Centrum Usług Wspólnych
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP:767-17-04-789 REGON:366052269
tel. 67 2669 145, 67 2669 715

ZARZĄDZENIE NR 11/2021
DYREKTORA CENTRUM USŁUG WSPÓLNYCH W OKONKU
z dnia 23.08.2021 roku
w sprawie wdrożenia Polityki Ochrony Danych

W związku z Rozporządzeniem 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 (Dziennik Urzędowy UE - 4.5.2016 L 119/3) oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r., poz. 1781).

zarządza się, co następuje:

§ 1.

Wprowadzam w życie w Centrum Usług Wspólnych w Okonku zwanym dalej CUW, Polityki Ochrony Danych Osobowych i Politykę Zarządzania Ryzykiem w bezpieczeństwie przetwarzania danych, które stanowią odpowiednio załączniki 1 - 2 do zarządzenia.

§ 2.

Zadania związane z prawidłowością przetwarzania danych osobowych w CUW realizują wszyscy pracownicy, zatrudnieni w placówce, a za skuteczne funkcjonowanie Polityki Ochrony Danych odpowiedzialny jest dyrektor CUW który jest administratorem danych osobowych w Centrum Usług Wspólnych w Okonku.

§ 3.

Zasady ochrony danych określone są w Regulaminie Ochrony Danych, który stanowi załącznik nr 3 do zarządzenia.

§ 4.

Zobowiązuję wszystkich pracowników do zapoznania się z przepisami ochrony danych, obowiązujących w Centrum Usług Wspólnych w Okonku oraz złożenie pisemnego oświadczenia o zapoznaniu się z Regulaminem Ochrony Danych w Centrum Usług Wspólnych w Okonku w terminie do 30 września 2021r. Wzór oświadczenia stanowi załącznik nr 4 do zarządzenia.

§ 5.

Traci moc zarządzenie Nr 2 Dyrektora Centrum Usług Wspólnych z dnia 02.01.2017 roku, w którym zostały wprowadzone Polityka Bezpieczeństwa oraz Instrukcja Zarządzania Systemem Przetwarzania Danych Osobowych w Centrum Usług Wspólnych w Okonku.

§ 6.

Zarządzenie wchodzi w życie z dniem podpisania.

/ dyrektor jednostki/

DYREKTOR
Centrum Usług Wspólnych
w Okonku
Renata Zabrocka

Załączniki do zarządzenia:

1. Polityka Ochrony Danych w Centrum Usług Wspólnych w Okonku..... - załącznik 1
2. Polityka Zarządzania Ryzykiem w Centrum Usług Wspólnych w Okonku ..... - załącznik 2
3. Regulamin Ochrony Danych w Centrum Usług Wspólnych w Okonku..... - załącznik 3
4. Wzór oświadczenia pracownika ..... - załącznik 4

Centrum Usług Wspólnych
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP:767-17-04-789 REGON:366052269
tel. 67 2669 145, 67 2669 715

załącznik nr 1
do Zarządzenia Dyrektora Nr 11/2021
z dnia 23.08.2021 roku

Polityka Ochrony Danych Osobowych w Centrum Usług Wspólnych w Okonku

I. Wstęp

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora danych w Centrum Usług Wspólnych w Okonku w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

II. Inwentaryzacja danych

1. Administrator danych osobowych w Centrum Usług Wspólnych w Okonku dokonał inwentaryzacji przetwarzanych danych w formie określenia zbiorów danych. Inwentaryzacja danych ma formę opracowania pisemnego i stanowi dokument pt. „Rejestr zbiorów danych w Centrum Usług Wspólnych w Okonku, cz. I, II".

2. Rejestr zbiorów składa się z dwóch części. W pierwszej części rejestru określono:

1) nazwę zbioru i jego wewnętrznie nadany numer;
2) wykaz aktywów biorących udział w czynnościach przetwarzania danych w zbiorze;
3) podstawę przetwarzania danych wynikającą z art. 6 lub/i art. 9 RODO;
4) decyzja administratora o opracowaniu lub nie opracowaniu rejestru czynności przetwarzania;
5) decyzja administratora o przeprowadzeniu lub nie przeprowadzaniu oceny skutków przetwarzania;
6) cele przetwarzania;
7) rodzaj i zakres danych;
8) odbiorcy danych znajdujących się w zbiorze;
9) opis operacji przetwarzania;
10) czas przechowywania danych.

W drugiej części Rejestru wskazano miejsce lokalizacji zbiorów, w tym zbiorów rozproszonych oraz formy zastosowanych zabezpieczeń fizycznych.

3. Wykaz zbiorów uwzględnia wszystkie dane osobowe, które są przetwarzane przez administratora i ewentualnie przez współadministratorów, które podlegają ochronie ze względu na ryzyko naruszenia praw i wolności osób fizycznych.

4. Administrator danych w celu oszacowania ryzyk przetwarzania danych osobowych dokonał audytu wewnętrznego. Wyniki audytu udokumentowane są w formie pisemnego opracowania w postaci kart, zawierających nazwę zbioru i wykaz aktywów biorących udział w procesie przetwarzania danych w konkretnym zbiorze.

5. W CUW w Okonku została opracowana Polityka Zarządzaniem Ryzykiem w przetwarzaniu danych osobowych, określająca zasady szacowania skali ryzyka i prawdopodobieństwa jego wystąpienia, a tym samym istotności ryzyka.

6. Administrator w uzgodnieniu z Inspektorem Ochrony Danych, opracował karty zawierające analizę ryzyka dla poszczególnych operacji przetwarzania danych szczególnej kategorii.

III. Zapewnienie o przetwarzania danych osobowych zgodnie z prawem.

1. Administrator zapewnia, że:

   1) dane osobowe są przetwarzane legalnie na podstawie art. 6 i 9 RODO;

   2) zakres danych osobowych jest adekwatny do celów przetwarzania, z zachowaniem zasady minimalizacji danych;

   3) Administrator przechowuje dane osobowe przez konkretnie określony czas, z uwzględnieniem zasad określonych w Jednolity rzeczowym wykazie akt, zatwierdzonym przez Archiwum Państwowe w Poznaniu.

   4) wobec osób, których dane są przetwarzane wykonano obowiązek informacyjny (art. 13, 14 RODO) wraz ze wskazaniem im: prawa dostępu do danych osobowych, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, i „bycia zapomnianym";

   5) osoby, których dane osobowe są przetwarzane zostały poinformowane o funkcji IOD i przekazano jego dane kontaktowe;

   6) zapewniono ochronę danych osobowych w przypadku powierzenia danych w postaci umów powierzenia z podmiotami przetwarzającymi (art. 28 RODO).

2. Potwierdzenie przetwarzania danych osobowych zgodnie z prawem znajduje się w kolumnie „Cele przetwarzania" w Rejestrze Zbiorów Danych Osobowych.

3. Wzory klauzul informacyjnych znajdują się w dokumentacji ochrony danych – Klauzule Informacyjne.

IV. Upoważnienia

1. Administrator odpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych w zbiorach papierowych i systemach informatycznych.

2. Imienne upoważnienia umieszczane są w aktach osobowych poszczególnych pracowników.

3. Każda osoba składa pisemne oświadczenie poufności. Oświadczenie o poufności umieszcza się w aktach osobowych pracowników lub dołącza się do umowy powierzenia.

4. Osoba upoważniona może przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa.

5. Upoważnienia nadawane są do zbiorów na wniosek przełożonych osób. Upoważnienia określają zakres operacji na danych.

6. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych, udokumentowanego polecenia administratora w postaci umowy powierzenia.

7. Administrator prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych w formie dokumentu – Ewidencja osób upoważnionych do przetwarzania danych osobowych.

V. Procedura analizy ryzyka i ocena skutków

1. Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń.

2. Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru danych osobowych lub grupy zbiorów charakteryzujących się podobieństwem celów i sposobów przetwarzania.

3. W przypadku konieczności przeprowadzenia oceny skutków (art. 35) wykonano następujących czynności:

    1) dokonano opisu planowanych operacji przetwarzania i celów przetwarzania – opracowanie w dokumencie – Rejestr zbiorów danych osobowych;
    2) określono zagrożenia we wszystkich aktywach biorących udział w procesie przetwarzania;
    3) dokonano oceny ryzyk, zgodnie z zasadami wskazanymi w Polityce Zarządzania Ryzykiem;
    4) sporządzono mapę ryzyk ze wskazaniem istotności ryzyka;
    5) zaplanowano środki techniczne, organizacyjne i informatyczne dla ryzyk przekraczających istotność powyżej 4.

VI. Instrukcja postępowania z incydentami

Instrukcja definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego lub Inspektora Ochrony Danych.

2. Do typowych podatności bezpieczeństwa danych osobowych należą:

   1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
   2) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed zainfekowaniem, kradzieżą i utratą danych osobowych;
   3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

3. Do typowych incydentów niebezpieczeństwa danych osobowych należą:

   1) zdarzenia losowe zewnętrzne (pożar obiektu / pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
   2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych);
   3) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych / sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów / danych, działanie wirusów i innego szkodliwego oprogramowania).

4. W przypadku stwierdzenia wystąpienia incydentu, Administrator lub IOD prowadzi postępowanie wyjaśniające w toku, którego:

   1) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki;
   2) proponuje ewentualne działania dyscyplinarne;
   3) proponuje działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu;
   4) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.

5. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze – dokument: Formularz rejestracji incydentu.

6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.

7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.

VII. Regulamin Ochrony Danych

Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania – załącznik 3 do Zarządzenia Dyrektora z dnia 23.08.2021 roku – Regulamin Ochrony Danych Osobowych.

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania – załącznik 4 do Zarządzenia Dyrektora Nr 11/2021 z dnia 23.08.2021 roku – Oświadczenie poufności.

VIII. Procedura przywracania dostępności danych osobowych

Zgodnie z art. 32 RODO, Administrator powinien zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. Administrator opracował Procedury Przywracania Danych – dokument: „Plan ciągłości działania".

IX. Wykaz zabezpieczeń

1. Administrator prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych dokument: Wykaz zabezpieczeń.
2. W wykazie wskazano stosowane zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne, informatyczne i organizacyjne dokument: Wykaz zabezpieczeń.
3. Wykaz jest aktualizowany.

X. Szkolenia

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu i zapoznana z przepisami RODO.
2. Za przeprowadzenie szkolenia odpowiada Administrator danych.
3. Administrator dokonał szkolenia wszystkich pracowników CUW w formie e-szkolenia.
4. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.
5. Zgodnie z art. 32 RODO, Administrator zobowiązuje się regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

DYREKTOR
Centrum Usług Wspólnych
w Okonku
Renata Zabrocka

Okonek, 23.08.2021 rok

.....
(podpis Administratora)

Centrum Usług Wspólnych
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP:767-17-04-789 REGON:366052269
tel. 67 2669 145, 67 2669 715

załącznik nr 2
do Zarządzenia Dyrektora Nr 11/2021
z dnia 23.08.2021 roku

Polityka Zarządzania Ryzykiem

w procesie przetwarzania danych osobowych

w Centrum Usług Wspólnych w Okonku

Rozdział 1
Postanowienia ogólne

§ 1.1. Ilekroć w dokumencie jest mowa o:

1) **administratorze danych** – należy przez to rozumieć Dyrektora Centrum Usług Wspólnych

2) **aktywach** – należy przez to rozumieć środki materialne i niematerialne mające wpływ na przetwarzanie danych;

3) **proces przetwarzania danych** – zespół operacji (czynności) wykonywanych na danych osobowych lub zestawach danych w celu określonego celu przetwarzania;

4) **operacji przetwarzania danych** – należy przez to rozumieć każdą czynność wykonywaną na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka, jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adoptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawniane poprzez wysłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

5) **ryzyku** – należy przez to rozumieć możliwość zaistnienia zdarzenia, które będzie miało wpływ na realizację założonych celów w zakresie ochrony danych osobowych. Ryzyko mierzone jest siłą skutku oddziaływania oraz prawdopodobieństwem jego wystąpienia;

6) **zarządzanie ryzykiem** – należy przez to rozumieć realizowany przez administratora danych osobowych proces, którego celem jest identyfikacja potencjalnych ryzyk, które mogą mieć wpływ na realizację celów i zadań jednostki;

7) **mapa ryzyka** – tabela (macierz) odzwierciedlająca ocenę siły oddziaływania i prawdopodobieństwo wystąpienia zidentyfikowanego ryzyka w placówce;

8) **ocena ryzyka** – należy przez to rozumieć czynność polegającą na porównaniu wyników uzyskanych podczas analizy ryzyka z kryteriami oceny ryzyka określonymi na etapie projektowania systemu bezpieczeństwa danych;

9) **kryteriach akceptacji ryzyka** – są to kryteria, które określają dopuszczalność ryzyka, zdefiniowane poprzez wartość progową. Akceptowaną wartością jest ryzyko tylko w zakresie 0 - 4, przy przyjętych 5 – stopniowych skalach szacowania prawdopodobieństwa wystąpienia ryzyka i jego skutków;

10) **rejestr ryzyk** – należy przez to rozumieć dokument odzwierciedlający przeprowadzoną identyfikację i analizę ryzyk, a także przyjętą reakcję na ryzyko;

11) **bezpieczeństwie informacji** – zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;

12) **zdarzeniu związanym z bezpieczeństwem danych** – 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 danych;

13) **incydencie** związanym z bezpieczeństwem danych – jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem danych osobowych, które stwarzają znaczne zakłócenia zadań i zagrażają bezpieczeństwu danych;

14) **zagrożeniu** – to wszystkie niekorzystne czynniki mogące przyczynić się w trakcie pracy z danymi osobowymi do wystąpienia incydentu, mogącego mieć wpływ na ich ujawnienie bądź utratę;

15) **podatność** – słabość, która może być wykorzystana przez zagrożenie, powodując niekorzystne skutki;

16) **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;

17) **integralności** – należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony;

18) **poufności** — należy przez to rozumieć właściwość określającą, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym;

19) **informatycznym nośniku danych** — należy przez to rozumieć materiał służący do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej;

20) **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.

Celem analizy ryzyka jest zastosowanie środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku wynikającemu z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

§ 2.1. Polityka zarządzania ryzykiem w zakresie ochrony danych osobowych, zwana dalej „Polityką zarządzania ryzykiem", obejmuje:

1) zakres zadań i obowiązków podmiotów uczestniczących w procesie zarządzania ryzykiem;
2) zasady i tryb identyfikacji ryzyka;
3) zasady i tryb dokonywania analizy ryzyka;
4) zasady określania właściwej reakcji na ryzyko.

§ 3.1. Polityka zarządzania ryzykiem ma zastosowanie dla wszystkich czynności przetwarzania danych szczególnej kategorii lub danych, których ujawnienie narusza prawa i wolność osób, których dane osobowe administrator przetwarza.

§ 4. Zarządzanie ryzykiem jest procesem ciągłym i nie ogranicza się do działań określonych w § 2 ust. 1. Analizę ryzyka dokonuje się po każdym incydencie naruszenia bezpieczeństwa danych.

§ 5. Celem zarządzania ryzykiem jest zwiększenie prawdopodobieństwa osiągnięcia wyznaczonych celów i zadań w zakresie ochrony danych osobowych, poprzez ograniczenie prawdopodobieństwa wystąpienia ryzyka oraz zabezpieczanie się przed jego skutkami. Następuje to poprzez:

1) rozpoznanie – czyli identyfikowanie ryzyka, określenie rodzajów ryzyk, które wiążą się z działalnością placówki w zakresie ochrony danych osobowych i dokonywanie ich pomiaru;

2) ocenę ryzyka i jego istotności, przy pomocy skali określonej w § 8;

3) zarządzanie ryzykiem, które polega na badaniu efektywności i skuteczności podejmowanych działań, poprzez system kontroli instytucjonalnej i zewnętrznej;

4) kontrolę zarządzania ryzykiem, której istotą podjętych działań jest ocena zastosowanych metod redukcji ryzyka, prowadząca do skutecznego i efektywnego realizowania celów i nałożonych zadań.

Rozdział 2
Zakresy zadań i obowiązków

§ 6.1. Za realizację polityki zarządzania ryzykiem odpowiada Dyrektor CUW, który pełni funkcję administratora danych, poprzez:

1) kształtowanie i wdrażanie polityki zarządzania ryzykiem;
2) nadzór i monitorowanie skuteczności procesu zarządzania ryzykiem;
3) wyznaczanie poziomu akceptowalnego dla każdego ryzyka;
4) podejmowanie decyzji dotyczących sposobu reakcji na poszczególne ryzyka.

2. Pracownicy na samodzielnych stanowiskach odpowiadają za zarządzanie ryzykiem poprzez:

1) identyfikację ryzyk związanych z realizacją przydzielonych zadań w zakresie ochrony danych osobowych;
2) wskazywanie właścicieli zidentyfikowanych ryzyk;
3) przeprowadzanie analizy zidentyfikowanego ryzyka we współpracy z IOD;
4) proponowanie sposobu postępowania w odniesieniu do poszczególnych ryzyk;
5) wdrażanie działań zaradczych w stosunku do zidentyfikowanego ryzyka.

3. Pracownicy wymienieni w ust. 2 są zobowiązani do współpracy z administratorem danych i Inspektorem Ochrony Danych.

Rozdział 3
Identyfikacja ryzyka

§ 7.1. Identyfikacja ryzyka prowadzona jest dla wszystkich zbiorów danych zawierających dane osobowe szczególnej kategorii oraz dane istotne ze względu na ochronę praw i wolności osób fizycznych, z uwzględnieniem zagrożeń w poszczególnych aktywach biorących udział w procesie przetwarzania danego zbioru. Wyniki identyfikacji ryzyk w poszczególnych zbiorach rejestruje się na kartach, których wzór stanowi załącznik nr 1 do polityki.

2. W procesie identyfikacji ryzyka uwzględnia się zagrożenia. Ze względu na ich źródło ryzyka dzielą się na:

1) zewnętrzne – rodzaj ryzyka determinowanego przez czynniki zewnętrzne;
2) wewnętrzne – ryzyko to obejmuje działania wewnętrzne placówki i może być zarządzane wewnątrz jednostki.

3. Każde zidentyfikowane ryzyko ujmuje się w rejestrze, stanowiącym załącznik nr 2 do Polityki Zarządzania Ryzykiem. Załącznik nr 2 podlega ciągłej aktualizacji.

4. Dla każdego zidentyfikowanego ryzyka ustala się jego właściciela.

5. Każdy pracownik ma prawo i obowiązek zgłaszania swojemu bezpośredniemu przełożonemu ryzyk zidentyfikowanych podczas wykonywania przydzielonych zadań w zakresie ochrony danych osobowych.

Rozdział 4
Analiza ryzyka

§ 8. 1. Każde ryzyko w zakresie ochrony danych osobowych podlega analizie pod kątem jego istotności na osiąganie celów i zadań. Istotność ryzyka jest iloczynem skali prawdopodobieństwa jego wystąpienia i wartości oszacowanych potencjalnych skutków.

2. Każde ryzyko jest oceniane pod względem prawdopodobieństwa jego wystąpienia i skutku oddziaływania.

3. W celu dokonania oceny ryzyka wykorzystuje się Mapę Ryzyka, którą stanowi macierz prawdopodobieństwo – skutek – załącznik nr 3 do Polityki Zarządzania Ryzykiem.

4. Mapa ryzyka definiuje ryzyka na:

1) niskie o wartości 4 i mniejszej;
2) średnie o wartości powyżej 4 i mniejszej niż 9;
3) wysokie – o wartości powyżej 9 i mniejszej niż 16.
4) katastrofalne – o wartości powyżej 16.

5. Przy ocenie prawdopodobnych skutków wystąpienia ryzyka przyjmuje się skalę punktową od 1 do 5, gdzie;

1) 1 – oznacza skutek nieznaczny;
2) 2 – oznacza skutek mały;
3) 3 – oznacza skutek średni;
4) 4 – oznacza skutek poważny;
5) 5 – oznacza skutek katastrofalny.

6. Przy ocenie prawdopodobieństwa wystąpienia ryzyka przyjmuje się skalę punktową od 1 do 5, gdzie:

1) 1 – oznacza prawdopodobieństwo rzadkie (0-20 %);
2) 2 – oznacza prawdopodobieństwo małe (21 - 40%);
3) 3 – oznacza prawdopodobieństwo możliwe(41 - 60 %);
4) 4 – oznacza prawdopodobieństwo prawdopodobne(61 - 80 %);
5) 5 – oznacza prawdopodobieństwo prawie pewne (81 -100 %).

7. Wskaźniki do punktacji oceny prawdopodobieństwa i skutków ryzyka określa załącznik nr 4.

Rozdział 5
Reakcja na ryzyko

§ 9. Dla każdego istotnego zidentyfikowanego ryzyka właściciel ryzyka wskazuje optymalną reakcję. Przyjmuje się niżej wymienione reakcje na ryzyko:

1) tolerowanie – będzie to miało miejsce w przypadkach, kiedy koszty skutecznego przeciwdziałania ryzyku mogą przekraczać jego potencjalne korzyści, z zdolności do skutecznego przeciwdziałania są ograniczone lub wykraczające poza decyzje i działania wewnętrzne;

2) przeniesienie – dotyczyć to będzie kategorii ryzyk w odniesieniu do których nastąpi przeniesienie ich na inna instytucję, między innymi poprzez ubezpieczenie lub zlecenie usług na zewnątrz;

3) wycofanie się – dotyczyć to będzie grypy ryzyk dla których mimo podejmowanych działań nie udało się zmniejszyć ich istotności do akceptowanego poziomu;

4) przeciwdziałanie – dotyczyć to będzie kategorii ryzyk, które wymagać będą podjęcia zdecydowanych, przemyślanych i zaplanowanych działań prowadzących do ich likwidacji, lub znacznego ograniczenia.

Rozdział 6
Postanowienia końcowe.

§ 10.1. Strategia zarządzania ryzykiem obowiązuje od 23.08.2021 roku.

2. Pracownicy CUW obowiązani są do systematycznej analizy wystąpienia ryzyk na stanowiskach pracy i zgłaszania ich dyrektorowi CUW.

DYREKTOR
Centrum Usług Wspólnych
w Głogówku
Renata Zabrocka

.....
/administrator danych/

Załączniki do Polityki Zarządzania Ryzykiem:

1. *Załącznik nr 1 – Rejestr ryzyk w procesie przetwarzania danych osobowych w Centrum Usług Wspólnych w Okonku*

2. *Załącznik nr 2 – Rejestr potencjalnych ryzyk w procesie przetwarzania w poszczególnych zbiorach z uwzględnieniem aktywów biorących udział w procesie przetwarzania – wzór dokumentu.*

3. *Załącznik nr 3 – Mapa ryzyka/macierz – wzór dokumentu.*

4. *Załącznik nr 4 – Wskaźniki do szacowania prawdopodobieństwa i skutków.*

Centrum Usług Wspólnych
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP:767-17-04-789 REGON:366052269
tel. 67 2669 145, 67 2669 715

Załącznik nr 1
do Polityki Zarządzania Ryzykiem

Rejestr potencjalnych ryzyk w procesie przetwarzania danych osobowych w Centrum Usług Wspólnych w Okonku

ATAKI ZEWNĘTRZNE	
1.	**Ataki socjotechniczne**
Zagrożenie	**Opis**
phishing	mail z prośbą o zalogowanie się do „podróbki" strony, np. bankowe i w rezultacie przejęcie hasła.
cybersquatting	zachęcanie do zalogowania się do podrobionej strony o „wiarygodnym" adresie www.
wyłudzanie informacji	▪ maile od „przełożonych" do księgowego z dyspozycją wykonania przelewu, ▪ faxy, w których intruz podszywa się pod dostawcę i informuje o zmianie numeru konta bankowego, ▪ maile lub rozmowy tel., w których intruz podaje się np. za pracownika firmy dostarczającej oprogramowanie i prosi o hasło w celu „przetestowania uprawnień".
nakłanianie do wykonania czynności	maile, które zachęcają lub „zmuszają" do otwarcia załączników.
ataki telefoniczne	▪ intruz przedstawia się jako pracownik dostawcy łącza naprawiający usterkę i prosi o uruchomienie określonej strony internetowej, ▪ intruz przedstawia się jako inżynier lub programista dostawcy oprogramowania w celu np. przesłania „aktualizacji" lub prosi o udostępnienie pulpitu.
złośliwe oprogramowanie	▪ oprogramowanie szyfrujące pliki, ▪ oprogramowanie przechwytujące dane, ▪ trojany.

2.	Ataki na infrastrukturę
Zagrożenie	**Opis**
łamanie i pozyskiwanie haseł	▪ łamanie haseł, ▪ przechowywanie haseł na karteczkach, ▪ włamania do urządzeń nieaktualizowanych, ▪ odgadywanie zbyt słabych, najpopularniejszych haseł np. 123456789, ▪ stosowanie domyślnych haseł producenta i brak jego zamiany po pierwszym logowaniu, ▪ posiłkowanie się jednym hasłem do wielu systemów, programów, ▪ niezmieniane hasła, nawet po incydencie, ▪ włamania do urządzeń nieodpowiednio skonfigurowanych, ▪ włamania z użyciem niezabezpieczonych interfejsów lokalnych, włamania za pośrednictwem niepotrzebnych usług (np. telnet na routerze).
ataki na sprzęt	▪ włamania do urządzeń nieodpowiednio skonfigurowanych, ▪ włamania z użyciem niezabezpieczonych interfejsów lokalnych, ▪ włamania za pośrednictwem niepotrzebnych usług (np. telnet na routerze).
ataki na oprogramowanie	▪ wykorzystanie znanych atakującemu dziur w nieaktualizowanym oprogramowaniu, ▪ włamania z wykorzystaniem domyślnych haseł (łatwe hasła), ▪ włamania z wykorzystaniem najczęstszych błędów, ▪ włamania z wykorzystaniem API (interfejsów programistycznych).
skanowanie sieci i usług	atakujący poznaje wersję systemu operacyjnego lub wersję serwera www, a przez to potem może dobrać skuteczny atak
nielegalne wpięcie się do sieci (wifi, telefon, internet)	łatwo dostępne gniazdka sieciowe, gdzie atakujący może się podłączyć np. z własnym urządzeniem i za jego pomocą przeglądać zasoby sieci (możliwość podpięcia się np. pod drukarkę na korytarzu lub do gniazdka w świetlicy).
eskalacja uprawnień	▪ zwiększenie uprawnień użytkownika przez wykorzystanie błędów programistycznych, ▪ przejęcie uprawnień użytkownika zaawansowanego, ▪ przejęcie uprawnień administratora, ▪ przejęcie uprawnień systemowych, ▪ przejęcie certyfikatów elektronicznych.
DOS	zmasowany atak na stronę www, aby ją przeciążyć i „zakorkować".
DDOS	zmasowany atak komputerów-zombie na zlecenie atakującego na stronę www, aby ją przeciążyć i „zakorkować".

ataki tzn. "Man in the middle"	przejęcie komputera w placówce w celu włamania do sieci (w rezultacie możliwość przejęcia haseł).

3.	Zagrożenia dla sprzętu

Zagrożenie	Opis
włamanie do obiektów	może skutkować zainstalowaniem nieautoryzowanych urządzeń.
kradzież / zniszczenie sprzętu	kradzież komputerów w organizacji i laptopów poza nią, uszkodzenie sprzętu na skutek przepięcia, czy upadku.
pożar / eksplozja	pożar serwerowni, wybuch gazów technicznych.
zalanie	np. powódź, pęknięta rura kanalizacyjna, zalanie kawą.
przegrzanie	wysoka temperatura urządzeń lub w serwerowni.
awaria zasilania	skoki napięcia / przerwy w dostawie.
awaria sprzętu	awaria dysków, modułów, płyty głównej, sterowników, routerów.
starzenie się nośników danych	zbyt długie eksploatowanie nośników danych może powodować ryzyko utraty zawartości.

ZAGROŻENIA DANYCH	
Zagrożenie	**Opis**
Nieuprawniony dostęp	nadanie zbyt wysokich uprawnień użytkownikom lub brak kontroli nad dostępem do plików, baz, komputerów.
kradzież tożsamości	przejęcie poczty, pozyskanie danych z dowodu osobistego i w rezultacie np. założenie firmy „słupa", wyłudzenie kredytu, zakupy na cudze konto.
nieuprawniona modyfikacja / usunięcie	▪ niezamierzona lub w efekcie pomyłki, ▪ sfałszowanie danych przez osoby z wewnątrz lub zewnątrz placówki.

nieuprawnione kopiowanie danych	▪ kopiowanie danych z katalogów, dysków, baz, programów, kserowanie i robienie zdjęć przez pracownika lub przez osobę obcą.
kradzież danych lub nośników	na zewnątrz i wewnątrz placówki.
utrata / kradzież danych dostępowych	haseł, kluczy, certyfikatów.
błąd / awaria oprogramowania	uszkodzenie bazy danych, programu kadrowo-płacowego.
brak / błędy w wykonywaniu kopii bezpieczeństwa	doraźne lub zbyt rzadkie wykonywanie kopii, błędy podczas procesu wykonywania kopii, kopie dostępne w sieci lub archiwum bez zabezpieczeń.
udostępnianie danych osobom nieupoważnionym	upublicznienie danych w przestrzeni publicznej, dostęp przez internet, przesłanie lub wydawanie informacji osobie nieupoważnionej, wyrzucanie na śmietnik.
nieprawidłowe / brak procedur niszczenia nośników z danymi	wyrzucenie uszkodzonych nośników bez ich zniszczenia, wyrzucenie niezniszczonych pendrive, DVD, CD.
nieprawidłowe / brak procedur napraw w serwisach zewnętrznych	naprawa sprzętu z nośnikami w serwisie bez standardu bezpiecznej naprawy i bez umowy bezpieczeństwa.
korzystanie z nielicencjonowanego/ nielegalnego oprogramowania	wykorzystywanie nielegalnych, kradzionych, nielicencjonowanych aplikacji i oprogramowania.
BŁĘDY LUDZKIE	
Zagrożenie	**Opis**
nieprzestrzeganie procedur	świadome naruszenie pisemnych lub ustnych procedur, np. niewylogowanie się z systemu, przekazywanie haseł koledze, pozostawienie haseł na karteczce przy komputerze.

pomyłki administratorów, użytkowników	pomyłkowe udostępnienie, wysłanie do złego odbiorcy, błędne zabezpieczenia.
brak świadomości / wiedzy	braki wiedzy, nieszkolony personel, brak procedury niszczenia nośników danych.
błędy projektowe / konfiguracyjne	błędy programistów prowadzące do niewłaściwego przetwarzania danych, niezabezpieczenie danych w bazie www przed indeksacją.
ZAGROŻENIA CIĄGŁOŚCI DZIAŁANIA	
Zagrożenie	**Opis**
brak aktualnej dokumentacji	brak instrukcji, opisów, dokumentacji technicznej sprzętu i oprogramowania utrudnia przywracanie środowiska i zarządzanie nim, gdy np. odejdzie pracownik IT.
nieprawidłowe / brak umowy o współpracy	brak zapisów przenoszących odpowiedzialność na zleceniobiorcę lub podmiot przetwarzający dane.
nieprawidłowe / brak umowy gwarancyjnej lub wsparcia serwisowego	niewłaściwie skonstruowane umowy, nieprzedłużane umowy, zbyt długi czas reakcji serwisu na awarie.
upadek firmy współpracującej np. dostawcy oprogramowania/serwera	ryzyko braku zastępstw, np. dla hostingodawcy poczty, dla wsparcia do zakupionej aplikacji lub oprogramowania.
awaria łączy telekomunikacyjnych	awaria jest krytyczna w przypadku usług chmurowych.

Centrum Usług Wspólnych
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP:767-17-04-789 REGON:366052269
tel. 67 2669 145, 67 2669 715

Załącznik nr 2
do Polityki Zarządzania Ryzykiem

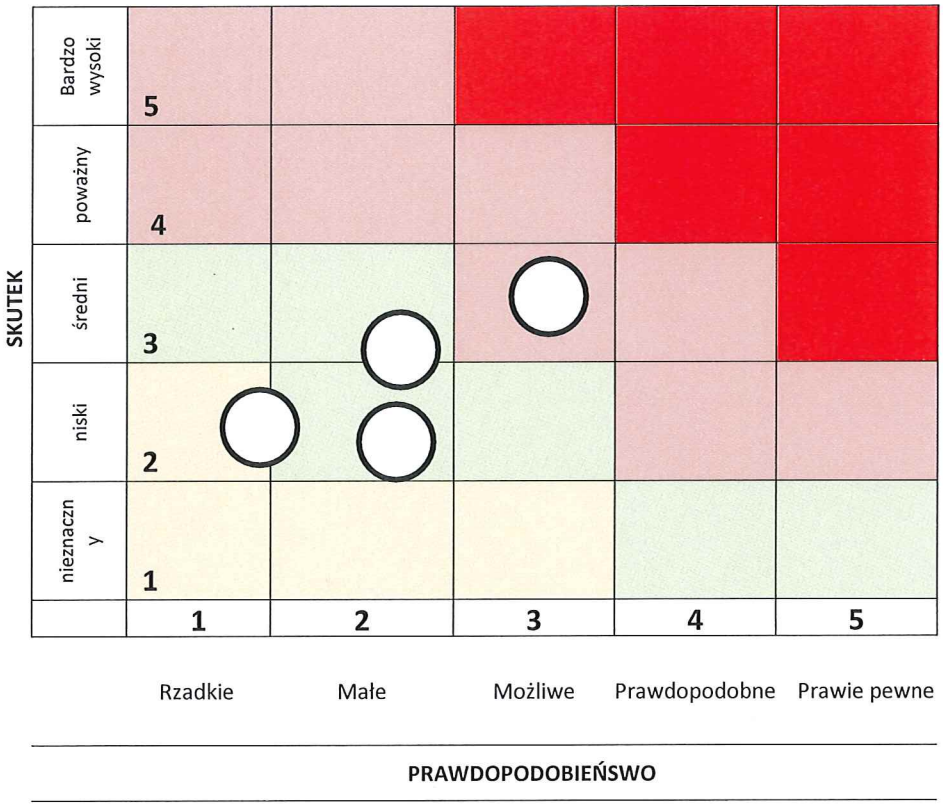
Rejestr ryzyk w procesie przetwarzania w poszczególnych zbiorach z uwzględnieniem sposobów zabezpieczeń – *wzór dokumentu*

Lp.	Zagrożenie	Opis zagrożenia	Zabezpieczenia	Prawdopodobieństwo (w skali od 1-5)	Skutek (w skali od 1-5)	Istotność ryzyka (P x S)	Reakcja na ryzyko
1.	**Zagrożenie danych**	1. Przesłanie maila z danymi osobowymi do osób nieuprawnionych					
		2. Udostępnianie danych (baz i plików) przez internet bez logowania					
		3. Przekazanie danych osobom nieuprawnionym, w tym współpracownikom, podmiotom kontrolującym, interesantom w formie bezpośredniej / telefonicznie lub drogą mailową					

Centrum Usług Wspólnych
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP:767-17-04-789 REGON:366052269
tel. 67 2669 145, 67 2669 715

Załącznik nr 3
do Polityki Zarządzania Ryzykiem

Mapa ryzyka/macierz – wzór dokumentu



Ocena istotności ryzyka

Oznaczenie poziomu	Opis działania
Niski	działania podejmowane w zależności od wymaganych nakładów
średni	działanie może zostać przesunięte w czasie, ale wymaga okresowego monitorowania
wysoki	działanie może zostać przesunięte w czasie, ale wymaga stałego monitorowania
katastrofalny	**wymaga natychmiastowego działania**

Centrum Usług Wspólnych
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP:767-17-04-789 REGON:366052269
tel. 67 2669 145, 67 2669 715

Załącznik nr 4
do Polityki Zarządzania Ryzykiem

Wskaźniki do szacowania prawdopodobieństwa i skutków

Skala prawdopodobieństwa wystąpienia ryzyka

Skala znaczenia ryzyka (oddziaływanie - skutek)

Opis prawdopodobieństwa wystąpienia	Oszacowane ryzyko	Opis oddziaływania (skutków)	Oszacowane ryzyko
Ryzyko nie występuje lub może wystąpić w zupełnie wyjątkowych sytuacjach. Przetwarzanie danych i jego zakresu określają zewnętrzne regulacje prawne. Przy przetwarzaniu danych współpracuje się z jednym bądź dwiema komórkami organizacyjnymi. Oprogramowanie wystandaryzowane i wykorzystywane powyżej roku od wprowadzenia. Nie wprowadzono w ostatnim roku zmian technologicznych, organizacyjnych i kadrowych.	**1** rzadkie	Organizacyjne: Niska niezgodność z procedurami / przepisami prawa. Nie występuje zagrożenie utraty dobrego wizerunku. Ewentualne zakłócenia bez wpływu na realizację zadań i osiąganie celów. Ewentualne skutki ograniczane (neutralizowane) przez istniejące procedury. Finansowe: Nie przewiduje się wystąpienia straty finansowej, dodatkowych kosztów - bądź nieznaczne do 1 000 zł.	**1** nieznaczne
Ryzyko prawdopodobnie nie wystąpi. Przy realizacji zadań w ramach danego obszaru / procesu współpracuje się z małą (ograniczoną) liczbą komórek organizacyjnych. W ostatnim okresie (np. 1 rok) obszar / proces nie podlegał zmianom technologicznym, organizacyjnym i kadrowym, bądź podlegał zmianom w minimalnym stopniu i uznaje się je za wdrożone. Obszar / proces w małym zakresie objęty regulacjami o charakterze zewnętrznym. Nie podlegały one zmianom. Niepożądane zakłócenia mogą powodować utrudnienia w realizacji zadań. Potencjalne zakłócenia wykonywania zadań nie mają wpływu na realizację celów.	**2** mało prawdopodobne	Organizacyjne: Średnia niezgodność z procedurami lub niska niezgodność z postanowieniami umów. Małe zakłócenia pracy, ewentualne utrudnienia w realizacji zadań, nie mające wpływu na osiąganie celów. Istniejące mechanizmy kontrolne powinny ograniczyć skutki ewentualnych zakłóceń. Małe zagrożenie utraty dobrego wizerunku. Finansowe: >1 000 do 5 000 zł	**2** niski
Ryzyko prawdopodobnie wystąpi w najbliższym okresie (od roku do pięciu lat). Przy realizacji zadań w ramach danego	**3** możliwe	Organizacyjne: Niska niezgodność z przepisami prawa lub średnia niezgodność z postanowieniami umów lub	**3** średnie

obszaru / procesu współpracuje się z innymi komórkami, bądź z podmiotami zewnętrznymi. W ciągu ostatniego roku obszar / proces podlegał ograniczonym zmianom organizacyjnym, technologicznym i kadrowym. Obszar / proces objęty w małym stopniu regulacjami zewnętrznymi, które mogły podlegać w ostatnim okresie zmianom. Może dotyczyć zadań o istotnym znaczeniu dla celów działalności.		poważna niezgodność z procedurami. Średnie zakłócenia pracy. Potencjalne zagrożenia mogą doprowadzić do niewykonywania podstawowych zadań w określonym zakresie. Istniejące mechanizmy kontrolne tylko w pewnym stopniu mogą ograniczyć skutki ewentualnych zakłóceń. Średnie zagrożenie utraty dobrego wizerunku. Finansowe: > 5 000 do 10 000 zł	
Istnieje duże prawdopodobieństwo na wystąpienie ryzyka w ciągu najbliższego okresu od roku do trzech lat. Obszar / proces wymaga współpracy z innymi komórkami bądź z podmiotami zewnętrznymi. W ciągu ostatniego roku obszar / proces podlegał zmianom technologicznym, organizacyjnym i kadrowym, z których część może wymagać poprawek i działań dostosowawczych. Obszar / proces objęty dużą liczbą regulacji prawnych (zewnętrznych i wewnętrznych). Zagrożenia mogą wywierać istotny wpływ na naruszenie praw lub wolności osób fizycznych bezpieczeństwo.	**4** prawdopodobne	Organizacyjne: Średnia niezgodność z przepisami prawa lub poważna niezgodność z postanowieniami umów. Brak szczegółowych procedur dla prowadzonych procesów. Poważne naruszenie zasad przetwarzania. Mogą doprowadzić do utraty bezpieczeństwa przetwarzania danych. Niska skuteczność istniejących mechanizmów kontrolnych. Wysokie zagrożenie utraty dobrego wizerunku. Finansowe: > 10 000 do 50 000 zł.	**4** poważne
Ryzyko z pewnością wystąpi w ciągu najbliższego roku. Obszar / proces związany jest z działalnością większej liczby komórek organizacyjnych, wymaga współpracy z podmiotami zewnętrznymi. W ciągu ostatniego roku obszar / proces podlegał istotnym zmianom technologicznym, organizacyjnym i kadrowym / obszar podlega częstym zmianom tego typu / obszar jest w trakcie zmian. Obszar działania / proces uregulowany jest dużą liczbą regulacji prawnych (wewnętrznych i zewnętrznych). Zagrożenia naruszają bezpieczeństwo danych, a przede wszystkich prawa lub wolność osób fizycznych.	**5** prawie pewne	Organizacyjne: Poważna niezgodność z przepisami prawa. Brak procedur dla danego procesu przetwarzania. Zagrożenia spowodują brak zachowania ciągłości procesów działania, utrzymania funkcjonalności systemów niezbędnych do wykonywania podstawowych celów. Niemożność zapewnienie bezpieczeństwa danych. Brak odpowiednich mechanizmów kontrolnych bądź istniejące mechanizmy okazują się nieskuteczne. Bardzo wysokie zagrożenie utratą dobrego wizerunku. Finansowe: > 50 000 zł, utrata znacznego majątku.	**5** bardzo wysoki

Centrum Usług Wspólnych
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP:767-17-04-789 REGON:366052269
tel. 67 2669 145, 67 2669 715

załącznik nr 3
do Zarządzenia Dyrektora Nr 11/2021
z dnia 23.08.2021 roku

Regulamin Ochrony Danych Osobowych w Centrum Usług Wspólnych w Okonku

Spis treści:

Rozdział 1
Postanowienia ogólne

1. Regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych w Centrum Usług Wspólnych w Okonku zgodnie z Rozporządzeniem PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.
2. Regulamin obowiązuje wszystkich pracowników CUW, podmioty przetwarzające dane osobowe na podstawie zawartych umów między przetwarzającym a powierzającym, użytkowników systemów informatycznych z dostępem do danych osobowych upoważnionych przez administratora na piśmie.
3. Każdy z wymienionych podmiotów jest zobowiązany do zapoznania się z dokumentem i bezwzględnego przestrzegania zawartych w nim zasad.
4. Administratorem danych osobowych w Centrum Usług Wspólnych w Okonku jest dyrektor CUW w Okonku.

Rozdział 2
Polityka korzystania z Internetu

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody w infrastrukturze IT spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo ze względu na zainstalowane na nich szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem.
5. Zabrania się w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą W tej sytuacji należy „kliknąć" na ikonę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet.

Rozdział 3
Polityka korzystania z poczty elektronicznej

1. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do korzystania z poczty elektronicznej tylko w celach służbowych.
2. W przypadku przesyłania danych osobowych poza CUW należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych dokumentów lub plików zzipowanych, podpis elektroniczny).
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.
4. Każdy użytkownik przed wysłaniem poczty jest zobowiązany sprawdzić poprawność adresu odbiorcy dokumentu.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. W celu ochrony przed zainfekowaniem komputera użytkownika i komputerów pracujących w sieci (kryptowirusy) zabrania się otwierania załączników (plików) w mailach nawet od prawdopodobnie znanych użytkownikowi nadawców bez weryfikacji nadawcy.

7. Zabrania się, bez weryfikacji wiarygodności nadawcy „klikać" na hiperlinki w mailach. Nieprzestrzeganie tej zasady może doprowadzić do zainfekowania komputera użytkownika i innych pracujących w sieci.

8. Wszystkie przypadki e-maili budzących podejrzenie należy zgłaszać administratorowi sieci.

9. Przy wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości".

10. Zabrania się rozsyłania maili z tzw. „ łańcuszkami szczęścia". Adres mailowy służbowy służy wyłącznie do korespondencji służbowej.

11. Nakazuje się okresowe czyszczenie poczty z nieaktualnych -e- mali i opróżnianie kosza.

12. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.

13. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.

14. Korzystanie z poczty elektronicznej dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.

15. Użytkownicy nie mają prawa korzystać z poczty elektronicznej w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub nietycznym i naruszającym cudzą godność i prywatność.

16. Zabrania się dokonywanie w sieci zakupów, rezerwacji usług lub świadczeń na rzecz użytkownika oraz dokonywania bankowych z prywatnego konta.

17. Użytkownik bez zgody Pracodawcy nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy / Zleceniodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

18. Wszelkie przesyłane dokumentów, opracowania, jak i innych treści przesyłane przez użytkownika podlegają zasadom ochrony prawa autorskiego i prawa własności przemysłowej, które użytkownik jest obowiązany przestrzegać.

Rozdział 4
Polityka użytkowania komputerów przenośnych

1. Każdy Użytkownik komputera przenośnego winien zapoznać się z Regulaminem użytkowania komputerów przenośnych oraz pisemnie zobowiązać się do jego przestrzegania.

2. W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę Pracodawcy, Użytkownik zobowiązany jest do ich przechowywania na dysku szyfrowanym, zabezpieczonym co najmniej 8-znakowym hasłem (duże, małe litery, znaki specjalne lub cyfry).

3. Na komputerach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny, o ile jest to możliwe, znajdować się dane osobowe lub stanowiące tajemnicę Pracodawcy.

4. W przypadku kradzieży lub zgubienia komputera przenośnego, Użytkownik powinien natychmiast powiadomić o tym osobę odpowiedzialną za ochronę danych tj. Administratora Danych lub IOD, zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.

5. Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu, a w szczególności:

   1) zaleca się przenoszenie go w specjalnym futerale;

   2) zabrania się pozostawiania komputera przenośnego w samochodzie podczas postoju w miejscu publicznym bez nadzoru;

   3) podczas jazdy samochodem zaleca się przechowywanie komputera przenośnego pod tylnym siedzeniem kierowcy.

6. W przypadku pozostawiania komputerów przenośnych w szkole zaleca się umieszczanie ich po zakończeniu pracy w zamykanych szafkach.

7. Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze lub na określonych nośnikach (pendrive, CD, DVD). Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych.

8. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, Użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.

Rozdział 5
Polityka wynoszenia nośników z danymi osobowymi poza CUW

1. Użytkownicy nie mogą wynosić poza CUW bez zgody Administratora danych żadnych wymiennych elektronicznych nośników informacji, tj. wymienne twarde dyski, pen-drive, płyty CD, DVD, pamięci typu Flash.

2. W sytuacjach koniecznych, za zgodą Administratora danych, wynoszone nośniki wymienne muszą być zaszyfrowane, a pliki opatrzone hasłem.

3. Zabrania się wynoszenia poza CUW dokumentacji papierowej, zwierającej dane osobowe. W przypadku innej dokumentacji należy ją przenosić w zamykanych teczkach lub w innej bezpiecznej formie.

4. W przypadku przesyłania dokumentacji j/w należy korzystać z zaufanych firm kurierskich, za pokwitowaniem i w opakowaniach gwarantujących niedostępność osób trzecich.

Rozdział 6
Polityka zabezpieczania dokumentacji papierowej z danymi osobowymi

1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. „**Polityki czystego biurka**". Polega ona na zabezpieczaniu (zamykaniu) dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.

2. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach lub utylizacji ich w specjalnych bezpiecznych pojemnikach z przeznaczeniem do bezpiecznej utylizacji.

3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach ogólnodostępnych.

4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np., na terenach publicznych miejskich lub w lesie.

Rozdział 7
Polityka tworzenia kopii zapasowych

1. Zbiory danych osobowych w systemie informatycznych są zabezpieczane przed utratą lub uszkodzeniem za pomocą:

1) urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej, sporządzania kopii zapasowych (kopie pełne).

2. Pełne kopie zapasowe zbiorów danych tworzone są 2 razy w ciągu roku. Kopie systemu kadrowo płacowego całościowe sporządzane są raz w miesiącu, a kopie przyrostowe raz dziennie.

3. W szczególnych sytuacjach, np. przed aktualizacją lub zmianą oprogramowania lub systemu należy wykonać bezwzględnie pełną kopię zapasową systemu.

4. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu. Za przeprowadzenie tych czynności odpowiada informatyk.

5. Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć w sposób uniemożliwiający odczyt danych.

6. Kopie całościowe przechowywane są przez 5 lat a kopie przyrostowe przez 1 miesiąc.

Rozdział 8
Polityka tworzenia kopii dokumentacji serwera

1. Kopie zapasowe dokumentacji serwera tworzone są w sposób zautomatyzowany w oparciu o wykorzystanie programowej funkcji serwera.

2. Kopie bezpieczeństwa sporządzane są także dla dokumentacji gromadzonej na dyskach stacji roboczych użytkowników w wybranym katalogu.

3. Kopie całościowe sporządzane są raz w miesiącu.

4. Kopie sporządzane są na wydzielonym twardym dysku wymiennym na komputerze w pomieszczeniu kadr.

Rozdział 9
Polityka niszczenia danych osobowych na nośnikach elektronicznych

1. W odniesieniu do nośników przenośnych (pen-drive'y) oraz nośników danych zainstalowanych w komponentach informatycznych – złomowanych stosowane są mechanizmy bezpiecznego kasowania informacji:
   1) za pomocą specjalistycznego oprogramowania;
   2) przy użyciu demagnetyzacji;
   3) poprzez fizyczne niszczenie (pocięcie, spalenie) nośników.
2. Wyznaczony administrator dokonuje kontroli prawidłowości usunięcia informacji.
3. Nośniki usuwalne, które nie mogą być ponownie wykorzystane, są niszczone.
4. Za właściwe skasowanie informacji zawartej na nośniku przenośnym lub w pamięci masowej stacji roboczej odpowiada użytkownik.
5. Za kasowanie informacji z pamięci masowych serwerów oraz nośników kopii archiwalnych i zapasowych odpowiada administrator danych.
6. Niszczenie nośnika zostaje odnotowane w protokole zniszczenia.

Rozdział 10
Polityka niszczenia danych na nośnikach papierowych

Dokumentacja papierowa niszczona jest w niszczarkach paskowych oraz w niszczarkach o podwyższonym standardzie.

Rozdział 11
Polityka napraw sprzętu IT w serwisach zewnętrznych

1. Komputery przeznaczone do naprawy należy wysyłać bez dysków a urządzenia mobilne bez kart pamięci.
2. W przypadku naprawy sprzętu z danymi osobowymi na nośniku należy je wpierw trwale usunąć z użyciem specjalistycznego oprogramowania.
3. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest zawarcie specjalnego zapisu w umowie serwisowej, gwarantującego bezpieczną naprawę (należy na to zwrócić uwagę przy zakupach sprzętu).
4. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest przekazywanie do naprawy uszkodzonego sprzętu z danymi zaszyfrowanymi na dysku / karcie pamięci. Sprzęt przekazywany jest do serwisu bez podawania hasła.
5. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw u klienta (umowy gwarancyjne on-site).

Rozdział 12
Postępowanie dyscyplinarne

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.

2. Postępowanie sprzeczne z powyższymi zasadami może też być uznane przez Pracodawcę za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.

Centrum Usług Wspólnych
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP:767-17-04-789 REGON:366052269
tel. 67 2669 145, 67 2669 715

Okonek, 23.08.2021 r.

.....

DYREKTOR
Centrum Usług Wspólnych
w Okonku
Renata Zabrocka

Centrum Usług Wspólnych
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP:767-17-04-789 REGON:366052269
tel. 67 2669 145, 67 2669 715

załącznik nr 4
do Zarządzenia Dyrektora Nr 11/2021
z dnia 23.08.2021 roku

OŚWIADCZENIE PRACOWNIKA – *wzór*

....., dn. .....

.....
(imię i nazwisko pracownika)

OŚWIADCZENIE O POUFNOŚCI

1. Oświadczam, że:

   1) zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, a w szczególności z treścią ogólnego Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r. oraz ustawy o Ochronie Danych Osobowych;

   2) zapoznano mnie z „Regulaminem Ochrony Danych Osobowych", obowiązującym w .....;

2. Zobowiązuję się do:

   1) przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora obowiązkach;
   2) nieujawniania danych zawartych w zbiorach danych, do których uzyskalam/em dostęp za upoważnieniem administratora danych;
   3) nieujawniania sposobów zabezpieczeń danych osobowych przetwarzanych wszkole;
   4) wykonywania operacji przetwarzania danych, zgodnie z Regulaminem Ochrony Danych Osobowych;
   5) zabezpieczenia tych danych przed dostępem osób nieupoważnionych;
   6) ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem;
   7) zgłaszania incydentów naruszenia zasad ochrony danych osobowych Inspektorowi Ochrony Danych lub bezpośredniemu przełożonemu.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Administratora za naruszenie przepisów Ustawy o Ochronie Danych osobowych oraz Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.

.....
(data, miejscowość)

.....
(podpis pracownika)

UPOWAŻNIENIE DLA PRACOWNIKÓW ADMINISTRACJI – KADRY, KSIĘGOWOŚĆ

Centrum Usług Wspólnych
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP:767-17-04-789 REGON:366052269
tel. [illegible]569 715

.....
(pieczęć CUW)

.....
(miejscowość)

UPOWAŻNIENIE NR ..... /2021

Administrator danych osobowych w Centrum Usług Wspólnych w Okonku na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dziennik Urzędowy UE - 4.5.2016 L 119/3)

upoważnia

Pana/Panią ..... do przetwarzania danych osobowych w zbiorach ....., zgodnie z zakresem Pana/Pani obowiązków na stanowisku pracy oraz poleceniami administratora.

Upoważnienie dotyczy przetwarzania danych osobowych **w systemach informatycznych:**

..... podać nazwy systemów lub programów..... .

Upoważnienie dotyczy przetwarzania danych osobowych w zbiorach papierowych:

.....podać nazwy tych zbiorów..... .

Jednocześnie zobowiązuję Pana/Panią do zachowania w tajemnicy informacji z którymi zapoznała się Pan/Pani wykonując obowiązki służbowe.

Pouczenie:

Naruszenie obowiązków w zakresie ochrony danych osobowych skutkuje przewidzianymi karami w art. 52 §1 pkt 1, art. 101 §1 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy (*tekst jedn.: Dz.U. z 2018 r., poz. 108),* art. 101 - 102 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (*Dz. U. z 2018 r, poz. 1000).*

Upoważnienie ważne od dnia ..... do dnia ..... / do odwołania

.....
(data i podpis upoważnionego)

.....
(podpis administratora danych)

Centrum Usług Wspólnych
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP:767-17-04-789 REGON:366052269
tel. 67 2669 145, 67 2669 715

EWIDENCJI OSÓB ZATRUDNIONYCH PRZY PRZETWARZANIU DANYCH OSOBOWYCH

L.p.	Imię i nazwisko	Stanowisko	Nr upoważnienia	Nr zbioru, do kórego jest upoważnienie	Data nadania upoważnienia	Data ustania upoważnienia

.....
Administrator danych osobowych

Centrum Usług Wspólnych
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP:767-17-04-789 REGON:366052269
tel. 67 2669 145, 67 2669 715

ARKUSZ ANALIZY RYZYKA I MAPA RYZYK

Dotyczy szacowania ryzyka w zbiorach: Pracownicy, Monitoring

Analiza dotyczy ryzyk w zbiorach wymagających jej przeprowadzenia, zgodnie z *Rejestrem zbiorów z kategorią danych osobowych* tj. Pracownicy, Monitoring.

Udokumentowane poniżej czynności identyfikacji oraz analizy ryzyka zawierają zestawienie wszystkich ryzyk istniejących w procesach przetwarzania danych osobowych w placówce.

W związku z faktem, że dane we wszystkich wymienionych zbiorach przetwarzane są przez te same aktywa (pracownicy, sprzęt, oprogramowanie, infrastruktura placówki) to są one obarczone tymi samymi ryzykami, których prawdopodobieństwo wystąpienia oraz skutki są również wspólne.

Zdefiniowane ryzyka dla w/w zbiorów:

1. **Nieuprawnione ujawnienie danych.**
2. **Nieuprawniony dostęp do danych osobowych podczas przesyłania.**
3. **Nieuprawniony dostęp do danych podczas przechowywania.**
4. **Przypadkowe lub niezgodne z prawem zniszczenie, uszkodzenie.**
5. **Przypadkowe lub niezgodne z prawem utracenie danych.**
6. **Przypadkowe lub niezgodne z prawem zmodyfikowanie danych.**

Tabela poniżej jest rejestrem zagrożeń, które mogą wystąpić w placówce.

Administrator danych określił reakcje na ryzyka wg zasady: **T** – tolerowanie, **P** – przeniesienie, **W** – wycofanie, **PD** - przeciwdziałanie

Lp.	Zagrożenie	Opis zagrożenia	Zabezpieczenia	Prawdopodobieństwo (w skali od 1-5)	Skutek (w skali od 1-5)	Istotność ryzyka (P x S)	Reakcja na ryzyko
2.	**Zagrożenie danych**	4. Przesłanie maila z danymi osobowymi do osób nieuprawnionych.	**1. Procedury:** 1) Regulamin ODO dla pracowników, w którym określono procedury bezpieczeństwa przy przetwarzaniu danych osobowych, w tym: a) zasady korzystania z internetu, b) zasady korzystania z poczty elektronicznej, c) zasady użytkowania komputerów przenośnych, d) zasady wynoszenia nośników elektronicznych poza jednostkę, e) zasady zabezpieczania dokumentacji papierowej, f) procedura niszczenia danych na nośnikach elektronicznych, g) Polityka naprawy sprzętu IT w serwisach zewnętrznych, h) Polityka dotycząca zasad gospodarki kluczami; i) Procedura zabezpieczenia systemów informatycznych.	1	3	3	T
		5. Udostępnianie danych (baz i plików) przez internet bez logowania.		1	2	2	T
		6. Przekazanie danych osobom nieuprawnionym, w tym współpracownikom, podmiotom kontrolującym, interesantom w formie bezpośredniej / telefonicznie lub drogą mailową		2	2	4	T

		7. Zagubienie lub kradzież nośników z danymi osobowymi poza placówką (laptopów, dysków wymiennych oraz dokumentów papierowych)	2) Osoby zatrudnione przy przetwarzaniu danych są świadome odpowiedzialności prawnej i karnej- podpisanie oświadczenia o poufności; 3) Szkolenie pracowników, w tym w formie e-learningu; 4) Stosowana jest Procedura audytu oraz uwzględniono kontrole przestrzegania zasad przetwarzania danych w Planie Kontroli Wewnętrznej; 5) Sporządzanie umów powierzenia z firmami zajmującymi się hostingiem serwera, naprawą komputerów, brakowaniem dokumentacji w składnicy akt. **2. Zabezpieczenia:** 1) Wyznaczono Administratora Systemu Informatycznego; 2) Wyznaczono strefy ograniczonego dostępu (sekretariat, księgowość); 3) Zabezpieczenie dostępu do pomieszczeń – drzwi zamykane na klucz; 4) Zabezpieczenie dokumentacji w pomieszczeniach – zamykane niemetalowe szafy; 5) Monitoring wizyjny w obrębie obiektu i otoczenia; 6) Ochrona fizyczna obiektu; 7) Zahasłowane wygaszacze ekranu aktywowane w przypadku nieaktywności użytkownika;	2	2	4	T
		8. Wyrzucenie niezniszczonych uprzednio dokumentów papierowych lub przekazanie do zniszczenia nielicencjonowanej firmie utylizacyjnej.		1	1	1	T
		9. Przekazanie do naprawy lub utylizacji sprzętu z nieusuniętymi danymi osobowymi np. komputerów z twardym dyskiem, drukarek		2	2	4	T
		10. Pozostawianie dokumentacji z danymi osobowymi bez nadzoru (brak wygaszaczy ekranu, opuszczenie stanowiska pracy, dopuszczenie osób trzecich poza strefę ograniczonego dostępu, niezamykanie szaf z		2	3	**6**	**PD**

		dokumentacją)	8) Poufne ustawienie monitorów; 9) Terminacja sesji.				
		11. Korzystanie z nielicencjonowanego/ nielegalnego oprogramowania		2	2	4	**PD**
	Nakłanianie do wykonania czynności	9. Wykonywanie przelewów /przesyłanie informacji na rzekomo zmienione konta fałszywych odbiorców.	**1. Procedury:** 1) Regulamin ODO dla pracowników, w którym określono procedury bezpieczeństwa przy przetwarzaniu danych osobowych, w tym: Zasady korzystania z internetu, zasady korzystania z poczty elektronicznej;	1	2	2	T
		10. Otwieranie załączników od niezindetyfikowanych nadawców.	2) Procedura weryfikacji przelewów księgowych – wewnętrzny Regulamin Działu Księgowości dotyczący zasad akceptacji i modyfikacji przelewów	2	3	**6**	T
		11. Otwieranie maili z prośbą o zalogowanie się (pod pretekstem weryfikacji danych lub na powiadomienie o próbie włamania się na konto) do „podrobionych" stron i tym samym udostępnienie hasła	3) Osoby zatrudnione przy przetwarzaniu danych są świadome odpowiedzialności prawnej i karnej- podpisanie oświadczenia o poufności; 4) Szkolenie pracowników, w tym w formie e-learningu; 5) Stosowana jest Procedura audytu oraz uwzględniono kontrole przestrzegania zasad przetwarzania danych w planie kontroli wewnętrznej.	2	3	**6**	T
		12. Logowanie się do podrobionej strony o zbliżonym adresie do adresów zapamiętanych jako wiarygodne	**2. Zabezpieczenia:** 1) System antywirusowy i antyspamowy instalowany na każdej jednostce stosowanej w przetwarzaniu danych; 2) Blokada dostępu do określonych stron.	3	2	**6**	T

.	**Ataki telefoniczne**	13. Wyłudzanie hasła pod pretekstem sprawdzania lub naprawy systemu informatycznego w placówce	**1. Procedury:** 1) Regulamin ODO dla pracowników, w którym określono procedury bezpieczeństwa przy przetwarzaniu danych osobowych, w tym: Zasady korzystania z internetu, zasady korzystania z poczty elektronicznej; **2. Zabezpieczenia** 1) Blokada dostępu do określonych stron; 2) Firewall sprzętowy i programowy; 3) Aktualizacje systemu operacyjnego.	1	3	**3**	T
		14. Polecenie dokonania logowania się na określone strony internetowe pod pretekstem testowania nowego oprogramowania, testowania łącza internetowego		2	2	**4**	T
.	**Ataki na infrastru-kturę**	15. Łamanie haseł metodami słownikowymi i siłowymi (brute force) do: a) baz danych, b) serwera, c) poczty, d) windows na stacjach roboczych, e) routera, f) firewalla.	**1. Procedury:** 1) Regulamin ODO; 2) Polityka tworzenia i zabezpieczenia haseł dostępu; 3) Procedura nadawania uprawnień do przetwarzania danych; 4) Zabezpieczenie dokumentacji w pomieszczeniach, w	2	2	4	T

		16. Tworzenie haseł łatwo dostępnych, łatwych lub standardowych	tym dokumentacji z umieszczonymi hasłami; 5) Szkolenia personelu, również w formach e-learningu. **2. Zabezpieczenia;** 1) Stosowana jest Procedura audytu oraz uwzględniono kontrole przestrzegania zasad przetwarzania danych w planie kontroli wewnętrznej; 2) Przechowywanie zabezpieczonych haseł w zamykanej szafie. 3) Użytkownicy sprzętu zobowiązani do samodzielnego zmieniania haseł z częstotliwością co 60 dni;	3	3	**9**	**PD**
.	**Ataki na sprzęt IT**	17. Włamania do urządzeń nieaktualizowanych	**1. Procedury:** 1) Regulamin ODO; 2) Polityka tworzenia i zabezpieczenia haseł dostępu; 3) Zabezpieczenie dokumentacji w pomieszczeniach, w tym dokumentacji z umieszczonymi hasłami 4) Szkolenia personelu, również w formach e-	2	2	4	T
		18. Włamania do urządzeń nieodpowiednio skonfigurowanych		1	2	2	T

		19. Włamania z użyciem niezabezpieczonych interfejsów lokalnych	learningu. **2. Zabezpieczenia:** 1) System antywirusowy i antyspamowy aktualizowany online; 2) Funkcja skanowania poczty; 3) Funkcja skanowania portów USB; 4) Zastosowano blokadę portów USB do korzystania z pendrivów.	2	2	4	T
		20. Włamania na sprzęt za pośrednictwem niepotrzebnych usług		2	2	4	T
.	**Ataki na oprogramo-wanie**	21. Włamania z wykorzystaniem luk typu „ zero-day"	**1. Procedury:** 1) Procedura zabezpieczenia systemu informatycznego, 2) Regulamin ODO; 3) Procedura audytu; 4) Procedura tworzenia kopii zapasowych; 5) Szkolenia personelu, również w formach e-learningu. **2. Zabezpieczenia** 1) System antywirusowy i antyspamowy	1	2	2	T
		22. Włamanie z wykorzystaniem najczęstszych błędów programistycznych		1	1	1	T
		23. Namierzanie wersji testowych np. strony www placówki		1	1	1	T

	Nielegalne wpięcie się do sieci (wifi, telefon, internet)	24. Uzyskanie dostępu do sieci wewnętrznej poprzez włamanie się do sieci bezprzewodowej	**1. Procedury:** 1) Polityka zabezpieczenia sieci. 2) Polityka tworzenia i zabezpieczenia haseł dostępu; **2. Zabezpieczenia** 1) Zapewniono uwierzytelnianie do sieci/poczty/dysków sieciowych	1	1	1	T
	Zagrożenia dla sprzętu	25. Włamanie do budynku, pomieszczeń biurowych, składnicy akt, serwerowni, miejsc przechowywania kopii zapasowych	**1. Procedury:** 1) Procedura „Polityka dotycząca zasad gospodarki kluczami", **2. Zabezpieczenia** 1) Monitoring; 2) Drzwi zamykane na klucz; 3) Alarm.	2	2	4	T
		26. Kradzież / zniszczenie sprzętu.		2	2	4	P
		27. Pożar/ eksplozja	**1. Procedury:** 1) Regulamin Bezpieczeństwa; 2) Plan ewakuacji;	2	2	4	P

			2. Zabezpieczenia 1) Gaśnice, 2) Czujniki dymowe,				
		28. Zalanie sprzętu	**1. Procedury:** 1) Regulamin Bezpieczeństwa; 2) Plan ewakuacji; **2. Zabezpieczenia** 1) Regularne szkolenia BHP pracowników CUW;	1	1	1	T
		29. Przegrzanie	Monitoring środowiskowy	1	1	1	T
		30. Awaria zasilania	**1. Procedury:** 1) Plan ciągłości działania; **2. Zabezpieczenia** 1) Przydział zadań i odpowiedzialności za awarie w zasilaniu; 2) Szkolenia personelu;	2	2	4	T

			3) Okresowe przeglądy stanu technicznego budynku. 4) UPS podtrzymujące zasilanie serwera i kluczowe elementy systemu IT/generator prądu.				
		31. Awaria sprzętu	**1. Procedury:** 1) Regulamin ODO; 2) Polityka naprawy sprzętu w serwisach zewnętrznych; 3) Szkolenia personelu, również w formach e-learningu.	3	2	**6**	PD
		32. Starzenie się nośników danych	Systematyczne przeglądy stanu technicznego i wymiana sprzętu w miarę posiadania środków finansowych	4	1	4	T
10.	**Błędy ludzkie**	33. Nieprzestrzeganie procedur bezpieczeństwa danych oraz procedur bezpieczeństwa w placówce.	**1. Procedury:** 1) Regulamin ODO; 2) Szkolenia personelu, również w formach e-learningu. 3) Plan kontroli wewnętrznej; 4) Regulamin oceny pracowników samorządowych na stanowiskach urzędniczych;	2	2	4	T
		34. Pomyłki administratorów użytkowników.		2	2	4	T

		35. Brak świadomości / wiedzy.	5) Procedura postepowania z dokumentacją szkolną; 6) Procedura odtwarzania dokumentacji pedagogicznej.	1	3	3	T
		36. Błędy projektowe / konfiguracyjne.		1	1	1	T
11.	**Zagrożenia ciągłości działania**	37. Brak aktualnej dokumentacji. 38. Brak umowy o współpracy. 39. Nieprawidłowe / brak umowy gwarancyjnej lub wsparcia serwisowego. 40. Upadek firmy współpracującej np. dostawcy oprogramowania/serwera 41. Awaria łączy telekomunikacyjnych	**1. Procedury:** 1) Plan ciągłości działania; 2) Regulamin audytu w ramach kontroli zarządczej.	3	2	**6**	T

MAPA RYZYKA

(Ocena istotności ryzyka)

zawierającą wszystkie istotne ryzyka, tj. te których wartość istotności ryzyka, wyniosła w zastosowanej skali co najmniej 6.