Kopia nr: Własność:

	Stanowisko lub dział	Data	Nazwisko	Podpis
Opracował	Inspektor Ochrony Danych	24.01.2019	Mirosław Jarek	INSPEKTOR OCHRONY DANYCH mgr Mirosław Jarek
Opiniował	Pełnomocnik Dyrektora ds. ZSZ	24.01.2019	Iwona Kowalik	
Opiniował	Koordynator Obszaru Zamówień Publicznych i Logistyki	24.01.2019	Jacek Gorszanów	
Opiniował	Koordynator Obszaru Zarządzania Informacja	24.01.2019	Paweł Rerak	
Opiniował	Dyrektor WSS5	24.01.2019	Alicja Cegłowska	p.o. DYREKTOR Wojewódzkiego Szpitala Specjalistycznego Nr 5 im. Św. Barbary w Sosnowcu dr n. med. Alicja Cegłowska

1. SPIS TREŚCI:

2. ZASADY OGÓLNE.

2.1. Niniejszy dokument określa podstawowe zasady odnoszące się do postępowania w relacjach z dostawcami, ze szczególnym uwzględnieniem występujących w nich ryzyk oraz zasad zachowania bezpieczeństwa informacji. W ramach relacji z dostawcami chcemy promować świadome podejście do ryzyk, które mogą występować w trakcie współpracy i bezpieczeństwa informacji, dostrzegając przy tym znaczący ich wkład w kształtowanie się biznesowej kultury zaufania.

2.2. Zasady postępowania mają zastosowanie do wszystkich aktualnych lub potencjalnych dostawców towarów i usług zewnętrznych. Usługami zewnętrznymi w WSS5 są między innymi:

- szkolenia,
- remonty,
- pomoc techniczna w zakresie aplikacji komputerowych,
- naprawa komputerów i sprzętu IT,
- naprawa aparatury i sprzętu medycznego,
- dostarczanie systemów IT,
- dostarczanie aparatury medycznej,
- obsługa kadrowo-księgowa,
- ochrona budynków,
- wideo monitoring budynku,
- sprzątanie,
- wywóz śmieci i nieczystości,
- usługi BHP (w tym szkolenia w zakresie BHP),
- usługi doradcze,
- usługi kserograficzne (drukowanie, kopiowanie),
- świadczenia opieki zdrowotnej,
- transport.

3. BEZPIECZEŃSTWO INFORMACJI W RELACJACH Z DOSTAWCAMI.

3.1. System zarządzania bezpieczeństwem informacji w relacji do zewnętrznych usługodawców powinien obejmować w szczególności:

a) analizę dostawców w ramach identyfikacji kontekstu działalności organizacji w celu podejmowania odpowiednich działań prewencyjnych,

b) ocenę wpływu dostawców jako strony zainteresowanej na zakres systemu zarządzania bezpieczeństwem informacji,

c) uwzględnienie relacji z dostawcami w analizie ryzyka bezpieczeństwa informacji,

d) nadzór nad bezpieczeństwem informacyjnym procesów lub zamówień, których wykonanie zlecono na zewnątrz.

3.2. W praktyce bezpieczeństwo informacji z relacjach z dostawcami oznacza kierowanie się trzema atrybutami:

a) **Poufność** – czyli zapewnienie, że informacje są dostępne tylko dla osób do tego uprawnionych, w szczególności będą to pracownicy lub podwykonawcy dostawcy, dla których wykonanie kontraktu lub zlecenia będzie wymagało dostępu do informacji poufnych [chronionych].

b) **Integralność** – czyli zagwarantowanie dokładności i kompletności informacji, oraz metod ich przetwarzania; poprzez sformalizowanie zasad współpracy z dostawcami;

c) **Dostępność** – czyli zapewnienie upoważnionym użytkownikom dostępu do informacji i związanych z nimi zasobów, zgodnie z określonymi potrzebami, w relacji z dostawcami przez potrzebę należy rozumieć wykonanie kontraktu lub zlecenia.

4. IDENTYFIKACJA ZAGROŻEŃ.

4.1. Ryzyka związane z bezpieczeństwem informacji.

Rodzaj ryzyka	Zakres występowania ryzyka	Opis
Kradzież sprzętu komputerowego lub zewnętrznych nośników pamięci	Firmy serwisujące, sprzątające, remontowe, szkoleniowe. Wszystkie firmy zewnętrzne wykonujące usługi regularne lub jednorazowe w budynku WSS5	Dotyczy głównie kradzieży urządzeń mobilnych oraz zewnętrznych nośników pamięci, pozostawionych w ogólnie dostępnych miejscach, do których dostęp posiadają również firmy zewnętrzne świadczące różnego rodzaju usługi w budynku WSS5
Fizyczna kradzież dokumentów	Firmy serwisujące, sprzątające, remontowe, szkoleniowe. Wszystkie firmy zewnętrzne wykonujące usługi regularne lub jednorazowe w budynku WSS5	Dotyczy kradzieży dokumentów papierowych pozostawionych o ogólnie dostępnych miejscach w wyniku niefrasobliwości pracowników w budynku WSS5, jak również w wyniku celowego działania
Brak sformalizowanych zasad współpracy z zewnętrznymi dostawcami towarów lub usług	Wszyscy aktualni i potencjalni dostawy	Brak formalnych zasad współpracy skutkuje niewiedzą dostawców w zakresie polityki bezpieczeństwa informacji, postępowania z informacjami poufnymi i sposobami zgłaszania incydentu naruszenia bezpieczeństwa informacji. Jednocześnie może oznaczać brak procedur zapewniających bezpieczeństwo danych oraz brak zdefiniowanych kar za naruszenie bezpieczeństwa danych

Zniszczenie lub uszkodzenie sprzętu komputerowego/lub nośników pamięci	Firmy serwisujące, sprzątające, remontowe, szkoleniowe. Wszystkie firmy zewnętrzne wykonujące usługi regularne lub jednorazowe w budynku WSS5	Działanie tego typu może być zamierzone (celowe) lub niezamierzone będące skutkiem wykonywania prac/usług w budynku WSS5, np. w wyniku nienależytego zabezpieczenia sprzętu komputerowego w trakcie wykonywania usługi, korzystania z wadliwych urządzeń specjalistycznych do wykonania usługi, nienależytego przeszkolenia pracowników dostawcy
Korzystanie z portali B2B (business-to-business)dostawcy	Wszyscy dostawcy wymagający realizacji bieżących zamówień poprzez własne portale typu B2B	Korzystanie z portali B2B dostawców, oznacza przechowywanie danych handlowych (lista zamawianych produktów, ceny, rabaty) na zewnętrznych serwerach, co wiąże się z ograniczonym wpływem na kontrolę sposobu w jaki są chronione
Przekazywanie informacji nieuprawnionym podmiotom (poprzez realizację usługi przez niezdefiniowanych wcześniej podwykonawców)	Potencjalnie wszyscy dostawcy, którzy przy realizacji kontraktu lub zlecenia mogą korzystać z pomocy podwykonawców	Ryzyko odnosi się do sytuacji, w której dostawca nie poinformował wcześniej o realizowaniu kontraktu lub zlecenia przy pomocy podwykonawców, przez co pozostają oni nierozpoznani i niezidentyfikowani dla WSS5
Ujawnienie danych poufnych	Wszyscy aktualni i potencjalni dostawcy	Może mieć charakter przypadkowy lub celowy. Może wystąpić zarówno w wyniku zaniedbań pracowników WSS5 jak i pracowników zewnętrznego dostawcy. Skutkuje to narażeniem na szwank reputacji szpitala lub ewentualnymi konsekwencjami prawnymi. Przykładem przypadkowego ujawnienia danych jest wyrzucenie na śmietnik wydruków archiwalnych szpitala lub utylizacja komputerów bez uprzedniego zniszczenia dysków twardych. Celowym ujawnieniem informacji poufnych może być umieszczenie w Internecie przez nielojalnego pracownika dostawcy części kodu źródłowego istotnego dla funkcjonowania w WSS5 oprogramowania
Zniszczenie danych (np. w postaci papierowej)	Firmy serwisujące, sprzątające, remontowe, szkoleniowe. Wszystkie firmy zewnętrzne wykonujące usługi regularne lub jednorazowe w budynku WSS5	Może mieć charakter przypadkowy - kiedy do zniszczenia dokumentów dochodzi w wyniku źle wykonywanej usługi (np. przy braku zabezpieczenia dokumentów podczas wykonywania prac remontowo-konserwatorskich), lub celowy - kiedy jest wynikiem złej woli
Dostęp do haseł zapisanych w postaci papierowej	Firmy serwisujące, sprzątające, remontowe, szkoleniowe, kurierskie Wszystkie firmy zewnętrzne wykonujące usługi regularne lub jednorazowe w budynku WSS5	Skutkuje uzyskaniem dostępu do ważnych aplikacji, które mogą zawierać informacje poufne lub kluczowe dla funkcjonowania WSS5
Brak szkoleń z zakresu bezpieczeństwa informacji dla pracowników zewnętrznych dostawców	Firmy serwisujące, sprzątające, remontowe, szkoleniowe, kurierskie Wszystkie firmy zewnętrzne	Zagrożenie może wystąpić w sytuacji, kiedy procedury z zakresu bezpieczeństwa informacji są na tyle złożone, iż wymagają oddzielnych szkoleń

	wykonujące usługi regularne lub jednorazowe w budynku WSS5	dla pracowników zewnętrznych dostawców prowadzonych przez przedstawicieli WSS5
Brak nadzoru nad pracą serwisów zewnętrznych	Firmy serwisujące i remontowe	Zbyt duże zaufanie do dostawców, które skutkuje pozostawieniem ich bez nadzoru w miejscach, w których mają dostęp do dokumentacji i informacji poufnych
Pomyłki pracowników	Wszyscy aktualni i potencjalni dostawcy	Wynikające z indywidualnych pomyłek pracowników, będące skutkiem niedopatrzenia, braku koncentracji lub niefrasobliwości (np. przesłanie do dostawcy niewłaściwego maila, zawierającego informacje nie przeznaczone dla niego)
Zbyt duże uprawnienie dostępu do budynków i pomieszczeń dla firm zewnętrznych	Firmy serwisujące, sprzątające, remontowe, szkoleniowe, kurierskie Wszystkie firmy zewnętrzne wykonujące usługi regularne lub jednorazowe w budynku WSS5	Zbyt duża swoboda poruszania się po budynkach i dostępu do pomieszczeń służbowych, w których przechowywane są dokumenty mogące zawierać informacje poufne
Duża rotacja pracowników firm zewnętrznych / brak dedykowanych opiekunów do realizacji kontraktu	Wszyscy aktualni i potencjalni dostawcy	Duża rotacja skutkuje przekazywaniem informacji zbyt dużej liczbie pracowników dostawcy. Brak dedykowanych opiekunów oznacza chaos informacyjny i brak transferu wiedzy.
Utrata wsparcia technicznego	Głównie dostawcy specjalistycznego lub dedykowanego oprogramowania.	Utrata wsparcia technicznego jest szczególnie groźna w przypadku oprogramowania niestandardowego, tworzonego na potrzeby WSS5. W przeciwieństwie do sprzętu, którego podzespoły zazwyczaj dostępne są na rynku i który można łatwo zastąpić innym o zbliżonych lub nawet tych samych parametrach wymiana oprogramowania bywa trudna i skomplikowana. Wiąże się często z koniecznością przeprowadzenia długotrwałego wdrożenia i konwersji danych między systemami. Najczęściej problem ten występuje w przypadku: - upadłości lub likwidacji właściciela oprogramowania, - zmiany formy prawnej lub organizacyjnej organizacji, - wygaśnięcia dotychczasowych umów, - zaprzestania wsparcia oprogramowania w związku z wprowadzeniem nowych wersji, - brakiem porozumienia, które może mieć przyczyny biznesowe, ekonomiczne, społeczne lub personalne

4.2. Ryzyka wynikające z korzystania z usług typu cloudcomputing.

Rodzaj ryzyka	Zakres występowania ryzyka	Opis
Przesunięcie kompetencji administratora danych, na dostawcę usługi w chmurze	Wszyscy aktualni oraz potencjalni dostawcy oferujący usługi w chmurze lub licencjonowany dostęp do usługi, nie wymagający wykorzystania infrastruktury informatycznej WSS5	Administrator nie zauważa naruszeń bezpieczeństwa informacji (poufności, integralności, dostępności danych), przywiązuje do nich mniejszą wagę. Działania te mogą prowadzić do popełnienia czynów naruszających przepisy ochrony danych i prywatności. Administrator danych lub strona trzecia nie będzie w stanie na odpowiednim poziomie monitorować dostawcy usługi w chmurze
Brak zdefiniowanych tzw. wiążących reguł korporacyjnych (BCR)	Wszyscy aktualni oraz potencjalni dostawcy oferujący usługi w chmurze lub licencjonowany dostęp do usługi, nie wymagający wykorzystania infrastruktury informatycznej WSS5	BCR zawierają indywidualne warunki, które nakładają na podmioty z nimi powiązane określone obowiązki w zakresie zwiększenia bezpieczeństwa danych. Dostawca cloud, który zobowiąże się do przestrzegania BCR jest bardziej wiarygodny, co wpływa na zwiększenie poziomu zaufania do swoich usług
Nieprzestrzeganie zdefiniowanych BCR (Wiążące zasady korporacyjne)	Wszyscy aktualni oraz potencjalni dostawcy oferujący usługi w chmurze lub licencjonowany dostęp do usługi, niewymagający wykorzystania infrastruktury informatycznej WSS5	Dostawca nie przestrzega wcześniej ustalonych BCR co skutkuje brakiem należytego zabezpieczenie danych
Przekazanie danych do jurysdykcji, które nie zapewniają odpowiedniego poziomu ochrony.	Wszyscy aktualni oraz potencjalni dostawcy oferujący usługi w chmurze lub licencjonowany dostęp do usługi, nie wymagający wykorzystania infrastruktury informatycznej WSS5	Dane mogę być przechowywane na serwerach znajdujących się poza granicami Polski, w kraju, gdzie obowiązuje inne prawo odnośnie zachowania bezpieczeństwa informacji
Brak możliwości ustalenia odpowiedzialności w łańcuchu usługodawców.	Wszyscy aktualni oraz potencjalni dostawcy oferujący usługi w chmurze lub licencjonowany dostęp do usługi, nie wymagający wykorzystania infrastruktury informatycznej WSS5	Jeżeli dostawca cloudcomputingu będzie korzystał z podwykonawców (firmy przetwarzające dane), to ustalenie odpowiedzialności w łańcuchu usługodawców może być niezwykle trudne
Wykorzystanie danych administratorów bez ich zgody	Wszyscy aktualni oraz potencjalni dostawcy oferujący usługi w chmurze lub licencjonowany dostęp do usługi, nie wymagający wykorzystania infrastruktury informatycznej WSS5	Istnieje ryzyko, iż korzystając z cloudcomputingu straci się kontrolę nad danymi i ich przetwarzaniem. Największym zagrożeniem jest możliwość wykorzystania danych administratorów danych przez dostawców usług cloud lub ich podwykonawcy do własnych celów bez wiedzy lub zgody administratorów danych
Zablokowanie dostępu do usługi	Wszyscy aktualni oraz potencjalni dostawcy oferujący usługi w chmurze lub licencjonowany dostęp do usługi,	W zależności od specyfiki działalności jak również czasu wystąpienia tego typu awarii, straty związane z brakiem dostępu do zasobów

	nie wymagający wykorzystania infrastruktury informatycznej WSS5	organizacji będą różne, uzależnione od wielu czynników, min. poziomu uzależnienia codziennej pracy od dostępu do zablokowanej usługi
Utrata danych	Wszyscy aktualni oraz potencjalni dostawcy oferujący usługi w chmurze lub licencjonowany dostęp do usługi, nie wymagający wykorzystania infrastruktury informatycznej WSS5	Może ona nastąpić zarówno w wyniku przypadkowego jak i celowego usunięcia zbiorów danych, a także uszkodzenia urządzeń służących do ich przechowywania. Skasowanie informacji często wiąże się z bezpowrotną utratą ich części lub całości. Dodatkowo skasowanie niewielkiej liczby danych może przez długi czas pozostać niezauważone
Vendor lock-in czyli uzależnienie od dostawcy	Wszyscy aktualni oraz potencjalni dostawcy oferujący usługi w chmurze lub licencjonowany dostęp do usługi, nie wymagający wykorzystania infrastruktury informatycznej WSS5	Uzależnienie kluczowych procesów w firmie bez uzgodnienia zasad zakończenia współpracy lub rozwiązania umowy oraz "odzyskania" przekazanych danych

4.3. Zakres umów z dostawcami oferującymi usługi z wykorzystaniem cloudcomputing.

Odpowiednio sformułowana umowa powinna zawierać klauzule:

- umożliwiające przenoszenie danych (portability) i kontrolowanie ich,
- zakazujące nielegalnego przekazywanie danych do jurysdykcji, bez wystarczającego poziomu ochrony danych
- dostawca usług opartych o cloud powinien zapewnić, że usunięcie danych osobowych z dysków oraz z innych nośników może być przeprowadzone w skuteczny sposób.

Istotne jest także zabezpieczenie dostępu do danych. Nikt poza klientem usług w chmurze nie powinien mieć dostępu do jego danych. Umowa lub inna forma porozumienia z dostawcą, powinna gwarantować także odpowiednie tworzenie i zapisywanie kopii zapasowych w bezpiecznych lokalizacjach oraz wprowadzać zasadę przejrzystości lokalizacji, w których dane mogą być przechowywane i przetwarzane.

5. PRZETWARZANIE DANYCH PRZEZ USŁUGODAWCÓW ZEWNĘTRZNYCH

W przypadku, gdy usługi zewnętrzne obejmują przetwarzanie danych (w szczególności danych o wysokim stopniu poufności [chronione]) poza infrastrukturą teleinformatyczną WSS5 (np. w modelu cloudcomputing lub innych formach modelu Application Service Provision, w zewnętrznych centrach przetwarzania danych itp.), należy w szczególności:

- wprowadzić odpowiednie mechanizmy kontrolne zapewniające poufność tych danych (np. poprzez ich szyfrowanie),
- zapewnić, aby informacje o wszelkich incydentach zagrażających bezpieczeństwu danych były raportowane przez dostawcę,
- zapewnić skuteczne mechanizmy pozwalające na bezpieczne zakończenie współpracy (w szczególności w zakresie zwrotu danych oraz ich usunięcia),
- zagwarantować możliwość weryfikacji stosowanych przez dostawcę mechanizmów kontrolnych, w tym w zakresie środków ochrony i kontroli dostępu do pomieszczeń usługodawcy, w których odbywa się świadczenie usług na rzecz WSS5.

6. ZASADY POSTĘPOWANIA Z INFORMACJAMI POUFNYMI.

6.1. W niniejszym dokumencie przyjmuje się, że informacje poufne [chronione], to wszystkie przekazane dostawcy informacje, materiały oraz dokumenty, które nie są publicznie udostępniane przez WSS5.Przetwarzanie informacji należących do WSS5 przez Podmiot Zewnętrzny (DOSTAWCÓW / WYKONAWCÓW) musi odbywać się z uwzględnieniem klasyfikacji informacji.

	Opis	Zasady oznaczania	Zasady kontroli	Zasady kopiowania	Dystrybucja informacji
Publiczne	Nie wymagające dodatkowych zabezpieczeń, ich utrata nie spowoduje istotnych szkód i strat; informacje nie mające wpływu na ciągłość działania WSS5 oraz jej wartości materialne i prawne	Umieszcza się w nagłówku - kategoria jawności: III (publiczne)	Brak szczególnych zasad bezpieczeństwa	Brak szczególnych zasad bezpieczeństwa	Brak szczególnych zasad bezpieczeństwa
Wewnętrzne	Informacja dostępna wszystkim pracownikom WSS5, dostęp na podstawie oświadczenia o zapoznaniu się z zasadami ochrony informacji obowiązującymi w WSS5, chronione przed nieuprawnioną modyfikacją, utrata może mieć wpływ na ciągłość działania WSS5 oraz jej wartości materialne i prawne;	Umieszcza się w nagłówku dokumentu kategoria jawności: II (wewnętrzne) lub na segregatorze / kopercie. Jeśli jest taka możliwość	Wytwórca informacji odpowiedzialny jest za właściwe oznaczenie informacji Właściciel grupy informacji odpowiada za przydział do odpowiedniej grupy informacji zgodnie z załącznikiem nr 2 do PO 30/2016 Odbiorca informacji: odpowiedzialny za należyte przechowywanie i kontrolę nośnika informacji (wersja tradycyjna, elektroniczna)	Limitowane kopie, mogą być zrobione tylko przez uprawnionych pracowników albo przez kontrahentów i osoby trzecie, które podpisały odpowiednie oświadczenie poufności	Na zewnątrz organizacji: zaleca się odpowiednie zabezpieczenie np. używanie zamkniętych kopert Forma elektroniczna: zaleca się przekazywanie za pośrednictwem wewnętrznej poczty. Możliwe umieszczanie w zasobach sieciowych WSS 5 (np. foldery sieciowe, ikonka "i"). W przypadku zewnętrznego konta zaleca się szyfrowanie transmisji Faksowanie: zaleca się zwrócenie szczególnej uwagi na numer faksu, na który jest wysyłana informacja
Chronione	Informacje o istotnym znaczeniu dla funkcjonowania WSS5, zasady ochrony tych informacji regulują przepisy zewnętrzne oraz wewnętrzne, utrata informacji może spowodować istotne utrudnienie w działalności statutowej, mieć wpływ na ciągłość działania WSS5 oraz jej wartości materialne i prawne	Umieszcza się w nagłówku dokumentu kategoria jawności: I (chronione) lub na segregatorze / kopercie. Jeśli jest taka możliwość.	Wytwórca informacji odpowiedzialny jest za upewnianie się, że chroniona informacja jest wykorzystywana zgodnie z przeznaczeniem/celem Odbiorca informacji odpowiedzialny jest za upewnianie się, że poufna informacja jest zakodowana i/lub znajduje się w zabezpieczonym pomieszczeniu/szafie pod kluczem.	Limitowane kopie mogą być zrobione tylko na podstawie pozwolenia wytwórcy informacji albo wg określonych przez niego zasad. Wymagane jest udokumentowanie faktu przekazania informacji. Wymagane jest upoważnienie do przetwarzania danych osobowych lub odrębne pełnomocnictwo.	Wewnętrznie: wykorzystanie kopert / teczek: dostarczać „do rąk własnych" jeśli to możliwe. Na zewnątrz organizacji: używać zwykłej zaklejonej koperty. Dostarczać „do rąk własnych" albo wysyłać przez zaufanego kuriera. Forma elektroniczna: wysyłać tylko jako zaszyfrowane dane lub umieszczać w zasobie sieciowym dostępnym tylko dla upoważnionych osób. Faksowanie: wymaga się potwierdzenia, wydruku/raportu poprawnego przesłania dokumentu niezwłocznie po wysłaniu dokumentu

- Osoby reprezentujące podmiot zewnętrzny, z którym WSS5 zawarł umowę, mogą uzyskać dostęp do

informacji należących do WSS5 wyłącznie po podpisaniu umowy o współpracę / zlecenia oraz dokumentu regulującego zasady i odpowiedzialność związaną z zachowaniem poufności przekazywanych informacji.

- Każdy z pracowników podmiotu zewnętrznego może posiadać dostęp wyłącznie do informacji, które są mu niezbędne do prawidłowej i sprawnej realizacji zadań i obowiązków wynikających z umowy podpisanej pomiędzy podmiotem zewnętrznym a WSS5.
- Dostawcy / Wykonawcy zobowiązują się akceptować i stosować wszystkie obowiązujące w WSS5 zasady związane z bezpieczeństwem informacji - odpowiednio do rodzaju i zakresu przyznanego im dostępu do zasobów informacyjnych.
- Oznaczanie informacji powstałych w wyniku pracy intelektualnej pracowników Dostawców / Wykonawców powinno być czytelne i nie pozostawiać wątpliwości, co do klasy oraz właściciela. Identyfikacja dotyczy wszystkich zapisów (w wersji ustnej, papierowej i elektronicznej).
- W przypadku wątpliwości dotyczących właściwej klasyfikacji informacji oraz w sytuacji, gdy mamy do czynienia z informacjami niesklasyfikowanymi, należy bezwzględnie traktować je jak informacje o najwyższym stopniu ochrony.
- Nośniki mobilne zawierające informacje należące do WSS5 sklasyfikowane jako wewnętrzne i chronione muszą zostać zaszyfrowanie programem wykorzystującym minimum standard AES 256.
- W przypadku zbywania lub wycofywania z użytku dokumentów lub nośników elektronicznych zawierających informacje wrażliwe (czyli wewnętrzne i/lub chronione) należy usunąć je w sposób uniemożliwiający odtworzenie.
    - Zapisy elektroniczne powinny być niszczone specjalnym oprogramowaniem lub/i fizycznie.
    - Zapisy papierowe muszą być niszczone w niszczarkach dwupłaszczyznowych.

7. WYMAGANIA WZGLĘDEM DOSTAWCÓW

7.1. Zarządzanie hasłami i kontami

7.1.1 Obowiązkiem Podmiotu Zewnętrznego jest ustanowienie odpowiedniego procesu zarządzania hasłami w systemach mających styczność z informacjami należącymi do WSS5 z uwzględnieniem następujących zasad:

- Przydzielanie haseł do systemów, w których znajdują się informacje należące do WSS5 musi być realizowane przez wyznaczony zespół lub osobę.
- Hasła powinny być unikatowe oraz spełniać wymagania dla tzw. „silnych" haseł.
- Hasła wykorzystywane do zabezpieczenia zasobów należących do Podmiotu Zewnętrznego nie mogą być wykorzystywane do ochrony kont prywatnych jej pracowników.
- Hasła do systemów muszą być zmieniane co najmniej co 30 dni.
- Przechowywanie haseł w wersji czytelnej niezależnie od tego czy są przechowywane w plikach czy zapisywane na papierze jest zabronione.
- Zabrania się zapamiętywania haseł na potrzeby procesów automatycznego logowania w programach takich jak przeglądarki internetowe, programy pocztowe itp.
- W przypadku, gdy hasło zostanie ujawnione lub gdy zaistnieje chociażby podejrzenie ujawnienia niepowołanym osobom należy je natychmiast zmienić lub zablokować konto.

7.1.2 Logowanie do systemów Podmiotu Zewnętrznego przetwarzających informacje należące do WSS5 z kawiarenek internetowych oraz innych urządzeń, które nie są administrowane przez Podmiot Zewnętrzny lub w miejscach nie przystosowanych do przetwarzania danych osobowych jest zabronione.

7.1.3 Wszystkie pliki oraz bazy danych zawierające hasła mogą być przechowywane wyłącznie w postaci zaszyfrowanej oraz chronione przed dostępem nieupoważnionych osób. W tym celu należy stosować techniki kryptograficzne oraz zapewnić odpowiednie środki bezpieczeństwa fizycznego urządzeń przetwarzających hasła.

7.1.4 Współdzielenie kont i haseł jest zabronione. Każda z osób posiadająca dostęp do systemów musi posiadać indywidualne konto dostępowe. Właściciel konta odpowiedzialny jest za wszystkie czynności zrealizowane przy jego użyciu.

7.2. Urządzenia przenośne i praca na odległość

7.2.1 Zaleca się, aby Podmiot Zewnętrzny ustanowił proces zabezpieczenia urządzeń przenośnych oraz nośników danych.

Proces musi uwzględniać następujące wytyczne:

- Pracownik zobowiązany jest dostarczyć podpisane oświadczenie dotyczące przestrzegania zasad dotyczących korzystania z urządzeń przenośnych podczas pracy poza siedzibą Podmiotu Zewnętrznego.
- Oprogramowanie na urządzeniach mobilnych wykorzystywanych przez pracowników Podmiotu Zewnętrznego powinno pochodzić wyłącznie z zasobów firmy oraz być zarejestrowane i zweryfikowane pod kątem legalności.
- W przypadku używania prywatnych urządzeń przenośnych lub nośników danych – Pracownik Podmiotu Zewnętrznego musi uzyskać akceptację osób z kierownictwa firmy.
- Podmiot Zewnętrzny musi zapewnić bezpieczeństwo urządzeń przenośnych i nośników z uwzględnieniem wymuszonych haseł BIOS, wygaszaczy (np. po 15 min) oraz szyfrowania.

7.2.2 Dostęp pracowników Podmiotu Zewnętrznego z sieci publicznych do jego systemów IT zawierających informacje WSS5 może być realizowany wyłącznie przy użyciu metod kryptograficznych takich jak VPN, tunele IPSec.

7.2.3 Komputery osobiste pracowników Podmiotu Zewnętrznego muszą być zabezpieczone za pomocą aktualnych i legalnych programów antywirusowych.

7.2.4 Infrastruktura przetwarzająca informacje WSS5 musi być chroniona za pomocą urządzeń typu Firewall.

7.3. Kopie bezpieczeństwa danych

7.3.1 Podmiot Zewnętrzny odpowiedzialny jest za wdrożenie i nadzorowanie procesu tworzenia kopii bezpieczeństwa wraz możliwością odzyskania danych i przywrócenia funkcji biznesowych w obszarze, gdzie są przetwarzane Informacje należące do WSS5.

7.4. Poczta elektroniczna

7.4.1 Podmiot Zewnętrzny odpowiedzialny jest za ustanowienie, wdrożenie i nadzorowanie procesu związanego z przepływem informacji za pomocą poczty elektronicznej.

7.4.2 Poczta elektroniczna musi być przetwarzana wyłącznie przy użyciu urządzeń będących własnością lub zaakceptowanych przez Podmiot Zewnętrzny.

7.4.3 Przechowywanie i przetwarzanie informacji będących własnością WSS5 przy pomocy systemów pocztowych nienależących do Podmiotu Zewnętrznego np. gmail.com, hotmail.com jest zabronione.

7.4.4 Podmiot Zewnętrzny powinien zwrócić uwagę pracownikom na niewłaściwość wykorzystywania konta pocztowego do dystrybucji treści określanych mianem „spamu", łańcuszków szczęścia oraz innych niepożądanych wiadomości.

7.4.5 System poczty elektronicznej Podmiotu Zewnętrznego musi specyfikować informacje (sygnatura) identyfikujące właściciela danego konta pocztowego takie jak: Imię, Nazwisko, nazwę obejmowanego stanowiska oraz nazwę firmy.

7.4.6 Zasady dotyczące poczty elektronicznej powinny jasno określać zakaz otwierania załączników poczty elektronicznej pochodzących z niewiadomych źródeł.

7.4.7 Podmiot Zewnętrzny zobowiązany jest wdrożyć system ochrony antywirusowej w zakresie poczty elektronicznej.

7.5. Ochrona danych osobowych

7.5.1 Podmiot zewnętrzny powinien zapewnić wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie danych osobowych spełniało wymogi ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych-RODO i chroniło prawa osób, których dane dotyczą. W szczególności powinien zagwarantować, że:

- przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora,
- zapewnia, by osoby upoważnione do przetwarzania danych zobowiązały się do zachowania tajemnicy,
- podejmuje wszelkie środki zapewniające bezpieczeństwo przetwarzania na mocy art. 32 RODO.
- w miarę możliwości pomaga administratorowi (za pomocą odpowiednich środków technicznych i organizacyjnych) wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w RODO (np. prawo do bycia zapomnianym, przenoszenia danych),
- pomaga administratorowi wywiązać się z obowiązków dotyczących bezpieczeństwa przetwarzania, zgłaszania naruszeń, oceny skutków dla ochrony danych i uprzednich konsultacji,
- po zakończeniu świadczenia usług związanych z przetwarzaniem, zależnie od decyzji administratora, usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa ich istniejące kopie, chyba że prawo UE lub prawo państwa członkowskiego nakazuje przechowywanie danych,
- udostępnia administratorowi informacje niezbędne do spełnienia obowiązków określonych w art. 28 RODO oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów (w tym inspekcji) i przyczynia się do nich.
- Dostawca / Wykonawca zobowiązuje się do spełnienia wymagań zapisów RODO w zakresie przeprowadzenia analizy ryzyka, z zagwarantowanym prawem Zamawiającego do rozliczalności tego obowiązku wobec Dostawcy / Wykonawcy.
- Dostawca / Wykonawca [podmiot przetwarzający] - gdy ma to zastosowanie – prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Zamawiającego [administratora danych] danych zgodnie z art. 30 ust 2 RODO.

7.6. Zarządzanie incydentami

7.6.1 Podmiot Zewnętrzny powinien ustanowić, wdrożyć i nadzorować proces zarządzania incydentami adekwatny do wielkości firmy. Proces ten może obejmować całość Organizacji lub dotyczyć zasobów przetwarzających informacje należące do WSS5 w zakresie aktywów informacyjnych należących do WSS5.Każdy incydent musi być zgłoszony Inspektorowi Ochrony Danych Osobowych oraz/lub Administratorowi Danych Osobowych ze strony WSS5.

7.6.2 Proces powinien również obejmować dalszą analizę zbiorczą incydentów zidentyfikowanych w organizacji. Do analizy można wykorzystać metodologię proponowaną przez COBIT lub normę ISO 27001 lub 9001.

7.6.3 Zarządzanie incydentami powinno obejmować szkolenia dla pracowników oraz czytelny opis procesu wraz z klasyfikacją incydentów i sposobem ich zgłaszania.

7.6.4 Zaleca się, aby Proces zarządzania incydentami zawierał wyspecyfikowane w sposób nie pozostawiający wątpliwości co do postępowania następujące obszary:

- zgłaszanie incydentów (analiza wstępna);
- rozpowszechnienie informacji (raportowanie i eskalacja);
- materiały dowodowe (zbieranie i zabezpieczenie);
- analiza końcowa.

7.7. Czysty ekran i czyste biurko

7.7.1 Podmiot Zewnętrzny powinien ustanowić, wdrożyć i nadzorować zasady dotyczące czystego biurka i czystego ekranu.

7.7.2 Zasady dotyczące czystego biurka powinny szczególnie obejmować:

- sposób zarządzania dokumentami papierowymi oraz w wersji elektronicznej przed, w trakcie i po użyciu;
- sposób przechowywania, archiwizacji i niszczenia dokumentów szczególnie w aspekcie zasobów, gdzie będą przetwarzane informacje należące do WSS5;
- zobowiązanie pracowników Podmiotu Zewnętrznego do uporządkowania swojego stanowiska po zakończeniu pracy, szczególnie w aspekcie dokumentów i nośników zawierających wrażliwe dane dla Podmiotu Zewnętrznego lub należące do WSS5.

7.7.3 Zasady dotyczące czystego ekranu powinny obejmować:

- zasady logowania i wylogowania się z komputerów osobistych, terminali i drukarek oraz sposobu ich zabezpieczenia po zakończeniu pracy w biurze Podmiotu Zewnętrznego;
- zasady zabezpieczenia komputera przed dostępem osób nieupoważnionych podczas nieobecności na stanowisku pracy lub po jej zakończeniu.

7.8. Dostęp do sieci

7.8.1 Dostęp do zasobów Podmiotu Zewnętrznego powinien być określony i usankcjonowany z zachowaniem następujących wymagań:

- przydzielenie uprawnień musi być zgodne z „zasadą wiedzy koniecznej". Oznacza to, że Pracownik Podmiotu Zewnętrznego może otrzymać tylko taki zakres uprawnień, który jest niezbędny do realizacji zadań mu powierzonych;
- pracownicy Podmiotu Zewnętrznego mogą uzyskiwać dostęp wyłącznie do standardowych systemów wykorzystywanych w obrębie działów, w których są zatrudnieni;
- w celu zachowania integralności przydzielonych uprawnień z rzeczywistymi potrzebami konieczne jest wykonywanie regularnej weryfikacji kont;
- wszystkie uprawnienia związane z dostępem elektronicznym oraz fizycznym muszą zostać bezwzględnie odebrane w przypadku odejścia z pracy pracownika Podmiotu Zewnętrznego.

7.9. Audyt drugiej strony

7.9.1 W celu zapewnienia bezpieczeństwa informacji należących do WSS5 i przetwarzanych przez Podmiot Zewnętrzny zastrzega się możliwość wykonania audytu przez Pracowników WSS5 lub firmę zewnętrzną.

7.9.2 Audyt obejmie swoim zakresem wszystkie obszary mające wpływ na bezpieczeństwo danych powierzanych Podmiotowi Zewnętrznemu przez WSS5.

8. RYZYKA NIE ZWIĄZANE Z BEZPIECZEŃSTWEM INFORMACJI

Rodzaj ryzyka	Zakres występowania ryzyka	Opis
Brak dedykowanych pracowników odpowiedzialnych za przekazywanie rzetelnych i dokładnych informacji.	Wszyscy aktualni i potencjalni dostawcy	Brak informacji kluczowych dla realizacji kontraktu lub zamówienia, zarówno po stronie zleceniodawcy jak i zleceniobiorcy.
Ryzyko związane z wyborem dostawcy / usługodawcy: ryzyko związane z upadłością dostawcy / usługodawcy, ryzyko związane z brakiem ciągłości w świadczeniu usługi, w wyniku zdarzeń losowych, ryzyko związane z nagłym wycofaniem się usługodawcy ze świadczenia usługi,	Wszyscy aktualni i potencjalni dostawcy	Procedury doboru usługodawców zewnętrznych powinny uwzględniać ryzyko związane z określonymi usługami i obejmować w szczególności ocenę sytuacji ekonomiczno-finansowej usługodawcy oraz jakości świadczonych usług (w miarę możliwości również na podstawie doświadczeń innych podmiotów biznesowych). Ryzyko związane z wyborem dostawcy można minimalizować poprzez zastosowanie odpowiednich procedur zakupowych i przetargowych, skłaniając się również w kierunku wdrożenia strategii dywersyfikacji dostaw.
Spadek jakości świadczonych usług	Wszyscy aktualni i potencjalni dostawcy	Spadek jakości usług może mieć różne przyczyny. Wskazane jest regularne monitorowanie jakości świadczonych usług. Zakres i częstotliwość monitorowania i raportowania powinny uwzględniać specyfikę świadczonych usług oraz ich istotność z perspektywy ciągłości i bezpieczeństwa działania WSS5. Dodatkowym zabezpieczeniem powinna być dywersyfikacja dostawców, która umożliwi płynne przejście od jednego do drugiego dostawcy, w przypadku znaczącego spadku jakości usług.
Pozycja monopolistyczna dostawcy / usługodawcy	Wszyscy aktualni i potencjalni dostawcy	Dywersyfikacja dostaw poprzez zastosowanie odpowiednich procedur zakupowych i przetargowych. Zagwarantowanie alternatywnych dostawców dla kluczowych obszarów jako element strategii przetargowo - zakupowej.
Nieadekwatne zapisy w umowach z dostawcami lub brak umów	Wszyscy aktualni i potencjalni dostawcy	Brak umowy może oznaczać równocześnie brak sformalizowanego narzędzia regulującego współpracę, brak zdefiniowanych ścieżek rozwiązywania sporów na linii zleceniodawca - zleceniobiorca oraz brak gwarancji dla bezpieczeństwa współpracy
Brak dywersyfikacji dostawców	Wszyscy aktualni i potencjalni dostawcy	Uzależnienie dostaw od jednego dostawcy, może generować wielowarstwowe problemy, min. brak ciągłości dostaw towarów i usług.
Brak płynności dostaw w obszarach kluczowych	Wszyscy aktualni i potencjalni dostawcy	Może prowadzić do utrudnień w codziennym funkcjonowaniu WSS5.

9. ZAKRES UMÓW PODPISYWANYCH Z DOSTAWCAMI.

9.1. Prawidłowo przygotowane umowy mogą zapobiec wystąpieniu problemów w obszarze współpracy z dostawcami i bezpieczeństwa informacji lub ułatwić ich szybkie rozwiązanie. Umowa przewidująca zagrożenia i ryzyka, które mogą wystąpić i zagrozić realizacji dostaw towarów i usług, zwiększa możliwość szybkiego i efektywnego działania. Zabezpieczenie w postaci zastosowania odpowiednich konstrukcji prawnych oddziałuje z jednej strony „prewencyjnie", wskazując pracownikom czy kontrahentom, na ich zobowiązania i potencjalnie negatywne konsekwencje ich niedopełnienia, z drugiej strony „reaktywnie", umożliwiając lub zdecydowanie ułatwiając dochodzenie roszczeń przed sądem.

Rodzaj umowy	Sugerowana zawartość umowy i zasady weryfikacji treści umów
Umowy z zewnętrznymi dostawcami usług teleinformatycznych	- zakresy odpowiedzialności stron umowy, - zakres informacji i dokumentacji przekazywanych przez usługodawcę w ramach świadczonych usług, - zasady wymiany i ochrony informacji, w tym warunki nadawania pracownikom podmiotów zewnętrznych praw dostępu do informacji oraz zasobów środowiska teleinformatycznego WSS5, uwzględniające w szczególności obowiązujące przepisy prawa oraz regulacje WSS5 w tym zakresie; w przypadku usługodawców posiadających dostęp do informacji o wysokim stopniu poufności, powinna zostać również uregulowana kwestia odpowiedzialności za zachowanie tajemnicy tych informacji w okresie wykonywania usług oraz po zakończeniu umowy, - zasady związane z prawami do oprogramowania (w tym jego kodów źródłowych) w trakcie współpracy i po jej zakończeniu, - parametry dotyczące jakości świadczonych usług oraz sposoby ich monitorowania i egzekwowania, - zasady i tryb obsługi zgłoszeń dotyczących problemów w zakresie świadczonych usług, - zasady i tryb dokonywania aktualizacji oprogramowania i komponentów infrastruktury znajdujących się pod kontrolą dostawcy, - zasady współpracy w przypadku wystąpienia incydentu bezpieczeństwa środowiska teleinformatycznego, - zasady w zakresie dalszego zlecania czynności podwykonawcom zewnętrznego dostawcy usług, - kary umowne związane z nieprzestrzeganiem warunków umownych, w szczególności w zakresie bezpieczeństwa informacji przetwarzanych przez dostawcę usług,
Umowy z zewnętrznymi dostawcami towarów i usług niebędących usługami teleinformatycznymi	- zapewnienie, że realizacja umowy odbywać się będzie zgodnie z wymaganiami prawnymi, regulacjami wewnętrznymi i zewnętrznymi oraz przyjętymi w WSS5 standardami, - umowy zawierane przez WSS5 z zewnętrznymi dostawcami usług powinny być weryfikowane w odpowiednim zakresie przez jednostki WSS5 odpowiedzialne za obszar prawny oraz obszar bezpieczeństwa środowiska teleinformatycznego, - regulacje dotyczące współpracy z pracownikami zewnętrznych dostawców usług, uwzględniające w szczególności: • warunki udzielania dostępu do informacji o wysokim stopniu poufności, • zasady sprawowania nadzoru nad działaniami pracowników

	zewnętrznych, • konieczność zapewnienia, że każdy pracownik zewnętrznych dostawców usług objęty jest co najmniej takimi samymi restrykcjami w zakresie bezpieczeństwa, jak pracownicy WSS5,

9.2. Zasady współpracy pomiędzy WSS5, a zewnętrznym dostawcą usług powinny uwzględniać reguły w zakresie komunikacji i koordynacji wykonywanych przez usługodawcę czynności (np. w zakresie przeprowadzania migracji danych, czynności konserwacyjnych, skanowania infrastruktury teleinformatycznej itp.), minimalizujące ich negatywny wpływ na jakość i bezpieczeństwo usług nie tylko teleinformatycznych.

10. KARTA ZMIAN.

Nr karty zmian	Symbol zmian	Podpis	Data	Nr karty zmian	Symbol zmian	Podpis	Data

Oświadczenie pracowników

.....

(komórka organizacyjna WSS5 - pieczątka)

Oświadczam, że zapoznałem/am się z treścią niniejszej polityki zobowiązuję się do przestrzegania wszystkich zaleceń w niej zawartych

.....

(nazwa instrukcji)

L.p	Nazwisko i imię	Stanowisko	Data	Podpis