Załącznik nr 1

OPIS PRZEDMIOTU ZAMÓWIENIA

Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Grudziądzu w ramach projektu „Podniesienie poziomu cyberbezpieczeństwa w Urzędzie Miejskim w Grudziądzu", zgodnie z Regulaminem Konkursu Grantowego „Cyberbezpieczny Samorząd" opublikowanego na stronie Centrum Projektów Polska Cyfrowa pod adresem: https://www.gov.pl/web/cppc/cyberbezpczny-samorzad. Przez skrót KSC rozumie się Krajowy System Cyberbezpieczeństwa, a przez skrót KRI rozumie się Krajowe Ramy Interoperacyjności.

1. ETAP I - Przeprowadzenie audytu wstępnego

Wykonawca przeprowadzi audyt dotyczący istniejącego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

Głównym celem audytu jest wykrycie potencjalnych luk i niezgodności w obszarze cyberbezpieczeństwa, które mogą wpływać na bezpieczeństwo systemów i danych Zamawiającego oraz ocena zgodności z wewnętrznymi politykami i procedurami bezpieczeństwa.

Przed rozpoczęciem audytu Wykonawca przeprowadzi wizję lokalną oraz zorganizuje wywiady z pracownikami, co umożliwi dokładniejsze zidentyfikowanie istniejących zagrożeń oraz ocenę aktualnego poziomu zabezpieczeń.

2. ETAP II - Opracowanie dokumentacji i procedur SZBI zgodnej z KSC i KRI. Wykonawca musi stworzyć kompleksową dokumentację, w tym Polityki Bezpieczeństwa Informacji, procedury operacyjne oraz procedury reagowania na incydenty.

Opracowanie SZBI ma zapewnić spełnienie wymogów Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2024, poz. 773) wydanego na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2024 r. poz. 1557 ze zm.).

2.1. Opracowanie dokumentacji i procedur SZBI

Wykonawca musi opracować kompletną dokumentację Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Struktura dokumentacji powinna być jasna i zrozumiała dla wszystkich użytkowników systemu Urzędu Miejskiego w Grudziądzu. Dokumentacja ma być zorganizowana w sposób umożliwiający łatwy dostęp dom poszczególnych sekcji i procedur, co ułatwi zarządzanie systemem i jego przegląd. Format dokumentacji powinien obejmować wersje elektroniczne, zapewniające pełną dostępność i możliwość archiwizacji, a także dostępność dla osób o różnych potrzebach, w tym osoby

z niepełnosprawnościami oraz promując praktyki zapewniające równość i niedyskryminację. Wersja w postaci papierowej nie jest wymagana.

2.2 Tworzenie Polityki Bezpieczeństwa Informacji

Wykonawca musi opracować Politykę Bezpieczeństwa Informacji, która stanie się fundamentem dla wszystkich działań związanych z ochroną informacji w Urzędzie Miejskim w Grudziądzu. Polityka Bezpieczeństwa Informacji musi określać główne zasady ochrony danych i informacji, cele bezpieczeństwa, a także zobowiązania organizacji do ciągłego doskonalenia SZBI. Polityka Bezpieczeństwa Informacji musi również uwzględniać wymagania prawne, regulacyjne oraz zobowiązania kontraktowe względem klientów i partnerów.

2.3 Opracowanie procedur operacyjnych i kontrolnych

Wykonawca musi opracować szczegółowe procedury operacyjne i kontrolne, które umożliwią skuteczne zarządzanie SZBI i odpowiednie reagowanie na incydenty bezpieczeństwa. Procedury te muszą zawierać instrukcje dotyczące zarządzania aktywami, zarządzania dostępem, oceny ryzyka, zarządzania incydentami bezpieczeństwa oraz procedur odzyskiwania danych. Procedury muszą uwzględniać mechanizmy monitorowania i przeglądu efektywności działań bezpieczeństwa, zapewniające ciągłą ochronę informacji zgodnie z najnowszymi standardami i najlepszymi praktykami.

2.4 Tabela z wykazem minimalnej ilości opisanych dokumentów (lub ich wzorów) i procedur, które wykonawca musi dostarczyć w ramach zamówienia. Dodatkowo, jeżeli wykonawca uzna, że konieczne jest dołączenie dodatkowych dokumentów lub procedur, może je włączyć do projektu w ramach wdrożenia, aby jeszcze bardziej dostosować system do specyficznych potrzeb Urzędu Miejskiego w Grudziądzu. Zamawiający dopuszcza także dokonywanie zmian w poniższej mapie dokumentów i procedur, o ile wprowadzone modyfikacje będą obejmowały obszar bezpieczeństwa ujęty w kolumnie “opis” .

Lp.	Nazwa procedury, polityki, dokumentacji	Opis
1	Kontekst organizacji	Dokument musi zawierać kompleksową analizę kontekstu operacyjnego organizacji, identyfikując wewnętrzne i zewnętrzne czynniki, które mogą wpłynąć na zarządzanie bezpieczeństwem informacji. Dokument musi określać zakres Systemu Zarządzania Bezpieczeństwem Informacji, obejmujący zidentyfikowane wymagania biznesowe, prawne i regulacyjne.

2	Podręcznik Systemu Zarządzania Bezpieczeństwem Informacji	Celem dokumentu jest dostarczenie kompleksowego przeglądu i wskazówek dotyczących wszystkich aspektów SZBI zaimplementowanego w organizacji. Podręcznik ten musi zawierać szczegółowy opis systemu, jego celów, zakresu działania oraz mechanizmów kontroli wdrażanych w celu ochrony danych i informacji przed potencjalnymi zagrożeniami.
3	Role, odpowiedzialności i uprawnienia w zakresie bezpieczeństwa informacji	Dokument Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), który ma zdefiniować strukturę organizacyjną oraz określa konkretne role i odpowiedzialności osób zaangażowanych w procesy bezpieczeństwa informacji. Dokument ten ma za zadanie zapewnić, że każdy pracownik, zarówno na poziomie kierowniczym, jak i operacyjnym, będzie rozumiał swoje zadania w kontekście ochrony danych i informacji oraz był świadomy swoich uprawnień do zarządzania zasobami informacyjnymi.
4	Deklaracja wsparcia kierownictwa (wzór)	Dokumentem będący zobowiązaniem i poparciem najwyższego kierownictwa dla wdrożenia i utrzymania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)
5	Polityka Bezpieczeństwa Informacji	Dokument w ramach Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), który określa ogólne zasady i kierunki działania organizacji w zakresie ochrony danych i informacji.
6	Protokół zebrania (wzór)	Formalny dokument, który służy do zapisywania kluczowych decyzji, działań i informacji omawianych podczas spotkań związanych z zarządzaniem bezpieczeństwem informacji.
7	Cele i plan bezpieczeństwa informacji	Dokument "Cele i plan bezpieczeństwa informacji" musi zawierać szczegółowe wytyczne i cele strategiczne dotyczące zarządzania bezpieczeństwem informacji w organizacji, a także plany ich realizacji.
8	Proces oceny i zarządzania ryzykiem	Dokument musi opisywać metodyki i procedury stosowane do identyfikacji, analizy i oceny ryzyk związanych z bezpieczeństwem informacji, a także strategie ich łagodzenia lub eliminacji.
9	Raport z oceny ryzyka	Dokument musi szczegółowo opisywać wyniki przeprowadzonej oceny ryzyka w organizacji. Musi zawierać analizę potencjalnych zagrożeń dla bezpieczeństwa informacji oraz ocenę

		prawdopodobieństwa ich wystąpienia i potencjalnych skutków.
10	Plan postępowania z ryzykiem	Dokument musi zawierać strategie i środki, które mają na celu zmniejszenie zidentyfikowanych ryzyk do akceptowalnego poziomu. Plan ten musi określać konkretne działania, które należy podjąć, aby zarządzać, zmniejszać lub unikać ryzyk związanych z bezpieczeństwem informacji, zgodnie z priorytetami ustalonymi w ramach oceny ryzyka.
11	Procedury zmian w SZBI	Dokument musi opisywać formalne procedury i kroki potrzebne do wprowadzania zmian w systemie zarządzania bezpieczeństwem informacji.
12	Rejestr zmian SZBI (wzór)	Dokument będzie zawierał chronologiczny zapis wszystkich zmian wprowadzonych w SZBI, w tym szczegółowe informacje na temat natury zmiany, daty jej wprowadzenia, osób odpowiedzialnych oraz wpływu zmian na system zarządzania bezpieczeństwem informacji.
13	Narzędzie do oceny i obróbki ryzyka oparte na aktywach (arkusz kalkulacyjny)	Arkusz kalkulacyjny służący do identyfikacji, oceny i zarządzania ryzykami związanymi z aktywami informacyjnymi w organizacji.
14	Oświadczenie o stosowaniu	Dokument musi opisywać, które z zabezpieczeń (kontrole) zostały wybrane do implementacji w organizacji oraz uzasadnienie dla tych wyborów.
15	Narzędzie do oceny i minimalizacji ryzyka na podstawie scenariuszy (arkusz kalkulacyjny)	Arkusz kalkulacyjny, który ma pozwalać na analizę ryzyka przez modelowanie różnych scenariuszy zagrożeń i ich potencjalnych skutków dla organizacji.
16	Procedura rozwoju kompetencji w zakresie bezpieczeństwa informacji	Dokument musi opisywać zasady i metody, które organizacja stosuje do identyfikacji, rozwijania i utrzymania kompetencji personelu odpowiedzialnego za zarządzanie bezpieczeństwem informacji. Procedura ta musi obejmować szkolenia, ocenę skuteczności szkoleń, a także plany rozwoju dla pracowników, aby zapewnić, że wszystkie osoby zaangażowane w zarządzanie bezpieczeństwem informacji posiadają odpowiednie umiejętności i wiedzę.

17	Procedura komunikacji w zakresie bezpieczeństwa informacji	Dokument musi określać metody, procedury i odpowiedzialności związane z komunikacją wewnętrzną i zewnętrzną dotyczącą aspektów bezpieczeństwa informacji w organizacji. Procedura ten ma na celu zapewnienie, że wszystkie istotne informacje dotyczące bezpieczeństwa są przekazywane odpowiednim osobom w odpowiednim czasie, aby poprawić świadomość i zrozumienie polityk, procedur oraz ryzyk związanych z bezpieczeństwem informacji w całej organizacji.
18	Procedura kontroli dokumentacji	Procedura musi definiować sposoby zarządzania dokumentowanymi informacjami w Systemie Zarządzania Bezpieczeństwem Informacji (SZBI). Procedura musi określać, jak dokumenty powinny być tworzone, przeglądane, zatwierdzane, dystrybuowane oraz jak należy je przechowywać i niszczyć.
19	Rejestr dokumentacji SZBI	Dokument musi zawierać pełną listę wszystkich dokumentów związanych z SZBI, w tym daty ich utworzenia, aktualizacji, przeglądu oraz zatwierdzenia.
20	Raport z rozwoju kompetencji w zakresie bezpieczeństwa informacji (wzór)	Dokument musi zawierać szczegółowe informacje i analizę efektywności programów szkoleniowych i inicjatyw realizowanych w celu poprawy kompetencji personelu w obszarze bezpieczeństwa informacji.
21	Wzajemne powiązania procesów SZBI	Dokument musi opisywać, jak różne procesy w ramach SZBI są ze sobą powiązane i współdziałają. Musi zawierać schemat lub mapę procesów, która ilustruje relacje i przepływy informacji między poszczególnymi elementami systemu.
22	Proces monitorowania, pomiaru, analizy i oceny	Dokument musi opisywać metody i techniki stosowane do oceny efektywności Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Proces ten musi obejmować regularne monitorowanie i mierzenie kluczowych wskaźników bezpieczeństwa, analizę zebranych danych oraz ocenę, czy cele bezpieczeństwa są osiągane.
23	Procedura zarządzania niezgodnościami	Dokument musi opisywać metody i procesy stosowane do identyfikacji, dokumentowania, analizy oraz zarządzania wszelkimi niezgodnościami w stosunku do wymagań Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

24	Rejestr niezgodności i działań korekcyjnych (wzór)	Dokument musi służyć do dokumentowania wszelkich stwierdzonych niezgodności w stosunku do wymagań Systemu Zarządzania Bezpieczeństwem Informacji oraz opisania podjętych działań korekcyjnych, mających na celu eliminację przyczyn tych niezgodności.
25	Harmonogram regularnych działań w SZBI (wzór)	Dokument to narzędzie planistyczne, które musi szczegółowo określać czas i zakres regularnie przeprowadzanych działań w ramach SZBI, mających na celu utrzymanie i poprawę poziomu bezpieczeństwa informacji.
26	Polityka korzystania z mediów społecznościowych	Dokument musi określać wytyczne i zasady dotyczące bezpiecznego i odpowiedzialnego użytkowania platform społecznościowych przez pracowników organizacji. Ma na celu ochronę informacji oraz reputacji urzędu w cyfrowym środowisku, zapobiegając nieautoryzowanemu ujawnianiu poufnych danych oraz promując odpowiednie i profesjonalne zachowania online.
27	Polityka bezpieczeństwa zasobów ludzkich	Dokument musi określać zasady i procedury związane z zarządzaniem bezpieczeństwem informacji w obszarze zasobów ludzkich. Polityka ta musi obejmować aspekty takie jak bezpieczeństwo danych pracowników, procesy rekrutacyjne, szkolenia z zakresu bezpieczeństwa informacji oraz procedury postępowania w przypadku zakończenia współpracy z pracownikiem.
28	Wytyczne dotyczące segregacji (rozdzielenie) obowiązków wraz z formularzem.	Wytyczne muszą opisywać zasady i procedury rozdzielenia obowiązków i uprawnień w ramach organizacji, aby zapobiegać konfliktom interesów, oszustwom oraz błędom. Formularz ma być narzędziem służącym do dokumentowania i analizy rozdzielenia obowiązków w organizacji w postaci np. arkusza kalkulacyjnego. Musi on umożliwiać identyfikację i zarządzanie potencjalnymi konfliktami interesów oraz ryzykiem nadużyć poprzez zapewnienie, że kluczowe zadania i odpowiedzialności są rozdzielone między różnych pracowników.
29	Polityka sygnalizacji naruszeń bezpieczeństwa informacji	Dokument musi określać zasady i procedury dla pracowników i współpracowników organizacji dotyczące zgłaszania wszelkich obaw lub podejrzeń o naruszenia zasad bezpieczeństwa informacji.

30	Kontakty z organami władzy	Dokument musi zawierać listę kontaktów do odpowiednich organów regulacyjnych i nadzorczych, które są istotne w kontekście przestrzegania prawnych i regulacyjnych wymagań dotyczących bezpieczeństwa informacji.
31	Kontakty z grupami zainteresowanych specjalistów	Dokument musi zawierać informacje kontaktowe do grup specjalistycznych, które zajmują się konkretnymi aspektami bezpieczeństwa informacji, takimi jak cyberbezpieczeństwo, ochrona danych osobowych, czy zarządzanie ryzykiem.
32	Polityka wywiadu w zakresie zagrożeń	Dokument musi określać zasady i metodyki gromadzenia, analizowania i wykorzystywania informacji o aktualnych i potencjalnych zagrożeniach bezpieczeństwa informacji.
33	Proces rozpoznawania zagrożeń	Dokument musi opisywać szczegółowo procedury i działania, które organizacja będzie realizować, aby skutecznie identyfikować, analizować i reagować na zagrożenia bezpieczeństwa informacji.
34	Wytyczne bezpieczeństwa informacji dla zarządzania projektami	Dokument musi definiować standardy i praktyki dotyczące wdrażania i utrzymywania bezpieczeństwa informacji w trakcie realizacji projektów.
35	Polityka zarządzania aktywami	Dokument musi określać zasady i procedury zarządzania aktywami informacyjnymi organizacji, w tym ich identyfikację, klasyfikację, użytkowanie i ochronę.
36	Inwentaryzacja aktywów informacyjnych	Dokument musi zawierać szczegółowy wykaz wszystkich aktywów informacyjnych, które organizacja posiada i za które odpowiada.
37	Polityka akceptowalnego użytkowania zasobów informacyjnych	Dokument musi definiować standardy i zasady odpowiedniego użytkowania zasobów informacyjnych organizacji przez jej pracowników i inne uprawnione osoby.
38	Polityka dostępu do Internetu	Dokument musi określać zasady i wytyczne dotyczące korzystania z Internetu przez pracowników oraz inne osoby mające dostęp do zasobów sieciowych organizacji.
39	Polityka komunikacji elektronicznej	Dokument musi określać zasady i procedury dotyczące bezpiecznego wykorzystywania narzędzi do komunikacji elektronicznej, takich jak e-mail,

		komunikatory internetowe oraz inne formy cyfrowego przekazu informacji.
40	Procedura postępowania z aktywami	Procedura musi opisywać zasady i procesy zarządzania aktywami informacyjnymi, obejmujące identyfikację, klasyfikację, przechowywanie, ochronę, a także usuwanie aktywów.
41	Procedura zarządzania utraconymi lub skradzionymi urządzeniami	Procedura musi określać kroki i działania, jakie należy podjąć w przypadku utraty lub kradzieży urządzeń zawierających informacje organizacji. Procedura ta musi obejmować zgłaszanie incydentu, ocenę ryzyka związanego z utratą danych, a także środki zaradcze i kroki mające na celu minimalizowanie potencjalnych szkód.
42	Polityka współpracy online	Polityka musi określać zasady i wytyczne dotyczące bezpiecznego korzystania z narzędzi do współpracy online, takich jak platformy do zarządzania projektami, narzędzia komunikacyjne i systemy do udostępniania plików.
43	Lista kontrolna dla nowego pracownika	Dokument ma być narzędziem używanym do zapewnienia, że nowi pracownicy przechodzą przez wszystkie niezbędne kroki w procesie wdrażania, zgodnie z politykami i procedurami bezpieczeństwa informacji organizacji. Lista ta musi obejmować elementy takie jak szkolenia z zakresu bezpieczeństwa, dostęp do zasobów informacyjnych, oraz zrozumienie zasad i procedur bezpieczeństwa.
44	Procedura klasyfikacji informacji	Procedura musi opisywać zasady i metody klasyfikowania informacji w organizacji, w celu zapewnienia odpowiedniego poziomu ochrony dla różnych rodzajów danych. Procedura ta musi określać kryteria klasyfikacji, kategorie informacji oraz wymagania dotyczące obsługi, przechowywania i udostępniania informacji,
45	Procedura etykietowania informacji	Procedura musi opisywać zasady i procesy związane z etykietowaniem informacji w organizacji. Celem tej procedury ma być zapewnienie, że wszystkie informacje są odpowiednio oznakowane zgodnie z ich klasyfikacją.
46	Procedura przesyłania informacji	Procedura musi opisywać zasady i metody bezpiecznego przesyłania informacji zarówno wewnątrz organizacji, jak i na zewnątrz.

47	Polityka kontroli dostępu	Polityka musi określić zasady i procedury dotyczące zarządzania dostępem do zasobów informacyjnych organizacji.
48	Proces zarządzania dostępem użytkowników	Proces musi opisywać zasady i procedury dotyczące przyznawania, modyfikowania i wycofywania dostępu użytkowników do zasobów informacyjnych organizacji.
49	Polityka bezpieczeństwa informacji w relacjach z dostawcami	Polityka musi określać zasady i wymagania dotyczące zarządzania bezpieczeństwem informacji w relacjach z dostawcami.
50	Umowa o bezpieczeństwie informacji z dostawcą (wzór)	Dokument musi określać zasady, warunki i wymagania dotyczące bezpieczeństwa informacji, które muszą być przestrzegane przez dostawców współpracujących z organizacją.
51	Procedura oceny należytej staranności dostawcy	Procedura musi opisywać zasady i metody przeprowadzania oceny dostawców w zakresie zgodności z wymaganiami bezpieczeństwa informacji.
52	Ocena należytej staranności dostawcy (arkusz kalkulacyjny)	Formularz będący narzędziem używanym do oceny dostawców pod kątem zgodności z wymaganiami bezpieczeństwa informacji.
53	Proces oceny bezpieczeństwa informacji u dostawcy	Proces musi opisywać zasady i procedury oceny dostawców pod kątem zgodności z wymaganiami bezpieczeństwa informacji.
54	Polityka korzystania z usług chmurowych	Polityka musi określać zasady i wytyczne dotyczące korzystania z usług chmurowych przez organizację.
55	Proces zarządzania usługami chmurowymi	Proces musi opisywać zasady i procedury dotyczące zarządzania usługami chmurowymi w organizacji.
56	Plan reagowania na incydenty ransomware	Plan musi opisywać zasady i procedury dotyczące postępowania w przypadku ataku ransomware na organizację. Celem tego planu ma być szybkie i skuteczne reagowanie na incydenty ransomware, minimalizowanie wpływu na operacje oraz zabezpieczanie danych. Plan musi obejmować kroki takie jak identyfikacja incydentu, izolacja zainfekowanych systemów, analiza i odzyskiwanie danych oraz komunikacja z odpowiednimi interesariuszami.
57	Plan reagowania na incydenty typu Denial of Service (DoS)	Plan musi opisywać zasady i procedury dotyczące postępowania w przypadku ataku DoS na organizację.

58	Plan reagowania na incydenty naruszenia bezpieczeństwa danych	Plan musi opisywać zasady i procedury dotyczące postępowania w przypadku naruszenia bezpieczeństwa danych w organizacji.
59	Procedura oceny zdarzeń bezpieczeństwa informacji	Procedura musi opisywać zasady i procedury dotyczące oceny zdarzeń związanych z bezpieczeństwem informacji w organizacji.
60	Procedura reagowania na incydenty bezpieczeństwa informacji	Procedura musi opisywać zasady i procedury dotyczące reakcji na incydenty związane z bezpieczeństwem informacji w organizacji.
61	Raport z wniosków wyciągniętych z incydentu (wzór)	Raport musi być narzędziem używanym do dokumentowania wniosków i lekcji wyciągniętych po analizie incydentów bezpieczeństwa informacji.
62	Proces analizy wpływu potencjalnych zdarzeń bezpieczeństwa na organizację	Proces musi opisywać zasady i procedury dotyczące oceny wpływu potencjalnych zdarzeń bezpieczeństwa na działalność organizacji. Celem tego procesu ma być identyfikacja krytycznych zasobów i procesów w organizacji, ocena potencjalnych konsekwencji ich zakłócenia oraz określenie priorytetów dla działań naprawczych.
63	Procedura reagowania na incydenty ciągłości działania ICT	Procedura musi opisywać zasady i procedury dotyczące reagowania na incydenty, które mogą zakłócić ciągłość działania systemów informatycznych organizacji.
64	Plan ciągłości działania ICT	Plan musi opisywać strategię i działania niezbędną do utrzymania i przywracania kluczowych usług informatycznych w przypadku wystąpienia zakłóceń.
65	Harmonogram ćwiczeń i testów ciągłości działania ICT	Harmonogram musi określić plan regularnych ćwiczeń i testów mających na celu sprawdzenie skuteczności planu ciągłości działania ICT.
66	Plan testów ciągłości działania ICT	Plan musi opisywać zasady i procedury przeprowadzania testów ciągłości działania systemów informatycznych.
67	Raport z testów ciągłości działania ICT (wzór)	Raport musi zawierać wyniki testów przeprowadzonych w celu oceny skuteczności planów ciągłości działania systemów informatycznych.
68	Procedura wymagań prawnych, regulacyjnych i kontraktowych	Procedura musi opisywać zasady i procedury identyfikacji, oceny i zarządzania wymaganiami prawnymi, regulacyjnymi i kontraktowymi, które mają wpływ na bezpieczeństwo informacji w organizacji.
69	Wymagania prawne, regulacyjne i kontraktowe	Dokument musi zawierać zestawienie i opis wymagań, które organizacja musi spełnić w kontekście zarządzania bezpieczeństwem informacji.

70	Polityka zgodności z prawami własności intelektualnej i prawami autorskimi	Polityka musi opisywać zasady i procedury dotyczące przestrzegania praw własności intelektualnej oraz praw autorskich w organizacji.
71	Procedura weryfikacji pracowników	Procedura musi opisywać zasady i procedury dotyczące sprawdzania przeszłości i kwalifikacji pracowników przed ich zatrudnieniem w organizacji.
72	Lista kontrolna weryfikacji pracowników (arkusz kalkulacyjny)	Narzędzie (arkusz kalkulacyjny) który ma służyć do sprawdzania, czy procesy rekrutacyjne i zarządzanie personelem są zgodne z wymaganiami bezpieczeństwa informacji.
73	Wytyczne dotyczące zapisów do włączenia do umów o pracę	Wytyczne muszą zawierać rekomendacje dotyczące elementów, które powinny znaleźć się w umowach o pracę, aby wspierać politykę bezpieczeństwa informacji
74	Procedura dyscyplinarna dla pracowników	Procedura musi opisywać kroki i zasady postępowania dyscyplinarnego stosowanego w przypadku naruszeń zasad bezpieczeństwa informacji przez pracowników.
75	Lista kontrolna zakończenia zatrudnienia i zmiany warunków pracy	Lista będzie używana do zapewnienia, że wszystkie istotne kwestie bezpieczeństwa są rozważone i odpowiednio zarządzane przy zwolnieniu pracownika lub zmianie jego warunków pracy.
76	Informacja dla osób odchodzących	Informacja musi być dokumentem przekazywanym pracownikom kończącym pracę w organizacji, który musi zawierać informacje dotyczące procedur bezpieczeństwa, obowiązków dotyczących zachowania poufności oraz inne istotne kwestie związane z zakończeniem zatrudnienia.
77	Wykaz umów o poufności (wzór)	Wykaz musi zawierać wykaz wszystkich obowiązujących umów o poufności.
78	Umowa o zachowaniu poufności (wzór)	Umowa musi być standardowym dokumentem prawnokontraktowym, który zobowiązuje pracowników oraz inne zainteresowane strony do zachowania poufności informacji poufnych i wrażliwych, chroniąc tym samym organizację przed ryzykiem wycieku danych.
79	Polityka pracy zdalnej	Polityka musi określać zasady i procedury bezpiecznej pracy zdalnej, które mają na celu ochronę informacji i zasobów organizacji podczas pracy poza tradycyjnym środowiskiem biurowym.

80	Procedura raportowania zdarzeń bezpieczeństwa informacji	Procedura musi opisywać formalne kroki i procesy, które pracownicy i inne osoby powinny podjąć w przypadku wykrycia lub podejrzenia naruszenia bezpieczeństwa informacji.
81	Polityka bezpieczeństwa fizycznego	Polityka musi określać zasady i procedury mające na celu zabezpieczenie fizycznych instalacji, lokalizacji, w których przechowywane są dane i systemy, w tym środki kontroli dostępu, monitoring i zabezpieczenia przeciwpożarowe.
82	Standardy projektowania bezpieczeństwa fizycznego	Standardy muszą zawierać szczegółowe wytyczne dotyczące projektowania i implementacji fizycznych środków bezpieczeństwa, takich jak zabezpieczenia budynków, systemy kontroli dostępu oraz metody zabezpieczenia przed nieautoryzowanym dostępem, mające na celu ochronę zasobów informacyjnych organizacji.
83	Procedura dostępu do centrum przechowywania danych	Procedura musi opisywać zasady i metody kontroli dostępu do centrów przechowywania danych, ma na celu zapewnienie, że tylko upoważnione osoby mogą uzyskać dostęp do kluczowych infrastruktur i danych. Procedura ta musi obejmować wymogi dotyczące identyfikacji, autoryzacji oraz monitorowania dostępów, co jest kluczowe dla zapewnienia bezpieczeństwa informacji w organizacji.
84	Polityka monitoringu wizyjnego CCTV	Polityka musi określać zasady i procedury dotyczące użytkowania systemów monitoringu CCTV w celu zabezpieczenia obiektów i zasobów organizacji. Polityka ta musi regulować aspekty takie jak zakres monitoringu, zarządzanie nagraniami, ochrona prywatności i przestrzeganie przepisów prawnych.
85	Procedura pracy w strefach zabezpieczonych	Procedura musi opisywać standardowe procedury i wymogi dotyczące pracy w obszarach, które wymagają szczególnych środków bezpieczeństwa, takich jak serwerownie czy archiwa danych.
86	Polityka czystego biurka i czystego ekranu	Polityka musi nakładać na pracowników obowiązek utrzymania porządku na biurkach i ekranach komputerów w celu minimalizowania ryzyka nieautoryzowanego dostępu do poufnych informacji i zasobów.
87	Procedura wynoszenia zasobów poza teren firmy	Procedura musi, określać zasady i procedury, które muszą być przestrzegane podczas

		przenoszenia zasobów informacyjnych lub innych kluczowych zasobów poza siedzibę firmy.
88	Procedura zarządzania nośnikami wymiennymi	Procedura musi opisywać protokoły i środki bezpieczeństwa, które należy zastosować przy użyciu nośników wymiennych, takich jak pendrive'y, dyski zewnętrzne czy płyty CD/DVD.
89	Procedura przekazywania nośników fizycznych	Procedura musi określać zasady i metody bezpiecznego przekazywania nośników danych, takich jak dyski twarde, płyty CD/DVD, pendrive'y, między różnymi lokalizacjami lub osobami wewnątrz organizacji.
90	Harmonogram konserwacji sprzętu (wzór)	Harmonogram ma być dokumentem służącym do planowania i śledzenia regularnych prac konserwacyjnych sprzętu IT, co ma na celu zapewnienie ciągłości działania systemów i ochrony danych przed ryzykiem awarii technicznej.
91	Procedura utylizacji nośników danych	Procedura musi opisywać metody bezpiecznego usuwania lub niszczenia nośników danych, takich jak dyski twarde, płyty CD, pendrive'y oraz inne media zawierające poufne informacje, które mają być wycofane z użycia.
92	Polityka urządzeń mobilnych	Polityka musi określać zasady korzystania z urządzeń mobilnych, takich jak smartfony i tablety, w kontekście codziennej pracy. Polityka musi zawierać wytyczne dotyczące zabezpieczeń, zarządzania, użytkowania oraz odpowiedzialności pracowników w celu minimalizacji ryzyk związanych z bezpieczeństwem danych i dostępem do systemów wykorzystywanych przez organizację z urządzeń mobilnych
93	Polityka BYOD	Polityka musi określać zasady i wytyczne dla pracowników korzystających z własnych urządzeń mobilnych (np. smartfonów, tabletów, laptopów) w celach służbowych. Polityka ta ma mieć na celu zabezpieczenie informacji firmowych przed zagrożeniami związanymi z prywatnymi urządzeniami, regulując dostęp do firmowych zasobów i zarządzając bezpieczeństwem tych urządzeń.
94	Polityka dynamicznej kontroli dostępu	Polityka musi opisuje zasady i metody zarządzania dostępem do systemów i danych na podstawie kontekstu, roli użytkownika oraz innych czynników (np. dostęp zależny od daty i czasu, roli użytkownika i kontekstu).

95	Polityka przeciwdziałania złośliwemu oprogramowaniu	Polityka musi określać strategie i procedury zastosowane przez organizację w celu zapobiegania, wykrywania i reagowania na złośliwe oprogramowanie.
96	Polityka zarządzania podatnościami technicznymi	Polityka musi określać metodyki i procedury służące do identyfikacji, oceny, reagowania i zarządzania podatnościami technicznymi w infrastrukturze informatycznej.
97	Procedura oceny podatności technicznych	Procedura musi określać kroki, które należy podjąć, aby systematycznie oceniać podatności w systemach i aplikacjach.
98	Polityka zarządzania konfiguracją	Polityka musi definiować zasady i procedury dotyczące odpowiedniego zarządzania konfiguracją sprzętu, oprogramowania oraz innych elementów systemów IT w organizacji.
99	Proces zarządzania konfiguracją	Proces musi opisywać szczegółowe procedury i kroki niezbędne do efektywnego zarządzania konfiguracją sprzętu i oprogramowania.
100	Polityka usuwania informacji	Polityka musi definiować procedury i metody usuwania danych, które nie są już potrzebne lub które muszą być usunięte zgodnie z obowiązującymi przepisami o ochronie danych.
101	Polityka zapobiegania wyciekom danych	Polityka musi definiować zasady i procedury mające na celu identyfikację, monitorowanie i ochronę poufnych danych organizacji, aby zapobiec ich przypadkowemu lub umyślnemu ujawnieniu poza kontrolowane środowisko.
102	Polityka tworzenia kopii zapasowych	Polityka musi określać zasady i procedury dotyczące tworzenia, przechowywania oraz testowania kopii zapasowych danych.
103	Polityka zarządzania ciągłością działania	Polityka musi definiować zasady i praktyki mające na celu zapewnienie ciągłej dostępności zasobów informatycznych i usług krytycznych dla funkcjonowania organizacji.
104	Polityka logowania i monitorowania	Polityka musi definiować zasady i procedury dotyczące systematycznego rejestrowania i monitorowania działań w systemach informacyjnych.
105	Polityka monitorowania	Polityka musi określać zasady i metody monitorowania działalności sieci, systemów oraz użytkowników w celu zapewnienia bezpieczeństwa informacji, identyfikacji potencjalnych zagrożeń oraz wsparcia dla procesów audytowych i zgodności z przepisami.

106	Rejestr programów narzędziowych z uprawnieniami specjalnymi (wzór)	Celem tego rejestru jest zapewnienie, że tylko autoryzowane i odpowiednio monitorowane osoby mają dostęp do narzędzi, które mogą wpływać na bezpieczeństwo systemów informacyjnych.
107	Polityka oprogramowania	Polityka musi definiować zasady dotyczące zakupu, instalacji, zarządzania i usuwania oprogramowania w organizacji.
108	Polityka bezpieczeństwa sieci	Polityka musi określać zasady i procedury dotyczące zarządzania i zabezpieczania sieci komputerowych organizacji.
109	Obowiązkowe zapisy w umowie o świadczenie usług sieciowych	Obowiązkowe zapisy umowne muszą opisywać warunki i zobowiązania związane z dostarczaniem usług sieciowych przez zewnętrznych dostawców lub wewnątrz organizacji.
110	Polityka filtrowania treści internetowych	Polityka musi określać zasady dotyczące monitorowania i kontroli dostępu do internetowych zasobów w celu zapobiegania dostępu do nieodpowiednich lub szkodliwych treści.
111	Polityka kryptografii	Polityka musi określać zasady dotyczące stosowania kryptografii w celu ochrony poufności, integralności i dostępności danych.
112	Proces zarządzania zmianami	Proces musi definiować procedury i kroki, które należy podjąć, aby zapewnić, że wszystkie zmiany w infrastrukturze IT są dokonywane w kontrolowany, bezpieczny i efektywny sposób.

2.5 Harmonogram wdrożenia

Zamawiający wymaga od Wykonawcy opracowania harmonogramu opracowania dokumentacji SZBI, od przygotowania planu wdrożeniowego po pełne opracowanie finalnej dokumentacji. Harmonogram ten musi być zatwierdzony przez Zamawiającego przed rozpoczęciem implementacji.

2.5.1.Szczegółowe wymagania dotyczące harmonogramu są następujące:

a) Harmonogram musi zostać przedłożony zamawiającemu do akceptacji przed rozpoczęciem jakichkolwiek działań w ramach projektu. Zatwierdzenie to musi być udokumentowane i może wymagać modyfikacji na żądanie zamawiającego w celu lepszego dopasowania do warunków operacyjnych zamawiającego.

b) Wykonawca jest zobowiązany do regularnego przeglądu i aktualizacji harmonogramu w odpowiedzi na zmieniające się okoliczności projektu lub na wniosek zamawiającego. Wszelkie zmiany w harmonogramie muszą być niezwłocznie komunikowane zamawiającemu i podlegają jego zatwierdzeniu.

c) Wykonawca jest odpowiedzialny za monitorowanie postępów w realizacji harmonogramu i regularne raportowanie statusu zamawiającemu. Raporty powinny zawierać informacje o ukończonych, bieżących oraz planowanych działaniach, a także o wszelkich wyzwaniach czy odchyleniach od pierwotnego planu. Wysyłanie raportu przez Wykonawcę powinno następować nie rzadziej niż raz na 30 dni.

2.5.2 Przygotowanie i zatwierdzenie planu wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI),

Wykonawca opracuje i zatwierdzi w porozumieniu z zamawiającym plan wdrożenia, który określi kluczowe działania, ich kolejność, przypisane zasoby, odpowiedzialności i terminy. Plan powinien także uwzględniać wszelkie zależności między działaniami oraz sposoby ich zarządzania.

2.5.3 Opracowanie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI):

a) Wykonawca musi zapewnić aby wszystkie komponenty SZBI, zapewniały ich integrację oraz funkcjonalność.
b) Wykonawca musi opracować i zaimplementować politykę bezpieczeństwa informacji, która będzie integralnie powiązana z kluczowymi procesami biznesowymi zamawiającego. Polityka ta określi standardy, procedury oraz odpowiedzialności związane z zarządzaniem informacjami.
c) Wykonawca musi zapewnić, że wszystkie wymagane dokumenty, takie jak polityki, procedury, instrukcje operacyjne i rejestry ryzyka, będą opracowane.
d) Wykonawca opracuje szablony dokumentów i narzędzia wspomagające, które będą wykorzystywane w codziennej pracy związanej z SZBI, takie jak formularze do zgłaszania incydentów bezpieczeństwa, checklisty audytowe, narzędzia do monitorowania zgodności itp.
e) Wykonawca stworzy i zaimplementuje procedury odpowiedzi na incydenty bezpieczeństwa informacji, które określą, jak identyfikować, reagować i zarządzać incydentami.

3. ETAP III - Przeprowadzenie szkoleń

Wykonawca przeprowadzi szkolenia w celu wsparcia pracowników zatrudnionych u Zamawiającego, którzy mają stosować się do nowo powstałej dokumentacji:

1) 2 szkolenia dla kadry kierowniczej po 120 minut każde, w siedzibie Zamawiającego dla około 60 pracowników
2) 2 szkolenia dla pracowników zatrudnionych u Zamawiającego w czasie trwania do 240 minut, w siedzibie Zamawiającego dla około 40 pracowników

Szkolenia realizowane w ramach zamówienia będą przeprowadzane przez wykwalifikowanego szkoleniowca posiadającego odpowiednie kompetencje, wiedzę merytoryczną oraz doświadczenie w prowadzeniu szkoleń z zakresu objętego zamówieniem.

Wykonawca zobowiązany będzie do udokumentowania przeprowadzenia szkoleń, tj. po realizacji III etapu przekaże dokumenty: program szkolenia, listy obecności.

4. ETAP IV - Audyt końcowy

1) Wykonawca przeprowadzi audyt końcowy, którego celem będzie ocena wdrożenia zaleceń oraz sprawdzenie poprawy stanu cyberbezpieczeństwa w odniesieniu do wniosków z audytu wstępnego. Wynikiem audytu końcowego zgodnie z wymogami programu Cyberbezpieczny Samorząd będzie uzupełniona ankieta, której wzór stanowi Załącznik nr 8 do zapytania ofertowego.

2) Wykonawca zobowiązuje się do przeprowadzenia audytu wdrożonego systemu zarządzania bezpieczeństwem informacji w związku z obowiązkiem ciążącym na Zamawiającym jako na kierownictwie podmiotu publicznego zgodnie z zapisami w § 20 ust. 2 pkt 14 rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2017 poz. 2247). Zakres audytu systemu bezpieczeństwa informacji wdrożonego w urzędzie JST obejmie zgodność z kryteriami zawartymi w § 20 ust. 2 ww. rozporządzenia KRI lub zgodność z wymaganiami normy PN-ISO/IEC 27001;

3) Wykonawca wykona raport z audytu systemu bezpieczeństwa informacji wdrożonego w urzędzie JST, który zostanie podpisany przez audytora dokonującego audyt systemu bezpieczeństwa informacji wdrożonego w urzędzie JST i dostarczony do Grantobiorcy (audytora zewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999) lub audytora wewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999) lub będącego audytorem zewnętrznym systemu zarządzania bezpieczeństwem informacji według normy PN-ISO/IEC 27001).