	QI_00 Deklaracja stosowania / Zabezpieczenia 27001	TTMS: QI_00	
		Poziom rewizji:	3.0
		Data rewizji:	2023-10-01
		Obowiązuje od:	2024-01-29

P: wymaganie prawne, U: zobowiązania umowne, B: wymagania biznesowe/dobre praktyki, AR: wynik analizy ryzyka.

Nr.	Zabezpieczenie	Opis zabezpieczenia	TTMS	Cele stosowania zabezpieczeń			
				P	U	B	AR
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							
A.5.1.1	Polityki bezpieczeństwa informacji	Zbiór polityk bezpieczeństwa informacji powinien być opracowany, zatwierdzony przez kierownictwo, opublikowany i zakomunikowany pracownikom i właściwym stronom zewnętrznym.	T			T	T
A.5.1.2	Przegląd polityk bezpieczeństwa informacji	Polityki bezpieczeństwa informacji należy poddawać przeglądom w zaplanowanych odstępach czasu lub wtedy, gdy wystąpią istotne zmiany, aby zapewnić, że nadal są właściwe, adekwatne i skuteczne.	T			T	T
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	Odpowiedzialność za bezpieczeństwo informacji powinna być określona i przypisana.	T	T		T	T
A.6.1.2	Rozdzielanie obowiązków	Obowiązki i odpowiedzialności pozostające w konflikcie ze sobą należy rozdzielić celem ograniczenia okazji do nieuprawnionej lub nie umyślnej modyfikacji lub nadużycia aktywów organizacji.	T	T		T	T
A.6.1.3	Kontakty z organami władzy	Należy utrzymywać stosowne kontakty z właściwymi organami władzy.	T	T	T		
A.6.1.4	Kontakty z grupami zainteresowanych specjalistów	Należy utrzymywać stosowne kontakty z grupami zainteresowanych specjalistów lub innymi specjalistycznymi forami oraz stowarzysze niami zawodowymi z obszaru bezpieczeństwa.	T			T	T
A.6.1.5	Bezpieczeństwo informacji w zarządzaniu projektami	Bezpieczeństwo informacji należy uwzględnić w zarządzaniu projektami, niezależnie od rodzaju projektu.	T	T	T	T	T
A.6.2 Urządzenia mobilne i telepraca							
Cel: Zapewnić bezpieczeństwo telepracy i stosowania urządzeń mobilnych.							

P: wymaganie prawne, U: zobowiązania umowne, B: wymagania biznesowe/dobre praktyki, AR: wynik analizy ryzyka.

A.6.2.1	Polityka stosowania urządzeń mobilnych	Należy wprowadzić politykę oraz wspierające ją zabezpieczenia w celu zarządzania ryzykami, wynikającymi z użytkowania urządzeń mobilnych.	T	T	T	T	T
A.6.2.2	Telepraca	Należy wdrożyć politykę oraz wspierające ją zabezpieczenia w celu ochrony informacji pobieranych, przetwarzanych i przechowywa nych w miejscach wykonywania telepracy.	T		T	T	T
A.7 Bezpieczeństwo zasobów ludzkich							
A.7.1 Przed zatrudnieniem							
Cel: Zapewnić, żeby pracownicy i kontrahenci rozumieli swoją odpowiedzialność i byli odpowiednimi kandy datami do wypełnienia ról, do których są							
A.7.1.1	Postępowanie sprawdzające	Historię wszystkich kandydatów do pracy należy zweryfikować zgodnie z odpowiednimi przepisami prawnymi, regulacjami i zasadami etycznymi oraz proporcjonalnie do wymagań biznesowych, klasyfikacji informacji, do których będzie potrzebny dostęp oraz dostrzeżonych ryzyk.	T	T		T	T
A.7.1.2	Warunki zatrudnienia	Umowy z pracownikami i kontrahentami powinny określać odpowiedzialność stron w obszarze bezpieczeństwa informacji.	T	T		T	T
A.7.2 Podczas zatrudnienia							
Cel: Zapewnić, żeby pracownicy i kontrahenci byli świadomi swoich obowiązków dotyczących bezpieczeń stwa informacji i wypełniali je.							
A.7.2.1	Odpowiedzialność kierownictwa	Kierownictwo powinno wymagać, aby wszyscy pracownicy i kontrahenci stosowali zasady bezpieczeństwa informacji zgodnie z obowiązującymi w organizacji politykami i procedurami.	T	T		T	T
A.7.2.2	Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji	Wszyscy pracownicy organizacji oraz, w stosownych wypadkach, kontrahenci powinni przejść stosowne kształcenie i szkolenie uświadamiające oraz regularnie otrzymywać aktualizacje polityk i procedur związanych z ich stanowiskiem pracy.	T	T		T	T
A.7.2.3	Postępowanie dyscyplinarne	Postępowanie dyscyplinarne wobec pracowników naruszających zasady bezpieczeństwa informacji należy prowadzić na podstawie ustalonych i przedstawionych im zasad.	T	T		T	T
A.7.3 Zakończenie i zmiana zatrudnienia							
Cel: Zabezpieczyć interesy organizacji w trakcie procesu zmiany lub zakończenia zatrudnienia.							

P: wymaganie prawne, U: zobowiązania umowne, B: wymagania biznesowe/dobre praktyki, AR: wynik analizy ryzyka.

A.7.3.1	Zakończenie zatrudnienia lub zmiana zakresu obowiązków	Należy określić i przedstawić pracownikowi lub kontrahentowi, które zakresy odpowiedzialności i obowiązki w zakresie bezpieczeństwa informacji pozostaną aktualne po zakończeniu lub zmianie zatrudnienia, a następnie egzekwować je.	T	T		T	T
A.8.1 Odpowiedzialność za aktywa							
Cel: Zidentyfikować aktywa organizacji i zdefiniować właściwą odpowiedzialność w dziedzinie ich ochrony.							
A.8.1.1	Inwentaryzacja aktywów	Należy zidentyfikować informacje, inne aktywa związane z informacjami oraz środkami przetwarzania informacji oraz sporządzić i utrzymywać ewidencję tych aktywów.	T			T	
A.8.1.2	Własność aktywów	Aktywa znajdujące się w ewidencji należy przypisać ich właścicielom.	T			T	
A.8.1.3	Akceptowalne użycie aktywów	Należy zidentyfikować, udokumentować i wdrożyć zasady akceptowalnego użycia informacji oraz aktywów związanych z informacjami i środkami przetwarzania informacji.	T			T	
A.8.1.4	Zwrot aktywów	Wszyscy pracownicy i użytkownicy podmiotów zewnętrznych, w momencie zakończenia zatrudnienia, umowy lub porozumienia, powinni zwrócić wszystkie posiadane aktywa organizacji.	T			T	
A.8.2 Klasyfikacja informacji							
Cel: Zapewnić przypisanie informacjom odpowiedniego poziomu ochrony, zgodnego z ich wagą dla orga nizacji.							
A.8.2.1	Klasyfikowanie informacji	Informacje powinny być klasyfikowane z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację.	T			T	
A.8.2.2	Oznaczanie informacji	Należy opracować i wdrożyć odpowiedni zbiór procedur oznaczania informacji, zgodnych z przyjętym w organizacji schematem klasyfikacji informacji.	T			T	
A.8.2.3	Postępowanie z aktywami	Należy opracować i wdrożyć procedury postępowania z aktywami, zgodnie z przyjętym przez organizację schematem klasyfikacji infor macji.	T			T	
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	Organizacja powinna wdrożyć procedury zarządzania nośnikami wymiennymi, zgodne ze schematem klasyfikacji przyjętym w organizacji.	T			T	T
A.8.3.2	Wycofywanie nośników	Nośniki, które nie będą dłużej wykorzystywane, należy bezpiecznie wycofać, zgodnie z formalnymi procedurami.	T			T	T
A.8.3.3	Przekazywanie nośników	Nośniki zawierające informacje należy chronić przed nieuprawnio nym dostępem, nadużyciem oraz utratą integralności podczas transportu.	T			T	T
A.9 Kontrola dostępu							

P: wymaganie prawne, U: zobowiązania umowne, B: wymagania biznesowe/dobre praktyki, AR: wynik analizy ryzyka.

A.9.1 Wymagania biznesowe wobec kontroli dostępu							
Cel: Ograniczyć dostęp do informacji i środków przetwarzania informacji.							
A.9.1.1	Polityka kontroli dostępu	Politykę kontroli dostępu należy ustanowić, udokumentować i poddawać przeglądom zgodnie z wymaganiami biznesowymi i wymaganiami bezpieczeństwa informacji.	T	T	T	T	T
A.9.1.2	Dostęp do sieci i usług sieciowych	Użytkownicy powinni mieć dostęp wyłącznie do tych sieci i usług sieciowych, do których otrzymali wyraźne uprawnienia.	T	T	T	T	T
A.9.2 Zarządzenie dostępem użytkowników							
Cel: Zapewnić dostęp uprawnionym użytkownikom i zapobiec nieuprawnionemu dostępowi do systemów i usług.							
A.9.2.1	Rejestrowanie i wyrejestrowywanie użytkowników	W celu umożliwienia przydzielania praw dostępu należy wdrożyć formalny proces rejestrowania i wyrejestrowywania użytkowników.	T	T	T	T	T
A.9.2.2	Przydzielanie dostępu użytkownikom	Należy wdrożyć formalny proces przydzielania dostępu użytkowni kom w celu nadawania lub odbierania praw dostępu do wszystkich systemów i usług wszystkim kategoriom użytkowników.	T	T	T	T	T
A.9.2.3	Zarządzanie prawami uprzywilejowanego dostępu	Przydzielanie i wykorzystanie praw uprzywilejowanego dostępu należy ograniczyć i nadzorować.	T	T	T	T	T
A.9.2.4	Zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników	Przydzielanie poufnych informacji uwierzytelniających powinno podlegać formalnemu procesowi zarządzania.	T	T	T	T	T
A.9.2.5	Przegląd praw dostępu użytkowników	Właściciele aktywów powinni przeglądać prawa dostępu użytkowników w regularnych odstępach czasu.	T	T	T	T	T
A.9.2.6	Odbieranie lub dostosowywanie praw dostępu	Przydzielone pracownikom i użytkownikom zewnętrznym prawa do stępu do informacji i środków przetwarzania informacji należy odbierać po zakończeniu zatrudnienia, umowy lub porozumienia lub dostosowywać do zaistniałych zmian.	T	T	T	T	T
A.9.3 Odpowiedzialność użytkowników							
Cel: Zapewnić rozliczalność użytkowników w celu ochrony ich informacji uwierzytelniających.							
A.9.3.1	Stosowanie poufnych informacji uwierzytelniających	Użytkownicy powinni mieć obowiązek przestrzegania przyjętych w organizacji zasad stosowania poufnych informacji uwierzytelniających.	T		T	T	T
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	Dostęp do informacji oraz funkcji systemu aplikacyjnego należy ograniczać zgodnie z polityką kontroli dostępu.	T	T	T	T	T
A.9.4.2	Procedury bezpiecznego logowania	Tam, gdzie polityka kontroli dostępu tego wymaga, dostęp do systemów i aplikacji powinien być kontrolowany przez procedurę bezpiecznego logowania.	T	T	T	T	T

P: wymaganie prawne, U: zobowiązania umowne, B: wymagania biznesowe/dobre praktyki, AR: wynik analizy ryzyka.

A.9.4.3	System zarządzania hasłami	Systemy zarządzania hasłami powinny być interaktywne i zapewniać wybór haseł dobrej jakości.	T	T	T	T	T
A.9.4.4	Użycie uprzywilejowanych programów narzędziowych	Wykorzystanie programów narzędziowych, umożliwiających obejście zabezpieczeń systemów i aplikacji, powinno podlegać ograniczeniom i ścisłemu nadzorowi.	T	T	T	T	T
A.9.4.5	Kontrola dostępu do kodów źródłowych programów	Dostęp do kodu źródłowego programów powinien być ograniczony.	T	T	T	T	T
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 stosowania zabezpieczeń kryptograficznych	Należy opracować i wdrożyć politykę stosowania zabezpieczeń kryptograficznych do ochrony informacji.	T	T	T	T	
A.10.1.2	Zarządzanie kluczami	Należy opracować politykę dotyczącą korzystania, ochrony i okresów ważności kluczy kryptograficznych i wdrożyć ją na wszystkich etapach cyklu życia kluczy.	T	T	T	T	
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							
A.11.1.1	Fizyczna granica obszaru bezpiecznego	Należy określić granice bezpieczeństwa i wykorzystać je do zabezpieczenia obszarów zawierających wrażliwe lub krytyczne informacje oraz środki przetwarzania informacji.	T	T		T	T
A.11.1.2	Fizyczne zabezpieczenie wejść	Bezpieczne strefy należy chronić odpowiednimi zabezpieczeniami wejść zapewniającymi dostęp wyłącznie osobom uprawnionym.	T	T		T	T
A.11.1.3	Zabezpieczenie biur, pomieszczeń i obiektów	Należy zaprojektować i stosować fizyczne zabezpieczenia biur, po mieszczeń i obiektów.	T	T		T	T
A.11.1.4	Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi	Należy zaprojektować i stosować fizyczne zabezpieczenia przed katastrofami naturalnymi, wrogim atakiem lub wypadkami.	T	T		T	T
A.11.1.5	Praca w obszarach bezpiecznych	Należy zaprojektować i stosować procedury pracy w obszarach bezpiecznych.	T	T		T	T

P: wymaganie prawne, U: zobowiązania umowne, B: wymagania biznesowe/dobre praktyki, AR: wynik analizy ryzyka.

A.11.1.6	Obszary dostaw i załadunku	Należy sprawować nadzór nad punktami dostępu takimi jak obszary dostaw i załadunku oraz innymi punktami, przez które nieuprawnione osoby mogą wejść do pomieszczeń i jeśli to możliwe odizolować je od środków przetwarzania informacji, aby zapobiec nieuprawnio nemu dostępowi.	T	T		T	T
A.11.2 Sprzęt							
Cel: Zapobiec utracie, uszkodzeniu, kradzieży lub utracie integralności aktywów oraz zakłóceniom w działaniu organizacji.							
A.11.2.1	Lokalizacja i ochrona sprzętu	Sprzęt należy umieścić i chronić w taki sposób, aby zredukować ryzyka wynikające z zagrożeń i niebezpieczeństw środowiskowych oraz okazje do nieuprawnionego dostępu.	T	T		T	T
A.11.2.2	Systemy wspomagające	Sprzęt należy chronić przez awariami zasilania oraz innymi przerwami spowodowanymi awariami systemów wspomagających.	T	T		T	T
A.11.2.3	Bezpieczeństwo okablowania	Okablowanie zasilające oraz telekomunikacyjne, przenoszące dane lub wspomagające usługi informacyjne, należy chronić przed przechwyceniem, zakłóceniem lub uszkodzeniem.	T	T		T	T
A.11.2.4	Konserwacja sprzętu	Sprzęt należy prawidłowo konserwować w celu zapewnienia jego ciągłej dostępności i integralności.	T	T		T	T
A.11.2.5	Wynoszenie aktywów	Sprzętu, informacji i programów nie należy wynosić poza siedzibę organizacji bez uzyskania wcześniejszego zezwolenia.	T	T		T	T
A.11.2.6	Bezpieczeństwo sprzętu i aktywów poza siedzibą	Aktywa wynoszone poza siedzibę organizacji należy zabezpieczyć przed wystąpieniem różnych ryzyk związanych z pracą poza siedzibą.	T	T		T	T
A.11.2.7	Bezpieczne zbywanie lub przekazywanie do ponownego użycia	Przed zbyciem lub przekazaniem sprzętu do ponownego użycia należy sprawdzić wszystkie jego składniki zawierające nośniki informacji, dla zapewnienia, że wszystkie wrażliwe dane i licencjonowane programy zostały usunięte lub bezpiecznie nadpisane.	T	T		T	T
A.11.2.8	Pozostawianie sprzętu użytkownika bez opieki	Użytkownicy powinni zapewnić odpowiednią ochronę sprzętu pozostawianego bez opieki.	T	T		T	T
A.11.2.9	Polityka czystego biurka i czystego ekranu	Należy wprowadzić politykę czystego biurka dla dokumentów papierowych i przenośnych nośników pamięci oraz politykę czystego ekranu dla środków przetwarzania informacji.	T	T		T	T
A.12 Bezpieczna eksploatacja							
A.12.1 Procedury eksploatacyjne i odpowiedzialność							
Cel: Zapewnić poprawną i bezpieczną eksploatację środków przetwarzania informacji.							

P: wymaganie prawne, U: zobowiązania umowne, B: wymagania biznesowe/dobre praktyki, AR: wynik analizy ryzyka.

A.12.1.1	Dokumentowanie procedur eksploatacyjnych	Procedury eksploatacyjne powinny być udokumentowane i udostępniane wszystkim potrzebującym ich użytkownikom.	T			T	
A.12.1.2	Zarządzanie zmianami	Zmiany w organizacji, procesach biznesowych, środkach przetwarzania informacji i systemach, które mają wpływ na bezpieczeństwo informacji, powinny być nadzorowane.	T			T	
A.12.1.3	Zarządzanie pojemnością	Należy monitorować i dostosowywać wykorzystanie zasobów oraz przewidywać wymaganą pojemność w przyszłości, dla zapewnienia właściwej wydajności systemu.	T			T	
A.12.1.4	Oddzielanie środowisk rozwojowych, testowych i produkcyjnych	Należy oddzielić środowiska rozwojowe, testowe i produkcyjne celem redukcji ryzyk związanych z nieuprawnionym dostępem lub zmianami w środowisku produkcyjnym.				T	
A.12.2 Ochrona przed szkodliwym oprogramowaniem							
Cel: Zapewnić informacjom i środkom przetwarzania informacji ochronę przed szkodliwym oprogramowa niem.							
A.12.2.1	Zabezpieczenia przed szkodliwym oprogramowaniem	Należy wdrożyć zabezpieczenia wykrywające, zapobiegające i odtwarzające, które służą ochronie przed szkodliwym oprogramowaniem, w połączeniu z właściwym uświadamianiem użytkowników.	T	T		T	T
A.12.3 Kopie zapasowe							
Cel: Chronić przed utratą danych.							
A.12.3.1	Zapasowe kopie informacji	Zapasowe kopie informacji, oprogramowania i obrazów systemów należy regularnie wykonywać i testować, zgodnie z ustaloną polityką kopii zapasowych.	T		T	T	
A.12.4 Rejestrowanie zdarzeń i monitorowanie							
Cel: Rejestrować zdarzenia i zbierać materiał dowodowy.							
A.12.4.1	Rejestrowanie zdarzeń	Należy tworzyć, przechowywać i systematycznie przeglądać dzienniki zdarzeń rejestrujące działania użytkowników, wyjątki, usterki oraz zdarzenia związane z bezpieczeństwem informacji.	T			T	T

P: wymaganie prawne, U: zobowiązania umowne, B: wymagania biznesowe/dobre praktyki, AR: wynik analizy ryzyka.

A.12.4.2	Ochrona informacji w dziennikach zdarzeń	Środki służące rejestrowaniu zdarzeń oraz informacje w dziennikach zdarzeń należy chronić przed manipulacją i nieuprawnionym dostępem.	T			T	T
A.12.4.3	Rejestrowanie działań administratorów i operatorów	Działania administratorów i operatorów systemów należy rejestrować, a dzienniki chronić i systematycznie przeglądać.	T			T	T
A.12.4.4	Synchronizacja zegarów	Zegary wszystkich istotnych systemów przetwarzania informacji w organizacji lub domenie bezpieczeństwa należy zsynchronizować z jednym wzorcowym źródłem czasu.	T			T	T
A.12.5 Nadzór nad oprogramowaniem produkcyjnym							
Cel: Zapewnić integralność systemów produkcyjnych.							
A.12.5.1	Instalacja oprogramowania w systemach produkcyjnych	Należy wdrożyć procedury nadzoru nad instalacją oprogramowania w systemach produkcyjnych.	T			T	
A.12.6 Zarządzanie podatnościami technicznymi							
Cel: Zapobiec wykorzystywaniu podatności technicznych.							
A.12.6.1	Zarządzanie podatnościami technicznymi	Informacje o podatnościach technicznych wykorzystywanych systemów informacyjnych należy niezwłocznie pozyskiwać, oceniać stopień narażenia organizacji na te podatności i podejmować odpowiednie środki w celu przeciwdziałania związanemu z nimi ryzyku.	T			T	T
A.12.6.2	Ograniczenia w instalowaniu oprogramowania	Należy ustanowić i wdrożyć zasady instalowania oprogramowania przez użytkowników.	T			T	T
A.12.7 Rozważania dotyczące audytu systemów informacyjnych							
Cel: Zminimalizować wpływ działań audytu na systemy produkcyjne.							
A.12.7.1	Zabezpieczenia audytu systemów informacyjnych	Należy starannie zaplanować i uzgodnić wymagania audytu oraz działania obejmujące weryfikację systemów produkcyjnych w celu zminimalizowania zakłóceń w procesach biznesowych.	T			T	
A.13 Bezpieczeństwo komunikacji							
A.13.1 Zarządzanie bezpieczeństwem sieci							
Cel: Zapewnić ochronę informacji w sieciach oraz wspomagających je środkach przetwarzania informacji.							

P: wymaganie prawne, U: zobowiązania umowne, B: wymagania biznesowe/dobre praktyki, AR: wynik analizy ryzyka.

A.13.1.1	Zabezpieczenia sieci	Sieci powinny być zarządzane i nadzorowane w celu ochrony informacji w systemach i aplikacjach.	T			T	T
A.13.1.2	Bezpieczeństwo usług sieciowych	Umowy dotyczące wszystkich usług sieciowych, świadczonych wewnętrznie przez organizację lub zlecanych na zewnątrz, powinny za wierać zidentyfikowane mechanizmy zabezpieczeń, poziomy świadczenia usług i wymagania dotyczące zarządzania.	T			T	T
A.13.1.3	Rozdzielanie sieci	Grupy usług informacyjnych, użytkowników i systemów informacyjnych powinny być rozdzielone w strukturze sieci.	T			T	T
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	Należy wdrożyć formalne polityki przesyłania informacji, procedury i zabezpieczenia w celu ochrony wymiany informacji przesyłanych z użyciem wszystkich rodzajów środków łączności.	T	T	T	T	
A.13.2.2	Porozumienia dotyczące przesyłania informacji	Porozumienia powinny uwzględniać bezpieczne przesyłanie informacji biznesowych między organizacją i podmiotami zewnętrznymi.	T	T	T	T	
A.13.2.3	Wiadomości elektroniczne	Informacje przekazywane w formie wiadomości elektronicznych po winny być odpowiednio chronione.	T			T	
A.13.2.4	Umowy o zachowaniu poufności	Należy zidentyfikować, regularnie przeglądać i dokumentować wymagania odnoszące się do umów o zachowaniu poufności lub nie ujawnianiu informacji, w sposób odzwierciedlający potrzeby organizacji w zakresie ochrony informacji.	T	T	T		
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. Dotyczy to również wymagań wobec systemów informacyjnych dostarczających usług w sieciach publicznych.							

P: wymaganie prawne, U: zobowiązania umowne, B: wymagania biznesowe/dobre praktyki, AR: wynik analizy ryzyka.

A.14.1.1	Analiza i specyfikacja wymagań bezpieczeństwa informacji.	Wymagania dotyczące bezpieczeństwa informacji należy włączyć do wymagań stawianych nowym systemom informacyjnym lub rozbudowie systemów istniejących.	T			T	
A.14.1.2	Zabezpieczanie usług aplikacyjnych w sieciach publicznych	Informacje przesyłane w sieciach publicznych, związane z usługami świadczonymi przez aplikacje, należy chronić przed nieuczciwymi działaniami, sporami dotyczącymi umów oraz nieuprawnionym ujawnieniem i zmianami.	T	T		T	
A.14.1.3	Ochrona transakcji usług aplikacyjnych	Informacje związane z transakcjami dokonywanymi w ramach usług świadczonych przez aplikacje należy chronić, aby zapobiec przerwaniu transmisji, błędom w trasowaniu, nieuprawnionym zmianom wiadomości, nieuprawnionemu ujawnieniu, nieuprawnionemu powieleniu lub odtworzeniu.	T	T		T	
A.14.2 Bezpieczeństwo w procesach rozwoju i wsparcia							
Cel: Zapewnić projektowanie i wdrożenie bezpieczeństwa informacji w ramach cyklu życia systemów infor macyjnych.							
A.14.2.1	Polityka bezpieczeństwa prac rozwojowych	Należy ustanowić zasady prac nad rozwojem oprogramowania i systemów oraz stosować je w pracach rozwojowych prowadzonych wewnątrz organizacji.				T	
A.14.2.2	Procedury kontroli zmian w systemach	Należy nadzorować zmiany w systemach podczas ich cyklu rozwojowego, z zastosowaniem formalnych procedur kontroli zmian.				T	
A.14.2.3	Przegląd techniczny aplikacji po zmianach w platformie produkcyjnej	Po dokonaniu zmian w platformach produkcyjnych należy przeprowadzić przegląd krytycznych aplikacji biznesowych oraz przetestować je, aby uzyskać pewność, że zmiany nie miały niekorzystnego wpływu na działalność organizacji lub bezpieczeństwo.				T	
A.14.2.4	Ograniczenia dotyczące zmian w pakietach oprogramowania	Modyfikacji w pakietach oprogramowania należy dokonywać z rozwagą i ograniczać się do zmian niezbędnych, a wszystkie takie zmiany ściśle nadzorować.				T	
A.14.2.5	Zasady projektowania bezpiecznych systemów	Należy ustanowić, udokumentować i utrzymywać zasady projektowania bezpiecznych systemów oraz stosować je do wszystkich prac implementacyjnych nad systemami informacyjnymi.				T	
A.14.2.6	Bezpieczne środowisko rozwojowe	Organizacje powinny ustanowić i odpowiednio chronić bezpieczne środowiska rozwojowe przeznaczone do rozwoju systemów oraz prac integracyjnych obejmujących całość cyklu rozwojowego systemów.				T	
A.14.2.7	Prace rozwojowe zlecane podmiotom zewnętrznym	Organizacja powinna nadzorować i monitorować prace rozwojowe nad systemami zlecone podmiotom zewnętrznym.		T	T	T	

A.14.2.8	Testowanie bezpieczeństwa systemów	Funkcje bezpieczeństwa należy testować w czasie prac rozwojowych.				T	
A.14.2.9	Testy akceptacyjne systemów	Dla nowych systemów informacyjnych, ich modernizacji i nowych wersji systemów należy ustanowić programy testów akceptacyjnych i kryteria z nimi związane.				T	
A.14.3 Dane testowe							
Cel: Zapewnić ochronę danych stosowanych do testów.							
A.14.3.1	Ochrona danych testowych	Dane testowe należy starannie wybierać, chronić i nadzorować.				T	
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	Należy uzgodnić z dostawcą i udokumentować wymagania bezpieczeństwa informacji celem zmniejszenia ryzyk związanych z dostępem dostawcy do aktywów organizacji.	T	T	T	T	
A.15.1.2	Uwzględnianie bezpieczeństwa w porozumieniach z dostawcami	Należy ustanowić wszystkie istotne **wymagania dotyczące bezpieczeństwa informacji** i uzgodnić je z każdym dostawcą, który może uzyskać dostęp, przetwarzać, przechowywać, przesyłać lub dostarczać elementy infrastruktury teleinformatycznej dla przetwarzania informacji należących do organizacji.	T	T	T	T	
A.15.1.3	Łańcuch dostaw technologii informacyjnych i telekomunikacyjnych	**Porozumienia z dostawcami** powinny uwzględniać wymagania odnoszące się do ryzyk w bezpieczeństwie informacji, związanych z usługami technologii informacyjnych i telekomunikacyjnych oraz łańcuchem dostaw produktów.	T	T	T	T	
A.15.2 Zarządzanie usługami świadczonymi 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	Organizacje powinny regularnie monitorować, przeglądać i audytować dostarczanie usług zewnętrznych.	T			T	
A.15.2.2	Zarządzenie zmianami w usługach świadczonych przez dostawców	Należy zarządzać zmianami w zakresie świadczenia usług przez dostawców, w tym utrzymaniem i doskonaleniem istniejących polityk bezpieczeństwa informacji, procedur i zabezpieczeń, z uwzględnieniem krytyczności informacji, systemów i procesów biznesowych, których dotyczą oraz ponownego szacowania ryzyka.	T			T	
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							

P: wymaganie prawne, U: zobowiązania umowne, B: wymagania biznesowe/dobre praktyki, AR: wynik analizy ryzyka.

A.16.1.1	Odpowiedzialność i procedury	Należy ustanowić odpowiedzialność kierownictwa oraz procedury zapewniające szybką, skuteczną i zorganizowaną reakcję na incydenty związane z bezpieczeństwem informacji.	T	T		T	
A.16.1.2	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji	Zdarzenia związane z bezpieczeństwem informacji należy zgłaszać odpowiednimi kanałami zarządczymi tak szybko, jak tylko to jest możliwe.	T			T	
A.16.1.3	Zgłaszanie słabości związanych z bezpieczeństwem informacji	Należy zobowiązać pracowników oraz kontrahentów korzystających z systemów i usług informacyjnych organizacji do odnotowania i zgłaszania wszelkich zaobserwowanych lub podejrzewanych słabości związanych z bezpieczeństwem informacji w systemach lub usługach.	T			T	
A.16.1.4	Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji.	Zdarzenia związane z bezpieczeństwem informacji należy ocenić i podjąć decyzję w sprawie zakwalifikowania ich jako incydentów związanych z bezpieczeństwem informacji.	T			T	
A.16.1.5	Reagowanie na incydenty związane z bezpieczeństwem informacji	Reakcja na incydenty związane z bezpieczeństwem informacji powinna być zgodna z udokumentowanymi procedurami.	T			T	
A.16.1.6	Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji	Wiedzę zdobytą podczas analizy i rozwiązywania incydentów związanych z bezpieczeństwem informacji należy wykorzystać do zredukowania prawdopodobieństwa wystąpienia lub skutków przyszłych incydentów.	T			T	
A.16.1.7	Gromadzenie materiału dowodowego	Organizacja powinna określić i stosować procedury identyfikacji, gromadzenia, pozyskiwania i utrwalania informacji, które mogą stanowić materiał dowodowy.	T	T		T	
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	Organizacja powinna określić wymagania dotyczące bezpieczeństwa informacji i ciągłości zarządzania bezpieczeństwem informacji w niekorzystnych sytuacjach np. w czasie kryzysu lub katastrofy.	T	T		T	
A.17.1.2	Wdrożenie ciągłości bezpieczeństwa informacji	Organizacja powinna ustanowić, udokumentować, wdrożyć i utrzymywać procesy, procedury i zabezpieczenia dla zapewnienia w niekorzystnej sytuacji wymaganego poziomu ciągłości bezpieczeństwa informacji.	T	T		T	
A.17.1.3	Weryfikowanie, przegląd i ocena ciągłości bezpieczeństwa informacji	Organizacja powinna weryfikować ustanowione i wdrożone zabezpieczenia ciągłości bezpieczeństwa informacji w regularnych odstępach czasu celem zapewnienia ich aktualności i skuteczności w niekorzystnych sytuacjach.	T	T		T	
A.17.2 Nadmiarowość							
Cel: Zapewnić dostępność środków przetwarzania informacji.							

P: wymaganie prawne, U: zobowiązania umowne, B: wymagania biznesowe/dobre praktyki, AR: wynik analizy ryzyka.

A.17.2.1	Dostępność środków przetwarzania informacji	Środki przetwarzania informacji należy wdrażać z nadmiarem wystarczającym do spełnienia wymagań dostępności.	T	T		T	
A.18 Zgodność							
A.18.1 Zgodność z wymaganiami prawnymi i umownymi							
Cel: Unikać naruszenia zobowiązań prawnych, regulacyjnych lub umownych związanych z bezpieczeń stwem informacji oraz innych wymagań dotyczących							
A.18.1.1	Określenie stosownych wymagań prawnych i umownych	Wszystkie istotne wymagania prawne, regulacyjne, umowne oraz podejście organizacji do ich przestrzegania należy zidentyfikować, udokumentować i aktualizować dla każdego systemu informacyjne go oraz całości organizacji.	T	T	T		
A.18.1.2	Prawa własności intelektualej	Należy wdrożyć odpowiednie procedury zapewniające zgodność z wymaganiami prawnymi, regulacyjnymi i umownymi, związanymi z prawami własności intelektualnej i użytkowaniem prawnie zastrze żonego oprogramowania.	T	T	T	T	
A.18.1.3	Ochrona zapisów	Zapisy należy chronić przed utratą, zniszczeniem, fałszowaniem, nieuprawnionym dostępem i nieuprawnionym opublikowaniem, stosownie do wymagań prawnych, regulacyjnych, umownych i biznesowych.	T	T	T	T	
A.18.1.4	Prywatność i ochrona danych identyfikujących osobę	Należy zapewnić prywatność i ochronę danych identyfikujących osobę stosownie do odpowiednich przepisów prawa i regulacji.	T	T	T		
A.18.1.5	Regulacje dotyczące zabezpieczeń kryptograficznych	Zabezpieczenia kryptograficzne należy stosować zgodnie z odpowiednimi umowami, przepisami i regulacjami.	T	T	T	T	
A.18.2 Przeglądy bezpieczeństwa informacji							
Cel: Zapewnić zgodne z politykami organizacji i procedurami wdrożenie i stosowanie zasad bezpieczeń stwa informacji.							
A.18.2.1	Niezależny przegląd bezpieczeństwa infomacji	Podejście organizacji do zarządzania bezpieczeństwem informacji oraz jego wdrożenie (tzn. cele stosowania zabezpieczeń, zabezpieczenia, polityki, procesy i procedury dotyczące bezpieczeństwa informacji) należy poddawać niezależnemu przeglądowi w zaplanowanych odstępach czasu lub wtedy, gdy nastąpią istotne zmiany.	T			T	
A.18.2.2	Zgodność z politykami bezpieczeństwa i standardami	Kierownicy powinni regularnie dokonywać przeglądu zgodności przetwarzania informacji i procedur z odpowiednimi politykami bezpieczeństwa, standardami i innymi wymaganiami dotyczącymi bezpieczeństwa, w zakresie przydzielonej im odpowiedzialności.	T			T	
A.18.2.3	Sprawdzanie zgodności technicznej	Należy regularnie przeglądać systemy informacyjne celem sprawdzenia ich zgodności z politykami bezpieczeństwa informacji i standardami obowiązującymi w organizacji.	T			T	