Cele stosowania zabezpieczeń i zabezpieczenia

A.5 Polityki bezpieczeństwa informacji		
A.5.1 Kierunki bezpieczeństwa informacji określane przez kierownictwo		
Cel: Zapewnienie przez kierownictwo wytycznych i wsparcia dla działań na rzecz bezpieczeństwa informacji, zgodnie z wymaganiami biznesowymi oraz właściwymi normami prawnymi i regulacjami.		
A.5.1.1	Polityki bezpieczeństwa informacji	Polityka Zintegrowanego Systemu Zarządzania, Polityka Bezpieczeństwa Informacji w Urzędzie Miasta Płocka oraz Deklaracja stosowania wymagań normy PN-ISO/IEC 27001:2017-06 zostały zatwierdzone przez kierownictwo i opublikowane w intranecie do wiadomości wszystkich pracowników oraz w BIP-ie Urzędu Miasta Płocka. Zakomunikowano tym samym te dokumenty właściwym stronom zewnętrznym. Polityka Bezpieczeństwa Informacji wspierana jest przez polityki tematyczne, standardy i zasady. ***Uzasadnienie wyboru zabezpieczenia: poinformowanie pracowników i innych stron zainteresowanych o celach bezpieczeństwa informacji i zobowiązaniu do spełnienia mających zastosowanie wymagań z zakresu bezpieczeństwa informacji w Urzędzie Miasta Płocka oraz ciągłego doskonalenia w tym obszarze.***
A.5.1.2	Przegląd polityk bezpieczeństwa informacji	Polityka Zintegrowanego Systemu Zarządzania, Polityka Bezpieczeństwa Informacji w Urzędzie Miasta Płocka oraz Deklaracja stosowania wymagań normy PN-ISO/IEC 27001:2017-06 są poddawane przeglądom i aktualizacjom w ramach procedury "Przegląd systemu przez Kierownictwo" oraz „Nadzór nad udokumentowanymi informacjami”. ***Uzasadnienie wyboru zabezpieczenia: zachowanie aktualności i adekwatności Polityki ZSZ, Polityki SZBI i innych dokumentów systemowych.***
A.6 Organizacja bezpieczeństwa informacji		
A.6.1 Organizacja wewnętrzna		
Cel: Ustanowić strukturę zarządzania w celu zainicjowania oraz nadzorowania, wdrażania i eksploatacji bezpieczeństwa informacji w organizacji.		
A.6.1.1	Role i odpowiedzialność za bezpieczeństwo informacji	Kierownictwo aktywnie wspiera bezpieczeństwo informacji w całej organizacji wskazując kierunki działania, oraz przyjmując odpowiedzialność w zakresie bezpieczeństwa informacji. Odpowiedzialność za ochronę poszczególnych aktywów i realizację określonych procesów bezpieczeństwa informacji została zdefiniowana. ***Uzasadnienie wyboru zabezpieczenia: zapewnienie zasobów ludzkich, materialnych i organizacyjnych odpowiednich dla utrzymywania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji w Urzędzie Miasta Płocka.***
A.6.1.2	Rozdzielanie obowiązków	Obowiązki i odpowiedzialności są w Urzędzie Miasta Płocka rozdzielone zgodnie z zapisami Regulaminu Organizacyjnego, regulaminów wewnętrznych poszczególnych komórek organizacyjnych Urzędu oraz właściwych dokumentów systemowych Zintegrowanego Systemu Zarządzania. ***Uzasadnienie wyboru zabezpieczenia: zapewnienie, że wszystkie osoby pełniące rolę w zarządzaniu bezpieczeństwem informacji są świadome swoich uprawnień i obowiązków w systemie.***

A.6.1.3	Kontakty z organami władzy	Dokumentacja ZSZ zawiera zapisy regulujące inicjowanie kontaktów z organami władzy oraz podejmowanie czynności na ich wniosek (kontakty z Prokuraturą, Policją i organami egzekwującymi przestrzeganie przepisów prawa w dziedzinie bezpieczeństwa informacji: Agencją Bezpieczeństwa Wewnętrznego oraz Urzędem Ochrony Danych Osobowych) w sytuacjach, gdy wymaga tego przepis prawa. ***Uzasadnienie wyboru zabezpieczenia: zapewnienie usystematyzowanego przebiegu kontaktów z tymi organami oraz udziału w nich wszystkich właściwych pracowników organizacji.***
A.6.1.4	Kontrakty z grupami zainteresowanych specjalistów	Organizacja utrzymuje stosowne kontakty z grupami zainteresowanych specjalistów oraz innymi specjalistycznymi forami oraz stowarzyszeniami zawodowymi z obszaru bezpieczeństwa informacji, w tym podmiotami objętymi Krajowym Systemem Cyberbezpieczeństwa. ***Uzasadnienie wyboru zabezpieczenia: ciągłe doskonalenie systemu, korzystanie z dobrych praktyk i doświadczeń innych podmiotów.***
A.6.1.5	Bezpieczeństwo informacji w zarządzaniu projektami	Organizacja zarządzając projektem każdorazowo uwzględnia zagadnienia z obszaru bezpieczeństwa informacji, w tym z wymaganiami stron zainteresowanych. ***Uzasadnienie wyboru zabezpieczenia: zrealizowanie projektu z uwzględnieniem wymogów bezpieczeństwa informacji.***
A.6.2 Urządzenia mobilne i telepraca ***Cel: Zapewnić bezpieczeństwo telepracy i stosowania urządzeń mobilnych***		
A.6.2.1	Polityka stosowania urządzeń mobilnych	Urząd Miasta Płocka wdrożył i utrzymuje Instrukcję podstawowych zasad bezpieczeństwa informacji dla pracowników Urzędu, w której poświęcono odrębny rozdział dla Polityki zarządzania mobilnymi urządzeniami teleinformatycznymi. Ponadto wdrożono Standard konfiguracji urządzeń do pracy zdalnej. ***Uzasadnienie wyboru zabezpieczenia: ustalenie i zakomunikowanie pracownikom Urzędu zasad i zagrożeń związanych z używaniem mobilnych urządzeń teleinformatycznych podczas pracy z informacją stanowiącą własność pracodawcy celem minimalizacji ryzyka utraty informacji podczas incydentu bezpieczeństwa informacji związanego z urządzeniem mobilnym.***
A.6.2.2	Telepraca	Zasady pracy zdalnej zostały określone w Instrukcji podstawowych zasad bezpieczeństwa dla pracowników (P-5/In-13), z uwzględnieniem ochrony danych osobowych podczas pracy zdalnej. Wdrożono Standard konfiguracji urządzeń do pracy zdalnej. ***Uzasadnienie wyboru zabezpieczenia: minimalizacja ryzyka utraty informacji podczas incydentu bezpieczeństwa informacji związanego z telepracą.***
A.7 Bezpieczeństwo zasobów ludzkich		
A.7.1 Przed zatrudnieniem ***Cel: Zapewnić, żeby pracodawcy i kontrahenci rozumieli swoją odpowiedzialność i byli odpowiednimi kandydatami do wypełniania ról do których są przewidziani.***		
A.7.1.1	Postępowanie sprawdzające	W Urzędzie Miasta Płocka wdrożono i stosuje się procedurę naboru na wolne stanowiska urzędnicze. Weryfikacja kandydatów przebiega zgodnie z odpowiednimi przepisami prawnymi, regulacjami wewnętrznymi i zasadami etycznymi oraz proporcjonalnie do wymagań i zadań administracji samorządowej, klasyfikacji

		informacji, do których będzie potrzebny dostęp oraz dostrzeżonych ryzyk. ***Uzasadnienie wyboru zabezpieczenia: zapewnienie odpowiedniej kadry urzędniczej do wykonywania zadań przewidzianych przepisami prawa dla jednostki samorządu terytorialnego.***
A.7.1.2	Warunki zatrudnienia	W dniu rozpoczęcia pracy, po odebraniu umowy o pracę, nowo zatrudniony pracownik składa oświadczenie o zachowaniu poufności i przestrzeganiu podstawowych zasad bezpieczeństwa informacji w Urzędzie Miasta Płocka. Ponadto każdy nowo zatrudniony pracownik otrzymuje upoważnienie do przetwarzania danych osobowych w systemie elektronicznego obiegu dokumentacji Mdok. ***Uzasadnienie wyboru zabezpieczenia: zabezpieczenie zasobów informacyjnych przed ich utratą lub modyfikacją.***
A.7.2 Podczas zatrudnienia ***Cel: Zapewnić, żeby pracownicy i kontrahenci byli świadomi swoich obowiązków dotyczących bezpieczeństwa informacji i wypełniali je.***		
A.7.2.1	Odpowiedzialność kierownictwa	Kierownictwo Urzędu Miasta Płocka wymaga, aby wszyscy pracownicy stosowali zasady bezpieczeństwa informacji zgodnie z obowiązującymi w organizacji politykami i procedurami. Ponadto instrukcja ogólna dotycząca wymagań dla umów, aneksów i porozumień przygotowywanych w Urzędzie Miasta Płocka nakłada warunek umieszczania w projektach umów: klauzuli poufności, klauzuli poufności przy powierzeniu przetwarzania danych osobowych, wymagań dla oprogramowania przeznaczonego do przetwarzania danych osobowych, klauzuli zapoznania się przez kontrahenta z Polityką ZSZ oraz dokumentami systemowymi dostępnymi na stronie internetowej Urzędu Miasta Płocka. Ponadto Prezydent Miasta Płocka wyznaczył Inspektora Ochrony Danych w Urzędzie Miasta Płocka. ***Uzasadnienie wyboru zabezpieczenia: zakomunikowanie pracownikowi oraz kontrahentowi wymagań związanych z bezpieczeństwem informacji .***
A.7.2.2	Uświadomienie, kształcenie i szkolenie z zakresu bezpieczeństwa informacji	Wszyscy pracownicy, stażyści i praktykanci przechodzą stosowne szkolenia z zakresu przestrzegania zasad bezpieczeństwa informacji, potwierdzone podpisem stwierdzającym zapoznanie się i przyjęcie do przestrzegania zapisów instrukcji podstawowych zasad bezpieczeństwa informacji w Urzędzie Miasta Płocka. Do podstawowych obowiązków pracownika, wymienionych w Regulaminie pracy, należy dochowanie tajemnicy ustawowo chronionej, zachowanie w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, należyte zabezpieczenie po zakończeniu pracy dokumentów, wyposażenia, urządzeń i pomieszczeń pracy oraz ochrona i zachowanie w tajemnicy danych osobowych. Referat Teleinformatyki udostępnia cyklicznie materiały (poradniki) związane z zachowaniem zasad bezpieczeństwa podczas pracy. Prowadzone są również szkolenia na rzecz poszerzania wiedzy i budowania świadomości z zakresu bezpieczeństwa informacji oraz technologii informacyjno – komunikacyjnych. ***Uzasadnienie wyboru zabezpieczenia: zakomunikowanie pracownikowi, stażyście i praktykantowi uprawnień i obowiązków w zakresie bezpieczeństwa informacji.***
A.7.2.3	Postępowanie dyscyplinarne	Postępowanie dyscyplinarne wobec pracowników naruszających zasady bezpieczeństwa informacji prowadzone jest na podstawie Regulaminu Pracy

		Urzędu Miasta Płocka oraz stosownych przepisów Kodeksu pracy. ***Uzasadnienie wyboru zabezpieczenia: przepisy prawa powszechnego.***
A.7.3 Zakończenie i zmiana zatrudnienia		
Cel: Zabezpieczyć interesy organizacji w trakcie procesu zmiany lub zakończenia zatrudnienia		
A.7.3.1	Zakończenie zatrudnienia lub zmiana zakresu obowiązków	W przypadku zakończenia pracy w Urzędzie Miasta Płocka następuje zablokowanie byłemu pracownikowi dostępu do systemu obiegu dokumentów oraz cofnięcie przez administratora uprawnień do wszelkich innych programów. Ponadto jest on zobowiązany do zwrotu wszystkich upoważnień i pełnomocnictw, pieczęci urzędowych, którymi posługiwał się w trakcie zatrudnienia oraz posiadanego zestawu do podpisu kwalifikowanego (karta + czytnik). Zwrot w/w zasobów potwierdzany jest na karcie obiegowej oraz w odpowiednich ewidencjach. ***Uzasadnienie wyboru zabezpieczenia: ochrona zasobów informacyjnych Urzędu przed nieuprawnionym dostępem.***
A.8 Zarządzanie aktywami		
A.8.1 Odpowiedzialność za aktywa		
Cel: Zidentyfikować aktywa organizacji i zdefiniować właściwą odpowiedzialność w dziedzinie ich ochrony.		
A.8.1.1	Inwentaryzacja zasobów	W ramach corocznej inwentaryzacji istotnych zasobów informacyjnych organizacja identyfikuje aktywa oraz środki ich przetwarzania oraz utrzymuje ewidencję tych aktywów. W przypadku zasobów informatycznych inwentaryzacja odbywa się za pomocą specjalistycznego oprogramowania monitorującego zmiany w trybie rzeczywistym. ***Uzasadnienie wyboru zabezpieczenia: uzyskanie, a następnie aktualizowanie wiedzy na temat posiadanych zasobów informacyjnych.***
A.8.1.2	Własność aktywów	Aktywa informacyjne organizacji zostały przypisane ich właścicielom. ***Uzasadnienie wyboru zabezpieczenia: zapewnienie identyfikowalności i rozliczalności aktywów.***
A.8.1.3	Akceptowalne użycie aktywów	System zarządzania bezpieczeństwem informacji określa zasady korzystania z grup aktywów i nadzoru nad nimi. Ponadto bezpośredni przełożony nadzoruje użycie aktywów przez podległych pracowników w trakcie pracy zdalnej. ***Uzasadnienie wyboru zabezpieczenia: przypisanie odpowiedzialności za zasoby informacyjne.***
A.8.1.4	Zwrot aktywów	Wszyscy pracownicy w momencie zakończenia zatrudnienia w Urzędzie Miasta Płocka, zakończenia realizacji umowy lub porozumienia zobowiązani są do zwrócenia organizacji wszystkich powierzonych aktywów. ***Uzasadnienie wyboru zabezpieczenia: zachowanie ciągłości dostępu do zasobów organizacji niezależnie od zmian kadrowych.***
A.8.2 Klasyfikacja informacji		
Cel: Zapewnić przypisanie informacjom odpowiedniego poziomu ochrony, zgodnego z ich wagą dla organizacji.		
A.8.2.1	Klasyfikowanie informacji	Informacje zgodnie z dokumentacją systemową procesu zarządzania bezpieczeństwem informacji są klasyfikowane z uwzględnieniem wymagań prawnych, wartości i krytyczności oraz wrażliwości na nieuprawnione ujawnienie lub modyfikację. Klasyfikacja informacji w Urzędzie Miasta Płocka wskazuje na 3

		kategorie główne informacji (jawne, wewnętrzne i chronione). ***Uzasadnienie wyboru zabezpieczenia: zapewnienie identyfikacji dokumentów pod względem sposobu postępowania z nimi i ich zabezpieczania.***
A.8.2.2	Oznaczanie informacji	Zasady oznaczania informacji w Urzędzie Miasta Płocka określone są w Instrukcji kancelaryjnej, przepisach dotyczących ochrony informacji niejawnych oraz dokumentacji systemowej ZSZ. Dokumenty oznaczane są numerem generowanym przez system obiegu dokumentów (UID, nr kancelaryjny, nr sprawy). ***Uzasadnienie wyboru zabezpieczenia: zapewnienie, że informacje są chronione oraz dostępne i nadają się do zastosowania, tam, gdzie są potrzebne i wtedy, gdy są potrzebne.***
A.8.2.3	Postępowanie z aktywami	Zasady postępowania z aktywami w Urzędzie Miasta Płocka określone są w Instrukcji kancelaryjnej, przepisach dotyczących ochrony informacji niejawnych oraz dokumentacji systemowej ZSZ, w szczególności w instrukcji P-5/In-21 Zarządzanie uprawnieniami dostępu do aktywów w Urzędzie Miasta Płocka. ***Uzasadnienie wyboru zabezpieczenia: zapewnienie, że aktywa są zidentyfikowane i chronione oraz dostępne tam, gdzie są potrzebne i wtedy, gdy są potrzebne.***
A.8.3 Postępowanie z nośnikami ***Cel: Zapobiec nieuprawnionemu ujawnieniu, modyfikacji, usunięciu lub zniszczeniu informacji zapisanych na nośnikach***		
A.8.3.1	Zarządzanie nośnikami wymiennymi	Zasady zarządzania nośnikami wymiennymi reguluje Instrukcja podstawowych zasad bezpieczeństwa informacji w Urzędzie Miasta Płocka. ***Uzasadnienie wyboru zabezpieczenia: zabezpieczenie informacji zapisanych na nośniku przed ujawnieniem, modyfikacją lub zniszczeniem.***
A.8.3.2	Wycofywanie nośników	Zasady wycofywania nośników wymiennych reguluje Instrukcja podstawowych zasad bezpieczeństwa informacji w Urzędzie Miasta Płocka oraz instrukcja niszczenia dokumentacji w Urzędzie Miasta Płocka (P-5/In-22). ***Uzasadnienie wyboru zabezpieczenia: zabezpieczenie informacji zapisanych na nośniku przed ujawnieniem lub nieuprawnionym zniszczeniem.***
A.8.3.3	Przekazywanie nośników	Zasady przekazywania nośników reguluje Instrukcja bezpiecznego usuwania danych ze sprzętu przekazywanego do ponownego użycia lub zniszczenia (P-5/In-15). ***Uzasadnienie wyboru zabezpieczenia: zabezpieczenie informacji zapisanych na nośniku przed ujawnieniem.***
A.9 Kontrola dostępu		
A.9.1 Wymagania biznesowe wobec kontroli dostępu ***Cel: Ograniczyć dostęp do informacji i środków przetwarzania informacji***		
A.9.1.1	Polityka kontroli dostępu	W Urzędzie Miasta Płocka wdrożono i stosuje się instrukcję zarządzania uprawnieniami dostępu do aktywów. Wszyscy pracownicy Urzędu posiadają stosowne upoważnienia do dostępu do danych osobowych, aplikacji i dokumentacji. ***Uzasadnienie wyboru zabezpieczenia: określenie stref dostępu.***

A.9.1.2	Dostęp do sieci i usług sieciowych	W Urzędzie Miasta Płocka wdrożono standard konfiguracji i eksploatacji sieci. Ponadto obowiązuje instrukcja ZSZ Zarządzanie kontami użytkowników (P-5/In-11). ***Uzasadnienie wyboru zabezpieczenia: zapewnienie, by użytkownicy mieli dostęp wyłącznie do tych sieci i usług sieciowych, do których są uprawnieni.***
A.9.2 Zarządzenie dostępem użytkowników ***Cel: Zapewnić dostęp uprawnionym użytkownikom i zapobiec nieuprawnionemu dostępowi do systemu i usług***		
A.9.2.1	Rejestrowanie użytkowników	Przyznawanie i odbieranie dostępu do wszystkich systemów i usług informacyjnych, odbywa się na podstawie instrukcji Zarządzanie kontami użytkowników (P-5/In-11) oraz przyjętymi zasadami i standardami pracy zdalnej. ***Uzasadnienie wyboru zabezpieczenia: zapewnienie, by użytkownicy mieli dostęp wyłącznie do tych sieci i usług sieciowych, do których są uprawnieni.***
A.9.2.2	Przydzielanie dostępu użytkownikom	Przyznawanie i odbieranie dostępu do wszystkich systemów i usług informacyjnych, odbywa się na podstawie instrukcji Zarządzanie kontami użytkowników (P-5/In-11) oraz przyjętymi zasadami i standardami pracy zdalnej. ***Uzasadnienie wyboru zabezpieczenia: zapewnienie, by użytkownicy mieli dostęp wyłącznie do tych sieci i usług sieciowych, do których są uprawnieni.***
A.9.2.3	Zarządzanie prawami uprzywilejowanego dostępu	Uprzywilejowany dostęp do systemów i usług jest ściśle reglamentowany i kontrolowany. ***Uzasadnienie wyboru zabezpieczenia: zapewnienie, by użytkownicy mieli dostęp wyłącznie do tych sieci i usług sieciowych, do których są uprawnieni.***
A.9.2.4	Zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników	Przydzielanie poufnych informacji uwierzytelniających podlega formalnemu procesowi zarządzania uprawnieniami. ***Uzasadnienie wyboru zabezpieczenia: zapewnienie, by użytkownicy mieli dostęp wyłącznie do tych sieci i usług sieciowych, do których są uprawnieni.***
A.9.2.5	Przegląd praw dostępu	Przegląd praw dostępu użytkowników odbywa się w regularnych odstępach czasu, zgodnie z instrukcją standardu konfiguracji stacji roboczych użytkowników oraz polityki haseł. ***Uzasadnienie wyboru zabezpieczenia: zapewnienie, by użytkownicy mieli dostęp wyłącznie do tych sieci i usług sieciowych, do których są uprawnieni.***
A.9.2.6	Odbieranie lub dostosowywanie praw dostępu	Przydzielone pracownikom i innym użytkownikom zewnętrznym prawa dostępu do informacji są odbierane po ustaniu zatrudnienia, zakończeniu realizacji umowy lub porozumienia, zakończeniu pracy zdalnej. ***Uzasadnienie wyboru zabezpieczenia: zabezpieczenie informacji przed nieuprawnionym ujawnieniem, modyfikacją lub zniszczeniem.***
A.9.3 Odpowiedzialność użytkowników ***Cel: Zapewnić rozliczalność użytkowników przez ochronę ich informacji uwierzytelniających***		
A.9.3.1	Stosowanie poufnych informacji uwierzytelniających	Użytkownicy w Urzędzie Miasta Płocka mają obowiązek stosowania przyjętych w organizacji zasad stosowania poufnych informacji uwierzytelniających, zgodnie z polityką bezpieczeństwa haseł, określoną w Instrukcji podstawowych zasad bezpieczeństwa informacji w Urzędzie. ***Uzasadnienie wyboru zabezpieczenia: zapewnienie rozliczalności pracowników***

		przez ochronę ich informacji uwierzytelniających.
A.9.4 Kontrola dostępu do systemów i aplikacji		
Cel: Zapobiec nieuprawnionemu dostępowi do systemów i aplikacji.		
A.9.4.1	Ograniczanie dostępu do informacji	Wszyscy użytkownicy mają unikalne identyfikatory (ID użytkownika) do swojego wyłącznego użytku i jest zastosowana odpowiednia technika uwierzytelnienia dla sprawdzenia deklarowanej tożsamości użytkownika. W przypadku systemów zewnętrznych wykorzystywane są również mechanizmy uwierzytelniania oparte na profilu zaufanym oraz kwalifikowanych i niekwalifikowanych certyfikatach. ***Uzasadnienie wyboru zabezpieczenia: zabezpieczenie przed nieautoryzowanym dostępem do informacji, rozliczalność czynności.***
A.9.4.2	Procedury bezpiecznego logowania się	Dostęp do systemów operacyjnych jest kontrolowany za pomocą procedur bezpiecznego logowania się. W przypadku systemów zewnętrznych nie zarządzanych przez Urząd Miasta Płocka logowanie opiera się na profilu zaufanym oraz kwalifikowanych i niekwalifikowanych certyfikatach. ***Uzasadnienie wyboru zabezpieczenia: zabezpieczenie przed nieautoryzowanym dostępem do informacji.***
A.9.4.3	System zarządzania hasłami	Zarządzanie hasłami opiera się na mechanizmach Active Directory zapewniających hasła odpowiedniej jakości. Polityka haseł zawarta jest w Instrukcji podstawowych zasad bezpieczeństwa informacji. ***Uzasadnienie wyboru zabezpieczenia: zabezpieczenie przed nieautoryzowanym dostępem do informacji.***
A.9.4.4	Użycie uprzywilejowanych programów narzędziowych	Zgodnie ze “Standardem konfiguracji stacji roboczych użytkowników”. ***Uzasadnienie wyboru zabezpieczenia: ograniczenie dostępu do potencjalnie niebezpiecznych narzędzi.***
A.9.4.5	Kontrola dostępu do kodów źródłowych programów	nie dotyczy – organizacja nie przechowuje kodów źródłowych programów.
A.10 Kryptografia		
A.10.1 Zabezpieczenia kryptograficzne		
Cel: Zapewnić właściwe i skuteczne wykorzystanie kryptografii do ochrony poufności, autentyczności i/lub integralności informacji.		
A.10.1.1	Polityka korzystania z zabezpieczeń kryptograficznych	Zabezpieczenia kryptograficzne występują jako element funkcjonalny niektórych narzędzi teleinformatycznych (np. VPN, szyfrowanie korespondencji elektronicznej zawierającej dane wrażliwe, do szyfrowania danych na urządzeniach przenośnych, oprogramowanie wykorzystywane do składania podpisów elektronicznych). Zgodnie z instrukcją zarządzania podpisami elektronicznymi, standardami konfiguracji urządzeń do pracy zdalnej, instrukcja podstawowych zasad bezpieczeństwa informacji dla pracowników Urzędu Miasta Płocka. ***Uzasadnienie wyboru zabezpieczenia: zabezpieczenie informacji przed nieuprawnionym ujawnieniem, modyfikacją lub zniszczeniem.***
A.10.1.2	Zarządzanie kluczami	Klucze kryptograficzne występują jako elementy kwalifikowanych podpisów elektronicznych oraz certyfikatów służących do uwierzytelniania usług sieciowych.

		Uzasadnienie wyboru zabezpieczenia: zabezpieczenie informacji przed nieuprawnionym ujawnieniem, modyfikacją lub zniszczeniem.
A.11 Bezpieczeństwo fizyczne i środowiskowe		
A.11.1 Obszary bezpieczne		
Cel: Zapobiec nieuprawnionemu fizycznemu dostępowi, szkodom i zakłóceniom w informacjach i środkach przetwarzania informacji należących do organizacji.		
A.11.1.1	Fizyczna granica obszaru bezpiecznego	W Urzędzie Miasta Płocka wytyczono odpowiednie strefy przetwarzania informacji zgodnie z klasyfikacją informacji. Opis stref ochronnych dla informacji niejawnych znajduje się w Planie ochrony informacji niejawnych. ***Uzasadnienie wyboru zabezpieczenia: fizyczne zabezpieczenie zasobów informacyjnych.***
A.11.1.2	Fizyczne zabezpieczenie wejść	Urząd Miasta Płocka stosuje politykę dostępu do pomieszczeń, zgodnie z instrukcją zmiany kodów systemów kontroli dostępu oraz systemów alarmowych oraz instrukcją podstawowych zasad bezpieczeństwa informacji w Urzędzie. ***Uzasadnienie wyboru zabezpieczenia: fizyczne zabezpieczenie zasobów informacyjnych.***
A.11.1.3	Zabezpieczenie biur, pomieszczeń i urządzeń	Urząd Miasta Płocka stosuje politykę dostępu do pomieszczeń, zgodnie z instrukcją zmiany kodów systemów kontroli dostępu oraz systemów alarmowych oraz instrukcją podstawowych zasad bezpieczeństwa informacji w Urzędzie. ***Uzasadnienie wyboru zabezpieczenia: fizyczne zabezpieczenie zasobów informacyjnych.***
A.11.1.4	Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi	Zgodnie ze standardem bezpieczeństwa fizycznego oraz procedurami awaryjnymi z procesu zarządzania środowiskowego. ***Uzasadnienie wyboru zabezpieczenia: zabezpieczenie aktywów na stanowiskach pracy.***
A.11.1.5	Praca w obszarach bezpiecznych	Zgodnie ze standardem bezpieczeństwa fizycznego. ***Uzasadnienie wyboru zabezpieczenia: kontrola dostępu do aktywów w obszarach wydzielonych.***
A.11.1.6	Obszary publicznie dostępne, dostaw i załadunku	Zgodnie ze standardem bezpieczeństwa fizycznego. ***Uzasadnienie wyboru zabezpieczenia: kontrola dostępu osób trzecich.***
A.11.2 Sprzęt		
Cel: Zapobiec utracie, uszkodzeniu, kradzieży lub naruszenia aktywów oraz przerwaniu działalności organizacji.		
A.11.2.1	Lokalizacja i ochrona sprzętu	W Urzędzie Miasta Płocka sprzęt jest rozmieszczony i chroniony w sposób zapewniający minimalizację ryzyka wynikającego z zagrożeń, w tym środowiskowych oraz wykluczający nieuprawniony dostęp. ***Uzasadnienie wyboru zabezpieczenia: zabezpieczenie sprzętu przed zniszczeniem, utratą danych lub nieautoryzowanym dostępem.***
A.11.2.2	Systemy wspomagające	Sprzęt jest chroniony przed awariami zasilania oraz innymi przerwami w pracy systemów wspomagających oraz zgodnie z instrukcją zarządzania kopiami zapasowymi.

		Uzasadnienie wyboru zabezpieczenia: zabezpieczenie sprzętu przed zniszczeniem i utratą danych.
A.11.2.3	Bezpieczeństwo okablowania	Okablowanie zasilające oraz telekomunikacyjne, przenoszące dane lub wspomagające usługi jest chronione przed przechwyceniem, zakłóceniem lub uszkodzeniem, zgodnie ze standardem bezpieczeństwa fizycznego. ***Uzasadnienie wyboru zabezpieczenia: zabezpieczenie transmisji przed nieuprawnionym dostępem***
A.11.2.4	Konserwacja sprzętu	Sprzęt jest konserwowany w celu zapewnienia jego ciągłej dostępności i integralności. ***Uzasadnienie wyboru zabezpieczenia: utrzymanie sprzętu w pełnej sprawności, zapewnienie ciągłości działania.***
A.11.2.5	Wynoszenie aktywów	Zabronione jest wynoszenie sprzętu, informacji i programów poza siedzibę Urzędu bez uzyskania wcześniejszego zezwolenia. Używanie aktywów podczas pracy zdalnej regulują przyjęte zasady pracy zdalnej. ***Uzasadnienie wyboru zabezpieczenia: zabezpieczenie sprzętu przed zniszczeniem, utratą danych lub nieautoryzowanym dostępem.***
A.11.2.6	Bezpieczeństwo sprzętu i aktywów poza siedzibą	Aktywa wynoszone poza siedzibę Urzędu Miasta Płocka są pod szczególną ochroną, zgodnie z instrukcją podstawowych zasad bezpieczeństwa informacji dla pracowników Urzędu. Używanie aktywów podczas pracy zdalnej regulują przyjęte zasady pracy zdalnej. ***Uzasadnienie wyboru zabezpieczenia: zabezpieczenie aktywów przez utratą lub nieautoryzowanym dostępem.***
A.11.2.7	Bezpieczne zbywanie lub przekazywanie do ponownego użycia	Zgodnie z instrukcją bezpiecznego usuwania danych ze sprzętu przekazywanego do ponownego użycia (P-5/In-15). ***Uzasadnienie wyboru zabezpieczenia: wykluczenie przypadkowego przekazania danych***
A.11.2.8	Pozostawienie sprzętu użytkownika bez opieki	Użytkownicy są zobowiązani do zapewnienia odpowiedniej ochrony sprzętu zgodnie z instrukcją podstawowych zasad bezpieczeństwa informacji dla pracowników Urzędu. ***Uzasadnienie wyboru zabezpieczenia: zabezpieczenie aktywów przez utratą lub nieautoryzowanym dostępem.***
A.11.2.9	Polityka czystego biurka i czystego ekranu	Zgodnie z Instrukcją podstawowych zasad bezpieczeństwa informacji dla pracowników Urzędu Miasta Płocka. ***Uzasadnienie wyboru zabezpieczenia: zabezpieczenie aktywów przez utratą lub nieautoryzowanym dostępem.***
A.12. Bezpieczna eksploatacja		
A.12.1 Procedury eksploatacyjne i odpowiedzialność ***Cel: Zapewnić poprawną i bezpieczną eksploatację środków przetwarzania informacji.***		
A.12.1.1	Dokumentowanie procedur eksploatacyjnych	Procedury eksploatacyjne są udokumentowane w ramach instrukcji ZSZ oraz dokumentacji technicznej sprzętu i aplikacji oraz udostępnione użytkownikom, zgodnie z klasyfikacją informacji oraz określonym upoważnieniami poziomem dostępu.

		Uzasadnienie wyboru zabezpieczenia: spełnienie wymagań prawnych i innych.
A.12.1.2	Zarządzanie zmianami	W Urzędzie Miasta Płocka ustanowiono i wdrożono Instrukcję zarządzania zmianami. ***Uzasadnienie wyboru zabezpieczenia: konieczność dostosowywania się do wymagań stron zainteresowanych oraz zmian przepisów prawnych przy efektywnej obsłudze klienta i ograniczeniu ryzyka negatywnego wpływu zmiany na organizacje pracy.***
A.12.1.3	Zarządzanie pojemnością	Wykorzystanie zasobów jest monitorowane z uwzględnieniem skalowania do przyszłej pojemności systemów. Za określenie danych do ustalenia docelowej funkcjonalności odpowiada właściciel przetwarzanych w danym systemie aktywów. ***Uzasadnienie wyboru zabezpieczenia: zabezpieczenie ciągłości działania w perspektywie dłuższego czasu***
A.12.1.4	Oddzielanie środowisk rozwojowych, testowych i produkcyjnych	Organizacja przestrzega zasad dotyczących testowania aplikacji rozwojowych w wydzielonym środowisku testowym. ***Uzasadnienie wyboru zabezpieczenia: zabezpieczenie zasobów przed niepożądanym wpływem zmiany na organizację pracy.***
A.12.2 Ochrona przed szkodliwym oprogramowaniem ***Cel: Zapewnić informacjom i środkom przetwarzania informacji ochronę przed szkodliwym oprogramowaniem.***		
A.12.2.1	Zabezpieczenia przed szkodliwym oprogramowaniem	Zainstalowano oprogramowanie antywirusowe oraz oprogramowanie zapory sieciowej na wszystkich stacjach roboczych wraz z uruchomionym mechanizmem aktualizacji oraz opracowano w ramach instrukcji podstawowych zasad bezpieczeństwa informacji politykę korzystania z mobilnych urządzeń teleinformatycznych. W przypadku wykorzystywania urządzeń do pracy zdalnej, nie będących własnością Urzędu Miasta Płocka, za zabezpieczenie odpowiada użytkownik. ***Uzasadnienie wyboru zabezpieczenia: zapewnienie integralności, poufności i dostępności do danych.***
A.12.3 Kopie zapasowe ***Cel: Chronić przed utratą danych***		
A.12.3.1	Zapasowe kopie informacji	Zgodnie z Instrukcją zarządzania kopiami zapasowymi. ***Uzasadnienie wyboru zabezpieczenia: zapewnienie integralności danych oraz dostępu do danych w razie awarii.***
A.12.4 Rejestrowanie zdarzeń i monitorowanie ***Cel: Rejestrować zdarzenia i zbierać materiał dowodowy***		
A.12.4.1	Rejestrowanie zdarzeń	Działania użytkowników oraz administratorów, usterki i zdarzenia związane z bezpieczeństwem informacji są odnotowywane w stosownych dziennikach zdarzeń. Zarządzanie incydentami bezpieczeństwa uregulowane jest w odpowiedniej instrukcji ZSZ. ***Uzasadnienie wyboru zabezpieczenia: zapewnienie bezpiecznego środowiska pracy aplikacji.***
A.12.4.2	Ochrona informacji	Podsystemy logowania oraz informacje zawarte w dziennikach są chronione przed

	w dziennikach zdarzeń	manipulacją i nieautoryzowanym dostępem. ***Uzasadnienie wyboru zabezpieczenia: zapewnienie bezpiecznego środowiska pracy aplikacji.***
A.12.4.3	Rejestrowanie działań administratorów i operatorów	Tworzone i zapisywane są logi zdarzeń systemów i aplikacji, które służą ustaleniu właściciela działania, a dzienniki są chronione i systematycznie przeglądane. ***Uzasadnienie wyboru zabezpieczenia: zapewnienie rozliczalności dostępu do zasobów.***
A.12.4.4	Synchronizacja zegarów	Zegary systemów przetwarzania informacji oraz stacji roboczych są synchronizowane z przyjętym jednym wzorcowym źródłem czasu. ***Uzasadnienie wyboru zabezpieczenia: zapewnienie bezpiecznego środowiska pracy aplikacji.***
A.12.5 Nadzór nad oprogramowaniem produkcyjnym ***Cel: Zapewnić integralność systemów produkcyjnych***		
A.12.5.1	Instalacja oprogramowania w systemach produkcyjnych	Instalacja oprogramowania w systemie produkcyjnym odbywa się na podstawie uzgodnień między stronami zainteresowanymi, po przeprowadzeniu testów (jeżeli są wymagane). ***Uzasadnienie wyboru zabezpieczenia: zapewnienie przetwarzania aktywów zgodnie z zidentyfikowanymi wymaganiami, zabezpieczenie systemów przed niekorzystnym wpływem zmiany.***
A.12.6 Zarządzanie podatnościami technicznymi ***Cel: Zapobiec wykorzystaniu podatności technicznych***		
A.12.6.1	Zarządzanie podatnościami technicznymi	Informacje o technicznych podatnościach wykorzystywanych systemów informacyjnych są pozyskiwane od ich producentów oraz z publicznie dostępnych, wiarygodnych źródeł; zgodnie z oszacowaniem stopnia narażenia organizacji na podatności są wdrażane odpowiednie środki adekwatne do związanych z nimi ryzyk. ***Uzasadnienie wyboru zabezpieczenia: ochrona systemów przed zagrożeniem z zewnątrz, zapewnienie szybkiej reakcji na awarię, ochrona przetwarzanych informacji.***
A.12.6.2	Ograniczenia w instalowaniu oprogramowania	Zgodnie ze standardem konfiguracji stacji roboczej użytkowników. ***Uzasadnienie wyboru zabezpieczenia: ochrona przed dokonaniem nieuprawnionej zmiany.***
A.12.7 Rozważania dotyczące audytu systemów informacyjnych ***Cel: Zminimalizować wpływ działań audytu na systemy produkcyjne***		
A.12.7.1	Zabezpieczenia audytu systemów informacyjnych	Realizacja audytu oraz działań związanych ze sprawdzeniem eksploatowanych systemów uwzględnia przyjęte standardy pracy i nie powoduje zakłóceń organizacyjnych bądź technologicznych w realizowanych procesach. ***Uzasadnienie wyboru zabezpieczenia: minimalizacja negatywnego wpływu procesu audytu na organizację pracy.***
A.13 Bezpieczeństwo komunikacji		
A.13.1 Zarządzanie bezpieczeństwem sieci		

Cel: Zapewnić ochronę informacji w sieciach oraz wspomagających je środkach przetwarzania informacji.		
A.13.1.1	Zabezpieczenia sieci	Sieci są zarządzane i nadzorowane zgodnie ze standardem bezpieczeństwa i konfiguracji sieci oraz standardem konfiguracji urządzeń do pracy zdalnej. ***Uzasadnienie wyboru zabezpieczenia: ochrona informacji w systemach i aplikacjach.***
A.13.1.2	Bezpieczeństwo usług sieciowych	Umowy dotyczące wszystkich usług sieciowych świadczonych wewnątrz lub zlecanych na zewnątrz zawierają zabezpieczenia i wymagania dotyczące bezpieczeństwa informacji, zgodnie ze standardem bezpieczeństwa i konfiguracji sieci oraz standardem konfiguracji urządzeń do pracy zdalnej. ***Uzasadnienie wyboru zabezpieczenia: ochrona informacji w systemach i aplikacjach.***
A.13.1.3	Rozdzielanie sieci	Grupy usług informacyjnych, użytkowników i systemów informacyjnych są rozdzielone w strukturze sieci, zgodnie ze standardem bezpieczeństwa i konfiguracji sieci oraz standardem konfiguracji urządzeń do pracy zdalnej. ***Uzasadnienie wyboru zabezpieczenia: ochrona informacji w systemach i aplikacjach.***
A.13.2 Przesyłanie informacji ***Cel: Utrzymać bezpieczeństwo informacji przesyłanych wewnątrz organizacji i wymienianych z podmiotami zewnętrznymi.***		
A.13.2.1	Polityki i procedury przesyłania informacji	Standard konfiguracji i eksploatacji sieci (S-4) oraz standard konfiguracji urządzeń do pracy zdalnej. ***Uzasadnienie wyboru zabezpieczenia: ochrona wymiany informacji przesyłanych przy użyciu wszystkich środków łączności.***
A.13.2.2	Porozumienia dotyczące przesyłania informacji	W Urzędzie Miasta Płocka wdrożono instrukcję dotyczącą przygotowywania umów, aneksów i porozumień, zawierającą klauzule w zakresie wymiany informacji, w szczególności zawierających dane osobowe. ***Uzasadnienie wyboru zabezpieczenia: ochrona wymiany informacji.***
A.13.2.3	Wiadomości elektroniczne	Ochrona informacji przesyłanych w wiadomościach elektronicznych opiera się na świadomości pracowników wysyłających wiadomości, przeszkolonych w zakresie podstawowych zasad bezpieczeństwa informacji. Do przekazywania informacji chronionych prawnie nie stosuje się wiadomości elektronicznych. ***Uzasadnienie wyboru zabezpieczenia: ochrona informacji***
A.13.2.4	Umowy o zachowaniu poufności	W Urzędzie Miasta Płocka wdrożono instrukcję dotyczącą przygotowywania umów, aneksów i porozumień, zawierającą klauzule w zakresie wymiany informacji, w szczególności zawierających dane osobowe. ***Uzasadnienie wyboru zabezpieczenia: ochrona wymiany informacji.***
A.14 Pozyskiwanie, rozwój i utrzymanie systemów		
A.14.1 Wymagania związane z bezpieczeństwem systemów informacyjnych ***Cel: Zapewnić, żeby bezpieczeństwo informacji było nieodłączną częścią systemów informacyjnych w całym cyklu życia.***		
A.14.1.1	Analiza i specyfikacja wymagań dla	Wymagania dotyczące bezpieczeństwa informacji są włączane do wymagań stawianych nowym systemom informacyjnym i podczas rozbudowy istniejących.

	bezpieczeństwa informacji	***Uzasadnienie wyboru zabezpieczenia: zapewnienie przetwarzania aktywów zgodnie z zidentyfikowanymi wymaganiami, zabezpieczenie systemów przed niekorzystnym wpływem zmiany.***
A.14.1.2	Zabezpieczenie usług aplikacyjnych w sieciach publicznych	Nie dotyczy Urzędu Miasta Płocka.
A.14.1.3	Ochrona transakcji usług aplikacyjnych	Informacje związane z transakcjami dokonywanymi w ramach usług świadczonych przez aplikacje są chronione. ***Uzasadnienie wyboru zabezpieczenia: zapobieżenie przerwaniu transmisji, nieuprawnionym zmianom wiadomości, nieuprawnionemu ujawnieniu, powieleniu lub odtworzeniu informacji.***
A.14.2 Bezpieczeństwo w procesach rozwoju i wsparcia ***Cel: Zapewnić, żeby bezpieczeństwo informacji było nieodłączną częścią systemów informacyjnych w całym cyklu życia.***		
A.14.2.1	Polityka bezpieczeństwa prac rozwojowych	Rozwój oprogramowania jest regulowany w normach prawa powszechnego dla administracji publicznej.
A.14.2.2	Procedury kontroli zmian w systemach	W Urzędzie Miasta Płocka ustanowiono i wdrożono Instrukcję zarządzania zmianami. ***Uzasadnienie wyboru zabezpieczenia: konieczność dostosowywania się do wymagań stron zainteresowanych oraz zmian przepisów prawnych przy efektywnej obsłudze klienta i ograniczeniu ryzyka negatywnego wpływu zmiany na organizacje pracy.***
A.14.2.3	Przegląd techniczny aplikacji po zmianach w platformie produkcyjnej	W Urzędzie Miasta Płocka ustanowiono i wdrożono Instrukcję zarządzania zmianami. ***Uzasadnienie wyboru zabezpieczenia: konieczność dostosowywania się do wymagań stron zainteresowanych oraz zmian przepisów prawnych przy efektywnej obsłudze klienta i ograniczeniu ryzyka negatywnego wpływu zmiany na organizacje pracy.***
A.14.2.4	Ograniczenia dotyczące zmian w pakietach oprogramowania	Zgodnie ze standardem konfiguracji stacji roboczych. ***Uzasadnienie wyboru zabezpieczenia: ograniczanie ryzyka negatywnego wpływu zmiany na organizację pracy.***
A.14.2.5	Zasady projektowania bezpiecznych systemów	Projektowanie systemów jest regulowane w normach prawa powszechnego dla administracji publicznej.
A.14.2.6	Bezpieczne środowisko rozwojowe	W Urzędzie Miasta Płocka wykorzystuje się bezpieczne środowisko testowe. ***Uzasadnienie wyboru zabezpieczenia: ograniczanie ryzyka negatywnego wpływu zmiany na organizację pracy.***
A.14.2.7	Prace rozwojowe zlecane podmiotom	Prace rozwojowe nad systemami zlecane podmiotom zewnętrznym podlegają stałemu nadzorowi od etapu opracowania koncepcji zmian poprzez etap wdrożenia

	zewnętrznym	do odbioru. ***Uzasadnienie wyboru zabezpieczenia: ograniczanie ryzyka negatywnego wpływu zmiany na organizację pracy, spełnienie wymagań prawnych i innych stawianych przed systemami w administracji publicznej.***
A.14.2.8	Testowanie bezpieczeństwa systemów	Testy akceptacyjne są regulowane przepisami prawa powszechnego. ***Uzasadnienie wyboru zabezpieczenia: ograniczanie ryzyka negatywnego wpływu zmiany na organizację pracy, spełnienie wymagań prawnych i innych stawianych przed systemami w administracji publicznej.***
A.14.2.9	Testy akceptacyjne systemów	Testy akceptacyjne są regulowane przepisami prawa powszechnego. ***Uzasadnienie wyboru zabezpieczenia: ograniczanie ryzyka negatywnego wpływu zmiany na organizację pracy, spełnienie wymagań prawnych i innych stawianych przed systemami w administracji publicznej.***
A14.3. Dane testowe ***Cel: Zapewnić ochronę danych stosowanych do testów.***		
A.14.3.1	Ochrona danych testowych	Dane testowe są starannie dobierane, chronione i nadzorowane. ***Uzasadnienie wyboru zabezpieczenia: ograniczanie ryzyka negatywnego wpływu zmiany na organizację pracy.***
A.15 Relacje z dostawcami		
A.15.1 Bezpieczeństwo informacji w relacjach z dostawcami ***Cel: Zapewnić ochronę aktywów organizacji udostępnianych dostawcom***		
A.15.1.1	Polityka bezpieczeństwa informacji w relacjach z dostawcami	W Urzędzie Miasta Płocka wdrożono instrukcję dotyczącą przygotowywania umów, aneksów i porozumień, zawierającą klauzule w zakresie wymiany informacji, w szczególności zawierających dane osobowe. ***Uzasadnienie wyboru zabezpieczenia: ochrona wymiany informacji.***
A.15.1.2	Uwzględnienie bezpieczeństwa w porozumieniach z dostawcami	W Urzędzie Miasta Płocka wdrożono instrukcję dotyczącą przygotowywania umów, aneksów i porozumień, zawierającą klauzule w zakresie wymiany informacji, w szczególności zawierających dane osobowe. ***Uzasadnienie wyboru zabezpieczenia: ochrona wymiany informacji.***
A.15.1.3	Łańcuch dostaw technologii informacyjnych i telekomunikacyjnych	W Urzędzie Miasta Płocka wdrożono instrukcję dotyczącą przygotowywania umów, aneksów i porozumień, zawierającą klauzule w zakresie wymiany informacji, w szczególności zawierających dane osobowe. ***Uzasadnienie wyboru zabezpieczenia: ochrona wymiany informacji.***
A.15.2 Zarządzanie usługami dostarczanymi przez dostawców ***Cel: Utrzymać uzgodniony poziom bezpieczeństwa informacji i świadczonych usług zgodnie z umowami z dostawcami***		
A.15.2.1	Monitorowanie i przegląd usług świadczonych przez dostawców	Usługi, raporty i zapisy dostarczane przez stronę trzecią są regularnie monitorowane i przeglądane, zaś ich wpływ na środowisko pracy organizacji podlega badaniom w ramach audytów wewnętrznych. Urząd Miasta Płocka nie prowadzi listy kwalifikowanych dostawców usług ze względu na obowiązek stosowania ustawy Prawo zamówień publicznych. Dla zabezpieczenia interesu

		organizacji w umowach stosowane są obligatoryjnie zapisy dotyczące zapłaty kary umownej. ***Uzasadnienie wyboru zabezpieczenia: kontrola realizacji usług istotnych dla ciągłości działania.***
A.15.2.2	Zarządzanie zmianami w usługach świadczonych przez dostawców.	Zmiany w dostarczaniu usług, włączając w to utrzymanie i doskonalenie istniejących polityk bezpieczeństwa, procedur i zabezpieczeń, są zarządzane zgodnie z Instrukcją zarządzania zmianami. ***Uzasadnienie wyboru zabezpieczenia: ograniczanie ryzyka negatywnego wpływu zmiany na organizację pracy.***
A.16 Zarządzanie incydentami związanymi z bezpieczeństwem informacji		
A.16.1 Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami ***Cel: Zapewnić, spójne i skuteczne podejście do zarządzania incydentami związanymi z bezpieczeństwem informacji, z uwzględnieniem informowania o zdarzeniach i słabościach.***		
A.16.1.1	Odpowiedzialność i procedury	Odpowiedzialność kierownictwa jest określona w Księdze Zintegrowanego Systemu Zarządzania, Regulaminie organizacyjnym Urzędu Miasta Płocka i innych właściwych dokumentach; opracowano procedury zapewniające szybką, efektywną i uporządkowaną reakcję na incydenty związane z bezpieczeństwem informacji. ***Uzasadnienie wyboru zabezpieczenia: jasne określenie uprawnień i odpowiedzialności.***
A.16.1.2	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji	Zgodnie z Instrukcją zarządzania incydentami bezpieczeństwa oraz z Instrukcją podstawowych zasad bezpieczeństwa dla pracowników Urzędu Miasta Płocka. ***Uzasadnienie wyboru zabezpieczenia: włączenie wszystkich uczestników przetwarzania informacji w nadzorowanie prawidłowości funkcjonowania systemów.***
A.16.1.3	Zgłaszanie słabości związanych z bezpieczeństwem informacji	Zgodnie z Instrukcją zarządzania incydentami bezpieczeństwa oraz z Instrukcją podstawowych zasad bezpieczeństwa dla pracowników Urzędu Miasta Płocka. ***Uzasadnienie wyboru zabezpieczenia: włączenie wszystkich uczestników przetwarzania informacji w nadzorowanie prawidłowości funkcjonowania systemów.***
A.16.1.4	Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji	Zgodnie z Instrukcją zarządzania incydentami bezpieczeństwa oraz z Instrukcją podstawowych zasad bezpieczeństwa dla pracowników Urzędu Miasta Płocka. ***Uzasadnienie wyboru zabezpieczenia: włączenie wszystkich uczestników przetwarzania informacji w nadzorowanie prawidłowości funkcjonowania systemów.***
A.16.1.5	Reagowanie na incydenty związane z bezpieczeństwem informacji	Zgodnie z Instrukcją zarządzania incydentami bezpieczeństwa oraz z Instrukcją podstawowych zasad bezpieczeństwa dla pracowników Urzędu Miasta Płocka. ***Uzasadnienie wyboru zabezpieczenia: zapewnienie adekwatności podejmowanych działań w obszarze reagowania na zagrożenia ciągłości działania.***
A.16.1.6	Wyciąganie wniosków z incydentów	Zgodnie z Instrukcją zarządzania incydentami bezpieczeństwa oraz z Instrukcją podstawowych zasad bezpieczeństwa dla pracowników Urzędu Miasta Płocka.

	związanych z bezpieczeństwem informacji	***Uzasadnienie wyboru zabezpieczenia: podnoszenie świadomości, doskonalenie systemu.***
A.16.1.7	Gromadzenie materiału dowodowego	Zgodnie z przepisami prawa. ***Uzasadnienie wyboru zabezpieczenia: zebranie materiału dowodowego zgodnie z przepisami prawa.***
A.17 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania		
A.17.1 Ciągłość bezpieczeństwa informacji ***Cel: Zaleca się uwzględnienie ciągłości bezpieczeństwa informacji w systemach zarządzania ciągłością działania organizacji.***		
A.17.1.1	Planowanie ciągłości bezpieczeństwa informacji	W Urzędzie Miasta Płocka ustanowiono strategię ciągłości działania, uwzględniającą aspekty bezpieczeństwa informacji. ***Uzasadnienie wyboru zabezpieczenia: ochrona krytycznych procesów przed skutkami niepożądanych zdarzeń dotyczących aktywów informacyjnych .***
A.17.1.2	Wdrożenie ciągłości bezpieczeństwa informacji	Strategia ciągłości działania, obejmująca ciągłość bezpieczeństwa informacji została wdrożona do stosowania i jest utrzymywana. ***Uzasadnienie wyboru zabezpieczenia: ochrona krytycznych procesów przed skutkami niepożądanych zdarzeń dotyczących aktywów informacyjnych.***
A.17.1.3	Weryfikowanie, przegląd i ocena ciągłości bezpieczeństwa informacji	Opracowano i wdrożono udokumentowane metody reagowania na zdarzenia krytyczne dla bezpieczeństwa informacji, zapewniające jego utrzymanie na wymaganym poziomie. Skuteczność stosowanych środków jest weryfikowana za pomocą testów, dokument strategii ciągłości bezpieczeństwa informacji jest poddawany przeglądowi ***Uzasadnienie wyboru zabezpieczenia: zapewnienie wznowienia działalności w wymaganym czasie, utrzymanie założonego poziomu bezpieczeństwa informacji podczas reagowania na zdarzenie.***
A.17.2 Nadmiarowość ***Cel: Zapewnić dostępność środków przetwarzania informacji.***		
A.17.2.1	Dostępność środków przetwarzania informacji	Przy projektowaniu systemów organizacja zakłada stosowną nadmiarowość środków przetwarzania informacji. ***Uzasadnienie wyboru zabezpieczenia: zapewnienie skalowalności systemów informatycznych.***
A.18 Zgodność		
A.18.1 Zgodność z przepisami prawnymi i umownymi ***Cel: Unikać naruszania zobowiązań prawnych, regulacyjnych lub umownych związanych z bezpieczeństwem informacji oraz innych wymaga dotyczących bezpieczeństwa.***		
A.18.1.1	Określenie stosownych wymagań prawnych i umownych	Przepisy prawa powszechnego zostały przypisane dla każdej komórki organizacyjnej w Regulaminie organizacyjnym Urzędu. Na ich podstawie prowadzone są działania regulaminowe. Pracownicy posiadają pełen dostęp do serwisu LEX oraz internetowych zasobów informacyjnych. ***Uzasadnienie wyboru zabezpieczenia: zapewnienie w Urzędzie bieżącej identyfikacji oraz dostępu do obowiązujących wymagań prawnych i innych, z***

		podziałem na przepisy związane z merytorycznym zakresem funkcjonowania komórki, bezpieczeństwem informacji oraz wymaganiami ochrony środowiska oraz wymaganiami bezpieczeństwa i higieny pracy, do których spełnienia organizacja jest zobowiązana.
A.18.1.2	Prawa do własności intelektualnej	Zgodnie z Deklaracją ochrony własności intelektualnej, zawartą w Polityce Bezpieczeństwa Informacji w Urzędzie Miasta Płocka. ***Uzasadnienie wyboru zabezpieczenia: zapewnienie przestrzegania wymagań prawnych związanych z ochroną własności intelektualnej.***
A.18.1.3	Ochrona zapisów organizacji	Wszystkie zapisy organizacji podlegają ochronie przed utratą, zniszczeniem lub utratą zgodnie z wymaganiami ustawowymi (instrukcja kancelaryjna), regulacjami wewnętrznymi (Regulamin organizacyjny) oraz wymaganiami kontraktowymi (zapisy umów). ***Uzasadnienie wyboru zabezpieczenia: zapewnienie zgodności z przepisami prawa i regulacjami wewnętrznymi.***
A.18.1.4	Prywatność i ochrona danych identyfikujących osobę	Dane osobowe i prywatność osób fizycznych podlegają w Urzędzie Miasta Płocka ochronie wynikającej z obowiązujących przepisów prawa. ***Uzasadnienie wyboru zabezpieczenia: zapewnienie zgodności z przepisami prawa i regulacjami wewnętrznymi.***
A.18.1.5	Regulacje dotyczące zabezpieczeń kryptograficznych	Zabezpieczenia kryptograficzne są stosowane przez użytkowników jako zabezpieczenie danych przechowywanych na urządzeniach przenośnych (szyfrowanie danych) oraz występują jako element funkcjonalny niektórych narzędzi teleinformatycznych (np. VPN, oprogramowanie wykorzystywane do składania podpisów elektronicznych). ***Uzasadnienie wyboru zabezpieczenia: zapewnienie zgodności z przepisami prawa i regulacjami wewnętrznymi.***
A.18.2 Przeglądy bezpieczeństwa informacji ***Cel: Zapewnić zgodnie z politykami organizacji i procedurami wdrożenie i stosowanie zasad bezpieczeństwa informacji***		
A.18.2.1	Niezależny przegląd bezpieczeństwa informacji	Urząd Miasta Płocka poddawany jest co roku ocenie ze strony jednostki certyfikującej. ***Uzasadnienie: obiektywna ocena skuteczności zintegrowanego systemu zarządzania.***
A.18.2.2	Zgodność z politykami bezpieczeństwa i normami	Kierownicy komórek organizacyjnych są zobowiązani do zapewnienia w podległym obszarze zgodności z politykami bezpieczeństwa i normami. ***Uzasadnienie: obiektywna ocena skuteczności zintegrowanego systemu zarządzania.***
A.18.2.3	Sprawdzanie zgodności technicznej	Systemy informacyjne są regularnie przeglądane pod kątem ich zgodności z polityką bezpieczeństwa informacji i standardami obowiązującymi w Urzędzie Miasta Płocka. ***Uzasadnienie: stosowanie wdrożonych zasad bezpieczeństwa.***