Zarządzenie nr 53/2025
Dyrektora Zespołu Placówek Oświatowych nr 3
w Mławie
z dnia 22 grudnia 2025 r.

w sprawie wprowadzenia dokumentacji Systemu Zarzadzania Bezpieczeństwem Informacji.

Na podstawie:
§ 15 – 20 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2024 r. poz. 773).
§ 6 ust. 2 pkt 9 i 11 Statutu Zespołu Placówek Oświatowych nr 3 w Mławie,

Dyrektor Zespołu Placówek Oświatowych nr 3 w Mławie zarządza, co następuje:

§ 1

W Zespole Placówek Oświatowych nr 3 w Mławie wprowadza się dokumentację Systemu Zarzadzania Bezpieczeństwem Informacji, w skład której wchodzą:

1. Załącznik nr 1 - Polityka Bezpieczeństwa Informacji w Zespole Placówek Oświatowych nr 3 w Mławie.
2. Załącznik nr 2 - Procedura Bezpieczeństwa Fizycznego.
3. Załącznik nr 3 Procedura Zarzadzania Systemem Informatycznym.

§ 2

Dokumentacja Systemu Zarzadzania Bezpieczeństwem Informacji, o której mowa w § 1 powyżej stanowi załącznik do niniejszego zarządzenia.

§ 3

Zarządzenie wchodzi w życie z dniem 1 stycznia 2026 r.

Dyrektor Zespołu Placówek
Oświatowych nr 3 w Mławie
Mariusz Lempek

POLITYKA BEZPIECZEŃSTWA INFORMACJI

w Zespole Placówek Oświatowych

nr 3 w Mławie

<table>
<tr><th colspan="4">POLITYKA BEZPIECZEŃSTWA INFORMACJI</th></tr>
<tr><td>SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI</td><td>Strona/ stron</td><td>1/22</td><td rowspan="2">Załącznik nr 1 do Zarządzenia nr 53/2025 Dyrektora Zespołu Placówek Oświatowych nr 3 w Mławie z dnia 22 grudnia 2025 r.</td></tr>
<tr><td>Cel dokumentu: Określenie zakresu i ramowych zasad obowiązywania Systemu Zarządzania Bezpieczeństwem Informacji w Zespole Placówek Oświatowych nr 3 w Mławie</td><td>Wersja nr: 1
Z dnia: 22 grudnia 2025 r.</td><td>1
1/2025</td></tr>
</table>

Spis treści

Rozdział I – Informacje ogólne

§1. Wprowadzenie

1. Polityka Bezpieczeństwa Informacji, zwana dalej „Polityką", określa podstawowe zasady zarządzania bezpieczeństwem informacji, jakie przyjmuje Zespół Placówek Oświatowych nr. 3 w Mławie, zwany dalej „Zespołem" w jednostkach wchodzących w skład Zespołu Placówek Oświatowych nr 3 w Mławie.
2. Zasady zarządzania bezpieczeństwem informacji w Zespole zostały opracowane zgodnie z obowiązującymi przepisami prawa w oparciu o wymagania Polskich Norm i standardów w obszarze bezpieczeństwa informacji, w tym w szczególności:
    a. Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
    b. Ustawą z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne.
    c. rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
    d. Normą PN-EN ISO/IEC 27001:2022 – Systemy zarządzania bezpieczeństwem informacji.
3. Polityką objęte są wszystkie informacje przetwarzane w Zespole – niezależnie od formy (elektronicznej, papierowej, ustnej itp.) i nośnika – będące własnością Zespołu lub powierzone jej na podstawie umów i porozumień. Dotyczy to w szczególności danych osobowych wychowanków, uczniów, rodziców i pracowników, dokumentacji szkolnej i przedszkolnej oraz innych informacji chronionych. Postanowienia Polityki obowiązują wszystkich pracowników Zespołu (nauczycieli, pracowników administracji i obsługi, osoby zatrudnione na podstawie umów cywilnoprawnych) oraz inne osoby mające dostęp do informacji chronionych Zespołu.
4. Polityką objęte są aktywa sprzętowe będące własnością Zespołu, służące do przetwarzania danych za które prawną odpowiedzialność ponosi Zespołu i przez nią zarządzane, obejmujące:
    a. Komputery administracji Zespołu,
    b. Sprzęt sieciowy,
    c. Urządzeń serwerowych oraz przechowywania danych (jeżeli występują).
5. Z niniejszej polityki wyłączone są (poza punktami ich dotyczącymi):
    a. Komputery nie będące własnością Zespołu, ale wykorzystywane w celach dydaktycznych po uzyskaniu wcześniejszej zgody

b. Komputery i sprzęt udostępniony uczniom do celów dydaktycznych, który nie służy do przetwarzania danych za które prawną odpowiedzialność ponosi Zespół.

§2. Terminy i definicje

1. **Zespół:** Zespół Placówek Oświatowych nr 3 w Mławie.
2. **Dyrektor**: Zespołu Placówek Oświatowych nr 3 w Mławie.
3. **Dostępność** - właściwość polegająca na tym, że informacja jest dostępna i użyteczna na żądanie upoważnionego podmiotu.
4. **Informacje chronione** – wszelkie informacje przetwarzane w Zespole, które nie są przeznaczone do publicznego rozpowszechniania (np. dane osobowe, dokumentacja wewnętrzna, tajemnice służbowe).
5. **Integralność** - właściwość polegająca na zapewnieniu dokładności i kompletności informacji.
6. **KRI** - Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych
7. **Obsługa informatyczna** – osoba lub podmiot wyznaczony do realizacji zadań w zakresie zarządzania, bieżącego nadzoru nad systemami informatycznymi oraz serwisu sprzętu komputerowego w Zespole;
8. **Poufność** - właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom.
9. **Użytkownik** - pracownik, stażysta, praktykant lub inna osoba wykonująca pracę bądź świadcząca usługi na podstawie umów cywilnoprawnych na rzecz Zespołu, która posiada dostęp do informacji chronionych w Zespole;
10. **ASI - Administrator systemów informatycznych –** Zespół Placówek Oświatowych nr 3 w Mławie lub wyznaczony administrator danego systemu informatycznego.
11. **Incydent** – zdarzenia pojedyncze lub seria niepożądanych zdarzeń związanych z bezpieczeństwem danych osobowych, informacji, które zagrażają przetwarzaniu danych osobowych, informacji lub naruszają zdefiniowane wymagania bezpieczeństwa albo stwarzają znaczne prawdopodobieństwo zakłócenia w prowadzeniu działań prawnych;
12. **Cyberbezpieczeństwo** odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

13. **Podatność** właściwość systemu informacyjnego, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa,
14. **Ryzyko** wpływ niepewności na cele.
15. **Zarządzanie Ryzykiem** system metod i działań zmierzających do obniżenia ryzyka do poziomu akceptowalnego, przy uwzględnieniu kosztów działania oraz zabezpieczenia się w racjonalny sposób przed jego skutkami, obejmuje identyfikowanie i ocenę ryzyka oraz reagowanie na nie; proces zarządzania ryzykiem obejmuje ryzyko występujące we wszystkich procesach decyzyjnych i na każdym szczeblu zarządzania.
16. **Identyfikacja Ryzyka** proces wyszukiwania, rozpoznawania i opisywania ryzyka.
17. **Analiza Ryzyka** proces dążący do poznania charakteru ryzyka oraz określenia poziomu ryzyka.
18. **Kryteria Ryzyka** poziomy odniesienia, względem których określa się sposób postępowania z ryzykiem.
19. **Zdarzenie** wystąpienie lub zmiana konkretnego zestawu okoliczności.
20. **Dostępność informacji** właściwość polegającą na tym, że informacja jest możliwa do wykorzystania przez uprawniony podmiot na jego żądanie, w założonym czasie.
21. **Integralność informacji** właściwość polegającą na tym, że informacja nie została zmodyfikowana w sposób nieuprawniony.
22. **Poufność informacji** właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom.
23. **Zgodność prawna** właściwość polegająca na tym, że dane działanie związane z informacją jest zgodne z przepisami powszechnie obowiązującego prawa, któremu podlega działalność Urzędu.

Rozdział II - Organizacja bezpieczeństwa informacji

§3. Role i odpowiedzialności

1. **Dyrektor Zespołu Szkół** ponosi nadrzędną odpowiedzialność za bezpieczeństwo informacji. Do zadań Dyrektora należy w szczególności:
    a. ustanawianie i zatwierdzanie polityk oraz procedur bezpieczeństwa, zapewnienie zgodności z przepisami (w tym KRI),
    b. wyznaczanie celów i zasobów niezbędnych do ochrony informacji,
    c. podejmowanie decyzji w sytuacjach naruszeń bezpieczeństwa,
    d. przeprowadzanie okresowych analiz ryzyka i przeglądów bezpieczeństwa, a także inicjowanie działań korygujących i doskonalących.

e. sprawowanie nadzoru nad przestrzeganiem niniejszej Polityki oraz powiązanych procedur przez wszystkich pracowników.

2. **Obsługa informatyczna (Administrator systemów informatycznych)** – zewnętrzny podmiot (CUW) lub osoba świadcząca usługi informatyczne na rzecz Zespołu. Do jego obowiązków należą:
   a. bieżące utrzymanie i zabezpieczanie infrastruktury teleinformatycznej Zespołu (sprzętu komputerowego, sieci, oprogramowania),
   b. zarządzanie kontami i uprawnieniami użytkowników systemów informatycznych,
   c. instalowanie aktualizacji i oprogramowania ochronnego (np. antywirusowego, zapór sieciowych),
   d. bieżące usuwanie awarii sprzętu i usterek systemowych,
   e. prowadzenie ewidencji sprzętu i oprogramowania,
   f. doradztwo techniczne dla Dyrektora.
   g. realizacja technicznych i organizacyjnych środków bezpieczeństwa określonych w Polityce oraz za reagowanie na incydenty informatyczne.
3. **Pracownicy Zespołu Szkół** – każdy pracownik (w tym nauczyciel oraz pracownik administracji i obsługi) jest zobowiązany do:
   a. przestrzegania niniejszej Polityki i związanych z nią procedur.
   b. właściwego zabezpieczania informacji, do których mają dostęp, w szczególności: zachowanie poufności danych (także po ustaniu zatrudnienia), stosowanie zasad bezpiecznego użytkowania systemów (np. używanie haseł, nieudostępnianie kont, zabezpieczanie dokumentów papierowych),
   c. natychmiastowego zgłaszania wszelkich incydentów bądź słabości zabezpieczeń przełożonemu, Dyrektorowi lub obsłudze informatycznej
   d. uczestniczenia w szkoleniach z zakresu bezpieczeństwa informacji i potwierdzenia znajomości obowiązujących regulacji wewnętrznych
4. Obowiązki i uprawnienia konkretnych ról mogą zostać uszczegółowione w zakresach czynności pracowników oraz w indywidualnych poleceniach służbowych Dyrektora Zespołu.

§4. Świadomość i szkolenia

1. Zespół zapewnia swoim pracownikom regularne **szkolenia** z zakresu bezpieczeństwa informacji i ochrony danych (np. szkolenie wstępne przy rozpoczęciu pracy oraz szkolenia okresowe raz do roku lub w miarę potrzeb).
2. Szkolenia obejmują m.in. zasady określone w niniejszej Polityce, procedury reagowania na incydenty, najlepsze praktyki przy korzystaniu z systemów informatycznych oraz przepisy o ochronie danych osobowych. Ponadto udostępniane są materiały edukacyjne (instrukcje, poradniki) przypominające o zasadach bezpieczeństwa.
3. Udział pracowników w szkoleniach wewnętrznych jest potwierdzany (np. listą obecności), zaś w szkoleniach zewnętrznych – odpowiednimi certyfikatami lub zaświadczeniami, archiwizowanymi w aktach osobowych.
4. Każdy pracownik po zapoznaniu się z Polityką i procedurami podpisuje oświadczenie o zapoznaniu się z nimi i zobowiązaniu do ich przestrzegania.

Rozdział III – Klasyfikacja informacji

§5. Rodzaje informacji

1. W Zespole dokonuje się klasyfikacji informacji w celu właściwego stosowania zabezpieczeń. Przyjmuje się podział na dwie podstawowe kategorie:
    a. **Informacje publiczne –** informacje jawne, przeznaczone do powszechnego udostępniania. Obejmują one w szczególności dane i komunikaty publikowane na oficjalnej stronie internetowej Zespołu, informacje udzielane na wniosek w trybie ustawy o dostępie do informacji publicznej oraz inne materiały oficjalnie przeznaczone do upublicznienia.
    b. **Informacje chronione –** wszelkie informacje o ograniczonym dostępie, nieprzeznaczone do publicznego ujawniania. Zaliczają się tu m.in. dane osobowe uczniów i wychowanków, rodziców i pracowników, dokumentacja pedagogiczna i administracyjna, informacje finansowe Zespołu, dane w systemach takich jak dziennik elektroniczny, System Informacji Oświatowej (SIO), wewnętrzna korespondencja służbowa itp. Informacje chronione wymagają zastosowania odpowiednich środków bezpieczeństwa i mogą być udostępniane wyłącznie osobom upoważnionym.

2. Wszyscy pracownicy są zobowiązani do właściwego postępowania z informacjami stosownie do ich klasyfikacji. Informacje chronione powinny być zabezpieczane przed dostępem osób nieuprawnionych. Udostępnienie informacji chronionych podmiotom zewnętrznym może nastąpić jedynie za zgodą Dyrektora i jeśli wynika to z przepisów prawa lub zawartych umów.

Rozdział IV – Postępowanie z ryzykiem

§6. Analiza ryzyka

1. W celu właściwego nadzoru nad bezpieczeństwem informacji przetwarzanych w Zespole wdraża się proces zarządzania ryzykiem. Polega on na identyfikacji i ocenie ryzyk mogących negatywnie wpłynąć na poufność, integralność lub dostępność informacji przetwarzanych w Zespole, a następnie na podejmowaniu odpowiednich działań w celu ograniczenia tych ryzyk do akceptowalnego poziomu.
2. **Analiza ryzyka** – co najmniej raz w roku oraz przy każdej istotnej zmianie (np. wdrożenie nowego systemu informatycznego, zmiana przepisów, powstanie nowych zagrożeń) Dyrektor Zespołu inicjuje przeprowadzenie analizy ryzyka. Analiza obejmuje zidentyfikowanie wartościowych aktywów informacyjnych, potencjalnych zagrożeń oraz podatności. Dla zidentyfikowanych zagrożeń szacuje się prawdopodobieństwo i skutki ich materializacji.
3. **Postępowanie z ryzykiem** – na podstawie wyników analizy ryzyka Dyrektor decyduje o rodzaju reakcji na ryzyka: może zlecić wdrożenie dodatkowych zabezpieczeń obniżających ryzyko (np. szkolenie pracowników, aktualizacja oprogramowania, zmiana procedur), może dokonać przeniesienia ryzyka (np. poprzez ubezpieczenie lub powierzenie zadania wyspecjalizowanemu podmiotowi), zaakceptować ryzyko na obecnym poziomie lub – w razie nieakceptowalnie wysokiego ryzyka – czasowo wstrzymać dany proces. Decyzje te są dokumentowane.
4. **Przegląd ryzyk** – Dyrektor zapewnia bieżący monitoring ryzyka bezpieczeństwa informacji. W razie wystąpienia incydentu bezpieczeństwa lub istotnej zmiany warunków (np. pojawienie się nowego zagrożenia cybernetycznego) ryzyko jest niezwłocznie ponownie analizowane i oceniane.
5. Celem zarządzania ryzykiem jest zapobieganie naruszeniom bezpieczeństwa informacji poprzez ciągłe doskonalenie stosowanych zabezpieczeń adekwatnie do zmieniających się zagrożeń i warunków działania Zespołu.

6. Szacowania ryzyka dokonuje się na **Arkuszu analizy ryzyka**, którego wzór stanowi **Załącznik nr 1** do niniejszej Polityki.

Rozdział V – Zabezpieczenia

§7. Deklaracja stosowania zabezpieczeń

1. Niniejszym Dyrektor Zespołu deklaruje, że zostały przeanalizowane wszystkie potencjalne zagrożenia odnoszące się do bezpieczeństwa informacji i na podstawie analizy ryzyka oraz wymagań prawnych wybrano do wdrożenia odpowiednie zabezpieczenia.

§8. Bezpieczeństwo fizyczne informacji

1. Budynek i pomieszczenia Zespołu są zabezpieczone przed dostępem osób postronnych oraz przed zagrożeniami środowiskowymi (pożarem, zalaniem itp.) zgodnie z ***Procedurą bezpieczeństwa fizycznego***. Wszystkie pomieszczenia, w których przetwarzane są informacje chronione (np. sekretariat, gabinet dyrektora, archiwum czy pokój nauczycielski), pozostają pod kontrolą upoważnionych pracowników i są zamykane na klucz poza godzinami pracy. Pomieszczenia zawierające najbardziej poufne informacje stanowią strefy o ograniczonym dostępie – dostęp do nich posiada jedynie ściśle określony personel za zgodą Dyrektora. Zespół wdrożyła monitoring wizyjny (CCTV) obejmujący wejścia do budynku i główne korytarze, celem ochrony uczniów, pracowników i mienia. Stosuje się środki ochrony przeciwpożarowej (gaśnice) oraz inne zabezpieczenia fizyczne adekwatne do zagrożeń.

§9. Kontrola dostępu do informacji i systemów

1. Dostęp do informacji chronionych oraz do systemów informatycznych jest ograniczony wyłącznie do osób upoważnionych i realizowany na zasadzie **minimum uprawnień** (każdy użytkownik otrzymuje tylko takie uprawnienia, jakie są niezbędne do wykonywania jego obowiązków służbowych).
2. Każdy pracownik korzysta z indywidualnego identyfikatora (loginu) i hasła do systemów – niedopuszczalne jest udostępnianie swojego konta lub hasła innym osobom.
3. Przyznawanie i odbieranie uprawnień odbywa się według formalnego procesu nadzorowanego przez Dyrektora (szczegóły reguluje ***Procedura zarządzania systemem informatycznym***).

W razie ustania potrzeby dostępu (np. zakończenie pracy danego pracownika) dostęp do informacji i systemów jest natychmiast odbierany – konta użytkownika są blokowane lub usuwane, a upoważnienia do danych osobowych odwoływane.

4. Stosuje się mechanizmy uwierzytelnienia użytkowników odpowiadające dobrym praktykom bezpieczeństwa: wymóg silnych haseł (o minimalnej długości i złożoności), okresowa zmiana haseł (zalecana co 90–180 dni lub niezwłocznie w razie podejrzenia, że hasło mogło zostać ujawnione), automatyczne blokowanie kont po wielokrotnym błędnym logowaniu (o ile przewiduje to dany system). Hasła nie są nigdzie przechowywane w formie otwartego tekstu ani przekazywane osobom nieuprawnionym. Użytkownicy zobowiązani są chronić swoje hasła przed ujawnieniem (nie wolno zapisywać haseł w miejscach dostępnych dla osób trzecich ani używać tych samych haseł do celów służbowych i prywatnych).
5. W miarę dostępności funkcjonalnej zaleca się wykorzystywanie uwierzytelniania dwuskładnikowego (2FA) dla kont uprzywilejowanych i dostępu zdalnego do systemów (np. dla administratorów usług chmurowych). W celu wykorzystania mechanizmów uwierzytelnienia wieloskładnikowego Zespół dopuszcza wykorzystanie własnego sprzętu w celu implementacji systemów i tokenów uwierzytelniających.

§10. Bezpieczne użytkowanie sprzętu i nośników informacji

1. Pracownicy są zobowiązani korzystać z komputerów, urządzeń mobilnych oraz nośników danych (np. pendrive'ów) w sposób zabezpieczający informacje przed utratą lub nieautoryzowanym wglądem. Należy:
    a. Zabezpieczać urządzenia przed dostępem osób postronnych: nie zostawiać włączonych komputerów bez nadzoru (obowiązek wylogowania się lub zablokowania ekranu przy opuszczeniu stanowiska), chronić urządzenia przenośne przed kradzieżą lub zagubieniem (np. nie pozostawiać laptopa czy telefonu bez opieki w miejscach publicznych);
    b. Wykorzystywać wyłącznie autoryzowane i legalne oprogramowanie oraz urządzenia: instalowanie nowego oprogramowania na komputerach szkolnych/przedszkolnych lub podłączanie prywatnych urządzeń do sieci szkolnej/przedszkolnej wymaga zgody obsługi informatycznej lub Dyrektora. Zabrania się samowolnego instalowania programów bez licencji lub niezatwierdzonych przez Zespół oraz kopiowania oprogramowania niezgodnie z licencją;
    c. Unikać działań mogących narazić systemy na zagrożenia: pracownicy nie powinni otwierać podejrzanych załączników e-mail ani korzystać z niezaufanych nośników

danych bez uprzedniego sprawdzenia ich programem antywirusowym. Nie wolno również wykorzystywać szkolnej/przedszkolnej infrastruktury IT do celów sprzecznych z prawem lub z zasadami etyki (np. rozsyłania spamu, treści obraźliwych).

2. Dopuszcza się wykorzystywanie prywatnych komputerów i smartfonów przez nauczycieli oraz uprawnionych pracowników do celów służbowych (np. zdalny dostęp do dziennika elektronicznego, poczty służbowej), jednakże użytkownik takiego urządzenia ma obowiązek zapewnić na nim adekwatny poziom zabezpieczeń. W szczególności:
    a. urządzenie prywatne używane do pracy powinno posiadać aktualne oprogramowanie systemowe i antywirusowe,
    b. być zabezpieczone silnym hasłem/PIN-em lub inną blokadą przed dostępem osób postronnych,
    c. o ile to możliwe – mieć włączone szyfrowanie danych (np. szyfrowanie dysku telefonu lub laptopa).
    d. na prywatnych urządzeniach nie należy przechowywać lokalnie wrażliwych danych szkolnych/przedszkolnych, chyba że jest to niezbędne i odpowiednio zabezpieczone,
    e. jeżeli z urządzenia korzystają osoby postronne, dane Zespołu muszą być zawarte na odrębnym, izolowanym i zabezpieczonym profilu urządzenia.
3. W razie utraty lub kradzieży prywatnego urządzenia wykorzystywanego do celów służbowych, użytkownik ma obowiązek niezwłocznie powiadomić o tym Dyrektora i Inspektora Ochrony Danych, aby można było podjąć działania chroniące przed ewentualnym wyciekiem informacji (np. zmiana haseł, zdalne wymazanie danych jeśli to możliwe).
4. Zespół zastrzega sobie prawo ograniczenia lub wycofania zgody na używanie prywatnych urządzeń do pracy, jeżeli stwarza to nadmierne ryzyko dla bezpieczeństwa informacji.
5. Nośniki danych zawierające informacje chronione (np. pendrive z danymi, płyty CD, dyski z kopiami zapasowymi) muszą być przechowywane w zabezpieczonych miejscach (zamykane szafki, sejfy) i dostępne tylko dla upoważnionych osób. Zaleca się stosowanie szyfrowania nośników przenośnych z danymi wrażliwymi.
6. Dokumenty papierowe zawierające informacje chronione powinny być pod bezpośrednim nadzorem pracownika uprawnionego lub przechowywane w zamkniętych szafach, aby osoby postronne (w tym uczniowie czy odwiedzający rodzice) nie miały do nich dostępu.
7. Po wykorzystaniu dokumentów zawierających dane chronione należy je zniszczyć w sposób uniemożliwiający odczyt (przekazać do zniszczenia niszczarką) – dotyczy to również wydruków próbnych lub błędnych.

§11. Bezpieczeństwo teleinformatyczne i techniczne

I. Zabezpieczenia sieciowe

1. Komputerowa sieć Zespołu jest chroniona przed dostępem z zewnątrz za pomocą sprzętowej i programowej zapory (firewall), w tym routera z odpowiednią konfiguracją bezpieczeństwa.
2. Dostęp do sieci bezprzewodowej Wi-Fi jest zabezpieczony hasłem i ograniczony do uprawnionych użytkowników (np. osobna sieć dla pracowników, osobna dla urządzeń uczniowskich lub gościnnych, z odseparowaniem od zasobów wewnętrznych administracji).
3. W miarę potrzeby stosuje się segmentację sieci (VLAN) w celu oddzielenia ruchu sieciowego różnych grup użytkowników i zwiększenia bezpieczeństwa, co ogranicza ryzyko rozprzestrzeniania się złośliwego oprogramowania.

II. Ochrona antywirusowa i aktualizacje

1. Wszystkie komputery w Zespole mają zainstalowane oprogramowanie antywirusowe z włączoną ochroną w czasie rzeczywistym. Bazy sygnatur wirusów oraz samo oprogramowanie zabezpieczające są aktualizowane automatycznie (lub na bieżąco przez obsługę informatyczną).
2. Obsługa informatyczna monitoruje stan zabezpieczeń antywirusowych – w przypadku wykrycia złośliwego oprogramowania podejmowane są niezwłoczne działania w celu usunięcia zagrożenia (oczyszczenie/zablokowanie zainfekowanego urządzenia, powiadomienie użytkownika i Dyrektora, przeanalizowanie źródła incydentu). Ponadto, na wszystkich komputerach aktywowane są lokalne zapory systemowe (firewall) i inne mechanizmy ochronne systemów operacyjnych.
3. Zespół dba o aktualność oprogramowania – systemy operacyjne, aplikacje użytkowe oraz urządzenia sieciowe są regularnie aktualizowane w celu eliminacji znanych podatności bezpieczeństwa. Administrator systemów informatycznych odpowiada za wdrażanie aktualizacji krytycznych niezwłocznie po ich udostępnieniu przez producentów (po upewnieniu się, że nie zakłócą one pracy systemu). Tam, gdzie to możliwe, włączone są automatyczne aktualizacje.

III. Kopie zapasowe i archiwizacja

1. Dla zabezpieczenia dostępności i integralności ważnych danych Zespołu wykonuje się regularne **kopie zapasowe** (backup). Dane krytyczne dla działania Zespołu, takie jak baza dziennika elektronicznego, są zabezpieczone kopiami wykonywanymi przez dostawcę usługi (zgodnie z umową z operatorem dziennika elektronicznego kopie bazy danych dziennika są tworzone i przechowywane na serwerach dostawcy).

2. Zespół zapewnia tworzenie kopii zapasowych istotnych danych przechowywanych lokalnie – np. dokumentów administracyjnych, baz danych czy konfiguracji urządzeń. Kopie zapasowe lokalnych danych mogą być wykonywane na szyfrowane nośniki zewnętrzne lub na zaszyfrowaną chmurę dyskową; częstotliwość ich wykonywania jest dostosowana do charakteru danych (np. codziennie dla często zmieniających się danych, tygodniowo lub miesięcznie dla pozostałych).
3. Nośniki z kopiami zapasowymi są przechowywane w bezpiecznej lokalizacji, chroniącej je przed zniszczeniem oraz dostępem niepowołanych osób.
4. Dostęp do kopii mają wyłącznie upoważnione osoby (np. Dyrektor, ASI).
5. Okresowo sprawdzana jest poprawność wykonanych kopii oraz możliwość odtworzenia z nich danych (testy przywracania), aby mieć pewność, że w razie awarii informacje mogą zostać odzyskane

Rozdział VII – Incydenty i naruszenia

§12. Incydenty bezpieczeństwa informacji

1. Kwalifikowanie incydentów bezpieczeństwa informacji

1. Incydent lub zdarzenie związane z bezpieczeństwem informacji może zgłosić każdy pracownik, petent, przedstawiciel instytucji, na każdym etapie procesów lub świadczonej usługi.
2. Pracownicy są zobowiązani do reagowania na zdarzenia związane z bezpieczeństwem informacji, incydenty związane z bezpieczeństwem informacji, w tym incydenty stanowiące naruszenie ochrony danych osobowych.
3. W zakresie obsługi incydentów pracownicy podlegają szkoleniu w ramach szkolenia wstępnego oraz obowiązkowo podczas szkoleń okresowych.
4. Za kontakty z osobami z zewnątrz jednostki w tym mediami odpowiedzialny jest **Dyrektor**.
5. Za incydent przyjmuje się praktycznie każde zdarzenie, które nie należy do standardowych operacji i które powoduje lub może powodować:
   1) zakłócenia lub przerwy w funkcjonowaniu urzędu, np. cyklicznie powtarzające się takie zdarzenia związane z określoną niedostępnością systemów mających wpływ na normalny tok pracy, lub możliwości świadczenia usług w okresie przekraczającym **15 min**,
   2) zmiany w zakresie informacji świadczące o braku integralności danych,
   3) ujawnienie lub dostęp do informacji przez osoby nieupoważnione,
   4) utrata danych.

4. Postępowanie z incydentami bezpieczeństwa informacji

4.1. Reakcja na incydent bezpieczeństwa informacji.

Dyrektor (lub upoważniona przez niego osoba) po otrzymaniu zgłoszenia incydentu dokonuje wstępnej oceny sytuacji, podejmuje natychmiastowe działania ograniczające skalę incydentu (np. odłączenie zainfekowanego komputera od sieci, zmiana haseł, zabezpieczenie miejsca zdarzenia) oraz zapewnia udokumentowanie okoliczności incydentu.

4.2. Zgłaszanie incydentów bezpieczeństwa informacji.

1. Zgłaszanie zdarzeń i incydentów bezpieczeństwa informacji realizowane jest w następujący sposób:
   1) Zgłaszanie i rejestrowanie incydentów **musi być przeprowadzone mailowo na adres incydent@mlawa.pl oraz do obsługi informatycznej**.
   2) Osoba odpowiedzialna za zarzadzanie incydentami Cyberbezpieczeństwa rejestruje i zgłasza zdarzenie.
   3) Każdy pracownik podczas obserwacji zdarzenia, incydentu związanego z bezpieczeństwem informacji powinien sprawdzić schemat postępowania. Jeżeli dla danego zdarzenia nie określono inaczej, pracownik ma obowiązek zgłosić zdarzenie lub incydent osobie odpowiedzialnej za zarzadzanie incydentami Cyberbezpieczeństwa.
   4) W przypadku nieobecności osoby, o której mowa powyżej, incydent zgłaszany jest bezpośredniemu przełożonemu, który rejestruje i zgłasza incydent.
   5) W przypadku nieobecności bezpośredniego przełożonego, incydent rejestruje i zgłasza bezpośrednio pracownik, który zaobserwował incydent związany z bezpieczeństwem informacji.
2. W przypadku, gdy incydent zgłasza strona zewnętrzna (np. dostawca, petent, gość), każdy pracownik zobowiązany jest do przyjęcia zgłoszenia i postępowania zgodnie z punktem powyżej.
3. Odbiorcą zgłoszenia przesłanego drogą mailową na adres **incydent@mlawa.pl** jest Osoba odpowiedzialna za utrzymywanie kontaktów w zakresie Cyberbezpieczeństwa (zgodnie z zarządzeniem Burmistrza UM Mława) w Urzędzie Miasta Mława.

4. W przypadku zgłoszeń związanych z naruszeniem ochrony danych osobowych Osoba odpowiedzialna za utrzymywanie kontaktów w zakresie Cyberbezpieczeństwa, na podstawie otrzymanego zgłoszenia przekazuje je na adres **iod@cuw.mlawa.pl** lub telefonicznie do Inspektora Ochrony Danych Osobowych.
5. Przekazując informację o zdarzeniu należy w szczególności wskazać (wzór zawiera Załącznik nr 1):
   a) Dane zgłaszającego: Imię i Nazwisko, email, telefon oraz stanowisko i komórkę organizacyjną,
   b) Datę i godzinę oraz miejsce obserwacji incydentu,
   c) Opis zdarzenia (zasięg incydentu, liczba osób których dotyczy zgłoszenie),
   d) Inne informacje mogące mieć wpływ na ocenę zdarzenia.
6. Jeżeli istnieje taka możliwość – pracownik zobowiązany jest do dostarczenia materiału dowodowego potwierdzającego incydent (np. zdjęcia, zapisy z systemów itd.) wraz ze zgłoszeniem incydentu.
7. Zebrany materiał dowodowy dla zgłoszenia incydentu podlega archiwizacji przez okres **co najmniej dwóch lat**.

4.2. Analiza zgłoszonych incydentów bezpieczeństwa informacji

1. Po dokonaniu zgłoszenia incydentu do właściwej osoby następuje weryfikacja zgłoszenia, pod kątem poprawności wypełnienia, w szczególności:
   1) kompletny opis zdarzenia / incydentu (wskazanie osób, sytuacji, zasobów uczestniczących w incydencie),
   2) wpływ incydentu na ryzyko naruszenia praw i wolności osób (w przypadku naruszenia ochrony danych osobowych) i zawiadomienia osób, których dane dotyczą oraz Urzędu Ochrony Danych Osobowych,
   3) wpływ incydentu na ryzyko zagadnienia cyberbezpieczeństwa,
   4) podjęte i zaplanowanie działania naprawcze w następstwie incydentu,
   5) skuteczność podjętych natychmiastowych działań naprawczych,
   6) ewentualne koszty podjętych działań naprawczych do strat spowodowanych przez naruszenie.
2. Informacja o incydentach powinna być okresowo przekazana do Inspektora Ochrony Danych w celu określenia potrzeby wykonania ponownej analizy ryzyka pod kątem bezpieczeństwa informacji.

3. Po przeprowadzeniu analizy, każdy incydent, który wymaga podjęcia dodatkowych środków naprawczych powinien zostać przedstawiony **Dyrektorowi** wraz z planem postępowania przez Osobę odpowiedzialną za utrzymywanie kontaktów w zakresie Cyberbezpieczeństwa.
4. Pracownicy biorący udział w incydencie powinni otrzymać informacje zwrotne co do jego obsługi i skutków oraz dodatkowe instrukcje, a w uzasadnionych przypadkach – zostają ponownie przeszkoleni z zasad bezpieczeństwa.
5. Wszystkie zaistniałe incydenty należy rejestrować (wzór rejestru zawiera Załącznik nr 2) oraz postępowanie z nimi podlega rocznemu przeglądowi. Podczas przeglądu zarządzania może być przeprowadzana analiza i mogą być ustalane ewentualne strategiczne działania korygujące wynikające długookresowej analizy incydentów.
6. Jeżeli Incydent stanowi incydent w zakresie cyberbezpieczeństwa, zdarzenie takie zgłaszane jest do CSIRT NASK w terminie 24 godzin od momentu wykrycia zdarzenia.
7. W zgłoszeniu uwzględnia się w szczególności:
   1) dane podmiotu zgłaszającego, w tym nazwę podmiotu, numer we właściwym rejestrze, siedzibę i adres,
   2) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby składającej zgłoszenie,
   3) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji,
   4) opis wpływu incydentu w podmiocie publicznym na realizowane zadanie publiczne, w tym:
      a) wskazanie zadania publicznego, na które incydent miał wpływ,
      b) liczbę osób, na które incydent miał wpływ,
      c) moment wystąpienia i wykrycia incydentu oraz czas jego trwania,
      d) zasięg geograficzny obszaru, którego dotyczy incydent,
      e) przyczynę zaistnienia incydentu i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne,
      f) informacje o przyczynie i źródle incydentu,
      g) informacje o podjętych działaniach zapobiegawczych,
      h) informacje o podjętych działaniach naprawczych,
      i) inne istotne informacje.

4.3. Współpraca z podmiotami zewnętrznymi

1. W razie poważnego incydentu, Zespół może skorzystać z pomocy wyspecjalizowanych służb i instytucji. Incydenty, które mogą mieć charakter przestępstwa (takie jak włamanie, kradzież lub cyberatak), powinny być zgłaszane odpowiednim organom ścigania (policji lub prokuraturze).
2. Dyrektor jest również odpowiedzialny za ewentualne udzielanie informacji mediom, rodzicom i organowi prowadzącemu Zespół – komunikacja taka powinna być skoordynowana i opierać się na faktach, by nie naruszyć dobra prowadzonego postępowania i nie ujawnić nadmiernych informacji o zabezpieczeniach.

Rozdział VIII – Ciągłość działania

§13. Zasady zarządzania ciągłością działania

1. Aby zapewnić skoordynowane podejście do odtworzenia działalności Zespołu po katastrofie lub innym incydencie zakłócającym działanie, Zespół zarządza ciągłością działania procesów krytycznych. Celem ustanowienia niniejszych zasad jest:
    a. umożliwienie nieprzerwanego świadczenia krytycznych procesów w czasie zakłócenia działalności;
    b. optymalne wykorzystanie personelu i innych zasobów w okresach ich niedoborów;
    c. skrócenie okresu zakłócenia oraz podjęcie normalnej pracy;
    d. ograniczenie finansowych i pozafinansowych skutków zakłócenia działania.
        i. osoby odpowiedzialne za działania w ramach planu
        ii. sposób raportowania w ramach planu
2. Dyrektor, we współpracy z gronem pedagogicznym oraz obsługą informatyczną, identyfikuje procesy i zasoby krytyczne, których ciągłość należy bezwzględnie chronić. Należą do nich m.in.: realizacja programu nauczania (lekcje), dostęp do informacji o uczniach i postępach (dziennik elektroniczny), kontakt z rodzicami i organami nadzoru (poczta elektroniczna, telefony), bezpieczeństwo fizyczne uczniów i wychowanków (monitoring) oraz rozliczenia finansowo-księgowe.
3. Dla każdego istotnego procesu określono minimalne wymagane zasoby i alternatywne sposoby działania na wypadek awarii:
4. Dyrektor Zespołu odpowiada za opracowanie i utrzymanie planów awaryjnych (planu ciągłości działania). Plany te określają role i zadania w sytuacjach kryzysowych. Plany awaryjne podlegają przeglądowi przynajmniej raz na rok oraz po każdym poważnym incydencie, aby uwzględnić wnioski i zmiany organizacyjne.
5. Po ustaniu przyczyny zakłócenia (np. naprawie awarii, zakończeniu sytuacji kryzysowej) Zespół dąży do jak najszybszego powrotu do normalnego funkcjonowania. Odtwarzanie utraconych danych odbywa się z dostępnych kopii zapasowych – obsługa informatyczna jest odpowiedzialna za przywrócenie systemów informatycznych do pełnej sprawności, w tym odtworzenie danych z backupu i weryfikację ich integralności. Jeżeli w trakcie awarii korzystano z procedur zastępczych (np. papierowych zapisów), zebrane dane zostają uzupełnione w systemach elektronicznych. Dyrektor nadzoruje proces powrotu do działalności Zespołu oraz informuje społeczność szkolną o przywróceniu zwykłego trybu pracy.
6. Wzór **Planu ciągłości działania** stanowi **Załącznik nr 3** do niniejszej Polityki.

Rozdział VIII - Logi systemowe

§14. Dokumentowanie działań w systemach informatycznych

1. Rejestrowanie zdarzeń w systemach informatycznych w postaci logów systemowych odbywa się w stosunku do wybranych aplikacji, w których przetwarzane są informacje chronione. Rejestrowane są istotne zdarzenia, w szczególności:
    a. Próby logowania (udane i nieudane),
    b. Zmiany haseł i uprawnień użytkowników,
    c. Dostęp do danych wrażliwych,
    d. Zmiany w konfiguracji systemów i aplikacji,
    e. Działania administracyjne i serwisowe.
2. Logi muszą zawierać co najmniej:
    a. Datę i czas zdarzenia (synchronizowane z precyzyjnym źródłem czasu),
    b. Identyfikator użytkownika lub procesu inicjującego zdarzenie,
    c. Opis zdarzenia,
    d. Adresy IP źródłowe i docelowe (w przypadku zdarzeń sieciowych).
3. Logi chronione są przed nieautoryzowanym dostępem, modyfikacją i usunięciem. Dostęp do logów mają jedynie upoważnieni pracownicy, zgodnie z nadanymi uprawnieniami.
4. Logi systemowe muszą być przechowywane przez okres co najmniej 2 lat, zgodnie z wymogami KRI. Archiwizacja logów odbywa się regularnie i w sposób zapewniający ich odtworzenie w razie potrzeby.
5. Logi powinny być regularnie monitorowane i analizowane w celu wykrywania nieautoryzowanych działań lub naruszeń bezpieczeństwa. W przypadku wykrycia incydentów bezpieczeństwa należy niezwłocznie podjąć odpowiednie działania zgodnie z procedurami reagowania na incydenty.
6. Wszystkie systemy muszą być zsynchronizowane z centralnym, wiarygodnym źródłem czasu, aby zapewnić dokładność i spójność znaczników czasowych w logach.
7. Za zarządzanie logami odpowiedzialna jest Obsługa Informatyczna, lub w przypadku systemów chmurowych – dostawca tego systemu.

Rozdział VIII – Przegląd i działania doskonalące

§15. Audyt wewnętrzny

1. Nie rzadziej niż raz w roku wykonywany jest audyt bezpieczeństwa informacji, pod kątem spełnienia wymagań KRI oraz UoKSC. Zakres audytu może być rozszerzony o normy dotyczące bezpieczeństwa informacji lub dobre praktyki zarządzania cyberbezpieczeństwem.
2. Audyt może być przeprowadzony przez pracownika Zespołu lub podmiot zewnętrzny, pod warunkiem posiadania kwalifikacji potwierdzonych certyfikatami wskazanymi w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu bezpieczeństwa systemu teleinformatycznego (Dz.U. 2018 poz. 1999)..
3. Co najmniej raz w roku Dyrektor Zespołu dokonuje oceny adekwatności i przestrzegania postanowień Polityki – może to nastąpić w formie wewnętrznego audytu bezpieczeństwa informacji lub samooceny. Dyrektor może powołać do przeprowadzenia audytu wewnętrznego Inspektora Ochrony Danych, osobę z obsługi informatycznej lub innego kompetentnego pracownika, ewentualnie zlecić audyt podmiotowi zewnętrznemu.
4. Audyt obejmuje sprawdzenie m.in.: stanu zabezpieczeń technicznych, zgodności działań pracowników z procedurami (np. czy prawidłowo zabezpieczają dokumenty, używają haseł), aktualności analiz ryzyka, skuteczności reakcji na incydenty oraz obszarów wymagających poprawy.
5. Wyniki audytu wewnętrznego są dokumentowane w postaci raportu przekazywanego Dyrektorowi.

§16. Działania doskonalące

1. Na podstawie wyników przeglądów, audytów oraz raportów z incydentów Dyrektor planuje działania korygujące i zapobiegawcze mające na celu ciągłe doskonalenie poziomu bezpieczeństwa informacji w Zespole. Działania te mogą obejmować m.in.: aktualizację niniejszej Polityki lub procedur szczegółowych, dodatkowe szkolenia i kampanie uświadamiające dla personelu, modernizację lub uzupełnienie zabezpieczeń technicznych (np. zakup oprogramowania zabezpieczającego, upgrade sprzętu), doprecyzowanie zakresów obowiązków pracowników w kontekście bezpieczeństwa, a także zmiany organizacyjne (np. wyznaczenie nowych osób odpowiedzialnych za wykonywanie zadań związanych z bezpieczeństwem). Wprowadzane zmiany są komunikowane pracownikom, a wszystkie

obowiązujące dokumenty w zakresie bezpieczeństwa informacji dostępne są dla uprawnionych osób w formie papierowej w sekretariacie.

2. Przegląd Systemy Zarządzania Bezpieczeństwem Informacji odbywa się w cyklu rocznym i jest realizowany przez Dyrektora Zespołu Szkół przy współudziale wicedyrektora, IOD, ASI oraz osób zainteresowanych.
3. Wyniki przeglądu zarządzania wraz z planami dalszego doskonalenia SZBI oraz wymaganymi inwestycjami są przekazywane jednostce nadzorującej, tj. Urzędowi Miasta Mława.

§17. Załączniki

1. Załącznik nr 1 – Arkusz analizy ryzyka
2. Załącznik nr 2 - Rejestr incydentów bezpieczeństwa
3. Załącznik nr 3 - Plan ciągłości działania

§18. KARTA ZMIAN

Wersja	Autor	Opis modyfikacji	Zaakceptował	Data
1.0	Cezary Lewandowski	Stworzenie dokumentu	Mariusz Lempek	22.12.2025 r.

Procedura bezpieczeństwa fizycznego w Zespole Placówek Oświatowych nr 3 w Mławie

Spis treści

§ 1. Cel procedury

1. Celem niniejszej procedury jest określenie zasad bezpieczeństwa fizycznego dotyczących zabezpieczenia informacji chronionych w budynkach i pomieszczeniach Zespołu przed zagrożeniami zewnętrznymi oraz środowiskowymi. Stosowanie zasad opisanych w procedurze ma na celu zminimalizowanie ryzyka utraty, nieuprawnionego dostępu, uszkodzenia lub zniszczenia informacji (oraz nośników, na których się znajdują) w wyniku takich zdarzeń jak włamanie, kradzież, wandalizm, pożar, zalanie, awaria itp. Wdrożenie środków bezpieczeństwa fizycznego ma również przeciwdziałać nadużyciom i zapobiegać potencjalnym stratom materialnym.

§ 2. Zakres stosowania

1. Procedura ma zastosowanie do wszystkich pracowników Zespołu – niezależnie od formy zatrudnienia – a także do innych osób wykonujących pracę lub przebywających na terenie jednostek wchodzących w skład Zespołu, które mogą mieć dostęp do pomieszczeń lub urządzeń, w których przetwarzane są informacje chronione.
2. Każdy pracownik Zespołu oraz osoba przebywająca naterenie jednostek wchodzących w skład Zespołu Placówek Oświatowych nr 3 w Mławie jest zobowiązana do przestrzegania zasad niniejszej procedury w zakresie, który jej dotyczy. Nadzór nad realizacją procedury sprawuje Dyrektor Zespołu Placówek Oświatowych nr 3 w Mławie.
3. Zasady przyjęte w procedurze obowiązują na terenie Zespołu Placówek Oświatowych nr 3 w Mławie mieszczącego się w następujących lokalizacjach:
    a) Miejskie Przedszkole Samorządowe nr 3 im. Jana Brzechwy w Mławie – 06-500 Mława, ul. Hoża 6,
    b) Miejskie Przedszkole Samorządowe nr 4 z oddziałami integracyjnymi im. Ewy Szelburg – Zarembiny w Mławie – 06-500 Mława, ul. Krasińskiego 7,
    c) Szkoła Podstawowa nr 7 im. Zuzanny Morawskiej w Mławie – 06-500 Mława, ul. Ordona 14.

§ 3. Definicje

Wszystkie pojęcia użyte w niniejszej procedurze zostały wyjaśnione w **Polityce bezpieczeństwa informacji.**

§ 4. Zasady ochrony fizycznej

I. Ogólne zasady ochrony fizycznej

1. Wszystkie pomieszczenia muszą być zabezpieczone przed dostępem osób nieuprawnionych, a także przed uszkodzeniem lub zniszczeniem wskutek zagrożeń środowiskowych (np. pożar, zalanie).
2. Budynki Zespołu są poza godzinami pracy zamknięty na klucz.
3. Pomieszczenia szczególnie chronione, takie jak archiwum, spełniają podwyższone wymagania zabezpieczenia konstrukcyjnego: są zamykane na oddzielny zamek, a dostęp do nich posiada ograniczona liczba osób.
4. Regularnie przeprowadzane są przeglądy i konserwacje środków zabezpieczeń fizycznych – sprawdzenie stanu zamków, drzwi, okien, sprawności systemu monitoringu wizyjnego.

II. Strefy bezpieczeństwa

1. W celu właściwego nadzoru nad informacjami chronionymi na terenie Zespołu wyznacza się dwie strefy bezpieczeństwa, różniące się poziomem dostępu:
    a. **Strefa publiczna (ogólnodostępna):** obszary dostępne dla rodziców oraz innych osób z zewnątrz w określonych godzinach pracy Zespołu. Są to miejsca, w których osoby postronne mogą przebywać bez stałego nadzoru pracowników (choć zwykle w zasięgu ich wzroku). Do strefy publicznej zalicza się przede wszystkim:
        i. główne wejście,
        ii. główny korytarz przy wejściu,
        iii. okazjonalnie strefą publiczną mogą stać się także inne obszary podczas wydarzeń otwartych dla gości (np. sala gimnastyczna czy korytarze podczas wywiadówek, dni otwartych szkoły/przedszkola itp.).
    b. **Strefa wewnętrzna (pracownicza i uczniowska):** obszary przeznaczone do użytku wewnętrznego przez społeczność szkolną – czyli pracowników oraz uczniów, podopiecznych – a także osoby z zewnątrz posiadające imienne upoważnienie lub będące pod nadzorem pracownika. W strefie wewnętrznej mieszczą się wszystkie pomieszczenia dydaktyczne i administracyjne poza strefą publiczną, w tym: sale dydaktyczne, pracownia komputerowa, biblioteka, pokoje nauczycielskie, sekretariat, gabinety Dyrektora i Wicedyrektora, korytarze szkolne (za wyjątkiem głównego korytarza przy wejściu zaliczonego do strefy publicznej). Strefa wewnętrzna jest dostępna dla uczniów, podopiecznych i pracowników w godzinach zajęć i pracy szkoły/przedszkola. Osoby postronne (np. rodzice, serwisanci) mogą przebywać w tej

strefie wyłącznie pod nadzorem upoważnionego pracownika Zespołu (np. pracownik oprowadzający serwisanta do prac w pracowni informatycznej, rodzic wchodzący do klasy jedynie w obecności nauczyciela, pomocy nauczyciela).

2. Zasady bezpieczeństwa w strefach:
   a. **Strefa publiczna:** Osoby z zewnątrz przebywające w strefie publicznej (rodzice, goście) mogą poruszać się wyłącznie w wyznaczonych ogólnodostępnych częściach budynku i tylko w godzinach pracy Zespołu. W strefie publicznej mogą znajdować się jedynie materiały informacyjne i ogłoszenia o charakterze publicznym – nie wolno pozostawiać tam żadnych dokumentów zawierających informacje chronione (np. dokumentacji uczniów lub podopiecznych, pism urzędowych). Istotne punkty w strefie publicznej są dodatkowo objęte monitoringiem wizyjnym. Podczas wydarzeń publicznych odbywających się na terenie Zespołu (zebrania z rodzicami, uroczystości szkolne itp.), należy zapewnić wzmożony nadzór nad mieniem Zespołu i kontrolę dostępu – np. wyznaczyć strefy, do których goście nie powinni wchodzić (pomieszczenia administracyjne, zaplecza). Zabrania się pozostawiania osób postronnych bez opieki w budynkach Zespołu. Jeśli w strefie publicznej zostaną znalezione jakiekolwiek przedmioty lub dokumenty, które mogły zostać pozostawione przez odwiedzających (np. zgubione dokumenty, klucze), należy je niezwłocznie przekazać do sekretariatu w celu zabezpieczenia i podjęcia próby zwrócenia właścicielowi.
   b. **Strefa wewnętrzna:** Dostęp do pomieszczeń strefy wewnętrznej mają wyłącznie pracownicy Zespołu, uczniowie, podopieczni oraz osoby posiadające stosowne upoważnienie lub będące pod nadzorem (np. personel sprzątający zatrudniony w Zespołu, upoważnieni serwisanci, praktykanci). W pomieszczeniach strefy wewnętrznej mogą być przetwarzane informacje chronione, pod warunkiem, że osoby nieuprawnione nie mają do nich wglądu. Pracownicy powinni dbać, by w trakcie pracy materiały poufne nie były pozostawione w miejscach widocznych lub dostępnych dla uczniów bądź osób odwiedzających (np. zasada czystego biurka: chowanie dokumentów do szuflad, odwracanie lub wygaszanie ekranu monitora, gdy do pokoju wchodzi osoba postronna). Uczniowie mogą przebywać samodzielnie w salach lekcyjnych oraz na korytarzach szkolnych w ramach zwykłego harmonogramu zajęć, jednak nie mogą bez opieki wchodzić do pomieszczeń administracyjnych (sekretariatu, gabinetu dyrektora, pokoju nauczycielskiego, magazynów sprzętu itp.), podopieczni przedszkola przebywają stale pod nadzorem wychowawców i opiekunów w salach. Po zakończeniu pracy lub zajęć wszystkie pomieszczenia w strefie wewnętrznej powinny zostać właściwie zabezpieczone: sprawdza się zamknięcie okien, wyłącza urządzenia

elektryczne według instrukcji (z wyjątkiem sprzętu, który musi działać ciągle, jak rejestrator monitoringu), a drzwi do pomieszczeń zamyka na klucz. Dokumenty zawierające informacje chronione muszą po godzinach pracy być przechowywane w zamkniętych szafach lub szufladach – nie wolno pozostawiać ich na biurkach na noc. Zabrania się wynoszenia dokumentów zawierających informacje chronione poza teren Zespołu bez zgody Dyrektora (dotyczy to także kopiowania danych na własne urządzenia – wszelkie takie działania muszą być uzasadnione i zatwierdzone). W przypadku potrzeby pracy z dokumentami poza Zespołem, należy stosować szczególne środki ostrożności w transporcie i przechowywaniu tych dokumentów, a po zakończeniu pracy – niezwłocznie zwrócić je do Zespołu.

III. Zasady zarządzania kluczami

1. Klucze do drzwi wejściowych do budynku posiadają Dyrektor/Wicedyrektor oraz osoby wyznaczone do otwierania i zamykania budynków Zespołu.
2. Prowadzona jest ewidencja osób upoważnionych do dostępu do określonych pomieszczeń, zgodnie z załącznikiem nr 1 do niniejszej procedury. Ewidencja dotyczy nadania i cofnięcia uprawnień, a nie każdorazowego pobierania kluczy.
3. Klucze do sal lekcyjnych, sal przedszkolnych i pozostałych pomieszczeń dydaktycznych przechowywane są w **pokoju nauczycielskim**. Dostęp do **pokoju nauczycielskiego** mają wyłącznie pracownicy pedagogiczni i pracownicy obsługi upoważnieni przez Dyrektora.
4. Klucze do gabinetów Dyrektora, Wicedyrektora oraz do pomieszczeń o podwyższonym poziomie ochrony (np. archiwum) są przechowywane **w sekretariacie**. Dostęp do tych pomieszczeń mają wyłącznie pracownicy obsługi upoważnieni przez Dyrektora.
5. Niedozwolone jest udostępnianie kluczy osobom nieuprawnionym. Pracownik, który otrzymał klucz, nie może przekazywać go dalej bez zgody przełożonego.
6. Klucze zapasowe są przechowywane w zamykanej skrzynce w pomieszczeniu technicznym i sekretariacie. Dostęp do kluczy zapasowych ma tylko Dyrektor lub upoważnieni pracownicy.
7. Klucze do pomieszczeń szkolnych powinny pozostawać na terenie placówki po godzinach pracy.
8. Należy unikać pozostawiania kluczy w drzwiach od strony zewnętrznej (np. klucz tkwiący w zamku drzwi klasy od strony korytarza) – po otwarciu pomieszczenia klucz należy niezwłocznie wyjąć. Nie wolno także odkładać kluczy w miejscach ogólnodostępnych (blaty w korytarzu, parapety) ani zostawiać ich bez nadzoru.
9. W przypadku zagubienia, kradzieży lub stwierdzenia uszkodzenia klucza do budynku lub pomieszczenia, pracownik jest zobowiązany niezwłocznie zgłosić ten fakt Dyrektorowi Zespołu

lub **kierownikowi gospodarczemu**. Dyrektor dokonuje oceny, czy istnieje możliwość, że ktoś niepowołany mógł wejść w posiadanie klucza i zidentyfikować, do jakich drzwi pasuje i podejmuje odpowiednie środki zaradcze. Mogą one obejmować np.: wymianę wkładki zamka (gdy zagubiony klucz stwarza zagrożenie nieautoryzowanego wejścia), dodatkowe zabezpieczenie drzwi do czasu wymiany zamka, przeszkolenie personelu co do ostrożności przy gospodarowaniu kluczami.

10. Dokumenty i nośniki informacji chronionych przechowywane są w meblach zamykanych na klucz (szafy, szuflady). Klucze do tych mebli podlegają podobnym zasadom – dostęp mają tylko upoważnieni pracownicy. Zapasowe klucze do ważnych szaf powinny być zdeponowane u Dyrektora lub w sejfie.

§ 5. Załączniki

1. Ewidencja osób upoważnionych do dostępu do określonych pomieszczeń.

Procedura zarządzania systemem informatycznym w Zespole Placówek Oświatowych nr 3 w Mławie

Spis treści

§ 1. Cel procedury

Celem niniejszej procedury jest ustanowienie jednolitych zasad zarządzania systemami informatycznymi w Zespole, tak aby zapewnić ich bezpieczne i efektywne funkcjonowanie, zgodne z obowiązującymi przepisami prawa i wymaganiami ochrony danych. Procedura określa sposób administrowania infrastrukturą teleinformatyczną Zespołu – w tym sprzętem komputerowym, siecią, oprogramowaniem i kontami użytkowników

§ 2. Zakres stosowania

Procedura ma zastosowanie do wszystkich osób uczestniczących w zarządzaniu lub użytkowaniu systemów informatycznych Zespołu. Dotyczy to w szczególności administratorów systemów (wewnętrznych lub zewnętrznych – obsługa informatyczna), a także użytkowników posiadających dostęp do szkolnych komputerów, sieci i aplikacji.

§ 3. Definicje

Wszystkie pojęcia użyte w niniejszej procedurze zostały wyjaśnione w **Polityce bezpieczeństwa informacji.**

§ 4. Zasady zarządzania systemami informatycznymi

I. Zarządzanie dostępem i uprawnieniami użytkowników

1. Użytkownik systemów informatycznych Zespołu posiada własne, imienne konto (login/użytkownik) zabezpieczone hasłem. Zabrania się współdzielenia kont imiennych pomiędzy różne osoby – używanie wspólnych loginów grupowych nie jest dopuszczalne (wyjątkiem mogą być konta systemowe, techniczne, ale dostęp do nich jest również ograniczony i nadzorowany)
2. Dopuszcza się dostęp więcej niż jednej osoby do konta pocztowego (mailowej) Zespołu.
3. Dostęp do systemów i zasobów informatycznych jest przyznawany wyłącznie osobom, które uzyskały odpowiednie upoważnienie do przetwarzania danych osobowych od Dyrektora Zespołu.
4. W przypadku konieczności nadania, zmiany lub odebrania dostępu do systemu informatycznego Dyrektor Zespołu wysyła zlecenie e-mailem do ASI lub do Administratora danego systemu. Z treści wiadomości musi wynikać zakres dostępu (jakich systemów dotyczy i jaką rolę pełni użytkownik, np. nauczyciel – dostęp do dziennika elektronicznego dla

określonych klas). Administrator systemu zakłada nowe konto zgodnie z dyspozycją, ustawia hasło startowe (które użytkownik musi zmienić przy pierwszym logowaniu). Jeśli Administratorem systemu jest Dyrektor Zespołu – nie stosuje się odrębnego odnotowania.

5. Dyrektor Zespołu prowadzi rejestr użytkowników zawierający:
    a. Imię, Nazwisko i identyfikator użytkownika,
    b. Informacje o system(ach) i poziomie uprawnień,
    c. Data nadania lub odebrania uprawnienia,
    d. Informacja czy użytkownik posiada uprawnienia administracyjne.
6. Odebranie uprawnień polega na zablokowaniu konta w systemie lub w stosownych przypadkach na jego usunięciu.
7. Użytkownicy są zobowiązani do utrzymywania w tajemnicy swoich haseł i stosowania silnych haseł. Hasło:
    a. powinno zawierać zalecaną minimalną liczbę znaków (co najmniej 12 znaków, o ile system nie wymusza dłuższego) oraz kombinację różnych kategorii znaków (duże i małe litery, cyfry, znaki specjalne) – chyba że system posiada własne wymagania co do hasła,
    b. nie powinno być oczywiste ani łatwe do odgadnięcia (należy unikać informacji powiązanych z użytkownikiem jak imię, nazwisko, data urodzenia czy proste wzorce klawiaturowe),
    c. nie może być identyczne z hasłami używanymi przez pracownika do celów prywatnych poza systemami szkolnymi,
    d. powinno być zmieniane okresowo – co 90 dni dla kont z szerokimi uprawnieniami (administratorzy) oraz co 180 dni dla zwykłych użytkowników, chyba że system wymusza inny okres - w razie podejrzenia, że hasło mogło zostać ujawnione osobom nieuprawnionym, użytkownik bądź administrator musi niezwłocznie zmienić to hasło niezależnie od harmonogramu wymiany.
8. Stosuje się czasowe blokowanie konta po 5 nieudanych próbach zalogowania.
9. Na stanowiskach komputerowych wymuszone jest wylogowanie po okresie 5 minut nieaktywności użytkownika.
10. Dla szczególnie wrażliwych systemów lub kont (np. konto administratora pocztowego czy administracyjnego w dzienniku elektronicznym) stosuje się, tam gdzie to możliwe, dodatkowe mechanizmy uwierzytelnienia wieloskładnikowego (2FA/MFA) – np. kod SMS lub aplikacja mobilna jako drugi składnik przy logowaniu.

II. Bezpieczna eksploatacja i użytkowanie systemów

1. Na komputerach i urządzeniach szkolnych/przedszkolnych dozwolone jest instalowanie oraz używanie wyłącznie oprogramowania legalnego posiadającego ważne licencje, które zostało zatwierdzone przez Szkołę. Wykaz autoryzowanego oprogramowania prowadzi Administrator Systemów Informatycznych (ASI).
2. Zabrania się samowolnego instalowania jakichkolwiek programów spoza tego wykazu, w szczególności pochodzących z nieznanych źródeł lub nielegalnych, na sprzęcie służbowym. W razie potrzeby użycia nowego oprogramowania pracownik zgłasza ten fakt Dyrektorowi lub ASI – po sprawdzeniu legalności i kompatybilności oprogramowania może ono zostać zainstalowane przez upoważnioną osobę.
3. Dostęp do Internetu w Zespole służy przede wszystkim realizacji zadań edukacyjnych i administracyjnych. Pracownicy mogą w rozsądny sposób korzystać z Internetu do celów prywatnych incydentalnie (np. sprawdzenie wiadomości w przerwie), o ile nie zakłóca to ich obowiązków i nie narusza przepisów ani zasad etyki.
4. Zabronione jest odwiedzanie stron o treściach nielegalnych lub niestosownych (pirackich, pornograficznych, obraźliwych itp.) z użyciem sprzętu lub sieci szkolnej. Służbowa poczta elektroniczna (e-mail) służy do komunikacji w sprawach służbowych – zabronione jest używanie prywatnych skrzynek pocztowych do wysyłania danych służbowych, zwłaszcza zawierających informacje chronione. Jednocześnie zabronione jest przesyłanie na służbowe adresy wiadomości niezwiązanych z pracą.
5. Przesyłanie poufnych danych osobowych za pośrednictwem maila może się odbywać wyłącznie w zaszyfrowanym załączniku. Hasło należy przekazać innym kanałem.
6. Każdy komputer stacjonarny czy laptop używany w Zespołu jest chroniony aktualnym programem antywirusowym oraz zaporą sieciową. Użytkownicy nie mają uprawnień administracyjnych na swoich stacjach roboczych, aby uniemożliwić przypadkowe lub celowe wprowadzenie zmian systemowych zagrażających bezpieczeństwu. Stacje robocze są konfigurowane tak, by minimalizować ryzyka: zbyteczne usługi i porty sieciowe są wyłączane, na każdym komputerze aktywowane jest automatyczne pobieranie aktualizacji systemu operacyjnego. Użytkownik nie może zmieniać ustawień systemowych dostarczonych przez administratora (np. wyłączać skanera antywirusowego, zmieniać reguł zapory).
7. W celu zapobiegania przypadkowemu ujawnieniu informacji, pracownicy zobowiązani są przestrzegać zasady czystego pulpitu/ekranu – w szczególności:
    a. po zakończeniu pracy (choćby krótkotrwałym odejściu od komputera) użytkownik blokuje komputer lub wylogowuje się, aby osoby trzecie, w tym uczniowie lub

członkowie rodziny w przypadku pracy w domu - nie widziały otwartych dokumentów ani nie mogły korzystać z zalogowanej sesji;

b. w razie pracy przy komputerze w obecności osób nieuprawnionych (np. rodzica siedzącego obok w sekretariacie) pracownik powinien minimalizować okna zawierające dane wrażliwe lub ustawić ekran w taki sposób, by postronni nie widzieli zawartości;

c. na biurku nie zostawia się rozłożonych dokumentów zawierających dane osobowe, jeśli w pokoju mogą pojawić się osoby niepowołane (np. inny rodzic, pracownik nieupoważniony do tych danych). Dokumenty papierowe, gdy nie są używane, powinny być schowane do szuflady lub szafki.

8. Szkoła korzysta z usług chmurowych (poczta) oraz specjalizowanych systemów (dziennik elektroniczny, SIO) dostarczanych przez zewnętrznych dostawców. Pracownicy nie mogą używać innych, niezatwierdzonych programów do przechowywania szkolnych danych chronionych. W szczególności zabronione jest przenoszenie służbowych dokumentów czy baz danych na prywatne konta w usługach typu Dropbox, Google Drive itp. bez wyraźnej zgody Dyrektora i sprawdzenia umowy powierzenia danych. Jeżeli zachodzi potrzeba udostępnienia plików pomiędzy pracownikami czy uczniami, należy korzystać z oficjalnie wdrożonych rozwiązań (np. dedykowane repozytoria w e-dzienniku).

§ 5. Utrzymanie i zabezpieczenie infrastruktury IT

III. Aktualizacje i poprawki bezpieczeństwa

1. Administrator systemów informatycznych na bieżąco śledzi informacje o dostępnych aktualizacjach oprogramowania systemowego (Windows, macOS itp.) i aplikacji używanych w Zespołu, a także o pojawiających się istotnych podatnościach (np. komunikaty CERT, bazy CVE).
2. W przypadku opublikowania krytycznej poprawki bezpieczeństwa – instaluje ją niezwłocznie na wszystkich odpowiednich urządzeniach (po uprzednim przetestowaniu, jeśli to możliwe). Mniej krytyczne aktualizacje są wdrażane cyklicznie (np. co miesiąc). Proces aktualizacji obejmuje również firmware urządzeń sieciowych (routera, punktów dostępowych Wi-Fi, przełączników).

IV. Konfiguracja urządzeń sieciowych

1. Wszystkie urządzenia aktywne w sieci Zespołu (router, switche zarządzalne, punkty dostępowe Wi-Fi) są skonfigurowane zgodnie z zasadami bezpieczeństwa: zmieniono na nich fabryczne domyślne hasła administracyjne na silne, wyłączono zbędne usługi (np. zdalny dostęp od strony

WAN, jeśli nieużywany), a interfejsy konfiguracyjne dostępne są tylko dla administratora z zaufanej lokalizacji.

2. Sieć Wi-Fi dla pracowników jest zabezpieczona protokołem WPA2/WPA3 z silnym hasłem, okresowo zmienianym (przynajmniej raz w roku lub po odejściu pracownika znającego hasło).
3. Komputery w pracowni komputerowej odizolowane są w wydzielonej podsieci.

V. Monitorowanie systemów

1. ASI monitoruje podstawowe parametry pracy systemów – zarówno pod kątem wydajności/dostępności, jak i bezpieczeństwa. Oznacza to m.in.: regularne sprawdzanie dostępności usług krytycznych, obserwację wykorzystania zasobów (miejsce na dyskach, obciążenie łącza) oraz przeglądanie dzienników zdarzeń (logów) tam, gdzie może to wskazać na problemy (np. logi serwera antywirusowego – czy nie ma stacji od dawna nieaktualizowanej, logi systemów operacyjnych – błędy dysku, próby logowania). W przypadku zaobserwowania anomalii bądź powtarzających się błędów, podejmowane są działania prewencyjne zanim dojdzie do awarii.

VI. Zabezpieczenie infrastruktury wspomagającej

1. **Zasilanie i podtrzymanie energii**
   a. Kluczowe urządzenia (router, przełącznik główny,) podłączone są do zasilaczy awaryjnych UPS zapewniających min. 15 minut podtrzymania.
   b. Raz w roku przeprowadza się test obciążeniowy UPS-ów oraz wymienia akumulatory zgodnie z zaleceniami producenta.
   c. Wszystkie gniazda komputerowe chronione są listwami antyprzepięciowymi.
2. **Okablowanie strukturalne**
   a. Przewody sieciowe prowadzone są w zamkniętych kanałach lub peszlach; nadmiarowe gniazda w strefach publicznych pozostają dezaktywowane.
3. **Ochrona przeciwpożarowa**
   a. Gaśnice rozmieszczone są na korytarzach, w sali chemicznej, na stołówce szkolnej i w kotłowni - przegląd gaśnic wykonywany jest co 12 miesięcy.
4. **Uziemienie i ochrona odgromowa**
   a. Instalacja odgromowa budynku podlega przeglądowi nie rzadziej niż co 5 lat, a wyniki kontroli archiwizowane są w gabinecie Kierownika gospodarczego.

VII. Współpraca z Dostawcami i Bezpieczeństwo Łańcucha Dostaw

1. Wszelkie zakupy wyposażenia informatycznego Szkoły odbywają się za wiedzą i przy udziale ASI. Przed nabyciem nowego oprogramowania analizuje się wymagania licencyjne,

kompatybilność z istniejącą infrastrukturą oraz aspekty bezpieczeństwa (np. czy program spełnia wymogi ochrony danych osobowych). Przy zakupach sprzętu komputerowego bierze się pod uwagę wsparcie techniczne producenta, dostępność aktualizacji, parametry gwarancji.

2. Nowe systemy informatyczne planowane do wdrożenia powinny być konsultowane z Inspektorem Ochrony Danych pod kątem spełnienia wymogów RODO (np. zabezpieczenia danych, minimalizacja gromadzonych danych, możliwa konieczność przeprowadzenia oceny skutków dla ochrony danych).
3. Zarządzanie łańcuchem dostaw odbywa się poprzez staranną selekcję dostawców, zawieranie umów z klauzulami bezpieczeństwa oraz nadzór nad usługami zewnętrznymi.
4. Za dostawców krytycznych uznaje się podmioty, których usługi są niezbędne do bieżącego funkcjonowania infrastruktury teleinformatycznej Szkoły, w szczególności:
    a. operatora podstawowego i awaryjnego łącza internetowego (OSE + LTE),
    b. serwisanta urządzeń sieciowych i stacji roboczych,
    c. dostawcę oprogramowania kluczowego (np. dziennik elektroniczny),
    d. podmiot świadczący obsługę systemu monitoringu wizyjnego lub alarmowego.
5. Umowy lub zlecenia zawierane z dostawcami krytycznymi muszą określać:
    a. maksymalny czas reakcji i przywrócenia usługi (SLA),
    b. obowiązek niezwłocznego zgłaszania incydentów oraz przedstawienia planu ich usunięcia,
    c. uprawnienie Szkoły do uzyskania aktualnych kopii danych lub ich eksportu na żądanie,
    d. zobowiązanie dostawcy do bezpiecznego usunięcia danych Szkoły po zakończeniu współpracy.
6. Nie później niż 30 dni przed wygaśnięciem umowy z dostawcą krytycznym ASI inicjuje procedurę wyjścia obejmującą:
    a. pozyskanie i weryfikację końcowej kopii danych Szkoły,
    b. zmianę lub odebranie wszelkich poświadczeń dostępowych dostawcy,
    c. uzyskanie pisemnego potwierdzenia trwałego usunięcia danych Szkoły z systemów dostawcy

§ 6. Licencje oprogramowania

1. Szkoła prowadzi ewidencję posiadanego oprogramowania wraz z informacjami licencyjnymi – liczba licencji/stanowisk, okres ważności (jeśli licencja czasowa), klucze licencyjne, dowody zakupu.

2. Ewidencja ta jest utrzymywana przez Dyrektora Zespołu. Przed upływem okresu ważności licencji płatnej (np. rocznej subskrypcji antywirusa) ASI informuje Dyrektora o potrzebie odnowienia, aby uniknąć przerw w ochronie lub naruszenia warunków umowy licencyjnej.
3. Dokumenty potwierdzające legalność oprogramowania (faktury, certyfikaty, umowy licencyjne, ewentualne nośniki instalacyjne i klucze produktu) są przechowywane w sekretariacie.

VIII. Kopie konfiguracji

1. Ważne urządzenia sieciowe i systemy (np. router szkolny, rejestrator monitoringu, kluczowe bazy danych) mają wykonywane kopie zapasowe swoich konfiguracji lub danych – na wypadek konieczności odtworzenia po awarii.

§ 7. Kopie zapasowe i odtwarzanie danych

1. ASI prowadzi wykaz kopii zapasowych uwzględniający nazwę systemu lub zasobu, typ kopii zapasowej, częstotliwość i metodę tworzenia kopii oraz okres przechowywania. Wykaz jest dokumentem poufnym, do którego dostęp posiada wyłącznie ASI i Dyrektor Szkoły.
2. Nośniki z kopiami zapasowymi są zabezpieczone przed nieuprawnionym dostępem i zdarzeniami losowymi. Dyski zewnętrzne używane do backupów muszą być szyfrowane i przechowywane w innej lokalizacji niż oryginalne dane. W przypadku korzystania z chmury do backupu, należy upewnić się, że dostęp do niej jest odpowiednio chroniony (silne hasło, 2FA).
3. ASI ustala sposób i harmonogram testowania kopii bezpieczeństwa, aby zagwarantować ich przydatność w razie konieczności odtworzenia.

§ 8. Inwentaryzacja sprzętu

1. Szkoła prowadzi ewidencję posiadanych zasobów informatycznych. Rejestr obejmuje co najmniej: komputery (z podaniem modelu, numeru seryjnego/inwentarzowego, roku zakupu, aktualnego użytkownika lub lokalizacji), urządzenia peryferyjne (drukarki, skanery, projektory), aktywne urządzenia sieciowe (router, switche, punkty dostępowe – z danymi identyfikacyjnymi).
2. Rejestr jest prowadzony w formie elektronicznej przez Administratora systemów we współpracy z osobą prowadzącą ewidencję środków trwałych.

§ 9. Konserwacja i naprawy

1. Sprzęt IT jest poddawany konserwacji i czyszczeniu zgodnie z zaleceniami producenta lub według potrzeb.

2. W przypadku przekazania urządzenia do zewnętrznego serwisu, należy zabezpieczyć dane: usunąć/wymontować nośniki danych przed wysyłką (jeśli to możliwe), albo zawrzeć umowę powierzenia z serwisem gwarantującą ochronę danych na czas naprawy. Po powrocie sprzętu z naprawy, ASI weryfikuje jego działanie i ponownie instaluje niezbędne oprogramowanie.

§ 10. Wycofywanie i utylizacja sprzętu

1. W przypadku likwidacji, wymiany lub przekazania innej instytucji sprzętu komputerowego, należy trwale usunąć lub zniszczyć wszelkie dane zawarte na nośnikach tego sprzętu. Czynność usuwania danych przed likwidacją jest dokumentowana w protokole likwidacji sprzętu
2. Po upewnieniu się, że dane nie mogą zostać odczytane, sprzęt można przekazać do utylizacji (firmie recyklingowej) lub dalszego użytkowania.

§ 11. Załączniki

1. Wykaz kopii zapasowych (dokument nie podlega upublicznieniu).
2. Wykaz uprawnień.