EDU ODO – Kacper Gordeew
Ul. Zamiejska 14,44-270 Rybnik
NIP: 6423203506, biuro@eduodo.pl

Podsumowanie realizacji audytu

Nazwa jednostki audytowanej: *Centrum Kształcenia Zawodowego i Ustawicznego nr 1 w Gliwicach, ul. Kozielska 1, 44-100 Gliwice.*
Data przeprowadzenia audytu: *14 marca 2023 r.*
Audytorzy: *Aleksandra Cnota-Mikołajec – Inspektor Ochrony Danych*

Wstęp

Niniejszy audyt bezpieczeństwa informacji przeprowadzony został w celu regularnej weryfikacji, czy ochrona danych osobowych w jednostce spełnia wymogi określone w przepisach o ochronie danych osobowych.

Cel zadania audytowego

Celem badania audytowego było ustalenie czy w jednostce dane osobowe są prawidłowo przetwarzane i chronione. Głównym przedmiotem badania było ustalenie, czy wdrożone i opracowane dokumenty i procedury związane z ochroną danych osobowych są aktualne i stosowane w praktyce przez osoby upoważnione oraz ocena, czy stosowane rozwiązania zapewniają przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa, ze szczególnym uwzględnieniem ochrony praw i wolności osób, których dane osobowe są przetwarzane.
Niniejszy raport skupia się na ochronie danych osobowych od strony formalno-prawnej oraz na ocenie rozwiązań technicznych i organizacyjnych stosowanych do ochrony danych przetwarzanych w formie papierowej i elektronicznej.

Podstawa prawna audytu

Za podstawę przeprowadzenia audytu uznaje się Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz Ustawę o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz. U. 2019 poz. 1781)

Zastosowana metodologia

Audyt został przeprowadzony z wykorzystaniem następujących metod:

- *Zebranie informacji z przygotowanej ankiety audytowej,*
- *Wywiad z pracownikami oraz administratorem danych osobowych,*
- *Analiza udostępnionej dokumentacji,*
- *Audyt wizyjny siedziby podmiotu.*

Analiza polityk bezpieczeństwa oraz procedur dotyczących bezpieczeństwa przetwarzania danych osobowych

Obszar audytowany: *Sprawdzenie, czy wprowadzona dokumentacja jest aktualna względem stanu faktycznego.*
Stan faktyczny: *W jednostce wprowadzono wszystkie niezbędne dokumenty i procedury związane z przetwarzaniem danych osobowych. W jednostce przeprowadza się też okresowo wymagane oceny skutków i analizy ryzyka przy przetwarzaniu danych osobowych. Do tej pory sporządzono je dla następujących obszarów przetwarzania: monitoringu wizyjnego, systemu informacji oświatowej. Wszystkie dokumenty prowadzone są poprawnie, w sposób zgodny z przepisami. Są one również aktualne względem stanu faktycznego. W przypadku konieczności naniesienia zmian na dokumentacje została wyznaczona osoba odpowiedzialna za ich aktualizację. Osobą tą jest Inspektor Ochrony Danych.*
Rekomendacja: *Zaleca się podtrzymanie zasad stosowanych do tej pory.*

Analiza stanu upoważnień do przetwarzania danych osobowych

Obszar audytowany: *Sprawdzenie stanu upoważnień do przetwarzania danych osobowych*
Stan faktyczny: *Do przetwarzania danych osobowych zgodnie z ustawą mogą być dopuszczone wyłącznie osoby posiadające upoważnienie wydane przez Administratora Danych. W trakcie działań audytorskich stwierdzono, iż wszystkie osoby mające dostęp do danych osobowych na terenie podmiotu posiadają stosowne upoważnienia. Zatrudnienie nowych pracowników zgłaszane jest Inspektorowi Ochrony Danych, który przygotowuje w dniu zatrudnienia upoważnienie. Te z kolei przekazywane jest Administratorowi, który w momencie podpisywania umowy z pracownikiem upoważnia go do przetwarzania danych osobowych.*
Rekomendacja: *Zaleca się podtrzymanie aktualnie panujących zasad i zgłaszanie konieczności przygotowania dokumentów niezbędnych przy zatrudnieniu Inspektorowi Ochrony Danych.*

Analiza regulacji związanych z monitoringiem wizyjnym

Obszar audytowany: *Weryfikacja zgodności wprowadzonego monitoringu wizyjnego względem wymogów prawnych oraz sprawdzenie wprowadzonych dokumentów.*
Stan faktyczny: *Jednostka została zabezpieczona systemem kamer, który umożliwia rejestrację obrazu. Monitoring nie umożliwia rejestracji fonii. System monitoringu obejmuje teren zewnętrzny wokół budynków wraz z bramami wjazdowymi oraz teren wewnątrz budynku głównego – wejście główne i korytarze na parterze i piętrach. Do nagrań dostęp posiadają wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania danych w systemie monitoringu wizyjnego. W jednostce wprowadzono regulamin monitoringu wizyjnego, który na dzień przeprowadzania działań audytorskich jest aktualny względem przepisów oraz stanu faktycznego. Administrator podpisał również odpowiednie oświadczenie o wprowadzeniu monitoringu, a wszyscy zatrudnieni pracownicy podpisali oświadczenia, z których treści wynika, iż zostali oni poinformowani o tym fakcie. Obowiązek informacyjny, którego spełnienie jest istotne w przypadku stosowania monitoringu wizyjnego spełniany jest w zrozumiałej formie i zgodnie z literą prawa poprzez zamieszczenie klauzuli informacyjnej m.in. na stronie internetowej oraz na wejściach do jednostki. Każda osoba wchodząca na teren jednostki jest informowana o stosowaniu monitoringu wizyjnego przez tabliczki z napisem „obiekt monitorowany". Tabliczki są umieszczone w taki sposób, aby osoby wchodzące na teren zostały poinformowane zanim ich wizerunek zostanie przetworzony w systemie.*

Rekomendacja: *Zaleca się podtrzymanie aktualnego stanu oraz informowanie IOD o zachodzących zmianach w systemie monitoringu wizyjnego.*

Analiza zapewnienia aktualności systemów operacyjnych

Obszar audytowany: *Sprawdzenie aktualności systemów operacyjnych stosowanych na stacjach roboczych w jednostce*
Stan faktyczny: *W toku działań audytorskich ustalono, że jednostka posiada wyłącznie system Windows. Aktualizowany jest on każdorazowo, gdy dostępna jest aktualizacja. Jednostka posiada wyłącznie systemy, dla których oferowane jest wsparcie producenta – Windows 10 i Windows 11.*
Rekomendacja: *Zaleca się utrzymywanie aktualnie panujących zasad.*

Analiza zapisów związanych z bezpieczeństwem informacji na stronie internetowej

Obszar audytowany: *Sprawdzenie spełnienia obowiązku informacyjnego na stronie internetowej jednostki oraz sprawdzenie wprowadzenia zapisów związanych z przetwarzaniem plików Cookies.*
Stan faktyczny: *Jednostka posiada własną stronę internetową znajdującą się pod adresem: http://www.ckziu.gliwice.pl/. W związku z tym, jednostka winna spełniać następujące wymogi:*

- *Zamieszczenie obowiązku informacyjnego: spełnia – klauzula zamieszczona jest w zakładce „RODO",*
- *Zabezpieczenie strony certyfikatem SSL: nie spełnia – strona nie jest zabezpieczona certyfikatem,*
- *Umieszczenie na stronie danych kontaktowych Inspektora Ochrony Danych: spełnia – dane zamieszczone są w zakładce na górze strony,*
- *Wyświetlanie paska lub okienka informującego użytkownika strony o przetwarzaniu plików Cookies: spełnia częściowo – w pasku zamieszczono hiperłącze przenoszące użytkownika do niewłaściwej zakładki,*
- *Utworzenie Polityki Prywatności dla strony: spełnia – Polityka zamieszczona jest na stronie szkoły.*

Jednostka posiada także stronę BIP pod adresem: https://ckziu1.bip.gliwice.eu/. Na stronie znajduje się aktualna klauzula informacyjna.

Rekomendacja: *Konieczne jest zabezpieczenie strony certyfikatem. Zaleca się zastosowanie hiperłącza przenoszącego użytkownika do zakładki „Polityka prywatności" w pasku informującym o przetwarzaniu plików Cookies.*
Na stronie głównej BIP zaleca się umieścić dane Inspektora Ochrony Danych: Aleksandra Cnota-Mikołajec, aleksandra@eduodo.pl.

Analiza naruszeń przepisów o ochronie danych osobowych

Obszar audytowany: *Sprawdzenie, czy w audytowanej jednostce odnotowano naruszenia przepisów o ochronie danych osobowych*
Stan faktyczny: *W trakcie działań audytorskich przeprowadzono wywiad z pracownikami oraz administratorem danych osobowych. Zgodnie z ich ustnymi oświadczeniami w jednostce nie doszło do*

żadnego naruszenia przepisów o ochronie danych osobowych, który wymagałby przeprowadzenia postępowania wyjaśniającego i sporządzenia protokołu wewnętrznego z naruszenia.
Rekomendacja: *Zaleca się systematycznie przypominać pracownikom o konieczności zgłaszania do administratora danych lub inspektora ochrony danych każdego przypadku naruszenia przepisów o ochronie danych osobowych.*

Przeprowadzenie wizji lokalnej wraz z weryfikacją wprowadzenia zaleceń z poprzednich audytów bezpieczeństwa informacji

Obszar audytowany: *Sprawdzenie obszarów przetwarzania danych osobowych pod kątem przestrzegania przepisów, procedur i zasad związanych z bezpieczeństwem informacji*
Stan faktyczny: *Dostęp do budynku ograniczony jest poprzez stosowanie zamykanych drzwi i okien. Dostęp do pomieszczeń ograniczony jest poprzez stosowanie zamykanych drzwi. W trakcie działań audytorskich nie stwierdzono otwartych pomieszczeń pozostawionych bez opieki pracownika. Zasady czystego biurka oraz czystego ekranu są stosowane przez pracowników wzorowo. Monitory wszystkich komputerów są ustawione tak, aby osoby postronne nie miały w nie wglądu. Dodatkowo wszystkie komputery zabezpieczone są hasłem systemowym, wygaszaczem ekranu i automatyczną blokadą dostępu w przypadku dłuższej nieobecności pracownika.*
Rekomendacja: *Brak zaleceń w tym zakresie.*

Aleksandra Cnota-Mikołajec
Inspektor Ochrony Danych

.....

(pieczęć i podpis audytora)

Ocena skutków oraz analiza zagrożeń przy przetwarzaniu danych w ramach systemu obiegu dokumentacji

Nazwa podmiotu wprowadzającego	Centrum Kształcenia Zawodowego i Ustawicznego nr 1 w Gliwicach
Data wprowadzenia	15 marca 2023 r
Podpis ADO	

§1

Ilekroć w dokumencie jest mowa o:

1. **ANALIZIE RYZYKA** – rozumie się przez to systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka;
2. **SZACOWANIU RYZYKA** – rozumie się przez to proces oceny i analizy ryzyka;
3. **OCENIE RYZYKA** – rozumie się przez to proces porównania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka;
4. **POSTĘPOWANIU Z RYZYKIEM** – rozumie się przez to wdrażanie środków modyfikujących ryzyko;
5. **ZARZĄDZANIU RYZYKIEM** – rozumie się przez to działania dotyczące kierowania i nadzorowania organizacją w odniesieniu do ryzyka;
6. **RYZYKU SZCZĄTKOWYM** – rozumie się przez to ryzyko pozostające po procesie postępowania z ryzykiem;
7. **AKCEPTOWANIU RYZYKA** – rozumie się przez to decyzja, aby zaakceptować ryzyko;
8. **BEZPIECZEŃSTWIE INFORMACJI** – rozumie się przez to zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
9. **ZDARZENIU ZWIĄZANYM Z BEZPIECZEŃSTWEM INFORMACJI** – rozumie się przez to zdarzenie związane z bezpieczeństwem informacji, jako określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe naruszenie Polityki Bezpieczeństwa Informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem;
10. **INCYDENCIE ZWIĄZANYM Z BEZPIECZEŃSTWEM INFORMACJI** – rozumie się przez to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne zakłócenia zadań biznesowych i zagrażają bezpieczeństwu informacji;
11. **AKTYWACH** – rozumie się przez to wszystko, co ma wartość dla organizacji;

12. **ZAGROŻENIACH SYSTEMU** – rozumie się przez to wszystkie niekorzystne czynniki mogące przyczynić się w trakcie pracy z danymi osobowymi do wystąpienia incydentu, mogącego mieć wpływ na ich ujawnienie bądź utratę;
13. **DOSTĘPNOŚCI** —należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym;
14. **INCYDENCIE BEZPIECZEŃSTWA TELEINFORMATYCZNEGO** —należy przez to rozumieć takie pojedyncze zdarzenie lub serię zdarzeń, związanych z bezpieczeństwem informacji niejawnych, które zagrażają ich poufności, dostępności lub integralności;
15. **INFORMATYCZNYM NOŚNIKU DANYCH** —należy przez to rozumieć materiał służący do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej;
16. **INTEGRALNOŚCI** —należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony;
17. **OPROGRAMOWANIU ZŁOŚLIWYM** —należy przez to rozumieć oprogramowanie, którego celem jest przeprowadzenie nieuprawnionych lub szkodliwych działań w systemie teleinformatycznym;
18. **PODATNOŚCI** — należy przez to rozumieć słabość zasobu lub zabezpieczenia systemu teleinformatycznego, która może zostać wykorzystana przez zagrożenie;
19. **POŁĄCZENIU MIĘDZYSYSTEMOWYM** —należy przez to rozumieć techniczne albo organizacyjne połączenie dwóch lub więcej systemów teleinformatycznych, umożliwiające ich współpracę, a w szczególności wymianę danych;
20. **POUFNOŚCI** —należy przez to rozumieć właściwość określającą, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym;
21. **PRZEKAZYWANIU INFORMACJI** —należy przez to rozumieć zarówno transmisję informacji, jak i przekazywanie informacji na informatycznych nośnikach danych, na których zostały utrwalone;
22. **TESTACH BEZPIECZEŃSTWA** —należy przez to rozumieć testy poprawności i skuteczności funkcjonowania zabezpieczeń w systemie teleinformatycznym;
23. **ZABEZPIECZENIU** —należy przez to rozumieć środki o charakterze fizycznym, technicznym lub organizacyjnym zmniejszające ryzyko;
24. **ZAGROŻENIU** —należy przez to rozumieć potencjalną przyczynę niepożądanego zdarzenia, które może wywołać szkodę w zasobach systemu teleinformatycznego;
25. **ZASOBACH SYSTEMU TELEINFORMATYCZNEGO** –należy przez to rozumieć informacje przetwarzane w systemie teleinformatycznym, jak również osoby, usługi, oprogramowanie, dane i sprzęt oraz inne elementy mające wpływ na bezpieczeństwo tych informacji;

1. PODSTAWA PRAWNA:

§1

a) Ustawa o Ochronie Danych Osobowych z dnia 10 Maja 2018 (Dz. U. 2019, poz. 1781),
b) Rozporządzenie Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

2. OGÓLNE WYMOGI BEZPIECZEŃSTWA:

§1

W czasie przetwarzania danych osobowych w ramach systemu obiegu dokumentacji w Centrum Kształcenia Zawodowego i Ustawicznego nr 1 w Gliwicach informacje występują w postaci:

- plików lub informacji przechowywanych na dysku twardym komputera,
- plików lub informacji przechowywanych w pamięci operacyjnej komputera,
- plików lub informacji zapisanych na nośnikach komputerowych,
- plików lub informacji zapisanych na serwerze lokalnym,
- plików lub informacji zapisanych na serwerze zewnętrznym.

§2

Bezpieczeństwo przetwarzanych lub przechowywanych informacji zawierających dane osobowe wymaga:

- zapewnienia ochrony fizycznej i technicznej stanowiska komputerowego przed nieuprawnionym dostępem,
- zapewnienia ochrony fizycznej i technicznej serwera wewnętrznego przed nieuprawnionym dostępem,
- sporządzenia umowy gwarantującej odpowiedni poziom bezpieczeństwa danych osobowych przetwarzanych na serwerze z zewnętrznym dostawcą miejsca serwerowego,
- ochrony nośników technicznych dokumentów wytwarzanych przy pomocy sprzętu komputerowego, w tym określenia zasad postępowania z nimi przed nieuprawnionym dostępem,
- zabezpieczenia przed nieupoważnionym dostępem do danych osobowych znajdujących się w zasobach systemu informatycznego,
- zapewnienia dostępności do danych osobowych znajdujących się na technicznych nośnikach informacji oraz w pamięci systemu informatycznego dla upoważnionych użytkowników,
- zapewnienia możliwości kontroli dostępu do zasobów systemu informatycznego oraz wykonywanych na nim czynności,
- zapewnienia możliwości kontroli nośników na których przetwarzano lub przechowywano dane osobowe.

3. ZAGROŻENIA DLA SYSTEMU:

§1

Biorąc pod uwagę specyfikę prac wykonywanych przy pomocy systemu informatycznego, przeznaczonego do przygotowania dokumentów zawierających dane osobowe, podstawowe zagrożenia to: utrata poufności, integralności i rozliczalności dokumentów zawierających dane osobowe:

- poufność to zapewnienie że dane osobowe nie są udostępniane nieupoważnionym podmiotom,
- integralność to zapewnienie, aby wszystkie zmiany wykonywane w systemie informatycznym, w systemie jego katalogów oraz poszczególnych plikach zawierających dane osobowe były

skutkiem zaplanowanych działań użytkowników systemu. Właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

- rozliczalność to właściwość zapewniająca, że działania podmiotu przetwarzającego dane osobowe mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

§2

Zagrożenia w zakresie poufności obejmują:

- nieuprawniony dostęp do pomieszczenia, w którym przetwarzane są dane osobowe,
- ujawnienie haseł dostępu do stanowiska komputerowego lub serwera, na którym przetwarzane są dane osobowe,
- ujawnienie kodów dostępu do systemu obiegu dokumentacji,
- nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik,
- utrata nośnika zawierającego dane osobowe,
- klęska żywiołowa, w wyniku której utracono poufność danych osobowych,
- nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym.

§3

Zagrożenia w zakresie rozliczalności obejmują:

- brak kontroli nad dokumentami wykonywanymi na stanowisku komputerowym lub serwerowym w zakresie ich kopiowania, drukowania lub usuwania
- wyparcie się pracy na stanowisku komputerowym lub serwerowym, gdzie przetwarza się dane osobowe,
- wprowadzenie zmian w treści dokumentu, zawierającego dane osobowe,
- błędy oprogramowania lub sprzętu.

§4

Zagrożenia w zakresie integralności obejmują:

- nielegalny dostęp do danych osobowych, w tym do stanowiska komputerowego lub serwera,
- błędy i pomyłki użytkowników,
- błędy i awarie oprogramowania,
- brak mechanizmów uniemożliwiających skanowanie lub zmianę logów przez administratora danych lub administratora systemu informatycznego,
- wadliwe działanie systemu operacyjnego,
- wirus lub inne złośliwe oprogramowanie
- brak w wykorzystywanych aplikacjach mechanizmów zapewniających integralność danych.

§5

Źródłami zagrożeń dla stanowisk komputerowych oraz serwera, gdzie przetwarza się dane osobowe mogą być:

- siły natury – zdarzenia, które nie wynikają z działalności człowieka, tzn.:

- uderzenie pioruna,
- pożar będący konsekwencją ww. uderzenia pioruna,
- starzenie się sprzętu,
- starzenie się nośników pamięci,
- smog, kurz,
- katastrofy budowlane,
- ulewny deszcz,
- huragan,
- ekstremalne temperatury, wilgotność.

- ludzie – mogą to być pracownicy lub osoby z zewnątrz, którzy działają w sposób celowy lub przypadkowy; zagrożenia te to przede wszystkim:

- błędy lub pomyłki użytkowników lub administratorów,
- błędy utrzymania systemu w poufności, rozliczalności i integralności,
- zaniedbania użytkowników przy przesyłaniu, udostępnianiu i kopiowaniu,
- zagubienie nośnika zawierającego dane osobowe,
- niewłaściwe zniszczenie nośnika,
- nielegalne użycie oprogramowania,
- choroba ważnych osób i nieuprawnione zastępstwo,
- podpalenie obiektu,
- katastrofa budowlana będąca konsekwencją przypadkowego działania człowieka,
- zakłócenia elektromagnetyczne lub radiotechniczne,
- podłożenie i wybuch bomby lub ładunku wybuchowego,
- użycie broni,
- zmiany napięcia w sieci,
- utrata prądu,
- zbieranie się ładunków elektrostatycznych,
- utrata kluczowych pracowników,
- niedobór pracowników,
- szpiegostwo,
- terroryzm,
- defekty oprogramowania,
- destrukcja zbiorów i programów impulsem elektromagnetycznym,
- kradzież,
- włamanie do systemu,
- wyłudzanie, fałszowanie dokumentów,
- podszycie się pod uprawnionego użytkownika,
- podsłuch,
- użycie złośliwego oprogramowania,
- wykorzystanie promieniowa ujawniającego.

§6

Każde z wyżej wymienionych zagrożeń wynikających z działalności człowieka może być ograniczone poprzez:

- rygorystyczne przestrzeganie zasad postępowania z danymi osobowymi,
- fizyczne zabezpieczenie obiektu, w którym działa system,
- techniczne zabezpieczenie systemu,

- wdrożenie systemu kontroli użytkowników,
- brak połączenia stanowisk komputerowych systemu z siecią internetową,
- stosowanie bezpiecznych metod połączenia z siecią internetową urządzeń mających dostęp do systemu obiegu dokumentacji.

§7

Zagrożenia wynikające z działania sił natury można ograniczyć poprzez właściwe zabezpieczenie budynków i pomieszczeń, w których znajduje się stanowisko komputerowe oraz serwer, na których przetwarzane są dane osobowe.

Potencjalne ataki mogą być wykonywane poprzez: posłuch, wyłudzenie, fałszowanie dokumentów.

4. STOPIEŃ WAŻONOŚCI INFORMACJI:

§1

Stopień ważności informacji zawierających dane osobowe określa poziom ochrony oraz zastosowanie właściwych środków bezpieczeństwa. W Centrum Kształcenia Zawodowego i Ustawicznego nr 1 w Gliwicach przetwarza się dane osobowe zwykłe oraz wrażliwe – merytorycznie zawiązane z zakresem obowiązków użytkownika.

Ponieważ przeważająca część danych osobowych oraz informacji przesyłana jest drogą elektroniczną do systemu obiegu dokumentacji, wielkość potencjalnych skutków ujawnienia, czy utraty informacji w nich zawartych jest stosunkowo duża, dlatego też należy oszacować poziom utraty poufności, jako wysoki [8 w skali od 1 do 10]. Dotyczy to każdej kategorii ww. przetwarzanych zasobów danych osobowych.

Dokładność i kompletność realizowanych czynności w zakresie przetwarzanych spraw administracyjnych są zapewnione poprzez odpowiednie usytuowanie stanowisk komputerowych, na których się przetwarza dane osobowe (stanowiska jednoosobowe). Według oceny osób odpowiedzialnych za ochronę danych osobowych wymagania związane z potrzebą zachowania integralności informacji zawierających dane osobowe w systemie są średnie [4-7 w skali od 1-10]. Dotyczy to każdej kategorii ww. przetwarzanych zasobów danych osobowych.

Bezpieczeństwo fizyczne i techniczne w zakresie zabezpieczenia serwera wewnętrznego jest zapewnione poprzez odpowiednie zabezpieczenie fizyczne i programowe oraz odpowiednie usytuowanie serwera, na którym przetwarza się dane osobowe. Według oceny osób odpowiedzialnych za bezpieczeństwo informacji wymagania związane z potrzebą zachowania integralności w systemie są niskie [1-3 w skali od 1-10].

Wytwarzane dokumenty zawierające dane osobowe są rejestrowane, przechowywane do wglądu, a następnie niszczone lub archiwizowane przez osoby posiadające stosowne upoważnienie. Można zatem określić wymagania związane z zachowaniem rozliczalności, jako średnie [4-6 w skali od 1 do 10].

5. PODATNOŚĆ SYSTEMU NA ZAGROŻENIA:

§1

Podatność systemu na zagrożenia może wynikać z:

- dostępności systemu wynikającego np. z braku ochrony fizycznej budynku lub znacznej liczby personelu, mającego potencjalnie dostęp do systemu oraz wiedzę jak obsługiwać system,
- dostępność informacji znajdujących się w systemie za pośrednictwem połączeń zewnętrznych,
- możliwość celowego wprowadzenia luk w sprzęcie i oprogramowaniu lub wprowadzenia wirusów komputerowych,
- możliwość awarii sprzętu lub oprogramowania ze względu na uszkodzenia, błędy projektowe lub umyślną interwencję,
- przesyłanie informacji przez niezabezpieczone łącza telekomunikacyjne,
- dostęp do informacji za pośrednictwem niezabezpieczonych łączy telekomunikacyjnych.

§2

Podatność systemu na zagrożenia została ograniczona poprzez:

- ochronę fizyczną i techniczną stanowisk komputerowych,
- ochronę fizyczną i techniczną serwera wewnętrznego,
- zagwarantowanie odpowiedniego poziomu bezpieczeństwa fizycznego i technicznego serwera zewnętrznego poprzez umowę z dostawcą,
- kontrolę dostępu do pomieszczeń, gdzie przetwarzane są dane osobowe,
- wydzielenie stref ochronnych,
- ograniczenie liczby personelu, mającego potencjalnie dostęp do stanowisk komputerowych oraz wiedzę jak je obsługiwać,
- zbudowanie stabilnej sieci zasilającej,
- przeglądy okresowe nośników,
- kontrolę zmian konfiguracji,
- testowanie oprogramowania,
- audyt,
- zabezpieczenie haseł,
- użycie oprogramowania antywirusowego,
- backupy,
- zabezpieczenie sieci internetowej,
- zapewnienie bezpiecznych metod łączenia z siecią internetową.

§3

W celu oszacowania potencjalnych strat wynikających z utraty (ujawnienia) danych osobowych przetwarzanych na stanowiskach komputerowych wykonano analizę ryzyka na podstawie przewidywanych zagrożeń dla zasobów.

6. ANALIZA ZAGROŻEŃ I RYZYKA:

§1

Analiza zagrożeń i ryzyka polega na identyfikacji ryzyka wystąpienia niepożądanego czynnika (ujawnienia, przechwycenia itd.) określenia jego wielkości i zidentyfikowania obszarów wymagających zabezpieczeń tak, aby to ryzyko zminimalizować lub całkowicie zlikwidować.

§2

Aby przeprowadzić poprawnie analizę ryzyka na początku należy określić:

- zasoby, które będziemy chronić,
- zagrożenia – czynnik, który może powodować wystąpienie incydentu,
- podatność – słabość zasobów, która może być wykorzystana przez potencjalne zagrożenie,
- skutki – jaki wpływ będzie miał zaistniały incydent na system informatyczny.

§3

Zasobami systemu są wszystkie elementy służące do przetwarzania, przechowywania lub przekazywania informacji oraz do zapewnienia im właściwego poziomu bezpieczeństwa, tzn.

- sprzęt komputerowy przechowujący dane – dysk twardy, serwer,
- pracownicy przetwarzający dane osobowe,
- aplikacje, w których przetwarzane są dane osobowe,
- pomieszczenia, w których pracują osoby przetwarzające dane osobowe,
- koszty dodatkowych zabezpieczeń oraz odbudowy systemu po incydencie.

§4

Zagrożenia systemu to wszystkie niekorzystne czynniki mogące przyczynić się w trakcie pacy z danymi osobowymi do wystąpienia incydentu, mogącego mieć wpływ na ich ujawnienie bądź utratę, tzn.:

- poufność – właściwość polegająca na tym, że informacja nie jest dostępna lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom tj.: nieuprawniony dostęp do informacji, kradzież, pomyłka, sabotaż, itp.,
- rozliczalność – właściwość pozwalająca na rozliczenie osoby pracującej na stanowisku komputerowym systemu przewarzającego dane osobowe w zakresie dostępu do pomieszczenia, w którym ono jest zainstalowane oraz rozliczenie czynności wykonanych przy pomocy tego stanowiska komputerowego, w systemie katalogów oraz pojedynczych zbiorach,
- integralność – właściwość polegająca na zapewnieniu dokładności i kompletności aktywów, tyj. Atak wirusa, pożar, itp.

§5

Podatność systemu to słabości zasobów, które mogą być wykorzystane do ujawnienia informacji niejawnych lub ich utraty. Skutki przetwarzania określają wysokość strat w systemie informatycznym po zaistnieniu incydentu.

7. WNIOSKI:

§1

Ww. analiza przeprowadzona dla wszystkich chronionych zasobów oraz wszystkich możliwych zagrożeń dała pełny obraz na co zwrócić szczególną uwagę w jednostce, jakie zastosować dodatkowe środki bezpieczeństwa i pozwala na stworzenie dobrze działającej polityki bezpieczeństwa (regulaminu ochrony danych) występującego systemu informatycznego, w którym przetwarzane są dane osobowe. Dodatkowo ułatwia też stworzenie stosownej dokumentacji.

§2

W związku z powyższym na podstawie ww. analizy największym potencjalnym zagrożeniem występującym w Centrum Kształcenia Zawodowego i Ustawicznego nr 1 w Gliwicach dla bezpieczeństwa danych osobowych jest:

- nieuprawniony dostęp,
- kradzież (włamanie do systemu),
- nieumyślne działanie osoby upoważnionej.

Innymi zagrożeniami są:

- awaria sprzętu,
- atak wirusa,
- włamanie do sieci.

W celu zmniejszenia ww. zagrożeń szczególną uwagę należy zwrócić na:

- przetwarzanie danych osobowych tylko przez osoby upoważnione,
- zabezpieczenie obiektu i systemu informatycznego w zakresie ochrony antywłamaniowej oraz przestrzeganie ustalonych zasad w tym zakresie,
- przestrzeganie instrukcji obsługi sprzętu i zasad posługiwania się nim,
- stosowanie nowoczesnych zabezpieczeń antywłamaniowych.

Aby skutecznie wyeliminować ww. zagrożenia należy wprowadzić następujące dodatkowe zabezpieczenia:

- przestrzegać zasad korzystania ze sprzętu informatycznego oraz zabezpieczeń określonych w Regulaminie Ochrony Danych, ze zwróceniem szczególnej uwagi na dostęp osób postronnych,
- przestrzegać rygorystycznie przepisów w zakresie ochrony danych osobowych,
- przestrzegać zasad posługiwania się sprzętem komputerowym (kopiowanie, przesyłanie, udostępnianie),
- stosować procedury Regulaminu Ochrony Danych z zakresu korzystania z systemu informatycznego, w którym przetwarzane są dane osobowe.

SKALA:

- identyfikacja skutków utraty zasobów, dla atrybutu poufności danych osobowych:

Wartość	Skutki
0	Brak skutków utraty poufności
1-3	Niski skutek utraty poufności
4-7	Średni skutek utraty poufności
8-9	Wysoki skutek utraty poufności
10	Całkowita utrata poufności

- identyfikacja skutków utraty zasobów, dla atrybutu rozliczalności danych osobowych:

Wartość	Skutki
0	Utrata dostępności nie występuje
1-3	Niski skutek utraty rozliczalności
4-6	Średni skutek utraty rozliczalności
7-8	Wysoki skutek utraty rozliczalności
9	Ekstremalny skutek utraty rozliczalności
10	Absurdalny skutek utraty rozliczalności

- identyfikacja skutków utraty zasobów, dla atrybutu integralności danych osobowych:

Wartość	Skutki
0	Utrata integralności nie występuje
1-3	Niski skutek utraty integralności
4-7	Średni skutek utraty integralności
8-9	Wysoki skutek utraty integralności
10	Bezwzględny skutek utraty integralności

- identyfikacja podatności systemu informatycznego na określone zagrożenia:

Wartość	Podatność
0	Brak podatności
1-4	Niski poziom
5-7	Średni poziom
8-9	Wysoki poziom
10	Ekstremalny poziom

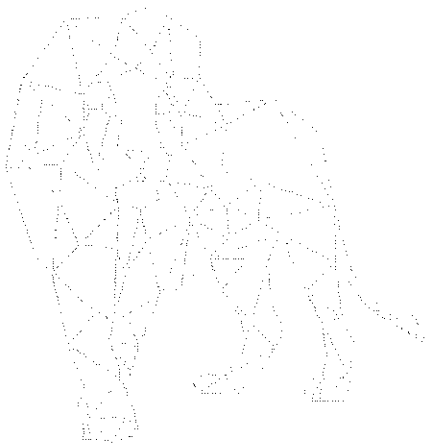
Ryzyko = iloczyn wartości skutków i podatności zasobów systemu (max. = 100)

- skala poziomu ryzyka:

Wartość	Poziom ryzyka
1-20	Niski poziom ryzyka utraty bezpieczeństwa danych osobowych
21-60	Średni poziom ryzyka utraty bezpieczeństwa danych osobowych
61-80	Wysoki poziom ryzyka utraty bezpieczeństwa danych osobowych
81-100	Maksymalny poziom ryzyka utraty bezpieczeństwa danych osobowych

Ryzyko ogólne (średnio) = 25,9111 / 100

tzn. występuje średnie ryzyko utraty bezpieczeństwa danych osobowych.



		Zagrożenia																		
		Poufność						Rozliczalność						Integralność						
Zasoby	Szacowanie	Nieuprawniony Dostęp	Kradzież	Atak wirusa	Pożar	Odcięcie Zasilania	Awaria Sprzętu	Nieuprawniony Dostęp	Kradzież	Atak wirusa	Pożar	Odcięcie Zasilania	Awaria Sprzętu	Nieuprawniony Dostęp	Kradzież	Atak wirusa	Pożar	Odcięcie Zasilania	Awaria Sprzętu	Razem (średnia)
Sprzęt	Skutki	8	10	8	0	0	8	8	10	8	8	6	9	4	10	8	1	1	5	
	Podatność	8	2	7	7	9	7	3	3	4	3	6	8	3	7	3	1	2	7	
	Ryzyko	64	20	56	0	0	56	24	30	32	24	36	72	12	70	24	1	2	35	31
Ludzie	Skutki	8	10	8	0	0	6	7	8	8	7	4	7	8	10	8	7	7	7	
	Podatność	6	3	6	9	4	4	3	3	4	4	4	7	8	7	3	3	7	8	
	Ryzyko	32	30	48	0	0	24	21	24	32	28	16	49	64	70	24	21	49	56	32,66667
Aplikacje	Skutki	8	10	8	0	0	6	6	8	8	7	8	5	8	8	8	7	7	7	
	Podatność	6	1	7	0	8	4	4	3	7	4	4	2	3	3	3	3	3	2	
	Ryzyko	48	10	56	0	0	24	24	24	56	28	32	10	24	24	24	21	21	14	24,44444
Pomieszczenia	Skutki	10	10	7	0	0	7	8	10	7	8	4	4	10	8	8	8	3	2	
	Podatność	9	5	3	7	3	3	3	3	3	4	3	3	3	3	3	3	3	3	
	Ryzyko	90	50	21	0	0	21	24	30	21	32	12	12	30	24	24	24	9	6	23,88889
Dodatkowe zabezpieczenia	Skutki	8	10	5	0	0	5	8	10	8	2	2	5	8	10	8	8	8	8	
	Podatność	4	3	2	2	2	2	4	2	3	2	1	2	3	3	3	2	3	3	
	Ryzyko	32	30	10	0	0	10	32	20	24	4	2	10	24	30	24	16	24	24	17,55556
Ogółem	**(średnia)**	53,2	28	38,2	0	0	27	25	25,6	33	23,2	19,6	30,6	30,8	43,6	24	16,6	21	27	26,51111

Analiza ryzyka dla ogólnego bezpieczeństwa informacji

Nazwa podmiotu wprowadzającego	Centrum Kształcenia Zawodowego i Ustawicznego nr 1 w Gliwicach
Data wprowadzenia	15 marca 2023 r.
Podpis ADO	

§1

Ilekroć w dokumencie jest mowa o:

1. **ANALIZIE RYZYKA** – rozumie się przez to systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka;
2. **SZACOWANIU RYZYKA** – rozumie się przez to proces oceny i analizy ryzyka;
3. **OCENIE RYZYKA** – rozumie się przez to proces porównania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka;
4. **POSTĘPOWANIU Z RYZYKIEM** – rozumie się przez to wdrażanie środków modyfikujących ryzyko;
5. **ZARZĄDZANIU RYZYKIEM** – rozumie się przez to działania dotyczące kierowania i nadzorowania organizacją w odniesieniu do ryzyka;
6. **RYZYKU SZCZĄTKOWYM** – rozumie się przez to ryzyko pozostające po procesie postępowania z ryzykiem;
7. **AKCEPTOWANIU RYZYKA** – rozumie się przez to decyzja, aby zaakceptować ryzyko;
8. **BEZPIECZEŃSTWIE INFORMACJI** – rozumie się przez to zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
9. **ZDARZENIU ZWIĄZANYM Z BEZPIECZEŃSTWEM INFORMACJI** – rozumie się przez to zdarzenie związane z bezpieczeństwem informacji, jako określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe naruszenie Polityki Bezpieczeństwa Informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem;
10. **INCYDENCIE ZWIĄZANYM Z BEZPIECZEŃSTWEM INFORMACJI** – rozumie się przez to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne zakłócenia zadań biznesowych i zagrażają bezpieczeństwu informacji;
11. **AKTYWACH** – rozumie się przez to wszystko, co ma wartość dla organizacji;
12. **ZAGROŻENIACH SYSTEMU** – rozumie się przez to wszystkie niekorzystne czynniki mogące przyczynić się w trakcie pracy z danymi do wystąpienia incydentu, mogącego mieć wpływ na ich ujawnienie bądź utratę;

13. **DOSTĘPNOŚCI** —należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym;
14. **INCYDENCIE BEZPIECZEŃSTWA TELEINFORMATYCZNEGO** —należy przez to rozumieć takie pojedyncze zdarzenie lub serię zdarzeń, związanych z bezpieczeństwem informacji niejawnych, które zagrażają ich poufności, dostępności lub integralności;
15. **INFORMATYCZNYM NOŚNIKU DANYCH** —należy przez to rozumieć materiał służący do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej;
16. **INTEGRALNOŚCI** —należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony;
17. **OPROGRAMOWANIU ZŁOŚLIWYM** —należy przez to rozumieć oprogramowanie, którego celem jest przeprowadzenie nieuprawnionych lub szkodliwych działań w systemie teleinformatycznym;
18. **PODATNOŚCI** — należy przez to rozumieć słabość zasobu lub zabezpieczenia systemu teleinformatycznego, która może zostać wykorzystana przez zagrożenie;
19. **POŁĄCZENIU MIĘDZYSYSTEMOWYM** —należy przez to rozumieć techniczne albo organizacyjne połączenie dwóch lub więcej systemów teleinformatycznych, umożliwiające ich współpracę, a w szczególności wymianę danych;
20. **POUFNOŚCI** —należy przez to rozumieć właściwość określającą, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym;
21. **PRZEKAZYWANIU INFORMACJI** —należy przez to rozumieć zarówno transmisję informacji, jak i przekazywanie informacji na informatycznych nośnikach danych, na których zostały utrwalone;
22. **TESTACH BEZPIECZEŃSTWA** —należy przez to rozumieć testy poprawności i skuteczności funkcjonowania zabezpieczeń w systemie teleinformatycznym;
23. **ZABEZPIECZENIU** —należy przez to rozumieć środki o charakterze fizycznym, technicznym lub organizacyjnym zmniejszające ryzyko;
24. **ZAGROŻENIU** —należy przez to rozumieć potencjalną przyczynę niepożądanego zdarzenia, które może wywołać szkodę w zasobach systemu teleinformatycznego;
25. **ZASOBACH SYSTEMU TELEINFORMATYCZNEGO** –należy przez to rozumieć informacje przetwarzane w systemie teleinformatycznym, jak również osoby, usługi, oprogramowanie, dane i sprzęt oraz inne elementy mające wpływ na bezpieczeństwo tych informacji;

1. PODSTAWA PRAWNA:

§1

a) Ustawa o Ochronie Danych Osobowych z dnia 10 Maja 2018 r.
b) Rozporządzenie Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE
c) Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M.P. 2019 poz. 666)

2. OGÓLNE WYMOGI BEZPIECZEŃSTWA:

§1

W czasie przetwarzania danych osobowych oraz ogólnych informacji, występują one w postaci:

- plików lub informacji przechowywanych na dysku twardym komputera,
- plików lub informacji przechowywanych w pamięci operacyjnej komputera,
- plików lub informacji zapisanych na nośnikach komputerowych,
- wersji roboczych lub gotowych dokumentów wydrukowanych na papierze.

§2

Bezpieczeństwo przetwarzanych lub przechowywanych informacji wymaga:

- zapewnienia ochrony fizycznej stanowiska komputerowego przed nieuprawnionym dostępem,
- ochrony nośników technicznych i wydruków dokumentów wytwarzanych przy pomocy sprzętu komputerowego, w tym określenia zasad postępowania z nimi przed nieuprawnionym dostępem,
- zabezpieczenia przed nieupoważnionym dostępem do danych znajdujących się w zasobach systemu informatycznego,
- zapewnienia dostępności do danych znajdujących się na technicznych nośnikach informacji oraz w pamięci systemu informatycznego dla upoważnionych użytkowników,
- zapewnienia możliwości kontroli dostępu do zasobów systemu informatycznego oraz wykonywanych na nim czynności,
- zapewnienia możliwości kontroli nośników na których przetwarzano lub przechowywano dane.

3. ZAGROŻENIA DLA SYSTEMU:

§1

Biorąc pod uwagę specyfikę prac wykonywanych przy pomocy systemu informatycznego, przeznaczonego do przygotowania dokumentów zawierających informacje, podstawowe zagrożenia to: utrata poufności, integralności i rozliczalności dokumentów:

- poufność to zapewnienie że dane nie są udostępniane nieupoważnionym podmiotom,
- integralność to zapewnienie, aby wszystkie zmiany wykonywane w systemie informatycznym, w systemie jego katalogów oraz poszczególnych plikach zawierających dane były skutkiem zaplanowanych działań użytkowników systemu. Właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
- rozliczalność to właściwość zapewniająca, że działania podmiotu przetwarzającego dane mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

§2

Zagrożenia w zakresie poufności obejmują:

- nieuprawniony dostęp do pomieszczenia, w którym przetwarzane są informacje,
- ujawnienie haseł dostępu do stanowiska komputerowego, na którym przetwarzane są informacje,
- ujawnienie kodów dostępu do systemów,
- nieuprawnione przeniesienie informacji na inny nośnik,
- utrata nośnika zewnętrznego,
- klęska żywiołowa, w wyniku której utracono poufność,

- nieuprawnione wyniesienie informacji zawartych na nośniku elektronicznym lub w formie papierowej.

§3

Zagrożenia w zakresie rozliczalności obejmują:

- brak kontroli nad dokumentami wykonywanymi na stanowisku komputerowym w zakresie ich kopiowania i drukowania,
- wyparcie się pracy na stanowisku komputerowych, gdzie przetwarza się dane ,
- wprowadzenie zmian w treści dokumentu, zawierającego dane,
- błędy oprogramowania lub sprzętu.

§4

Zagrożenia w zakresie integralności obejmują:

- nielegalny dostęp do danych, w tym do stanowiska komputerowego,
- błędy i pomyłki,
- brak mechanizmów uniemożliwiających skanowanie lub zmianę logów przez administratora lub innego użytkownika,
- wadliwe działanie systemu operacyjnego,
- wirus,
- brak w wykorzystywanych aplikacjach mechanizmów zapewniających integralność danych.

§5

Źródłami zagrożeń dla stanowisk komputerowych, gdzie przetwarza się dane mogą być:

- siły natury – zdarzenia, które nie wynikają z działalności człowieka, tzn.:
  - uderzenie pioruna,
  - pożar będący konsekwencją ww. uderzenia pioruna,
  - starzenie się sprzętu,
  - starzenie się nośników pamięci,
  - smog, kurz,
  - katastrofy budowlane,
  - ulewny deszcz,
  - huragan,
  - ekstremalne temperatury, wilgotność,
  - epidemia.
- ludzie – mogą to być pracownicy lub osoby z zewnątrz, którzy działają w sposób celowy lub przypadkowy; zagrożenia te to przede wszystkim:
  - błędy lub pomyłki użytkowników lub administratorów,
  - błędy utrzymania systemu w poufności, rozliczalności i integralności,
  - zaniedbania użytkowników przy przesyłaniu, udostępnianiu i kopiowaniu,
  - zagubienie nośnika zawierającego dane,

- niewłaściwe zniszczenie nośnika,
- nielegalne użycie oprogramowania,
- choroba ważnych osób i nieuprawnione zastępstwo,
- podpalenie obiektu,
- katastrofa budowlana będąca konsekwencją przypadkowego działania człowieka,
- zakłócenia elektromagnetyczne lub radiotechniczne,
- podłożenie i wybuch bomby lub ładunku wybuchowego,
- użycie broni,
- zmiany napięcia w sieci,
- utrata prądu,
- zbieranie się ładunków elektrostatycznych,
- utrata kluczowych pracowników,
- niedobór pracowników,
- szpiegostwo,
- terroryzm,
- defekty oprogramowania,
- destrukcja zbiorów i programów impulsem elektromagnetycznym,
- kradzież,
- włamanie do systemu,
- wyłudzanie, fałszowanie dokumentów,
- podszycie się pod uprawnionego użytkownika,
- podsłuch,
- użycie złośliwego oprogramowania,
- wykorzystanie promieniowa ujawniającego.

§6

Każde z wyżej wymienionych zagrożeń wynikających z działalności człowieka może być ograniczone poprzez:

- rygorystyczne przestrzeganie zasad postępowania z informacjami,
- fizyczne zabezpieczenie obiektu, w którym działa system,
- wdrożenie systemu kontroli użytkowników,
- brak połączenia stanowisk komputerowych systemu z siecią internetową.

§7

Zagrożenia wynikające z działania sił natury można ograniczyć poprzez właściwe zabezpieczenie budynków i pomieszczeń, w których znajduje się stanowisko komputerowe, na którym przetwarzane są dane.

Potencjalne ataki mogą być wykonywane poprzez: posłuch, wyłudzenie, fałszowanie dokumentów.

4. STOPIEŃ WAŻONOŚCI INFORMACJI:

§1

Stopień ważności informacji określa poziom ochrony oraz zastosowanie właściwych środków bezpieczeństwa.

Ponieważ przeważająca część danych osobowych oraz informacji przesyłana jest drogą elektroniczną, wielkość potencjalnych skutków ujawnienia, czy utraty informacji w nich zawartych jest stosunkowo duża, dlatego też należy oszacować poziom utraty poufności, jako średni [6 w skali od 1 do 10]. Dotyczy to każdej kategorii ww. przetwarzanych zasobów.

Dokładność i kompletność realizowanych czynności w zakresie przetwarzanych spraw administracyjnych są zapewnione poprzez odpowiednie usytuowanie stanowisk komputerowych, na których się przetwarza dane (stanowiska jednoosobowe). Według oceny osób odpowiedzialnych za ochronę danych osobowych wymagania związane z potrzebą zachowania integralności informacji zawierających dane w systemie są średnie [4 w skali od 1-10]. Dotyczy to każdej kategorii ww. przetwarzanych zasobów.

Wytwarzane dokumenty zawierające dane są rejestrowane, przechowywane do wglądu, a następnie niszczone lub archiwizowane przez osoby posiadające stosowne upoważnienie. Można zatem określić wymagania związane z zachowaniem rozliczalności, jako niskie [2 w skali od 1 do 10].

5. PODATNOŚĆ SYSTEMU NA ZAGROŻENIA:

§1

Podatność systemu na zagrożenia może wynikać z:

- dostępności systemu wynikającego np. z braku ochrony fizycznej budynku lub znacznej liczby personelu, mającego potencjalnie dostęp do systemu oraz wiedzę jak obsługiwać system,
- dostępność informacji znajdujących się w systemie za pośrednictwem połączeń zewnętrznych,
- możliwość celowego wprowadzenia luk w sprzęcie i oprogramowaniu lub wprowadzenia wirusów komputerowych,
- możliwość awarii sprzętu lub oprogramowania ze względu na uszkodzenia, błędy projektowe lub umyślną interwencję,
- przesyłanie informacji przez niezabezpieczone łącza telekomunikacyjne.

§2

Podatność systemu na zagrożenia została ograniczona poprzez:

- ochronę fizyczną stanowisk komputerowych,
- kontrolę dostępu do pomieszczeń, gdzie przetwarzane są dane,
- wydzielenie stref ochronnych,
- ograniczenie liczby personelu, mającego potencjalnie dostęp do stanowisk komputerowych oraz wiedzę jak je obsługiwać,

- zbudowanie stabilnej sieci zasilającej,
- przeglądy okresowe nośników,
- kontrolę zmian konfiguracji,
- testowanie oprogramowania,
- audyt,
- zabezpieczenie haseł,
- użycie oprogramowania antywirusowego,
- backupy.

§3

W celu oszacowania potencjalnych strat wynikających z utraty (ujawnienia) danych przetwarzanych na stanowiskach komputerowych wykonano analizę ryzyka na podstawie przewidywanych zagrożeń dla zasobów.

6. ANALIZA ZAGROŻEŃ I RYZYKA:

§1

Analiza zagrożeń i ryzyka polega na identyfikacji ryzyka wystąpienia niepożądanego czynnika (ujawnienia, przechwycenia itd.) określenia jego wielkości i zidentyfikowania obszarów wymagających zabezpieczeń tak, aby to ryzyko zminimalizować lub całkowicie zlikwidować.

§2

Aby przeprowadzić poprawnie analizę ryzyka na początku należy określić:

- zasoby, które będziemy chronić,
- zagrożenia – czynnik, który może powodować wystąpienie incydentu,
- podatność – słabość zasobów, która może być wykorzystana przez potencjalne zagrożenie,
- skutki – jaki wpływ będzie miał zaistniały incydent na system informatyczny.

§3

Zasobami systemu są wszystkie elementy służące do przetwarzania, przechowywania lub przekazywania informacji oraz do zapewnienia im właściwego poziomu bezpieczeństwa, tzn.

- sprzęt komputerowy przechowujący dane – dysk twardy,
- pracownicy przetwarzający dane,
- aplikacje, w których przetwarzane są dane,
- pomieszczenia, w których pracują osoby przetwarzające dane,
- koszty dodatkowych zabezpieczeń oraz odbudowy systemu po incydencie.

§4

Zagrożenia systemu to wszystkie niekorzystne czynniki mogące przyczynić się w trakcie pacy z danymi do wystąpienia incydentu, mogącego mieć wpływ na ich ujawnienie bądź utratę, tzn.:

- poufność – właściwość polegająca na tym, że informacja nie jest dostępna lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom tj.: nieuprawniony dostęp do informacji, kradzież, pomyłka, sabotaż, itp.,
- rozliczalność – właściwość pozwalająca na rozliczenie osoby pracującej na stanowisku komputerowym systemu przewarzającego dane w zakresie dostępu do pomieszczenia, w którym ono jest zainstalowane oraz rozliczenie czynności wykonanych przy pomocy tego stanowiska komputerowego, w systemie katalogów oraz pojedynczych zbiorach,
- integralność – właściwość polegająca na zapewnieniu dokładności i kompletności aktywów, tyj. Atak wirusa, pożar, itp.

§5

Podatność systemu to słabości zasobów, które mogą być wykorzystane do ujawnienia informacji niejawnych lub ich utraty. Skutki przetwarzania określają wysokość strat w systemie informatycznym po zaistnieniu incydentu.

7. WNIOSKI:

§1

Ww. analiza przeprowadzona dla wszystkich chronionych zasobów oraz wszystkich możliwych zagrożeń dała pełny obraz na co zwrócić szczególną uwagę w placówce, jakie zastosować dodatkowe środki bezpieczeństwa i pozwala na stworzenie dobrze działającej polityki bezpieczeństwa (regulaminu ochrony danych) występującego systemu informatycznego, w którym przetwarzane są dane. Dodatkowo ułatwia też stworzenie stosownej dokumentacji.

§2

W związku z powyższym na podstawie ww. analizy największym potencjalnym zagrożeniem występującym w Centrum Kształcenia Zawodowego i Ustawicznego nr 1 w Gliwicach dla bezpieczeństwa informacji jest:

- nieuprawniony dostęp,
- kradzież (włamanie do systemu).

Innymi zagrożeniami są:

- awaria sprzętu,
- atak wirusa,
- pożar obiektu w którym znajduje się Centrum Kształcenia Zawodowego i Ustawicznego nr 1 w Gliwicach.

W celu zmniejszenia ww. zagrożeń szczególną uwagę należy zwrócić na:

- przetwarzanie danych tylko przez osoby upoważnione,
- zabezpieczenie obiektu i systemu informatycznego w zakresie ochrony antywłamaniowej oraz przestrzeganie ustalonych zasad w tym zakresie,
- przestrzeganie instrukcji obsługi sprzętu i zasad posługiwania się nim,
- stosowanie nowoczesnych zabezpieczeń antywłamaniowych.

Aby skutecznie wyeliminować ww. zagrożenia należy wprowadzić następujące dodatkowe zabezpieczenia:

- przestrzegać zasad korzystania ze sprzętu informatycznego określonych w Regulaminie Ochrony Danych, ze zwróceniem szczególnej uwagi na dostęp osób postronnych,
- przestrzegać rygorystycznie przepisów w zakresie ochrony danych osobowych,
- przestrzegać zasad posługiwania się sprzętem komputerowym (kopiowanie, przesyłanie, udostępnianie),
- stosować procedury Regulaminu Ochrony Danych korzystania z systemu informatycznego, w którym przetwarzane są dane.

SKALA:

- identyfikacja skutków utraty zasobów, dla atrybutu poufności danych:

Wartość	Skutki
0	Brak skutków utraty poufności
1-3	Niski skutek utraty poufności
4-7	Średni skutek utraty poufności
8-9	Wysoki skutek utraty poufności
10	Całkowita utrata poufności

- identyfikacja skutków utraty zasobów, dla atrybutu rozliczalności danych:

Wartość	Skutki
0	Utrata dostępności nie występuje
1-3	Niski skutek utraty rozliczalności
4-6	Średni skutek utraty rozliczalności
7-8	Wysoki skutek utraty rozliczalności
9	Ekstremalny skutek utraty rozliczalności
10	Absurdalny skutek utraty rozliczalności

- identyfikacja skutków utraty zasobów, dla atrybutu integralności danych:

Wartość	Skutki
0	Utrata integralności nie występuje
1-3	Niski skutek utraty integralności

4-7	Średni skutek utraty integralności
8-9	Wysoki skutek utraty integralności
10	Bezwzględny skutek utraty integralności

- identyfikacja podatności systemu informatycznego na określone zagrożenia:

Wartość	Podatność
0	Brak podatności
1-4	Niski poziom
5-7	Średni poziom
8-9	Wysoki poziom
10	Ekstremalny poziom

Ryzyko = iloczyn wartości skutków i podatności zasobów systemu (max. = 100)

- skala poziomu ryzyka:

Wartość	Poziom ryzyka
1-20	Niski poziom ryzyka utraty bezpieczeństwa danych
21-60	Średni poziom ryzyka utraty bezpieczeństwa danych
61-80	Wysoki poziom ryzyka utraty bezpieczeństwa danych
81-100	Maksymalny poziom ryzyka utraty bezpieczeństwa danych

Ryzyko ogólne (niskie) = 19,8333 / 100

tzn. występuje niskie ryzyko utraty bezpieczeństwa informacji.

Zasoby	Szacowanie	Zagrożenia: Poufność: Nieuprawniony Dostęp	Poufność: Kradzież	Poufność: Atak wirusa	Poufność: Pożar	Poufność: Odcięcie Zasilania	Poufność: Awaria Sprzętu	Rozliczalność: Nieuprawniony Dostęp	Rozliczalność: Kradzież	Rozliczalność: Atak wirusa	Rozliczalność: Pożar	Rozliczalność: Odcięcie Zasilania	Rozliczalność: Awaria Sprzętu	Integralność: Nieuprawniony Dostęp	Integralność: Kradzież	Integralność: Atak wirusa	Integralność: Pożar	Integralność: Odcięcie Zasilania	Integralność: Awaria Sprzętu	Razem (średnia)
Sprzęt	Skutki	8	7	8	0	0	7	8	10	8	7	7	5	8	7	8	6	3	7	
	Podatność	4	2	5	7	5	7	2	2	4	3	6	6	3	3	3	7	8	7	
	Ryzyko	32	14	40	0	0	49	16	20	32	21	42	30	24	21	24	42	24	49	26,66667
Ludzie	Skutki	8	7	8	0	0	7	7	8	8	7	6	5	4	4	2	7	7	7	
	Podatność	1	0	5	7	4	4	5	3	4	4	4	4	5	3	4	3	7	7	
	Ryzyko	8	0	40	0	0	28	35	24	32	28	24	20	20	12	8	21	49	49	22,11111
Aplikacje	Skutki	8	7	8	0	0	3	6	8	8	7	8	5	8	8	8	7	7	7	
	Podatność	2	2	3	4	4	3	2	2	5	4	4	6	3	3	3	3	3	2	
	Ryzyko	16	14	24	0	0	9	12	16	40	28	32	30	24	24	24	21	21	14	19,38889
Pomieszczenia	Skutki	8	8	1	0	0	5	8	10	7	8	4	4	8	8	2	4	3	2	
	Podatność	3	8	0	7	3	3	3	3	3	4	3	3	3	3	3	3	3	3	
	Ryzyko	24	64	0	0	0	15	24	30	21	32	12	12	24	24	6	12	9	6	17,5
Dodatkowe zabezpieczenia	Skutki	7	8	5	0	0	5	8	8	5	2	2	5	7	8	5	5	5	5	
	Podatność	4	2	2	2	2	2	4	2	3	2	1	2	3	3	3	2	3	3	
	Ryzyko	28	16	10	0	0	10	32	16	15	4	2	10	21	24	15	10	15	15	13,5
Ogółem	**(średnia)**	**21,6**	**21,6**	**22,8**	**0**	**0**	**22,2**	**23,8**	**21,2**	**28**	**22,6**	**22,4**	**20,4**	**22,6**	**21**	**15,4**	**21,2**	**23,6**	**26,6**	[illegible]