Polityka Bezpieczeństwa Informacji

w Zespole Szkół Zawodowych nr 1 im. Marszałka Józefa Piłsudskiego w Skierniewicach
z dn.13.12.2023r.

Zespół Szkół Zawodowych nr 1 im. Marszałka Józefa Piłsudskiego w Skierniewicach
(dalej jako „ZSZ Nr 1")
wypracował i skodyfikował główne zasady działania
Systemu Zarządzania Bezpieczeństwem Informacji
(Information Security Management System)
(dalej jako „SZBI" lub „ISMS")
znajdujące swój wyraz w niniejszej Polityce Bezpieczeństwa Informacji
(dalej jako „Polityka" lub „PBI")

Spis treści:

1. POSTANOWIENIA OGÓLNE

1.1. Celem Polityki jest zapewnienie, że **System Zarządzania Bezpieczeństwem Informacji** został ustanowiony, wdrożony i jest eksploatowany, przeglądany i doskonalony w organizacji.

1.2. ZSZ Nr 1 posiada ubezpieczenie odpowiedzialności cywilnej, w pewnym zakresie obejmujące także przypadki swym zakresem obejmujące również przypadki naruszenia bezpieczeństwa informacji.

1.3. Dla skutecznej realizacji Polityki, uwzględniając zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia ZSZ Nr 1 zapewnia:

1.3.1. wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających zgodność przetwarzania Informacji z wymogami prawa oraz niezbędne zabezpieczenie przetwarzanych informacji;

1.3.2. stałe monitorowanie zgodności przetwarzania Informacji z wymogami prawa oraz poddawanie środków, o których mowa w ust.1.3.1. ciągłym przeglądom oraz uaktualnianiu, w oparciu o monitoring podejmowanych działań ocenianych praz pryzmat aktualnego prawodawstwa, obowiązującej linii orzeczniczej, wytycznych organów nadzoru z obszaru UE, oraz poglądów doktryny;

1.3.3. prowadzona jest stała ocena ryzyka ewentualnych możliwych naruszeń przetwarzania Informacji, mająca na celu natychmiastowe zastosowanie środków zaradczych. Stosowane podejście do szacowania ryzyka wywodzi się z rodziny norm ISO z grupy 270(…) i 31(…), w szczególności **norm ISO 27005 i ISO 31000**. Polega ono na analitycznym ustalaniu związków przyczynowo skutkowych materializacji potencjalnych zagrożeń dla

danych osobowych oraz analizie ilościowej poszczególnych czynników ryzyka: prawdopodobieństwa wystąpienia danego zagrożenia, oraz skutków ocenianych z perspektywy osoby, której potencjalne naruszenie może dotyczyć, wystąpienia zagrożenia dla celów organizacji z uwzględnieniem jej kontekstu;

1.3.4. kontrolę i nadzór nad przetwarzaniem Informacji.

1.4. Podejście do bezpieczeństwa informacji organizacji wywodzi się z trzech kluczowych kwestii:

1.4.1. Zapewnienia, że informacja jest udostępniana jedynie osobom upoważnionym (tzw. **reguła poufności informacji**);

1.4.2. Zapewnienia zupełnej dokładności i kompletności informacji oraz metod jej przetwarzania (tzw. **reguła integralności informacji**);

1.4.3. Zapewnienia, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów tylko wtedy, gdy istnieje taka potrzeba (tzw. **reguła dostępności informacji**).

1.5. Podstawowe zasady obowiązujące w ochronie informacji.

Każdy pracownik powinien zostać zapoznany z regułami oraz z kompletnymi i aktualnymi procedurami ochrony informacji w swoim dziale organizacyjnym.

Poniższe uniwersalne zasady są podstawą realizacji polityki bezpieczeństwa informacji:

1.5.1. Zasada uprawnionego dostępu. Każdy pracownik przeszedł szkolenie z zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji i podpisał stosowne oświadczenie o zachowaniu poufności;

1.5.2. Zasada przywilejów koniecznych. Każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań;

1.5.3. Zasada wiedzy koniecznej. Każdy pracownik posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań;

1.5.4. Zasada usług koniecznych. Organizacja świadczy tylko takie usługi, jakich wymaga klient;

1.5.5. Zasada asekuracji. Każdy mechanizm zabezpieczający musi być ubezpieczony drugim, (podobnym). W przypadkach szczególnych może być stosowane dodatkowe (trzecie) niezależne zabezpieczenie;

1.5.6. Zasada świadomości zbiorowej. Wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych organizacji i aktywnie uczestniczą w tym procesie,(przez które to pojęcie rozumie się osoby wchodzące w interakcję z ZSZ Nr 1, w szczególności lecz nie wyłącznie: uczeń i jego rodzice/opiekunowie prawni, nauczyciele, pracownicy administracyjni;

1.5.7. Zasada indywidualnej odpowiedzialności. Za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby;

1.5.8. Zasada obecności koniecznej. Prawo przebywania w określonych miejscach mają tylko osoby upoważnione;

1.5.9. Zasada stałej gotowości. System jest przygotowany na wszelkie zagrożenia. Niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających;

1.5.10. Zasada najsłabszego ogniwa. Poziom bezpieczeństwa wyznacza najsłabszy (najmniej zabezpieczony) element;

1.5.11. Zasada kompletności. Skuteczne zabezpieczenie jest tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania informacji;

1.5.12. Zasada ewolucji. Każdy system musi ciągle dostosowywać mechanizmy wewnętrzne do zmieniających się warunków zewnętrznych;

1.5.13. Zasada odpowiedniości. Używane mechanizmy muszą być adekwatne do sytuacji;
1.5.14. Zasad akceptowanej równowagi. Podejmowane środki zaradcze nie mogą przekraczać poziomu akceptacji;
1.5.15. Zasada świadomej konwersacji. Nie zawsze i wszędzie trzeba mówić, co się wie, ale zawsze i wszędzie trzeba wiedzieć, co gdzie i do kogo się mówi.

1.6. Celem wdrożonej Polityki Bezpieczeństwa Informacji jest osiągnięcie takiego poziomu organizacyjnego i technicznego, który:
1.6.1. będzie gwarantem pełnej ochrony danych własnych i Klientów oraz ciągłość procesu ich przetwarzania;
1.6.2. zapewni zachowanie poufności informacji chronionych, integralności i dostępności informacji chronionych oraz jawnych;
1.6.3. zagwarantuje odpowiedni poziom bezpieczeństwa informacji, bez względu na jej postać, we wszystkich systemach jej przetwarzania;
1.6.4. maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji, które wynikają z celowej bądź przypadkowej działalności człowieka oraz ich ewentualne wykorzystanie na szkodę organizacji.
1.6.5. zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów przetwarzania informacji;
1.6.6. zapewni gotowość do podjęcia działań w sytuacjach kryzysowych dla bezpieczeństwa organizacji i jej interesów oraz posiadanych i powierzonych jej informacji.

1.7. Powyższe cele realizowane są poprzez:
1.7.1. wyznaczenie struktury organizacyjnej zapewniającej optymalny podział i koordynację zadań i odpowiedzialności związanych z zapewnieniem bezpieczeństwa informacji;
1.7.2. wyznaczenie właścicieli dla kluczowych aktywów przetwarzających informację, którzy zobowiązani są do zapewnienia im możliwie najwyższego poziomu bezpieczeństwa;
1.7.3. przyjęcie za obowiązujące przez wszystkich pracowników cząstkowych polityk i procedur opisanych w dalszych rozdziałach;
1.7.4. podziale informacji na klasy i przyporządkowanie im zasad postępowania;
1.7.5. określeniu zasad przetwarzania informacji, w tym stref, w których może się ono odbywać;
1.7.6. przegląd i aktualizację polityk i procedur postępowania dokonywaną przez odpowiedzialne osoby w celu jak najlepszej reakcji na zagrożenia i incydenty;
1.7.7. ciągłe doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji funkcjonującego w organizacji zgodnie z wymaganiami analogicznymi do wymagań norm ISO/IEC 27001:2014, ISO/IEC 27005 i ISO/IEC 31000 i zaleceniami wszystkich zainteresowanych stron.

1.8. Polityka obowiązuje wszystkich pracowników oraz współpracowników ZSZ Nr 1 Za przestrzeganie i utrzymanie postanowień Polityki odpowiedzialni są:
1.8.1. ZSZ Nr 1 poprzez Dyrekcję w osobie Dyrektora, wspomaganego przez Wicedyrektorów;
1.8.2. Pracownicy - przez „Pracowników" rozumie się osoby pozostające w stosunku pracy z ZSZ Nr 1 oraz osoby stale współpracujące z ZSZ Nr 1 na podstawie umowy prawa cywilnego.

1.9. Nadzór nad przestrzeganiem postanowień polityki zapewnia **Dyrektor** ZSZ Nr 1, wspierany w swych działaniach przez **Inspektora Ochrony Bezpieczeństwa Informacji** (dalej: „**IBI**") oraz **Inspektora Ochrony Danych Osobowych** (dalej: „**IOD**"), które to funkcje łączy **Radca Prawny Kamil Suplewski** (wpis OIRP WA-13308, kamil.suplewski@gmail.com , +48 506 577 332). Nadzór, o którym mowa w zdaniu poprzedzającym zmierza w szczególności, ale nie wyłącznie do zapewnienia, że czynności związane z przetwarzaniem Informacji w ZSZ Nr 1 są zgodne z wymogami prawa oraz postanowieniami Polityki. Nadzór realizowany jest poprzez:

1.9.1. Nadzór nad realizacją polityki bezpieczeństwa informacji oraz innych dokumentów wewnętrznych związanych z ochroną informacji;
1.9.2. Decydowanie o współpracy w zakresie bezpieczeństwa z innymi podmiotami;
1.9.3. Wyrażanie zgody na udostępnienie stronom trzecim informacji stanowiących tajemnicę organizacji;
1.9.4. Uczestnictwo w opracowaniu szczególnych wymagań bezpieczeństwa i procedur bezpieczeństwa;
1.9.5. Zapewnienie przetwarzania danych osobowych zgodnie z ustawą o ochronie danych osobowych oraz innymi przepisami powszechnie obowiązującego prawa;
1.9.6. Wskazywanie kierunków działań w zakresie bezpieczeństwa;
1.9.7. Wykonywanie przeglądów polityki bezpieczeństwa informacji i Systemu Zarządzania Bezpieczeństwem Informacji;
1.9.8. Monitorowanie istotnych zmian narażenia aktywów informacyjnych na zagrożenia;
1.9.9. Wykonywanie przeglądu i monitorowanie naruszeń bezpieczeństwa informacji;
1.9.10. Dokonywanie analizy naruszeń bezpieczeństwa informacji.
1.9.11. Spotkania na przeglądach zarządzania oraz doraźne w sytuacjach mogących mieć istotny wpływ na bezpieczeństwo informacji;
1.9.12. Monitorowanie zmian w przepisach prawnych dotyczących sposobu zabezpieczenia danych oraz dostosowanie systemu do wymagań prawnych;
1.9.13. Koordynację zapewnienia bezpieczeństwa informacji oraz związanych z nim polityk i procedur;
1.9.14. Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń bezpieczeństwa informacji lub prób takich naruszeń;
1.9.15. Rozstrzyganie problemów dotyczących wątpliwości w stosowaniu dokumentacji systemu;
1.9.16. Przestrzeganie zasad ochrony informacji przez niego jak i przez pracowników,
1.9.17. Identyfikowanie i dokumentowanie zagrożeń zachowania bezpieczeństwa informacji;
1.9.18. Definiowanie oraz realizację działań zapobiegających zagrożeniom,
1.9.19. Zapoznanie pracowników z obowiązkami związanymi z ochroną informacji na stanowiskach pracy;
1.9.20. Kontroluje znajomość procedur bezpieczeństwa przez wszystkich użytkowników systemu w zakresie bezpieczeństwa teleinformatycznego;
1.9.21. Nadawanie i odbieranie uprawnień, do korzystania z danych w systemach. W tym nadzór nad użytkownikami posiadającymi uprawnienia administratorskie do systemów.
1.9.22. Nadzór i kontrola konfigurację systemu w zakresie dostępu do sieci teleinformatycznej;
1.9.23. Bieżącą kontrola zabezpieczeń oraz zgodność funkcjonowania systemu ze szczególnymi wymaganiami bezpieczeństwa;
1.9.24. Wdrażanie procedury ochrony antywirusowej, przed złośliwym oprogramowaniem oraz nieuprawnionym dostępem do zasobów systemów za pośrednictwem sieci teleinformatycznych;
1.9.25. Sprawdzanie poprawność działania systemu oraz jego zabezpieczeń w zakresie ochrony antywirusowej, przed złośliwym oprogramowaniem oraz innymi zagrożeniami mogącymi pochodzić z sieci teleinformatycznych;
1.9.26. Proponowanie zmian mających na celu zwiększenia bezpieczeństwa systemu lub sieci teleinformatycznej;
1.9.27. Nadzorowanie procesu sporządzania kopii zapasowych danych znajdujących się w systemach teleinformatycznych.

1.9.28. Nadzór nad zabezpieczeniem danych poprzez tworzenie i właściwe zabezpieczanie kopii zapasowych;
1.9.29. Analiza pracy systemu informatycznego w celu wykrycia potencjalnych zagrożeń;
1.9.30. Nadzór nad poprawnością pracy systemów informatycznych oraz mechanizmów zabezpieczających dane w tych systemach;
1.9.31. Prowadzenie szkoleń z zakresu bezpieczeństwa teleinformatycznego.

1.10. Odpowiedzialność za bezpieczeństwo informacji ponoszą wszyscy Pracownicy zgodnie z posiadanymi zakresami obowiązków. Każdy pracownik zobowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania informacji zgodnie z obowiązującymi przepisami wewnętrznymi w tym m. in.
1.10.1. Stosować zasady opisane w Polityce oraz innych dokumentach wewnętrznych;
1.10.2. Chronić informacje podlegające ochronie przed dostępem do nich osób nieuprawnionych;
1.10.3. Chronić dane przed przypadkowym lub umyślnym zniszczeniem, utratą lub modyfikacją;
1.10.4. Chronić sprzęt, nośniki magnetyczne i wydruki komputerowe zawierające dane chronione;
1.10.5. Utrzymywać w tajemnicy powierzone hasła, częstotliwość ich zmiany oraz szczegóły technologiczne systemów także po ustaniu;
1.10.6. Stosować się do szczegółowych zaleceń w zakresie ochrony antywirusowej, a także do innych zaleceń wynikających z Systemu Zarządzania Bezpieczeństwem Informacji;
1.10.7. Powiadomić Dyrektora, oraz bezpośredniego przełożonego:
- o ujawnieniu lub możliwości ujawnienia informacji chronionych osobo nieupoważnionym;
- o nieautoryzowanej zmianie informacji chronionych lub możliwości wprowadzenia nieautoryzowanych zmian;
- o zniszczeniu lub możliwości zniszczenia informacji chronionych;
- o zablokowaniu lub możliwości zablokowania pracy systemu informatycznego przetwarzającego informacje chronione lub uniemożliwienia innego dostępu do informacji chronionych;

1.11. ZSZ Nr 1 zapewnia zgodność postępowania kontrahentów ZSZ Nr 1 z postanowieniami Polityki w odpowiednim zakresie we wszystkich sytuacjach, w których dochodzi do przekazania tym podmiotom Informacji do przetwarzania, w tym przechowywania.

2. PODSTAWY SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

2.1. ZSZ Nr 1 zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych informacji we wszelkich lokalizacjach, tj. Siedziba główna ZSZ Nr 1 (ul. Pomologiczna 15, 96-100 Skierniewice), a także przetwarzanie informacji przez upoważnionych użytkowników na urządzeniach mobilnych, oraz w ramach pracy zdalnej (obszar UE, ew.EOG). Zasady pracy zdalnej określa Regulamin pracy zdalnej stanowiący **Załącznik nr 1** do Polityki.

2.2. Osoby upoważnione oraz wszystkie inne osoby, którym udostępnia się Informacje przetwarzane w ZSZ Nr 1 zobowiązane są do ich przetwarzania zgodnie z wymogami prawa oraz zgodnie z postanowieniami Polityki, jak również innych wewnętrznych aktów i procedur ZSZ Nr 1.

2.3. Przy zatrudnianiu Pracowników oraz w toku zatrudnienia ZSZ Nr 1 zapewnia, że (dotyczy to analogicznie osób współpracujących na podstawie umowy cywilnoprawnej):
2.3.1. Pracownicy przed przystąpieniem do wykonywania obowiązków służbowych otrzymują należytą wiedzę w zakresie zasad przetwarzania i ochrony Informacji w ZSZ Nr 1;

2.3.2. każdy z pracowników zostaje zobowiązany do zachowania poufności i integralności Informacji, zgodnie z wzorem stanowiącym **Załącznik nr 2** do Polityki. Zobowiązanie to może zostać podkreślone i doprecyzowane przy pomocy zawarcia z każdym z pracowników Umowy o poufności i zachowaniu tajemnicy (NDA – Non-disclosure agreement), nakładającej surowe rygory na Odbiorcę Informacji, według wzoru zawartego w **Załączniku nr 3** do Polityki.

2.4. ZSZ Nr 1 zapewnia zgodność przetwarzania informacji, ze szczególnym uwzględnieniem danych osobowych, z wymogami prawa również poprzez zaprojektowanie, wprowadzenie i utrzymywanie Systemu Zarządzania Bezpieczeństwem Informacji. Na System składają się środki organizacyjne oraz środki techniczne ochrony, adekwatne do poziomu ryzyka zidentyfikowanego dla poszczególnych kategorii informacji. Na System składają się w szczególności następujące środki:

2.4.1. siedziba ZSZ Nr 1 chroniona jest alarmem oraz przez firmę ochroniarską. Objęta jest także całodobowym monitoringiem. Dostęp do podglądu monitoringu oraz dysków z zapisem ma jedynie Dyrektor i upoważniony pracownik. Kwestie stosowania monitoringu szczegółowo reguluje Regulamin monitoringu wizyjnego w ZSZ Nr 1 zawarty w **Załączniku Nr 4**, będącym integralną częścią Polityki.

2.4.2. ograniczenie dostępu do pomieszczeń, w których przetwarzane są informacje, jedynie do osób upoważnionych oraz zapewnienie, że inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania danych osobowych wyłącznie w towarzystwie osoby upoważnionej;

2.4.3. zamykanie pomieszczeń na czas nieobecności Pracowników, w sposób uniemożliwiający dostęp do nich osobom trzecim;

2.4.4. zapewnienie zabezpieczenia obszaru użytkowanego przez ZSZ Nr 1 przed czynnikami losowymi, takimi jak pożar lub powódź;

2.4.5. wykorzystywanie zamykanych szafek, szuflad lub innych środków technicznych uniemożliwiających osobom niepowołanym dostęp do przechowywanych w nich informacji;

2.4.6. wdrożenie Polityki czystego biurka, która stanowi **Załącznik nr 5** do Polityki;

2.4.7. wdrożenie zasady „czystego ekranu" - stosowanie środków uniemożliwiających wgląd osobom trzecim do informacji przetwarzanych na ekranie komputera jak automatyczne ustawienia blokady ekranu po określonym czasie braku aktywności i obowiązek blokowania stacji roboczej przed opuszczeniem stanowiska pracy,

2.4.8. wdrożenie „Polityki kluczy", która stanowi **Załącznik nr 6** do Polityki;

2.4.9. zapewnienie bezpieczeństwa sprzętowego i informatycznego, w szczególności poprzez następujące działania:

2.4.9.1. przyjęcie **Instrukcji Zarządzania Systemem Informatycznym**, stanowiącym **Załącznik nr 7** do Polityki, w której znajdują się szczegółowe rozwiązania;

2.4.9.2. wewnętrzna sieć komputerowa, w obszarze siedziby ZSZ Nr 1, została odseparowana od sieci publicznej za pomocą firewall i oprogramowania antywirusowego na poziomach połączenia z siecią zewnętrzną, serwerów oraz stacji roboczych,

2.4.9.3. sprzęt komputerowy podlega cyklicznej inwentaryzacji firmowych systemów informatycznych oraz sprzętu - wraz z numerami seryjnymi, adresami MAC kart sieciowych oraz na stałe przypisanymi adresami IP w ramach wewnętrznej sieci

2.4.9.4. sprzęt komputerowy zabezpieczono poprzez zastosowanie indywidualnej ochrony antywirusowej i firewall oraz szyfrowania stacji danych w przypadku

przenośnych stacji roboczych, a ponadto każdy komputer posiada możliwość włączenia funkcję szyfrowania dysku,

2.4.9.5. dopuszcza się do korzystania jedynie z zapewnionych przez ZSZ Nr 1 zaufanych dysków wirtualnych, rozwiązań chmurowych zapewniających gwarancję bezpieczeństwa przetwarzanych danych na poziomie wysokim,

2.4.9.6. jednostki mobilne (laptopy, telefony, pen-drive) zostały zabezpieczone zgodnie z obowiązującą zgodnie z Instrukcja Zarządzania Systemem Informatycznym w ZSZ Nr 1

2.4.9.7. dopuszcza się wykorzystywanie prywatnego sprzętu komputerowego w celach realizacji zadań służbowych jedynie za pisemną zgodą Dyrektora,

2.4.9.8. sprzęt komputerowy zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania i hasła dostępowego,

2.4.9.9. gdy niezbędne jest przetwarzanie informacji i ich przesyłane elektronicznie jest szyfrowany za pomocą protokołu SSL/TSL 1.3 (oraz 1.2 - wymagany przez niektóre starsze przeglądarki). Transfer jest protokołowany.

2.4.9.10. konta użytkowników wykorzystywane do bieżącej realizacji zadań nie mają uprawnień administracyjnych w systemie informatycznym,

2.4.9.11. stworzona została procedura przywracania systemu (jako całość i tylko wybranych części), podlegająca cyklicznym testom praktycznym.

2.4.9.12. stosowane są urządzenia pozwalające na utrzymanie ciągłości zasilania energetycznego przez okres pozwalający na bezpieczne zakończenie pracy w systemie informatycznym: agregaty prądotwórcze, lokalne urządzenia UPS,

2.4.9.13. w pomieszczeniach serwerowni istnieje możliwość zainstalowane są urządzenia zapewniające odpowiednie parametry fizyczne środowiska pracy (wilgotność, temperatura);

2.4.9.14. dopuszcza się instalowanie w wybranych pomieszczeniach systemów gaszenia pożaru gazem, z zachowaniem środków bezpieczeństwa osób, które mogą znaleźć się w strefie oddziaływania takiego systemu,

2.4.9.15. możliwość zapewnienie zastępczego dostawcy dostępu do sieci Internet.

2.4.10. wdrożenie zapewniającego bezpieczeństwo systemu obiegu dokumentów, który swój wyraz znalazł w **Instrukcji Zarządzania Obiegiem Dokumentów**, stanowiącym **Załącznik nr 8** do Polityki,

2.4.11. zapewnienie skutecznego usuwania lub niszczenia dokumentów zawierających informacje, ze szczególnym uwzględnieniem danych osobowych, w sposób uniemożliwiający ich późniejsze odtworzenie, poprzez:
- pewne usuwanie przez nadpisywanie
- zniszczenie nośnika danych
- anonimizacja poprzez całkowite usunięcie odniesienia do danych os.
- zautomatyzowane procedury usuwania
- manualne procedury usuwania

2.4.12. przeprowadzanie analizy ryzyka dla czynności przetwarzania Informacji lub ich kategorii;

2.4.13. realizację standardów weryfikacji i doboru Podmiotów przetwarzających, jak również warunków powierzenia Przetwarzania danych na rzecz poszczególnych Podmiotów przetwarzających, w tym weryfikacja niekaralności.

2.4.14. monitorowanie zmian w zakresie procesów Przetwarzania Informacji w ZSZ Nr 1 oraz na bieżąco zarządza zmianami mającymi wpływ na ochronę Informacji w ZSZ Nr 1;

2.4.15. szkolenia pracowników i kadry kierowniczej.

3. OGÓLNE ZASADY BEZPIECZEŃSTWA, PRZYWRACANIE SYSTEMU I PLANOWANIE AWARYJNE

3.1. W trybie ciągłym ZSZ Nr 1 monitoruje pracę systemów oraz zapewnia pełną archiwizację danych.

3.2. Celem opracowania Przywracania Systemu i Planowania Awaryjnego jest utrzymanie maksymalnych poziomów dostępności świadczonych usług edukacyjnych, oraz pewność, że odzyskanie sprawności działania po nieplanowanych przerwach nastąpi w możliwie najkrótszym czasie.

3.3. Regulacje w zakresie bezpieczeństwa fizycznego na terenie obiektów pod kątem postępowania w sytuacjach alarmowych, które to regulacje w sposób pośredni i bezpośredni wpływają na zapewnienie bezpieczeństwa przetwarzania informacji w ZSZ Nr 1, określa Instrukcja Alarmowa stanowiąca **Załącznik nr 9** do Polityki.

3.4. Regulacje w zakresie kontroli trzeźwości pracowników Licem oraz osób przebywających na terenie obiektów ZSZ Nr 1, które to regulacje w sposób pośredni i bezpośredni wpływają na zdolność zobowiązanych osób do zapewnienia bezpieczeństwa przetwarzania informacji w ZSZ Nr 1, określa Regulamin przeprowadzania kontroli trzeźwości, stanowiący **Załącznik nr 10** do Polityki

3.5. Obecnie dane w postaci cyfrowej przechowywane są w serwerowni ZSZ Nr 1, z wykorzystaniem sprzętu własnego, znajdującej się w siedzibie ZSZ Nr 1. Na ile to możliwe, usługi kluczowe dla zachowanie ciągłości pracy działania ZSZ Nr 1 (np. systemy wspomagania edukacji, obsługi kadrowo-placowej) świadczone są na rzecz ZSZ Nr 1 przez podmioty zewnętrzne wykorzystujące rozwiązania chmurowe.

3.6. W pierwszej kolejności, w odpowiedzi na powiadomienia o awarii konkretnego systemu, działanie podejmuje programista dyżurujący w celu rozpoznania problemu i przywrócenia poprawnego działania danego systemu. W przypadku złożonego problemu informuje w trybie awaryjnym Dyrektora i IBI (lub też IOD). Przywrócenie danych następuje z backupu lub, w przypadku świeżych danych, z logów bieżących. Dane backupowane są cyklicznie w bezpiecznych lokalizacjach i przywracane zgodnie ze standardową procedurą odtwarzania.

3.7. Planowanie awaryjne w obszarze IT ma na celu ograniczenie skutków materializacji ryzyka braku ciągłości działania, stanowi uzupełnienie procesu zarządzania mającego na celu zapobieganie występowaniu sytuacji awaryjnych – opisanych w ust.3.3., realizowanego w obszarze IT głównie poprzez:
- zarządzanie bieżącą eksploatacją środowiska IT oraz jego zabezpieczeniami
- zapewnienie skalowalności, wydajności, pojemności komponentów IT
- zarządzanie rozwojem infrastruktury (wdrożenie, zmiany w środowisku IT)
- testowanie przedwdrożeniowe, testy bezpieczeństwa i ciągłości działania
- proces zarządzania incydentami (wykrywanie i wczesne reagowanie)

3.8. Planowanie awaryjne - główne etapy procesu:
I etap - akcja ewakuacyjna i ratownicza (ochrona życia i zdrowia)
- identyfikacja zagrożeń (urządzenia wspierające detekcję zdarzeń)
- powiadamianie pracowników, klientów i służb ratowniczych (urządzenia alarmowe, komunikacja, łączność)
- automatyczne systemy ochrony jeśli istnieją (zasilanie, automatyczne gaszenie, oddymianie)
- ewakuacja (systemy dostępu, windy, oświetlenie awaryjne, bramki etc.)
- miejsce zbiorek, ustalenie liczby poszkodowanych (nieobecnych)

II etap (po zakończeniu akcji ratowniczej)
- zabezpieczenie dokumentów i danych
- zabezpieczenie mienia
- zabezpieczenie materiału dowodowego (np. zapis video.)
- ocena skutków zdarzenia
- powiadomienie odpowiednich instytucji zewnętrznych
- ustalenie priorytetów w zakresie likwidacji skutków zdarzenia
- powiadomienie usługodawców i dostawców, ubezpieczycieli

III etap - odtworzenie działalności (plan awaryjny)
- zapewnienie łączności i bieżącej informacji
- ustalenie priorytetów i harmonogramu działań (procedury awaryjne)
- udostępnienie zasobów awaryjnych (lokalizacje zastępcze, procedury odtworzeniowe, sprzęt, systemy IT, awaryjne kopie danych)
- odtworzenie środowiska teleinformatycznego w zasobach awaryjnych
- odtworzenie konfiguracji, uprawnień użytkowników i danych z kopii
- uruchomienie testowe systemów i aplikacji
- kontrola poprawności działania systemów i aplikacji
- powrót systemów i procesów do stanu sprzed awarii, katastrofy

3.7. Testy planów BCP, metodologia:
- określenie zakresu i częstotliwości testów (analiza ryzyka)
- plan testów: zatwierdzenie, wykonanie, organizacja
- scenariusze testów (wybrane komponenty IT)
- udział podmiotów zewnętrznych (usługodawców) i podmiotów zależnych
- analizy wyników testów vs. przyjęte założenia
- udział pracowników komórek merytorycznych
- raportowanie wyników testów (do Dyrekcji i IOD i IBI)
- ocena zdolności do utrzymania ciągłości działania krytycznych procesów i usług w przypadku wystąpienia awarii
- ocena zdolności do odtworzenia działalności w przypadku wystąpienia rozległych awarii i katastrof (zdolność do szybkiego uruchomienia i prowadzenia działalności w oparciu o zapasowy ośrodek przetwarzania)
- decyzje i działania zarządcze

3.8. Elementy ograniczające występowanie zdarzeń i ich skutków
- monitorowanie ryzyka operacyjnego – wczesne sygnały,
- monitorowanie jakości procesu (aktualność i zakres planów, zakres i wyniki testów, etc.)
- wczesna identyfikacja problemów IT, awarii, błędów, incydentów, systemy wspierające
- linie obrony (dyżurny, administrator)
- stosowanie redundantnych rozwiązań i środowisk teleinformatycznych (zasoby awaryjne działające w czasie rzeczywistym)
- standaryzacja środowisk, efektywne zarządzanie architekturą, zmianą, rozwojem, incydentami
- technika wirtualizacji, automatyzacja procesu kopiowania i odtworzenia środowiska, centralne repozytoria (dostępność kopii awaryjnych)
- repozytoria dokumentacji systemowej i awaryjnej,
- kompleksowy proces testowania i działania naprawcze (wyniki testów)
- wybór lokalizacji i lokalizacji zastępczych dla ośrodków przetwarzania
- rezerwy kadrowe, szkolenia.

4. AUDYTY WEWNĘTRZNE

4.1. ZSZ Nr 1 przeprowadza cyklicznie wewnętrzne audyty Systemu Zarządzania Bezpieczeństwem Informacji w celu stwierdzenia czy cele stosowanych zabezpieczeń, zabezpieczenia, procesy i procedury są:
- zgodne z wymaganiami norm ISO/IEC 27000 do ISO/IEC 27005 oraz ISO/IEC 31000 a także wszelkimi innymi obowiązującymi wymaganiami prawnym;
- zgodne ze zidentyfikowanymi wymaganiami bezpieczeństwa informacji;
- skutecznie wdrożone i utrzymywane zgodne z oczekiwaniami

4.2. Metodyka i terminarz przeprowadzania audytów wewnętrznych określa Dyrektor korzystając ze wsparcia IOD i IBI, dostosowując je do bieżących potrzeb ZSZ Nr 1.

5. NARUSZENIE OCHRONY INFORMACJI

5.1. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony Informacji uważa się w szczególności, ale nie wyłącznie:
- 5.1.1. naruszenie bezpieczeństwa systemów informatycznych, w których przetwarzane są dane osobowe;
- 5.1.2. udostępnienie Informacji osobom nieupoważnionym;
- 5.1.3. przetwarzanie Informacji niezgodnie z założonym zakresem i celem ich przetwarzania;
- 5.1.4. nieuprawnione lub przypadkowe uszkodzenie, utratę, zniszczenie lub zmianę Informacji.

5.2. W przypadku stwierdzenia naruszenia ochrony Informacji pracownik, który odkryje fakt naruszenia obowiązany jest niezwłocznie powiadomić o tym fakcie kierownika danej jednostki organizacyjnej, który również niezwłocznie informuje Inspektora Ochrony Bezpieczeństwa Informacji, oraz Inspektora Ochrony Danych Osobowych. IBI (z/lub IOD) sporządzi raport z tego naruszenia i przekaże ten raport Administratorowi Danych. Raport powstanie w oparciu o wzory formularzy, które zawarte są w **Załączniku Nr 11**.

5.3. Dyrektor, po przeprowadzeniu w ścisłym współdziałaniu z Inspektorem Ochrony Bezpieczeństwa Informacji i Inspektorem Ochrony Danych Osobowych, postępowania wyjaśniającego, dokona oceny, czy zachodzi potrzeba zgłoszenia naruszenia do Prezesa Urzędu Ochrony Danych Osobowych, a następnie odstępuje od zgłoszenia lub niezwłocznie zgłasza naruszenie, jeśli zachodzi wysokie prawdopodobieństwo, że naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Sporządzenie zgłoszenia lub opinii o niezasadności zgłoszenia spoczywa na IOD, na podstawie formularza stanowiącego **Załącznik nr 12**

5.4. Od momentu wykrycia faktu naruszenia do ewentualnego zgłoszenia nie może upłynąć więcej niż 72 godziny.

5.5. Jeżeli ryzyko naruszenia praw i wolności podmiotu, którego Informacje dotyczą jest wysokie, ZSZ Nr 1 zawiadamia o incydencie także ten podmiot, chyba że:
- 5.5.1. ZSZ Nr 1 wdroży odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do Informacji, których dotyczy naruszenie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych Informacji;
- 5.5.2. ZSZ Nr 1 zastosuje następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności w/w podmiotu; lub
- 5.5.3. wymagałoby to niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Ocena powyższa zostaje podjęta w ścisłym współdziałaniu z Inspektorem Ochrony Danych Osobowych.

5.6. Procedura powiadomienia osoby, której naruszenia ochrony danych dotyczą, jest analogiczna do procedury opisanej w ustępach 5.3. i 5.4.

5.7. Niezależnie od obowiązków wskazanych w niniejszym paragrafie, ZSZ Nr 1 w ścisłym współdziałaniu z Inspektorem Ochrony Bezpieczeństwa Informacji dokumentuje wszelkie naruszenia ochrony Informacji, w tym okoliczności naruszenia ochrony Informacji, jego skutki oraz podjęte działania zaradcze. Wzór rejestru naruszeń ochrony Informacji stanowi **Załącznik nr 13** do Polityki.

6. UDOSTĘPNIANIE INFORMACJI

6.1. Administrator udostępnia Informacje wyłącznie osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa;

6.2. Informacje udostępniane są:

6.2.1. na podstawie wniosku od podmiotu uprawnionego do otrzymywania Informacji na podstawie przepisów (np. organy ścigania, sądy, inne podmioty za zgodą osoby, której dane dotyczą),

6.2.2. na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych w granicach obowiązujących przepisów;

6.3. Wniosek o udostępnienie danych podmiotowi lub osobie, której dane nie dotyczą powinien zawierać:

- nazwę i adres wnioskodawcy,
- wskazanie podstawy prawnej do przetwarzania przez wnioskodawcę Informacji, o które prosi,
- wskazanie celu przetwarzania tych danych,
- wskazanie zakresu wnioskowanych danych i jeżeli to możliwe zbioru, w jakim są przetwarzane.

6.4. Niedopuszczalne jest udostępnianie odbiorcom danych osobowych w celach innych niż te, dla jakich zostały zgromadzone przez Administratora;

6.5. Wnioskodawcę lub stronę umowy należy poinformować, że udostępnione Informacje mogą być wykorzystane wyłącznie zgodnie z celem, dla którego zostały wydane;

6.6. Odmawia się udostępnienia danych w przypadku, gdy spowodowałoby to istotne naruszenie dóbr osobistych właściciela danych lub innych osób, a także, jeżeli żądane dane osobowe nie mają istotnego związku ze wskazanymi motywami działania wnioskodawcy;

6.7. Administrator prowadzi ewidencję udostępnianych z systemów informatycznych danych obejmujących informację o odbiorcach danych, dacie i zakresie udostępnienia (**Załącznik nr 14**);

6.8. W przypadku zapytania dotyczącego treści danych osobowych złożonego przez osobę, której te dane dotyczą odpowiedzi udziela się w terminie nie dłuższym niż 30 dni od daty otrzymania zapytania.

6.9. Działania powyższe podejmowane są w ścisłym współdziałaniu z Inspektorem Ochrony Danych Osobowych, oraz z Inspektorem Ochrony Bezpieczeństwa Informacji.

7. POSTANOWIENIA KOŃCOWE

7.1. Polityka wchodzi w życie z dniem 01.01.2024r..

7.2. Polityka jest przechowywana i udostępniana w wersji, pisemnej, dokumentowej oraz elektronicznej w siedzibie ZSZ Nr 1, oraz w wersji elektronicznej na stronie internetowej ZSZ Nr 1.

7.3. Jedyną wersją legalną Polityki jest język polski. Dokumentacja w języku angielskim pełni jedynie funkcje pomocnicze w sprawach dotyczących obrotu międzynarodowego.

7.4. Politykę udostępnia się:

7.4.1. obligatoryjnie wszystkim osobom upoważnionym do przetwarzania Informacji w ZSZ Nr 1, celem zapewnienia osobom upoważnionym należytej wiedzy oraz informacji na temat zasad i wymogów dotyczących przetwarzania Informacji w ZSZ Nr 1;

7.4.2. osobom zainteresowanym, w szczególności osobom fizycznym, których dane dotyczą – w formie elektronicznej lub papierowej w siedzibie ZSZ Nr 1. W tym przypadku Załączniki pozostają niejawne, za wyjątkiem dokumentów o nazwie „Polityka Ochrony Danych Osobowych", „Regulamin monitoringu", „Instrukcja alarmowa" i „Regulamin kontroli trzeźwości".

7.5. W sprawach nieuregulowanych w Polityce odpowiednie zastosowanie znajdują postanowienia stanowiącego integralną część Polityki **Załącznika nr 15** - Polityka Ochrony Danych Osobowych w ZSZ Nr 1, wraz z jego załącznikami, stanowiącymi jego integralną część.

7.6. Wszelkie zmiany lub uzupełnienia do Polityki wymagają dla swej skuteczności formy pisemnej pod rygorem nieważności i wchodzą w życie nie wcześniej, niż w dniu następującym po dniu ogłoszenia w siedzibie ZSZ Nr 1.

7.7. Do Polityki dołączono następujące Załączniki (w przypadku kilku z nich z przyczyn technicznych zasadnym było ograniczenie istnienia tych Załączników do formy elektronicznej), stanowiące jej integralną część:

- Załącznik nr 1 – Regulamin pracy zdalnej
- Załącznik nr 2 – Wzór zobowiązania do zachowania poufności oraz informacja dla pracownika
- Załącznik nr 3 – Wzór Umowy o poufności i zachowaniu tajemnicy (Non-disclosure agreement)
- Załącznik nr 4 – Regulamin monitoringu
- Załącznik nr 5 – Polityka czystego biurka
- Załącznik nr 6 – Polityka Kluczy
- Załącznik nr 7 – Instrukcja Zarządzania Systemem Informatycznym
- Załącznik nr 8 – Instrukcja Zarządzania Obiegiem Dokumentów
- Załącznik nr 9 – Instrukcja Alarmowa
- Załącznik nr 10 – Regulamin przeprowadzania kontroli trzeźwości
- Załącznik nr 11 – Wzory formularzy dot. naruszenia ochrony informacji
- Załącznik nr 12 – Wzór zgłoszenia naruszenia
- Załącznik nr 13 – Wzór Rejestru naruszeń
- Załącznik nr 14 – Ewidencja udostępnień Informacji
- Załącznik nr 15 – Polityka Ochrony Danych Osobowych w ZSZ Nr 1 wraz z Załącznikami:
    a) Załącznik nr 1 – Kategorie danych i narzędzia przetwarzania;
    b) Załącznik Nr 2 – Ocena Ryzyka (DPIA)
    c) Załącznik nr 3 – Wykaz pomieszczeń
    d) Załącznik nr 4 - Wzór Upoważnienia do przetwarzania danych osobowych
    e) Załącznik nr 5 - Wzór Ewidencji osób upoważnionych
    f) Załącznik nr 6 - Wzór zobowiązania do zachowania poufności oraz informacja dla pracownika
    g) Załącznik Nr 7 - Wzór NDA
    h) Załącznik Nr 8 - Regulamin monitoringu
    i) Załącznik nr 9 - Polityka czystego biurka
    j) Załącznik nr 10 - Polityka Kluczy
    k) Załącznik nr 11 - Rejestr czynności przetwarzania
    l) Załącznik nr 12 - Info RODO
    m) Załącznik Nr 13 - Rejestr żądań osób
    n) Załącznik nr 14 - Raport z naruszenia

o) Załącznik Nr 15 - Wzory formularzy dot. naruszenia ochrony danych osobowych
p) Załącznik nr 16 - Wzór Rejestru naruszeń
q) Załącznik nr 17 - Wzór umowy powierzenia - DPA
r) Załącznik nr 18 - Ewidencja udostępnianych danych osobowych
s) Załącznik nr 19 - Notatka z czynności w ramach sprawdzenia okresowego

Na oryginale właściwe:
Data, pieczęć i podpis Dyrektora

Przygotował dn.13,12.2023r.:
Radca Prawny Kamil Suplewski
OIRP Warszawa: WA-13308

Na oryginale właściwe:
Data, pieczęć i podpis Mecenasa.

Adnotacje o aktualizacjach:
- brak.