*Załącznik Nr 1 do Zarządzenia nr 47/2019*

 *Dyrektora Szkoły Podstawowej nr 2 w Czeladzi z dn.14 sierpnia 2019r.*

**Polityka Ciągłości Działania**

1. CEL

Zapewnienie ciągłości działania i ochrona procesów biznesowych przed skutkami zdarzeń losowych i sytuacji kryzysowych.

1. ZAŁOŻENIA
	1. Nieprzestrzeganie niniejszej Polityki będzie skutkować pociągnięciem do odpowiedzialności dyscyplinarnej.
* **Szkoła Podstawowa nr 2 im. Marii Konopnickiej w Czeladzi** posiada Plan Ochrony ppoż. i ustalony sposób komunikacji na wypadek klęsk żywiołowych zalanie, pożar itp.
* W zakresie ciągłości funkcjonowania Jednostka wykonuje kopie zapasowe
w wersji elektronicznej wszystkich istotnych danych dotyczących biznesowej działalności Jednostki.
* Archiwizowane dane elektroniczne przechowane są w szafie pancernej.
* Dokumenty papierowe archiwizowane są w archiwum – nie wykonuje się kopii zapasowej tych dokumentów. Pomieszczenie zabezpieczone jest odpowiednim zamkiem.
* Instrukcja ppoż. jest opracowywana i aktualizowana przez inspektora BHP, który odpowiedzialny jest za jej dostępność oraz przeszkolenie pracowników Jednostki.
* Instrukcje ppoż. przeglądane są pod kątem ich adekwatności i aktualności przez Inspektora BHP.
* Za przestrzeganie zasad wynikających z tej polityki odpowiedzialny jest Dyrektor.
* Dyrektor odpowiada za bezpieczeństwo pracy użytkowanych pomieszczeń
i aktualną instrukcje ppoż., by była dostępna w miejscu jej stosowania oraz za organizację szkoleń pracowników w tym zakresie.
* W przypadku utraty danych elektronicznych dane te są odtwarzane z kopii zapasowych.
* Dyrektor odpowiada za organizację, wyznaczenie osób odpowiedzialnych za ewakuację z pomieszczeń firmy dokumentów, danych i sprzętu w przypadku pożaru lub zalania użytkowanych pomieszczeń.

| Nr egz: | Stanowisko  | Imię i nazwisko | Data  | Podpis  |
| --- | --- | --- | --- | --- |
| Zatwierdził | Dyrektor | Marta Świderek |  |  |

**Polityka Czystego Biurka i pulpitu**

1. CEL

Zapobieganie utracie, uszkodzeniu lub możliwości nieuprawnionego dostępu
do informacji oraz do urządzeń przetwarzających informacje.

1. ZAKRES

Procedura swoim zakresem obejmuje wszystkich pracowników.

1. OPIS POSTĘPOWANIA
	1. Nieprzestrzeganie niniejszej procedury będzie skutkować pociągnięciem
	do odpowiedzialności dyscyplinarnej.
	2. Aby zapewnić bezpieczeństwo danych obowiązuje szereg zasad czystego biurka i czystego pulpitu.
	3. Czynności
		1. Biurko
* Wszystkie dokumenty i ruchome nośniki danych (płyty CD, dyski przenośne, pamięć zewnętrzna itp.) nie są pozostawiane na biurku. W momencie,
gdy przestają być używane – chowane są do szafek i biurek. W przypadku informacji wrażliwych / zastrzeżonych, zamykane są na klucz, a dane z nich usuwa się gdy stają się niepotrzebne.
* Na biurku znajdują się jedynie dokumenty aktualnie wykorzystywane
przez pracownika/personel. W przypadku opuszczenia stanowiska pracy (wyjście do WC, na przerwę śniadaniową / obiadową, poza siedzibę) wszystkie dokumenty i ruchome nośniki danych oraz pieczęcie znajdują się
w szafkach i szufladach. W przypadku informacji wrażliwych i zastrzeżonych, ruchome nośniki i pieczęcie, zamykane są na klucz.
* Dyrektor lub pracownik wyznaczony przez Dyrektora przeprowadza po godzinach pracy okresowe przeglądy z zakresu stosowania postanowień czystego biurka i pulpitu oraz zabezpieczenia informacji wrażliwych/zastrzeżonych przed nieuprawnionym dostępem.
	+ 1. Pulpit
* W odniesieniu do urządzeń przetwarzających informacje (komputer) stosuje się zasadę czystego pulpitu – nie prowadzi się zapisywania, tymczasowego zapisywania plików. Na pulpicie znajdują się tylko skróty do plików oraz katalogów.
* Po odejściu od stanowiska pracy należy się wylogować (przełączenie użytkownika)
* Dyrektor lub pracownik wyznaczony przez Dyrektora przeprowadza po godzinach pracy okresowe przeglądy z zakresu stosowania postanowień czystego pulpitu oraz wylogowania się z sieci w przypadku opuszczenia stanowiska pracy

| Nr egz: | Stanowisko  | Imię i nazwisko | Data  | Podpis  |
| --- | --- | --- | --- | --- |
| Zatwierdził | Dyrektor | Marta Świderek | . |  |

**Polityka Kontroli Oprogramowania**

1. CEL

Zapewnienie bezpieczeństwa, poufności, integralności i dostępności informacji
i oprogramowania.

1. ZAŁOŻENIA
	1. Nieprzestrzeganie niniejszej Polityki będzie skutkować pociągnięciem do odpowiedzialności dyscyplinarnej.
	2. Ochrona przed szkodliwym oprogramowaniem:
* Szkodliwe oprogramowanie to wirusy komputerowe, robaki sieciowe, konie trojańskie i inne oprogramowanie mogące skutkować naruszeniem bezpieczeństwa, poufności, integralności i dostępności informacji.
* Na komputerach z systemem operacyjnym Windows, które są podłączone do Internetu instalowane jest oprogramowanie antywirusowe.
* Oprogramowanie antywirusowe na komputerach jest regularnie aktualizowane.
* Aktualizacja oprogramowania następuje automatycznie gdy pojawiają się jego nowsze wersje bezpośrednio z serwera producenta oprogramowania.
* Wszystkie pliki zewnętrzne i wewnętrzne (w tym poczta e-mail) są automatycznie monitorowane i skanowane przez program antywirusowy.
	1. Kontrola legalności oprogramowania komputerowego:
* Obowiązuje bezwzględny zakaz instalowania bez zgody Dyrektora nielegalnego lub zewnętrznego (nie zakupionego przez Jednostkę) oprogramowania komputerowego na komputerach (także laptopach) i serwerach będących własnością Jednostki.
* Nowe oprogramowanie jest nadzorowane przez Informatyka lub pracownika Jednostki wyznaczonego przez Dyrektora.
* Prowadzony jest rejestr oprogramowania zainstalowanego na każdym komputerze/serwerze w postaci „Zestawienia Zbiorczego dla Zestawu” (użytkownik, oprogramowanie).
* Obowiązuje bezwzględny zakaz udostępniania programów będących własnością Jednostki osobom trzecim, oraz instalowania programów jednostanowiskowych na innych stanowiskach.
* Licencje oprogramowania są przechowywane w segregatorach i szafkach przez Informatyka.
	1. Pracownik Jednostki ma obowiązek niezwłocznie zgłosić do Informatyka każdy problem związany z niewłaściwym funkcjonowaniem sprzętu komputerowego lub oprogramowania.
	2. Instalację lub reinstalację oprogramowania systemowego i użytkowego na stanowiskach komputerowych dokonuje Informatyk na wniosek Dyrektora lub użytkownika sprzętu.
	3. System komputerowy jest chroniony przed wirusami komputerowymi poprzez regularne, automatyczne skanowanie systemu programem antywirusowym.

| Nr egz: | Stanowisko  | Imię i nazwisko | Data  | Podpis  |
| --- | --- | --- | --- | --- |
| Zatwierdził | Dyrektor | Marta Świderek | . |  |

**Polityka Postępowania ze Sprzętem i Nośnikami**

1. CEL

Zapobieganie utracie, uszkodzeniu, możliwości nieuprawnionego dostępu do sprzętu i nośników danych lub innym naruszeniom bezpieczeństwa danych.

1. ZAŁOŻENIA
	1. Nieprzestrzeganie niniejszej Polityki będzie skutkować pociągnięciem do odpowiedzialności dyscyplinarnej.
	2. **Rozmieszczenie, ochrona i konserwacja sprzętu:**
* Sprzęt należy ustawiać w taki sposób, aby zminimalizować niepożądany dostęp do obszarów roboczych; monitory komputerowe powinny być ustawione tyłem do drzwi, drukarki, kopiarki, faksy i inne urządzenia służące do gromadzenia lub przetwarzania danych powinny znajdować się w pokojach służbowych.
* Urządzenia do przetwarzania informacji wrażliwych i informacji niejawnych są odizolowane – umiejscowione w strefach bezpieczeństwa.
* Spożywanie posiłków odbywa się w wyznaczonym do tego miejscu z dala od urządzeń przetwarzających informacje oraz od dokumentów papierowych.
* Sprzęt jest konserwowany i przeglądany przez Informatyka lub osobę wyznaczoną przez Dyrektora w miarę bieżących potrzeb oraz na podstawie zgłoszenia awarii. Serwery podlegają serwisowi zewnętrznemu.
W przypadku wykonywanych prac przy serwerze przez firmę zewnętrzną zawsze wymagana jest obecność Informatyka.
	1. **Zapewnienie zasilania, łączności i innych warunków środowiskowych:**
* Sprzęt komputerowy chroniony jest przed awariami zasilania i innymi zakłóceniami elektrycznymi poprzez zapewnienie właściwego zasilania zgodnie z zaleceniami producenta – stosowanie zabezpieczeń typu dwustopniowe zabezpieczenia przeciw przepięciowe, urządzenia podtrzymujące zasilanie (UPS)
* W pomieszczeniach zapewnione są odpowiednie warunki środowiskowe – stała temperatura zapewniona.
	1. **Zabezpieczenie danych w siedzibie:**
* Prowadzone są spisy inwentaryzacyjne sprzętu.
* Nośniki danych zawierające informacje wrażliwe i zastrzeżone każdorazowo są chowane przy wyjściu do toalety i do domu – zasada czystego biurka. Szafki oraz biurka gdzie przechowywane są nośniki danych zamykane są na klucz.
* Dostęp do Internetu oraz do poczty elektronicznej zabezpieczony jest poprzez Firewall.
* Komputery automatycznie wylogowują użytkownika i wygaszają ekran
w przypadku dłuższej bezczynności, po zakończeniu pracy każdy pracownik ma obowiązek wylogować się z systemu.
* Każdy użytkownik komputera ma nadane hasło i login, które musi wprowadzać za każdym razem po uruchomieniu, wygaszeniu lub wylogowaniu. Hasło jest zmieniane co 1 miesiąc.
* Wszelkie drukowane, kopiowane oraz faksowane dokumenty zabierane są od razu z drukarki, kopiarki lub faksu.
	1. **Zabezpieczenie sprzętu i danych poza siedzibą:**
* Obowiązuje zasada, że sprzęt komputerowy, dokumenty, dane oraz nośniki danych nie są wynoszone poza siedzibę Jednostki.
* Tylko osoby, które otrzymały zezwolenie na wyniesienie poza siedzibę sprzętu lub nośników danych (pendrive, taśmy, dokumentacja papierowa) mogą wynosić w/w zasoby. Osoby te ponoszą pełną odpowiedzialność za powierzone zasoby.
* Sprzęt i nośniki zabierane z siedziby nie są pozostawiane bez nadzoru
w miejscach publicznych (np. nie są pozostawiane w samochodzie). Należy odpowiednio obchodzić się ze sprzętem (zgodnie z zaleceniami producenta) oraz chronić go przed zniszczeniem i utratą (nie rzucać sprzętu, przewozić
w taki sposób, który nie zdradza zawartości bagażu). Sprzęt należy odpowiednio zabezpieczyć przed dostępem osób niepowołanych – hasło, login.
* Dane na nośnikach magnetycznych należy chronić przed polem magnetycznym oraz wysoką temperaturą.
	1. **Zasady postępowania z nośnikami danych (taśmy, dyski, kasety, płyty CD/DVD, dyskietki, pendrive, pamięć zewnętrzna, kartki papieru – wydruki, dokumenty, rejestry, itp.):**
* Nośniki danych np. dyski twarde, nosiki USB, płyty CD/DVD (niewłaściwie nagrane dane) które są już zużyte, niszczone są fizycznie lub dane na nich są trwale usuwane (wielokrotne nadpisanie danych).
* W przypadku zmiany nośnika lub właściciela sprzętu każda informacja zawarta na dysku jest usuwana lub pozostawiona (zależy to od przeznaczenia nośnika).
* Uszkodzone dyski są utylizowane przez firmę zewnętrzna, która posiada uprawnienia do wykonywania takich usług.
* W przypadku zmiany właściciela sprzętu dysk jest formatowany w taki sposób, aby danych z dysku nie można było odtworzyć i tylko taki sprzęt jest przekazany nowemu użytkownikowi.
* Nośniki z danymi wrażliwymi lub zastrzeżonymi powinny być każdorazowo chowane – zamykane na klucz w szafie lub biurku w sytuacji opuszczenia stanowiska pracy (wyjście do ubikacji, do domu). Obowiązuje zasada czystego biurka.
* W przypadku przechowywania danych przez dłuższy czas należy je odświeżyć w zależności od nośnika w celu sprawdzenia dostępności i integralności danych.
1. **CZYNNOŚCI**
* Każdy pracownik stosuje zasadę czystego biurka i czystego pulpitu.
* Informatyk usuwa w sposób trwały informacje z nośników danych - jeżeli wymaga tego sytuacja.
* Informatyk deponuje uszkodzone nośniki w zamykanej szafie (w uzasadnionych przypadkach przekazuje je firmie utylizującej).

| Nr egz: | Stanowisko  | Imię i nazwisko | Data  | Podpis  |
| --- | --- | --- | --- | --- |
| Zatwierdził | Dyrektor | Marta Świderek | . |  |

**Polityka Szacowania Ryzyka**

1. **Cel**

Zapewnienie, że Metodyka Szacowania Ryzyka przyjęta w Jednostce jest spójna ze zidentyfikowanymi wymaganiami biznesowymi i prawnymi w zakresie ochrony bezpieczeństwa informacji, zawiera kryteria akceptacji ryzyka
i zapewnia uzyskanie porównywalnych wyników w całej organizacji podczas kolejnych szacowań ryzyka.

1. **Założenia**
	1. **Nieprzestrzeganie niniejszej Polityki będzie skutkować pociągnięciem do odpowiedzialności dyscyplinarnej.**
	2. Szacowanie ryzyka prowadzi wyznaczony pracownik ds.ZSBI wraz z Inspektorem ds. ochrony danych osobowych.
	3. Szacowanie ryzyka przeprowadzane jest przynajmniej raz do roku
	oraz w przypadku zajścia następujących zdarzeń:
* zidentyfikowania zasobów informacyjnych, co do których dotychczas
nie przeprowadzono szacowania ryzyka
* zmian w technologii (w tym informatycznej), mogących powodować zmianę zagrożenia bezpieczeństwa informacji
* zidentyfikowania nowych lub zmienionych procesów zachodzących, które wykraczają poza dotychczas zdefiniowany zakres systemu SZBI.
	1. W szacowaniu ryzyka biorą udział właściciele zasobów po to, aby:
* zapewnić poczucie odpowiedzialności właściciela za powierzony mu zasób
i zwiększyć jego świadomość co do wagi bezpieczeństwa informacji
* zapewnić realistyczne oszacowanie rodzaju zagrożeń, wartości zasobu, podatności i prawdopodobieństwa wystąpienia zagrożeń.
	1. Aby zapewnić udział właścicieli zasobów, Szacowanie Ryzyka rozsyłane jest
	do rejestracji pocztą elektroniczną. Wyniki szacowania ryzyka
	z poszczególnych działów są scalane a następnie analizowane przez Inspektora ds. ochrony danych osobowych.
	2. Skale ocen stosowane podczas szacowania ryzyka

*Skale ocen* stanowią element Metodyki Szacowania Ryzyka i zawarte
są w pliku Szacowanie Ryzyka w arkuszu Metodyka. Są to skale ocen dotyczące wartości zasobów, podatności, prawdopodobieństwa, poufności itp.

Skala ocen jest skonstruowana w taki sposób, aby wszystkie osoby biorące udział w szacowaniu ryzyka rozumiały je i stosowały jednolicie, przez co wyniki szacowania ryzyka są porównywalne, a rezultaty powtarzalne. W tym celu, każda skala ocen zawiera następujące elementy:

* wynik na skali, określony poprzez liczbę (np. 1-4) lub słownie (np. mało ważna, średnio ważne, ważne, bardzo ważne)
* opis wyniku, określający co rozumie się poprzez przyjęcie danego wyniku
* skrótowe określenie słowne danego wyniku, stanowiące lapidarne podsumowanie przyjętego wyniku.
1. Czynności
	1. Opracowanie metodyki szacowania ryzyka
* Metodyka Szacowania Ryzyka znajduje się w pliku Szacowanie Ryzyka. Jest ona taka sama dla całej jednostki, co zapewnia porównywalne i powtarzalne rezultaty. Za opracowanie metodyki odpowiedzialny jest wyznaczony pracownik ds. SZBI oraz Inspektor ds. ochrony danych osobowych.
	1. Identyfikacja ryzyka

Dyrektor/Inspektor ds. ochrony danych osobowych:

* identyfikują zasoby informacyjne (plik Szacowanie Ryzyka, zakładka Inwentaryzacja) oraz określają właścicieli tych zasobów,
* dzielą informacje na grupy (np. dane kadrowe, dane osobowe, dane produkcyjne itp.), informacji nie należy dzielić na szczegółowe grupy dotyczące pojedynczych zasobów, lecz na ogólne grupy, które mogą być rozbite przy samym szacowaniu ryzyka na podgrupy.
* określają miejsca przechowywania, przetwarzania danych grup informacyjnych,
* określają w zakładce Inwentaryzacja miejsca występowania poszczególnych grup informacyjnych,
* przenoszą zinwentaryzowane zasoby do pliku Szacowanie Ryzyka
do zakładki z poszczególnymi działami, gdzie kontynuują szacowanie ryzyka.
* ustalają potencjalne szkody/wartość zasobów informacyjnych,
* określają w pliku szacowanie ryzyka, stosując przyjętą w metodyce skalę,
jakie skutki miałaby utrata poufności, integralności oraz dostępności każdej
z zidentyfikowanych grup informacyjnych
* identyfikują zagrożenia w stosunku do zasobów informacyjnych,
* identyfikują i oceniają podatności zasobów informacyjnych, które mogą zostać wykorzystane przez zagrożenia.
	1. Analiza i ocena ryzyka

Inspektor ds. ochrony danych osobowych/Dyrektor:

* w pliku Szacowanie Ryzyka, zakładka z szacowaniem poszczególnych ryzyk, określają stosując przyjętą w metodyce skalę, w stosunkudo każdego zagrożenia i podatności, jakie jest prawdopodobieństwo wystąpienia każdego ryzyka,
* określają poziom ryzyka, które zostaje wpisane automatycznie w pliku Szacowanie Ryzyka, zakładka Metodyka na podstawie macierzy pobieranej
z pliku.
	1. Decyzja co do postępowania z ryzykiem

Dyrektor/Inspektor ds. ochrony danych osobowych

* Na postawie wyliczonego wcześniej poziomu ryzyka wpisują decyzję
co do postępowania z danym ryzykiem. Możliwe decyzje to: zastosowanie zabezpieczeń, akceptacja ryzyka, unikanie ryzyka, przeniesienie ryzyka.
* W przypadku podjęcia decyzji o zastosowaniu zabezpieczeń (redukcji ryzyka), wybierają do danych ryzyk odpowiednie cele i zabezpieczenia.
* Wybrane zabezpieczenia muszą wynikać z szacowania ryzyka dla danego zasobu i uwzględniać również wymagania prawne oraz wynikające z umów.
* Zabezpieczeniem może być procedura (polityka) albo zabezpieczenie fizyczne (np. zamontowanie bramek fizycznego dostępu do pomieszczeń).
* Wybrane zabezpieczenia zapisują w pliku Plan Postępowania z Ryzykiem. Ostateczną decyzję odnośnie wprowadzenia zabezpieczeń podejmuje Dyrektor.
* Po odpowiednim zabezpieczeniu wykonywane jest szacownie ponowne (szczątkowe)
	1. **Przygotowanie Deklaracji Stosowania**

Na podstawie wyników Szacowania Ryzyka Inspektor ds. ochrony danych osobowych przygotowuje Deklarację Stosowania i umieszcza ją w pliku Deklaracja Stosowania. Deklaracja Stosowania stanowi podsumowanie decyzji podjętych w wyniku szacowania ryzyka.

Deklaracja Stosowania zawiera:

* wybrane zabezpieczenia wraz z określeniem przyczyn ich wyboru, zabezpieczenia obecnie stosowane,
* wyłączenia zabezpieczeń zawartych w załączniku A do normy
ISO 27001 wraz o określeniem przyczyn ich wyłączenia.
	1. **Przygotowanie Planu Postępowania z Ryzykiem**

Na podstawie wyników Szacowania Ryzyka oraz Deklaracji Stosowania Inspektor ds. ochrony danych osobowych/Dyrektor przygotowuje Plan Postępowania z Ryzykiem. Plan Postępowania z Ryzykiem zawiera:

* działania, które należy podjąć w związku ze zidentyfikowanym i ocenionym ryzykiem (wdrożenie zabezpieczeń),
* zasoby potrzebne do wdrożenia Planu,
* odpowiedzialności, priorytety i terminy wdrożenia poszczególnych elementów Planu.
	1. **Zatwierdzenie Planu Postępowania z Ryzykiem i przekazanie go do realizacji**

Wyniki Szacowania Ryzyka w postaci „Raportu z Szacowania Ryzyka”
oraz Plan Postępowania z Ryzyka są przedstawiane Dyrektorowi celem:

* Akceptacji pozostałego ryzyka (szczątkowe),
* Akceptacji wyników Szacowania Ryzyka i proponowanego Plan Postępowania
z Ryzykiem.
* Działania zawarte w Planie Postępowania z Ryzykiem przekazywane
są wymienionym w nim osobom do wdrożenia.

| Nr egz: | Stanowisko  | Imię i nazwisko | Data  | Podpis  |
| --- | --- | --- | --- | --- |
| Zatwierdził | Dyrektor | Marta Świderek |  |  |

**Polityka Zarządzania Incydentami**

1. Cel

Zapewnienie, że incydenty i słabości związane z systemami informacyjnymi
są zarządzane tak, aby umożliwić podejmowanie we właściwy sposób działań korygujących.

1. Założenia
	1. Nieprzestrzeganie niniejszej Polityki będzie skutkować pociągnięciem
	do odpowiedzialności dyscyplinarnej.
	2. *Incydent*rozumiany jest jako zdarzenie, które stwarza wzrost prawdopodobieństwo zakłócenia funkcjonowania i zagrażają bezpieczeństwu informacji np. włamanie do siedziby, pozostawienie wrażliwych danych na ekranie komputera, dokumentów bez nadzoru itp.
	3. *Słabość* systemu rozumiana jest jako stan mogący powodować wystąpienie incydentu, np. zawieszenie się komputera, niezamknięte drzwi, próba włamania do systemu, do siedziby, podejrzenie o włamaniu itp.
2. Czynności
	1. W przypadku wystąpienia jakiegokolwiek incydentu, (np. Osoby nieupoważnione bez nadzoru w strefach bezpieczeństwa, dokumenty zawierające dane wrażliwe pozostawione bez nadzoru w miejscu ogólnie dostępnym), osoba, która zauważy zdarzenie ma obowiązek niezwłocznie poinformować Dyrektora o zaistniałej sytuacji i rozpocząć doraźne działania adekwatne do zaistniałej sytuacji. Zostają ustalone kroki postępowania.
	2. W przypadku wystąpienia incydentu typu pożar, zalanie itp. Pracownicy postępują zgodnie z instrukcjami ppoż. i bezpieczeństwa oraz wytycznymi Dyrektora i Inspektora ds. BHP. Kierownictwo współpracuje ze sztabem kryzysowym oraz odpowiednimi władzami w celu usunięcia skutków incydentu i dojścia do przyczyny jego wystąpienia. Po uzyskaniu informacji, przekazywane są one do Inspektora ds. ochrony danych osobowych celem podjęcia szacowania ryzyka i zabezpieczenia.
	3. W przypadku wystąpienia incydentu związanego z awarią sprzętu / sieci komputerowej, np. zawieszenie się systemu, próba włamania, nieoczekiwany komunikat na ekranie komputera, należy niezwłocznie zgłosić zdarzenie Informatykowi lub pracownikowi wyznaczonemu przez Dyrektora i nie podejmować żadnych działań na własną rękę. Informatyk lub wyznaczony pracownik przez Dyrektora informuje Inspektora ds. Ochrony danych osobowych o zaistniałym incydencie oraz podejmuje odpowiednie działania.
	4. Wyznaczona osoba prowadzi Rejestr Incydentów, gdzie odnotowane są wszystkie zgłoszenia błędów, awarii systemu oraz innych incydentów.
	5. Informatyk lub osobowa wyznaczona przez Dyrektora prowadzi okresowe przeglądy rejestru incydentów oraz dokonuje analizy wpisów. W uzasadnionych sytuacjach podejmuje działania korygujące lub zapobiegawcze zgodnie z procedurą działań korygujących i zapobiegawczych. Wyniki analiz są przedstawiane na Przeglądach Zarządzania.

| Nr egz: | Stanowisko  | Imię i nazwisko | Data  | Podpis  |
| --- | --- | --- | --- | --- |
| Zatwierdził | Dyrektor | Marta Świderek |  |  |

RAPORT ANALIZY RYZYKA

Z przeprowadzonej analizy szacowania ryzyka wynika, że w 1 przypadku wymagane jest podjęcie działań korygujących. Działania te należy podnieść
w odniesieniu do następujących aktywów:

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Dział | Aktyw | Decyzja |
| 1. | Dział IT | Dane uczniów / taśmy kopii  | zabezpieczenia |
| 2. |  |  |  |
| 3. |  |  |  |
| 4. |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |
| 7 |  |  |  |
| 8 |  |  |  |
| 9 |  |  |  |
| 10 |  |  |  |

Na podstawie tego dokumentu zostanie opracowany „Plan postępowania
z ryzykiem”.

....……………………………………………….

/data i podpis Inspektora ds. ochrony danych osobowych

....………………………………

/data i podpis Dyrektora/

**REGULAMIN POMIARU SKUTECZNOŚCI**

**ZABEZPIECZEŃ I SYSTEMU ZARZĄDZANIA**

**BEZPIECZEŃSTWEM INFORMACJI**

**§ 1.**

**Organizacja procesu pomiaru skuteczności zabezpieczeń i systemu zarządzania bezpieczeństwem informacji**

1. Nadzór nad procesem pomiaru skuteczności zabezpieczeń oraz SZBI sprawuje Dyrektor/Administrator Danych Osobowych lub pracownik wyznaczonyds. SZBI przez Dyrektora.
2. Pracownik ds. SZBI wyznaczony przez Dyrektora w uzgodnieniu
z Dyrektorem/ADO podejmuje decyzje dotyczące poziomów wskaźników bezpieczeństwa informacji.
3. Do szczegółowych zadań pracownika ds. SZBI wyznaczonego do pomiaru skuteczności zabezpieczeń przez Dyrektora należy:
4. inicjowanie opracowywania metodyki pomiarów skuteczności zabezpieczeń
i SZBI,
5. zatwierdzanie metodyk i programów skuteczności,
6. monitorowanie osiągania celów programów pomiarów skuteczności,
7. zatwierdzanie zmian doskonalących system pomiarów skuteczności.
8. Pracownikds. SZBI wyznaczony do pomiaru skuteczności przez Dyrektora realizuje i koordynuje działania w systemie pomiaru skuteczności.
9. Do szczegółowych zadań wyznaczonego pracownika ds. SZBI należy:
10. opracowywanie metodyki pomiarów skuteczności oraz rekomendacji przedstawianych Dyrektorowi/ADO dotyczących zmian w metodyce,
11. rekomendowanie Dyrektorowi/ADO nowych lub modyfikacji istniejących wskaźników bezpieczeństwa informacji,
12. rozwój metodyki i narzędzi wspierających system pomiarów skuteczności,
13. opracowywanie programów pomiarów skuteczności,
14. koordynowanie działań związanych z pomiarami skuteczności, wymagających uczestnictwa komórek organizacyjnych lub podmiotów zewnętrznych,
15. przygotowywanie okresowych raportów dotyczących wyników pomiarów skuteczności oraz stopnia realizacji wskaźników bezpieczeństwa informacji,
16. szkolenie właścicieli aktywów w zakresie zbierania informacji dla systemu pomiarów skuteczności,
17. formułowanie rekomendacji dotyczących doskonalenia systemu pomiarów skuteczności.
18. Właściciele Aktywów udzielają niezbędnych informacji pracownikowi wyznaczonemu przez ADO w zakresie zbierania danych do realizacji pomiarów skuteczności.

**§ 2.**

**Zakres pomiarów skuteczności**

1. Programy pomiarów skuteczności obejmują wybrane zabezpieczenia, które zostały wskazane jako środki ograniczania ryzyka w planie postępowania z ryzykiem.
2. W miarę potrzeby, programy pomiarów skuteczności mogą obejmować większy zbiór zabezpieczeń, wskazanych przez ADO jako szczególnie istotne z punktu widzenia bezpieczeństwa informacji.
3. Program pomiarów skuteczności SZBI obejmuje ocenę:
4. skuteczności wdrożonych mechanizmów zarządzania,
5. realizacji działań w systemie zarządzania, w tym realizacji procedur systemu zarządzania.
6. Programy szacowania ryzyka mogą różnić się zasięgiem terytorialnym, oraz poziomem szczegółowości analizowanych zabezpieczeń i obejmują:
7. procesy zdefiniowane,
8. systemy teleinformatyczne i aplikacje użytkowe.
9. Spis zabezpieczeń oraz elementy SZBI, dla których są realizowane pomiary skuteczności zostały zawarte w załączniku nr 1 do niniejszego regulaminu.

**§ 3.**

**Funkcjonowanie systemu pomiarów skuteczności**

1. Pracownik wyznaczony przez ADO ds. SZBI stosuje zasady i szablony pomiarów skuteczności oraz określania wskaźników bezpieczeństwa informacji zatwierdzone przez Właściciela.
2. Właściciele Aktywów są odpowiedzialni za zbieranie danych służących do pomiaru skuteczności.
3. Pracownik wyznaczony przez ADO ds. SZBI wykonuje okresowe, nie rzadziej niż raz na rok, analizy pomiarów skuteczności na podstawie uzyskanych danych.
4. Pracownik wyznaczony przez ADO ds. SZBI prezentuje zbiorczą informację
o wynikach pomiarów skuteczności, zawierający zdefiniowane wskaźniki bezpieczeństwa informacji na posiedzeniach kierownictwa.
5. Pracownik wyznaczony przez ADO ds. SZBI przygotowuje raport
o funkcjonowaniu systemu pomiarów skuteczności na potrzeby przeglądu SZBI

**§ 4.**

**Pomiary skuteczności zabezpieczeń i SZBI**

* 1. Właściciele Aktywów gromadzą dane zgodnie z określonymi w załączniku nr 1 zasadami i przekazują pracownikowi wyznaczonemu przez ADO ds. SZBI, który wykonuje pomiar skuteczności.
	2. Pracownik wyznaczony przez ADO ds. SZBI wykonuje analizę wyników pomiaru i określa wskaźnik bezpieczeństwa, wykorzystując wyniki pomiarów z poprzednich okresów pomiarowych, postępując zgodnie z procedurą nadzoru nad zapisami.
	3. Pracownik wyznaczony przez ADO ds. SZBI po zgromadzeniu danych do wykonania pomiaru skuteczności SZBI dokonuje pomiaru, po którym wykonuje analizę wyników pomiaru i określa wskaźnik skuteczności systemu, wykorzystując wyniki pomiarów z poprzednich okresów pomiarowych.
	4. Po podsumowaniu wyników pomiarów skuteczności pracownik wyznaczony przez ADO ds. SZBI przedstawia kierownictwu raport z pomiarów skuteczności.
	5. W raporcie, o którym mowa w ust. 4, Pełnomocnik ds. SZBI przedstawia wnioski i rekomendacje w zakresie:
1. decyzji zarządczych zgodnie z kryteriami zdefiniowanymi dla odpowiednich mierników skuteczności,
2. zmian w zabezpieczeniach oraz systemie zarządzania bezpieczeństwem informacji wynikających z wyników pomiarów – np. zmiany sposobów wdrożenia i alokacji zasobów,
3. zmiany w systemie pomiarów skuteczności – np. rozszerzenie listy mierników, zmiany kryteriów decyzji.

**Załącznik nr 1 do Regulaminu**

**Lista zabezpieczeń oraz elementów systemu zarządzania bezpieczeństwem informacji objęta programem pomiarów skuteczności**

|  |  |  |  |
| --- | --- | --- | --- |
| **Pkt** | **Zabezpieczenie** | **Miernik/wskaźnik** | **Częstotliwość pomiaru** |
| A.5.1.1 | Dokument polityki bezpieczeństwa informacji | Ilość pracowników przeszkolonych z PBI/Ilość zatrudnionych | 1/rok |
| A.5.1.2 | Przegląd polityki bezpieczeństwa informacji |
| A.6.1.1 | Zaangażowanie kierownictwa w bezpieczeństwo informacji | Ilość stanowisk z określonym zakresem czynności, odpowiedzialności/ilości wszystkich stanowisk  | 1/rok |
| A.6.1.2 | Koordynacja bezpieczeństwa informacji |
| A.6.1.3 | Przypisanie odpowiedzialności w zakresie bezpieczeństwa informacji |
| A.6.1.4 | Proces autoryzacji środków przetwarzania informacji |
| A.6.1.5 | Umowy o zachowaniu poufności | Ilość umów zawierających klauzule poufności/Ilości wszystkich umów | 1/rok |
| A.6.1.6 | Kontakty z organami władzy | Ilość zdarzeń wymagających kontaktów z organami władzy | 1/rok |
| A.6.1.7 | Kontakty z grupamizainteresowaniabezpieczeństwem |
| A.6.1.8 | Niezależny przegląd bezpieczeństwa informacji | Ilość niezgodności stwierdzonych podczas auditów zewnętrznych | 1/rok |
| A.6.2.1 | Określenie ryzyk związanych ze stronami zewnętrznymi | 1. Ilość umów bez deklaracji poufności/ilości umów ogółem2. Ilość incydentów związanych ze stronami trzecimi | 1/rok |
| A.6.2.2 | Bezpieczeństwo w kontaktach z klientami |
| A.6.2.3 | Bezpieczeństwo w umowach ze stroną trzecią |
| A.7.1.1 | Inwentaryzacja aktywów | Częstotliwość zmian w analizie ryzyka | 1/rok |
| A.7.1.2 | Własność aktywów |
| A.7.1.3 | Akceptowalne użycie aktywów |
| A.7.2.1 | Zalecenia do klasyfikacji |
| A.7.2.2 | Oznaczanie i postępowanie z informacjami |
| A.8.1.1 | Role i odpowiedzialności | Ilość pracowników z wymaganymi kwalifikacjami/Ilości wszystkich pracowników.  | 1/rok |
| A.8.1.2 | Postępowanie sprawdzające |
| A.8.1.3 | Zasady i warunki zatrudnienia |
| A.8.2.1 | Odpowiedzialność kierownictwa | Liczba pracowników przeszkolonych z zakresu SZBI/Ilości pracowników ogółem w stosunku do których zaplanowano szkolenie | 1/rok |
| A.8.2.2 | Uświadomienie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji |
| A.8.2.3 | Postępowanie dyscyplinarne | Ilość pracowników zwolnionych ze względu na nie przestrzeganie PBI | 1/rok |
| A.8.3.1 | Odpowiedzialności związane z zakończeniem zatrudnienia | Ilość utraconych aktywówIlość niezgodności związanych z nieodebraniem praw dostępu  | 1/rok |
| A.8.3.2 | Zwrot aktywów |
| A.8.3.3 | Odebranie praw dostępu |
| A.9.1.1 | Fizyczna granica obszaru bezpiecznego | 1. Ilość nieautoryzowanych wejść do obiektu/incydentów2. Ilość zdarzeń związanych z brakiem dostępu lub nieupoważnionym dostępem do dokumentów z powodu niedostatecznego zabezpieczenia kluczy do szaf | 1/rok |
| A.9.1.2 | Fizyczne zabezpieczenie wejścia |
| A.9.1.3 | Zabezpieczenie biur, pomieszczeń i urządzeń |
| A.9.1.4 | Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi |
| A.9.1.5 | Praca w obszarach bezpiecznych |
| A.9.1.6 | Obszary publicznie dostępne, dostaw i załadunku |
| A.9.2.1 | Lokalizacja i ochrona sprzętu | 1. Ilość uszkodzeń sprzętu/utraty danych spowodowanych zakłóceniami zasilania  | 1/rok |
| A.9.2.2 | Systemy wspomagające |
| A.9.2.3 | Bezpieczeństwo okablowania |
| A.9.2.4 | Konserwacja sprzętu |
| A.9.2.5 | Bezpieczeństwo sprzętu poza siedzibą |
| A.9.2.6 | Bezpieczne zbywanie lub przekazywanie do ponownego użycia |
| A.9.2.7 | Wynoszenie mienia |
| A.10.3.1 | Zarządzanie pojemnością systemów | Ilość incydentów związanych z brakiem możliwości zapisania danych w związku z niedostateczna ilością miejsca na dysku/serwerze | 1/rok |
| A.10.9.1 | Handel elektroniczny | Wyłączenie | N/D |
| A.10.9.2 | Transakcje on-line |
| A.11.3.1 | Używanie haseł | Ilość niezgodności podczas auditów  | 1/rok |
| A.11.3.2 | Pozostawienie sprzętu użytkownika bez opieki |
| A.11.3.3 | Polityka czystego biurka i czystego ekranu |
| A.11.7.1 | Przetwarzanie i komunikacja mobilna | 1. Ilość incydentów związanych z utraceniem danych | 1/rok |
| A.11.7.2 | Praca na odległość |
| A.13.1.1 | Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji | Ilość incydentów rozwiązanych/Ilość zgłoszonych incydentów | 1 / rok |
| A.13.1.2 | Zgłaszanie słabości systemu bezpieczeństwa |
| A.13.2.1 | Odpowiedzialność i procedury | Czas rozwiązania incydentów w odniesieniu do założonego czasu  | 1 / rok |
| A.13.2.2 | Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji |
| A.13.2.3 | Gromadzenie materiału dowodowego |
| A.14.1.1 | Włączanie bezpieczeństwa informacji do procesu zarządzania ciągłością działania | Wyniki testowania PCD/skuteczność PCD – zgodność działań z określonym planem | 1/rok |
| A.14.1.2 | Ciągłość działania i szacowanie ryzyka |
| A.14.1.3 | Opracowanie i wdrożenie planów ciągłości uwzględniających bezpieczeństwo informacji |
| A.14.1.4 | Struktura planowania ciągłości działania |
| A.14.1.5 | Testowanie, utrzymanie i ponowna ocena planów ciągłości działania |
| A.15.1.1 | Określenie odpowiednich przepisów prawnych | Zgodność z przepisami  | 1/rok |
| A.15.1.3 | Ochrona zapisów organizacji | Ilość zniszczonych dokumentów i zapisów przed upływem okresu archiwizacji | 1/rok |

# Procedura Metodyka Szacowania Ryzyka

# CEL

Celem instrukcji jest określenie zasad szacowania ryzyka dla bezpieczeństwa informacji.

## PRZEDMIOT INSTRUKCJI

Przedmiotem instrukcji jest określenie trybu postępowania pracowników w zakresie:

* Ogólne zasady szacowania ryzyka,
* Identyfikacji aktywów, procesów i określenie celów dla procesów;
* Szacowania ryzyka,
* Oceny wyników szacowania ryzyka i planowanie reakcji,
* Kategorii zagrożeń,
* Skala do oceny prawdopodobieństwa í skutku.

# ZAKRES OBOWIĄZYWANIA

Instrukcja obowiązuje we wszystkich jednostkach i komórkach organizacyjnych.

Instrukcja odnosi się do szacowania ryzyka w odniesieniu do bezpieczeństwa informacji.

# ODPOWIEDZIALNOŚĆ

Wyznaczony pracownik ds. SZBI

* nadzór nad wdrożeniem i realizacją postanowień niniejszej instrukcji,
* planowanie przeprowadzenia analizy ryzyka,
* koordynacja działań podległych pracowników,
* wnioskowanie o zasoby niezbędne do realizacji postanowień instrukcji,
* nadzór nad realizacją niniejszej instrukcji w aspekcie działania SZBI.

Pracownicy - odpowiadają za realizację postanowień instrukcji, zgodnie z zakresem przydzielonych im obowiązków służbowych.

# OZNACZENIA

Oznaczenia zgodnie z dokumentacją SZBI.

# DEFINICJE

# Szacowanie ryzyka dla bezpieczeństwa informacji

## Ogólne zasady szacowania ryzyka

## Stosowane podejście do szacowania ryzyka wywodzi się z normy ISO 31000.

## Polega ono na analitycznym ustalaniu związków przyczynowo skutkowych materializacji potencjalnych zagrożeń dla bezpieczeństwa informacji oraz analizie ilościowej poszczególnych czynników ryzyka: prawdopodobieństwa wystąpienia danego zagrożenia, oraz skutków biznesowych wystąpienia zagrożenia dla celów organizacji z uwzględnieniem jej kontekstu.

## Wyznaczony pracownik ds. SZBI Planuje termin i harmonogram przeprowadzenia oszacowania ryzyka.

## Identyﬁkacja aktywów informacyjnych, procesów i celów dla procesów.

* + 1. Pierwszym zadaniem realizowanym podczas procesu szacowania ryzyka jest wskazanie najważniejszych aktywów informacyjnych oraz zidentyfikowanie procesów mających wpływ na Bezpieczeństwo informacji i celów
		w poszczególnych procesach.
		2. Należy podać nazwę Aktywa, Procesu i Celu, które w sposób czytelny określać będą: Cel i do którego procesu jest on przypisany lub aktywo.

## Szacowanie ryzyka dla aktywów informacyjnych, procesów i celów dla procesów.

* + 1. Osoba prowadząca oszacowanie ryzyka identyfikuje Zagrożenia; Szanse związane z bezpieczeństwem informacji w odniesieniu do aktywów informacyjnych, celów organizacji, procesów, kontekstu i wymagań stron zainteresowanych.
		2. Należy wskazać zagrożenia, które mogą wpłynąć na zidentyfikowane cele lub aktywa np.:

Utrata danych osobowych w formie elektronicznej

Naruszenie przepisów prawa (ADO)

Przerwy w funkcjonowaniu

Awarie

Błędy ludzkie

* + 1. Następnie zagrożenia dla bezpieczeństwa informacji przyporządkowywane są do jednej z kategorii opisanych W punkcie 7.5 niniejszej instrukcji.
		2. Następnie należy wypisać jakie mogą być potencjalne Przyczyny wystąpienia zagrożenia - podatności / słabości / luki.
		3. Kolejny krok to określenie prawdopodobieństwa materializacji danego zagrożenia, co czynione jest w trzy stopniowej skali opisanej w punkcie 7.6 niniejszej instrukcji.

## Ocena wyników szacowania ryzyka i planowanie reakcji

* + 1. Osoba prowadząca oszacowanie ryzyka w danej lokalizacji przekazuje wyniki swojej pracy wyznaczonemu pracownikowi ds. ZSBI.
		2. Wyznaczony pracownik ds. ZSBI dokonuje przeglądu oszacowania ryzyka i wyjaśnia ewentualne wątpliwości i rozbieżności z osobami przygotowującymi oszacowania.
		3. Wyznaczony pracownik ds. ZSBI dokonuje analizy wyników oszacowania i przygotowuje raport z szacowania ryzyka.
		4. Wyznaczony pracownik ds. ZSBI przedstawia raport Dyrektorowi, a podjęte przez Dyrektora decyzje wpisuje do planu postępowania z ryzykiem.
		5. Możliwe są następujące kategorie reakcji na ryzyko:

Eliminacja - mająca na celu eliminację przyczyn i całkowite zlikwidowanie ryzyka,

* Redukcja - czyli działania mające ograniczyć możliwość wystąpienia lub skutki zapisanego ryzyka; formą redukcji jest też rozpoczęcie monitorowania danego ryzyka, aby być gotowym do podjęcia działań w przypadku, kiedy ryzyko zacznie się materializować,
* Przeniesienie - poprzez ubezpieczenie ryzyka,
* Akceptacja - ryzyko jest akceptowane i nie są planowane wobec niego żadne dalsze działania
* Podjęcie ryzyka w celu zwiększenia/wykorzystania szansy
* Zmiana prawdopodobieństwa
	+ 1. Realizacja planu postepowania z ryzykiem omawiana jest na przeglądach Zintegrowanego Systemu Zarządzania.

## Kategorie zagrożeń

## Zagrożenia dla bezpieczeństwa informacji to wszelkie zdarzenia, które jeżeli się wydarzą będą miały wpływ na informacje przetwarzane (związane) z analizowanymi aktywami informacyjnymi. Z uwagi na fakt, że oszacowanie prowadzone było po raz pierwszy, określonych zostało 6 typów zagrożeń:

* brak dostępu do informacji i utrata poufności;
* brak dostępu do informacji;
* czasowy brak dostępu do informacji;
* utrata spójności / kompletności informacji;
* utrata poufności informacji;
* niespełnienie wymagań prawa.

## Skale do oceny prawdopodobieństwa i skutku

* + 1. Prawdopodobieństwo wystąpienia zdarzenia oceniane jest w skali 1-3, natomiast skutki jego materializacji oceniane są w punktowej skali od 1 do 4
		2. Skala do oceny prawdopodobieństwa:
		3. Skala do oceny skutków:

|  |  |
| --- | --- |
| **OPIS** | **W skrócie:** |
| **SKUTKI** |
| 1. Mało ważne (utrata danych nie spowoduje utrudnień w pracy firmy) | 1. Pomijalne. |
| 2. Średnio ważne (utrata aktywa spowoduje zakłócenia w pracy i konieczność odtwarzania danych, ale są one odtwarzalne, zakłócenia potrwają najwyżej 1 dzień roboczy) | 2. Będzie mały problem |
| 3. Ważne (utrata zasobu spowoduje zakłócenia w pracy i konieczność odtwarzania danych, z trudem będą odtwarzalne, zakłócenia potrwają przynajmniej parę dni roboczych. Może też spowodować konsekwencje prawne lub straty materialne) | 3. Będzie poważny problem. |
| **4.** Bardzo ważne (utrata danych to katastrofa - nie można ich odtworzyć lub odtworzenie będzie zbyt kosztowne w stosunku do ich wartości. Konsekwencje prawne i materialne) | 4. Katastrofa. |
| **PRAWDOPODOBIĘSTWO** |
| 1. Zdarza się statystycznie - wiemy o tym, bo nam się już zdarzało albo słyszeliśmy, że się może zdarzyć, ale szansa jest odległa. | 1. Może się zdarzyć. |
| 2. Zdarza się statystycznie - wiemy o tym, bo nam się już zdarzało, zdarza się co jakiś czas. | 2. Prędzej czy później się zdarzy. |
| 3. Jeżeli nic z tym nie zrobimy, to prędzej czy później się zdarzy. | 3. Coś się na pewno zdarzy. |
| **PODATNOŚĆ** |
| 1. Niska szansa na incydent związany w bezpieczeństwem, bo są zastosowane pełne zabezpieczenia. | 1. Trudno o incydent. |
| 2. Zabezpieczenia są, ale niekompletne, a więc i tak w pewnych sytuacjach zagrożenie może je wykorzystać. | 2. Może się zdarzyć incydent. |
| 3. Zabezpieczenia są za słabe i łatwo może się zdarzyć incydent. | 3. Bardzo łatwo o incydent. |
| 4. Bardzo łatwo może się zdarzyć incydent (bo brak zabezpieczeń). | 4. Incydent pewny |

|  |
| --- |
| **Klasyfikacja informacji** |
| ***Typ*** | ***Opis*** | ***Przykład*** |
| Ogólnodostępna | Podlegają publikacji. Informacje mało wrażliwe, których ujawnienie / utrata nie spowoduje przerwy w działalności **placówki** i roszczeń stron trzecich. | Ogólnodostępne publikacje nie objęte ochroną danych osobowych, informacje na stronie www. |
| Wrażliwe | Trzeba je chronić bo ich utrata spowoduje szkody i przerwanie chwilowe działania **Placówki** | Wszelkiego rodzaju dane finansowe decyzje, itd. |
| Poufne | Informacje, których ujawnienie/utrata spowoduje sankcje karne albo bardzo dużą szkodę dla **Placówki** | Wszelkiego rodzaju dane osobowe, dane uczniów/dzieci/rodziców/opiekunów prawnych itd.. |

**Procedura Zarządzania Zmianami**

Wszelkie zmiany systemów informatycznych muszą być poprzedzone następującymi działaniami:

1. Zdefiniowanie wymagań funkcjonalnych dla nowych lub modyfikowanych systemów oraz utrzymywanie kontroli wersji oprogramowania.
2. Oszacowaniem ryzyka oraz analizą wpływu zmian na istniejącezabezpieczenia.
3. Analiza modyfikacji, zatwierdzenie lub odrzucenie.
4. Podpisanie umowy z firmą zewnętrzną na wykonanie zmiany lub realizacja projektu we własnym zakresie.
5. Ustalenie kanałów komunikacji i osób odpowiedzialnych za proces.
6. Wprowadzenie zmian na środowisko testowe.
7. Testowanie i ewentualne poprawki, w przypadku nowego systemu zaakceptowanie testów sytemu oraz podpisanie protokołu odbioru.
W odniesieniu do systemów niekrytycznych zaleca się stosowanie automatycznych uaktualnień (wgrywanie łat, uaktualnienia serwisowe).
8. Stworzenia kopii zapasowej przed wgraniem zmian na system produkcyjny.
9. Wprowadzenie zmian lub wdrożenie na system produkcyjny.

....……………………………………………….

/data i podpis Inspektora ds. ochrony danych osobowych/

....………………………………

/data i podpis Dyrektora/