprogramowanie, instalowane na serwerach,
- 13.2. W administracji bazami danych nigdy nie są używane główne konta predefiniowane (root), z wyjątkiem pierwszej konfiguracji.
- 13.3. Serwery baz danych instalowane są w obszarach sieci lokalnej o możliwie najbardziej ograniczonym dostępie. Dostęp do serwerów baz danych jest realizowany tylko:
  - 1) na poziomie maszynowym – przez aplikacje korzystające z tych baz,
  - 2) w trybie administracyjnym – przez upoważnionych administratorów za pomocą konsoli urządzenia, na którym baza jest zainstalowana lub zdalnie – w obrębie specjalnie wydzielonego fragmentu sieci (VLAN administracyjny).

### **14. Polityka wprowadzania zmian**

- 14.1. Wprowadza się trzy typy zmian:
  - 1) prosta,
  - 2) standardowa,
  - 3) awaryjna.
- 14.2. Zmiana prosta charakteryzuje się brakiem spadku poziomu bezpieczeństwa teleinformatycznego usług. Decyzja o zmianie musi być zaakceptowana przez właściwego administratora systemu. Zmiany tej nie poddaje się testom. Do zmian prostych zalicza się:
  - 1) rutynową kolejną instalację tego samego oprogramowania w tej samej wersji w systemie operacyjnym o tych samych parametrach,
  - 2) wymianę stacji roboczej na inną, skonfigurowaną w ten sam sposób,
- 14.3. Zmiana standardowa charakteryzuje się ingerencją w konfigurację systemów teleinformatycznych. Może mieć wpływ na obniżenie poziomu świadczonych usług oraz ich bezpieczeństwo teleinformatyczne. Zmianę standardową akceptuje dyrektor szkoły. Każda tego typu zmiana powinna być wcześniej poddana testom w środowisku testowym. Do zmian standardowych zalicza się:
  - 1) instalację nowego systemu operacyjnego lub oprogramowania,
  - 2) aktualizację systemu operacyjnego lub oprogramowania,
  - 3) zmiany konfiguracji sieci, systemów i aplikacji
  - 4) instalację nowego sprzętu w sieci lokalnej.

- 14.4. Zmiana awaryjna to zmiana zainicjowana przez incydent. Decyzja o takiej zmianie podejmowana jest przez ASI. Zmianę wykonuje się jak najszybciej w celu przywrócenia poziomu usług.
- 14.5. Wszelkie nowo instalowane oprogramowanie musi pochodzić z zaufanego źródła. ASI prowadzi listę zaufanych producentów oprogramowania. W pakietach oprogramowania nie należy dokonywać żadnych zmian.
- 14.6. Oprogramowanie tworzone wewnątrz szkoły lub przez podmiot trzeci na zamówienie szkoły musi spełniać warunki prawidłowego projektowania:
- 1) oprogramowanie tworzone jest na podstawie jasnych założeń obejmujących opis procesów realizowanych z jego pomocą, interfejsu użytkownika, funkcjonalności, ergonomii, wymiany danych i bezpieczeństwa informacji,
  - 2) na kolejnych etapach tworzenia oprogramowania należy kontrolować, czy w każdej fazie przetwarzania informacji (dane wejściowe, przetwarzanie wewnętrzne, dane wyjściowe) aplikacja zwraca wyniki zgodne z oczekiwaniami i czy spełnione są założenia projektowe,
  - 3) do walidacji prawidłowości przetwarzania informacji stosuje się scenariusze testowe przygotowane z udziałem właścicieli procesów, których dotyczy tworzone oprogramowanie.
- 14.7. Każde nowo instalowane oprogramowanie służące przetwarzaniu informacji podlega sprawdzeniu i jest dopuszczane do użytku przez ASI. Dowodem na dopuszczenie programu do użytku jest wprowadzenie go do ewidencji.
- 14.8. Środowisko testowe musi być wierną kopią środowiska produkcyjnego, tzn. mieć identyczne parametry środowiska sieciowego, serwera, systemu operacyjnego, zainstalowanych i działających aplikacji, baz danych oraz innych usług oraz być ściśle oddzielone od środowiska produkcyjnego.
- 14.9. Wszelkie zmiany są odnotowywane w dzienniku ASI.
- 14.10. Do konfiguracji stosowanych wielokrotnie w różnych obszarach systemu (np. ustawień stacji roboczych) stosuje się szablony konfiguracji zatwierdzone przez ASI.

## **15. Polityka archiwizacji, kopii zapasowych i usuwania informacji**

- 15.1. Dla wszystkich aktywów informatycznych określa się zasady archiwizacji i tworzenia kopii zapasowych. Przy określaniu zasad bierze się pod uwagę:
- 1) klasyfikację aktywów pod kątem jawności,
  - 2) zagrożenia i ryzyka związane z utratą integralności i dostępności (w tym ostatnim przypadku w funkcji czasu, w jakim dostępność jest utracona),
  - 3) możliwości techniczne,
  - 4) wymogi prawne i biznesowe,
  - 5) koszt.
- 15.2. Archiwizacja zasobów i wykonywanie kopii zapasowych odbywa się według planu archiwizacji i wykonywania kopii zapasowych, który stanowi załącznik nr 9 do niniejszej Instrukcji.
- 15.3. Dla kopii zapasowych określa się procedurę weryfikacji poprawności wykonanej kopii oraz procedurę odzyskiwania danych z kopii.

15.4. Za realizację planu archiwizacji i wykonywania kopii zapasowych odpowiada ASI.

15.5. Informację:

- 1) skutecznie zarchiwizowaną,
- 2) która nie będzie wykorzystywana a nie podlega archiwizacji,
- 3) zarchiwizowaną, dla której upłynął okres przechowywania, należy usunąć.

15.6. W odniesieniu do nośników przenośnych (pen-drive'y) oraz nośników danych zainstalowanych w komponentach informatycznych – złomowanych lub przekazywanych do naprawy poza siedzibą szkoły stosowane są mechanizmy bezpiecznego kasowania informacji poprzez fizyczne niszczenie (pocięcie, spalanie) nośników,

Wyznaczony administrator dokonuje kontroli prawidłowości usunięcia informacji.

15.7. Nośniki usuwalne, które nie mogą być ponownie wykorzystane, są niszczone.

15.8. Za właściwe skasowanie informacji zawartej na nośniku przenośnym lub w pamięci masowej stacji roboczej odpowiada użytkownik. Za kasowanie informacji z pamięci masowych serwerów oraz nośników kopii archiwalnych i zapasowych odpowiada właściwy administrator.

15.9. ASI dba o dostępność odpowiednich narzędzi umożliwiających bezpieczne usuwanie niepotrzebnych danych.

15.10. Użytkownik lub administrator kasujący dane stanowiące tajemnicę szkoły lub dane osobowe występuje o zgodę do dyrektora szkoły.

15.11. Niszczenie nośnika zostaje odnotowane w protokole zniszczenia, zgodnie z załącznikiem nr 10 do Instrukcji.

## **16. Zasady ochrony kryptograficznej**

16.1. W celu ochrony poufności przesyłanych oraz przechowywanych danych stosuje się zabezpieczenia kryptograficzne. Zabezpieczenia kryptograficzne występują przy:

- 1) wymianie danych z podmiotami zewnętrznymi,
- 2) wymianie poczty elektronicznej
- 3) szyfrowaniu informacji na nośnikach wymiennych,
- 4) szyfrowaniu informacji na urządzeniach mobilnych,
- 5) szyfrowaniu wiadomości poczty elektronicznej
- 6) szyfrowaniu baz danych

16.2. Do szyfrowania połączeń stosuje się połączenia szyfrowane SSL/TLS.

16.3. Do szyfrowania informacji na nośnikach przenośnych stosuje się szyfrowanie plików w kontenerach ZIP lub szyfrowanie plików aplikacjami MS Office ,

16.4. Do szyfrowania informacji na dyskach komputerów przenośnych stosuje się funkcje wbudowane systemu operacyjnego.

16.5. Serwer pocztowy szkoły jest skonfigurowany w sposób wymuszający nawiązanie połączenia bezpiecznego (TLS).

16.6. Wymiana danych z podmiotami zewnętrznymi odbywa się przy użyciu szyfrowania, niezależnie od protokołu.

16.7. W celu przesłania pocztą elektroniczną danych podlegających szczególnej ochronie, stosuje się szyfrowanie poczty za pomocą pary kluczy.

16.8. Klucze tworzone są przez użytkowników.

16.9. ASI odpowiada za:

- 1) przechowywanie danych związanych z ochroną kryptograficzną,
- 2) monitorowanie ważności wydanych certyfikatów i występowanie do podmiotów certyfikujących o ich przedłużenie.

16.10. W stosowaniu zabezpieczeń kryptograficznych bierze się pod uwagę okoliczności prawne, takie jak przepisy ogólnie obowiązujące, prawa autorskie, patenty i umowy.

### **17. Zasady pracy zdalnej**

17.1. Urządzenia mobilne (np. smartfon, tablet, , komputer przenośny) należy użytkować zgodnie z postanowieniami innych regulacji wewnętrznych.

17.2. Wykorzystanie do pracy zdalnej komputerów nie będących własnością szkoły (w szczególności urządzeń prywatnych użytkownika) możliwe jest wyłącznie w odniesieniu do aplikacji oferujących dostęp przez www i przy zachowaniu następujących zasad:

- 1) użytkownik może przechowywać informacje służbowe na urządzeniu, z którego następuje dostęp (pobieranie danych na dysk lokalny) tylko za zgodą dyrektora szkoły- w takiej sytuacji użytkownik powinien zapewnić ochronę stacji roboczej przed dostępem osób nieupoważnionych na poziomie odpowiednim do obowiązujących w szkole wymagań dla ochrony dostępu do tego rodzaju informacji,
- 2) zabrania się korzystania z komputerów dostępnych publicznie (na przykład znajdujących się w kawiarenkach internetowych).

### **18. Przenośne nośniki danych**

18.1. Na nośniku przenośnym dane powinny być przechowywane tylko przez czas do tego niezbędny. Po tym czasie muszą zostać skasowane.

18.2. Użytkownik wynoszący nośnik poza teren szkoły musi uzyskać zgodę dyrektora szkoły.

18.3. Wyniesienie nośnika poza teren szkoły jest odnotowywane wraz z określeniem celu wyniesienia danych przez sekretarza szkoły. Odnotowane powinno również zostać dostarczenie nośnika z powrotem do szkoły.

18.4. Nośniki przenośne podlegają inwentaryzacji prowadzonej przez ASI.

18.5. Nośniki powinny być oznakowane w sposób umożliwiający identyfikację informacji na nich zapisanych, jak również określenie klasyfikacji tej informacji.

18.6. Nośniki danych powinny być przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami losowymi.

## **19. Monitoring systemu**

19.1. ASI regularnie monitoruje wykorzystanie zasobów sprzętowych przez systemy oraz parametry pracy. Do podstawowych elementów, które są monitorowane należą:

- 1) wykorzystanie pamięci masowych,
- 2) wykorzystanie pamięci operacyjnych,
- 3) przepustowość kart sieciowych,
- 4) ruch sieciowy
- 5) obciążenie procesorów,
- 6) uwierzytelnienia w systemie
- 7) próby zdalnego dostępu do usług, portów i zasobów
- 8) pojemności skrzynek pocztowych
- 9) automatycznie wyzwalane procesy systemów operacyjnych
- 10) przebieg sesji pracy zdalnej
- 11) dostęp do Internetu z sieci lokalnej.

19.2. Przy monitoringu śledzi się trendy wykorzystania zasobów. Na ich podstawie przewiduje się konieczność zwiększenia zasobów dla konkretnych systemów.

19.3. Każdy system posiada włączone logowanie zdarzeń związanych z bezpieczeństwem umożliwiające identyfikację źródła zagrożenia. Pliki w których przechowywane są zebrane logi podlegają archiwizacji.

19.4. Logi systemowe są regularnie przeglądane przez administratorów pod kątem wykrycia wszelkich anomalii.

19.5. System tworzenia logów oraz proces ich archiwizacji i przechowywania chroni zapisy przed edycją i nieautoryzowanym dostępem.

19.6. Zegary urządzeń teleinformatycznych są zsynchronizowane w oparciu o serwer czasu pracujący w sieci lokalnej.

19.7. Administratorzy są obowiązani wykrywać wszelkie podatności systemów na zagrożenia związane z bezpieczeństwem informacji. W szczególności proces zarządzania technicznymi podatnościami obejmuje następujące zasady:

- 1) każda zmiana (np. instalacja, deinstalacja sprzętu, oprogramowania, zmiany w konfiguracji), skutkuje koniecznością oceny podatności związanej ze zmianą,
- 2) jeśli potencjalna podatność techniczna została zidentyfikowana, należy zidentyfikować także powiązane podatności i ryzyka,
- 3) jeśli potencjalna podatność techniczna została zidentyfikowana, należy natychmiast podjąć działania ograniczające ryzyko; podjęte działanie powinno pozostawać w zgodzie z zasadami zarządzania zmianami,
- 4) jeśli dostępna jest łąta dla elementu systemu, ryzyka związane z jej instalacją powinny być porównane z ryzykiem związanym z samą podatnością; łąty powinny być przetestowane i ocenione przed instalacją, aby upewnić się, że są skuteczne i nie powodują nietolerowanych efektów ubocznych.

5) Jeśli brak jest dostępnych łąt, można wziąć pod uwagę inne zabezpieczenia:

- wyłączenie usługi lub zasobów związanych z podatnością,
- dostosowanie (uzupełnienie) zabezpieczeń dostępu,
- podwyższony poziom kontroli celem wykrycia lub niedopuszczenia rzeczywistych ataków.

19.8. Dla poszczególnych systemów powinny zostać ustalone priorytety w zakresie kolejności działań w zakresie wykrywania podatności, systemy o wysokim ryzyku powinny być rozpatrywane jako pierwsze.

19.9. Dyrektor szkoły ma prawo do wglądu we wszystkie dane o charakterze służbowym stworzone przez lub dotyczące pracowników i współpracowników znajdujące się na sprzęcie i w oprogramowaniu należących do szkoły.

19.10. W przypadku nieoznaczenia przez użytkownika informacji o charakterze prywatnym, pracodawca nie odpowiada za przypadkowe naruszenie dóbr osobistych pracownika w wyniku wglądu w tę informację.

## **20. Zasady korzystania z Internetu**

20.1. Zasady korzystania z Internetu określają inne regulacje wewnętrzne.

20.2. Do publikacji informacji z Internetu stosuje się Regulamin publikacji informacji w Internetie, który stanowi załącznik nr 10 do Instrukcji.

## **Załączniki:**

- 1) **Załącznik nr 1** – Dziennik administratora
- 2) **Załącznik nr 2** – Ewidencja sprzętu i oprogramowania
- 3) **Załącznik nr 3** – Oświadczenie o poufności
- 4) **Załącznik nr 4** – Wniosek o nadanie upoważnienia
- 5) **Załącznik nr 5** – Ewidencja osób upoważnionych
- 6) **Załącznik nr 6** – Rejestr podmiotów zewnętrznych
- 7) **Załącznik nr 7** – Wykaz obszarów bezpiecznych
- 8) **Załącznik nr 8** – Plan archiwizowania kopii zapasowych
- 9) **Załącznik nr 9** – Protokół zniszczenia nośników komputerowych
- 10) **Załącznik nr 10** – Regulamin zamieszczania informacji w Internetie.