PROGRAM AUDITÓW

NAZWA I ADRES ORGANIZACJI:	

ROZDZIAŁ	KRYTERIA	USTALONY PROGRAM AUDITÓW PN-ISO/IEC 27001:2014											
		CERTYFIKACJA		I AUDIT NADZORU				II AUDIT NADZORU				RECERTYFIKACJA	
		PN	O	PN	O	ZO	KO	PN	O	ZO	KO	PN	O
4 KONTEKST ORGANIZACJI	Zrozumienie organizacji i jej kontekstu	4.1		4.1				4.1				4.1	
	Zrozumienie potrzeb i oczekiwań zainteresowanych stron	4.2		4.2				4.2				4.2	
	Określenie zakresu systemu zarzadzania bezpieczeństwem informacji	4.3		4.3				4.3				4.3	
	System zarzadzania bezpieczeństwem informacji	4.4		4.4				4.4				4.4	
5 PRZYWÓDZTWO	Przywództwo i zaangażowanie	5.1		5.1				5.1				5.1	
	Polityka	5.2		5.2				5.2				5.2	
	Role, odpowiedzialność i uprawnienia	5.3		5.3				5.3				5.3	
6 PLANOWANIE	Działania odnoszące się do ryzyk i szans	6.1		6.1				6.1				6.1	
	Cele systemu zarzadzania i planowanie ich osiągnięcia	6.2		6.2				6.2				6.2	
7 WSPARCIE	Zasoby	7.1		7.1				7.1				7.1	
	Kompetencje	7.2		7.2				7.2				7.2	
	Uświadamianie	7.3		7.3				7.3				7.3	
	Komunikacja	7.4		7.4				7.4				7.4	
	Udokumentowane informacje	7.5		7.5				7.5				7.5	
8 DZIAŁANIA OPERACYJNE	Planowanie i nadzór nad działaniami operacyjnymi	8.1		8.1				8.1				8.1	
	Szacowanie ryzyka w bezpieczeństwie informacji	8.2		8.2				8.2				8.2	
	Postepowanie z ryzykiem w bezpieczeństwie informacji	8.3		8.3				8.3				8.3	
9 OCENA WYNIKÓW	Monitorowanie, pomiary, analiza i ocena	9.1		9.1				9.1				9.1	
	Audity wewnętrzne	9.2		9.2				9.2				9.2	
	Przegląd zarzadzania	9.3		9.3				9.3				9.3	
10 DOSKONALENIE	Niezgodność i działania korygujące	10.1		10.1				10.1				10.1	
	Ciągłe doskonalenie	10.2		10.2				10.2				10.2	
ZAŁĄCZNIK A	Cele zabezpieczeń i zabezpieczenia	Zał. 1		Zał. 1				Zał. 1				Zał. 1	
		Auditor wiodący: ……..…….. Termin auditu: (dd.mm.rrrr)		Auditor wiodący: …… Termin auditu: (dd.mm.rrrr)				Auditor wiodący: …….. Termin auditu: (dd.mm.rrrr)				Auditor wiodący: ……..… Termin auditu: (dd.mm.rrrr)	

LEGENDA:

- zaznaczone na szaro pola są obowiązkowe na każdym audicie

PN – punkty normy odniesienia; **O** – ocena z przeprowadzonego auditu; **ZO** – obszary zaplanowane do przeauditowania; **KO** – zmiana obszarów zaplanowanych do przeauditowania

ZABEZPIECZENIE			CERTY-FIKACJA		I AUDIT NADZÓR				II AUDIT NADZÓR				RECERTY-FIKACJA	
ROZDZIAŁ	**GRUPA**	**PODGRUPA**	**PN**	**O**	**PN**	**O**	**ZO**	**KO**	**PN**	**O**	**ZO**	**KO**	**PN**	**O**
A.5 POLITYKI BEZP. INFORMACJI	A.5.1 Polityki bezpieczeństwa informacji	Polityki bezpieczeństwa informacji	A.5.1.1		A.5.1.1				A.5.1.1				A.5.1.1	
		Przegląd polityki bezpieczeństwa informacji	A.5.1.2		A.5.1.2				A.5.1.2				A.5.1.2	
A.6 ORGANIZACJA BEZPIECZEŃSTWA INFORMACJI	A.6.1 Organizacja wewnętrzna	Role i odpowiedzialność za bezpieczeństwo informacji	A.6.1.1		A.6.1.1				A.6.1.1				A.6.1.1	
		Rozdzielanie obowiązków	A.6.1.2		A.6.1.2				A.6.1.2				A.6.1.2	
		Kontakty z organami władzy	A.6.1.3		A.6.1.3				A.6.1.3				A.6.1.3	
		Kontakty z grupami zainteresowanych specjalistów	A.6.1.4		A.6.1.4				A.6.1.4				A.6.1.4	
		Bezpieczeństwo informacji w zarządzaniu projektami	A.6.1.5		A.6.1.5				A.6.1.5				A.6.1.5	
	A.6.2 Urządzenia mobilne i telepraca	Polityka stosowania urządzeń mobilnych	A.6.2.1		A.6.2.1				A.6.2.1				A.6.2.1	
		Telepraca	A.6.2.2		A.6.2.2				A.6.2.2				A.6.2.2	
A.7 BEZPIECZEŃSTWO ZASOBÓW LUDZKICH	A.7.1 Przed zatrudnieniem	Postepowanie sprawdzające	A.7.1.1		A.7.1.1				A.7.1.1				A.7.1.1	
		Warunki zatrudnienia	A.7.1.2		A.7.1.2				A.7.1.2				A.7.1.2	
	A.7.2 Podczas zatrudnienia	Odpowiedzialność kierownictwa	A.7.2.1		A.7.2.1				A.7.2.1				A.7.2.1	
		Uświadamianie, kształcenie i szkolenie z zakresu bezpieczeństwa informacji	A.7.2.2		A.7.2.2				A.7.2.2				A.7.2.2	
		Postępowanie dyscyplinarne	A.7.2.3		A.7.2.3				A.7.2.3				A.7.2.3	
	A.7.3 Zakończenia i zmiana zatrudnienia	Zakończenie zatrudnienia lub zmiana zakresu obowiązków	A.7.3.1		A.7.3.1				A.7.3.1				A.7.3.1	
A.8 ZARZĄDZANIE AKTYWAMI	A.8.1 Odpowiedzialność za aktywa	Inwentaryzacja aktywów	A.8.1.1		A.8.1.1				A.8.1.1				A.8.1.1	
		Własność aktywów	A.8.1.2		A.8.1.2				A.8.1.2				A.8.1.2	
		Akceptowalne użycie aktywów	A.8.1.3		A.8.1.3				A.8.1.3				A.8.1.3	
		Zwrot aktywów	A.8.1.4		A.8.1.4				A.8.1.4				A.8.1.4	
	A.8.2 Klasyfikacja informacji	Klasyfikowanie informacji	A.8.2.1		A.8.2.1				A.8.2.1				A.8.2.1	
		Oznaczanie informacji	A.8.2.2		A.8.2.2				A.8.2.2				A.8.2.2	
		Postępowanie z aktywami	A.8.2.3		A.8.2.3				A.8.2.3				A.8.2.3	
	A.8.3 Postepowanie z nośnikami	Zarządzanie nośnikami wymiennymi	A.8.3.1		A.8.3.1				A.8.3.1				A.8.3.1	
		Wycofywanie nośników	A.8.3.2		A.8.3.2				A.8.3.2				A.8.3.2	
		Przekazywanie nośników	A.8.3.3		A.8.3.3				A.8.3.3				A.8.3.3	
A.9 KONTROLA DOS	A.9.1 Wymagania biznesowe wobec kontroli dostępu	Polityka kontroli dostępu	A.9.1.1		A.9.1.1				A.9.1.1				A.9.1.1	
		Dostęp do sieci i usług sieciowych	A.9.1.2		A.9.1.2				A.9.1.2				A.9.1.2	

ZABEZPIECZENIE			CERTY-FIKACJA		I AUDIT NADZÓR				II AUDIT NADZÓR				RECERTY-FIKACJA	
ROZDZIAŁ	GRUPA	PODGRUPA	PN	O	PN	O	ZO	KO	PN	O	ZO	KO	PN	O
	A.9.2 Zarządzanie dostępem użytkowników	Rejestrowanie i wyrejestrowywanie użytkowników	A.9.2.1		A.9.2.1				A.9.2.1				A.9.2.1	
		Przydzielanie dostępu użytkownikom	A.9.2.2		A.9.2.2				A.9.2.2				A.9.2.2	
		Zarządzanie prawami uprzywilejowanego dostępu	A.9.2.3		A.9.2.3				A.9.2.3				A.9.2.3	
		Zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników	A.9.2.4		A.9.2.4				A.9.2.4				A.9.2.4	
		Przegląd praw dostępu użytkowników	A.9.2.5		A.9.2.5				A.9.2.5				A.9.2.5	
		Odbieranie lub dostosowywanie praw dostępu	A.9.2.6		A.9.2.6				A.9.2.6				A.9.2.6	
	A.9.3 Odpowiedzialność użytkowników	Stosowanie poufnych informacji uwierzytelniających	A.9.3.1		A.9.3.1				A.9.3.1				A.9.3.1	
	A.9.4 Kontrola dostępu do systemów i aplikacji	Ograniczanie dostępu do informacji	A.9.4.1		A.9.4.1				A.9.4.1				A.9.4.1	
		Procedury bezpiecznego logowania	A.9.4.2		A.9.4.2				A.9.4.2				A.9.4.2	
		System zarządzania hasłami	A.9.4.3		A.9.4.3				A.9.4.3				A.9.4.3	
		Użycie uprzywilejowanych programów narzędziowych	A.9.4.4		A.9.4.4				A.9.4.4				A.9.4.4	
		Kontrola dostępu do kodów źródłowych programów	A.9.4.5		A.9.4.5				A.9.4.5				A.9.4.5	
A.10 KRYPTOGRAFIA	A.10.1 Zabezpieczenia kryptograficzne	Polityka stosowania zabezpieczeń kryptograficznych	A.10.1.1		A.10.1.1				A.10.1.1				A.10.1.1	
		Zarządzanie kluczami	A.10.1.2		A.10.1.2				A.10.1.2				A.10.1.2	
A.11 BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE	A.11.1 Obszary bezpieczne	Fizyczna granica obszaru bezpiecznego	A.11.1.1		A.11.1.1				A.11.1.1				A.11.1.1	
		Fizyczne zabezpieczenie wejść	A.11.1.2		A.11.1.2				A.11.1.2				A.11.1.2	
		Zabezpieczenie biur, pomieszczeń i obiektów	A.11.1.3		A.11.1.3				A.11.1.3				A.11.1.3	
		Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi	A.11.1.4		A.11.1.4				A.11.1.4				A.11.1.4	
		Praca w obszarach bezpiecznych	A.11.1.5		A.11.1.5				A.11.1.5				A.11.1.5	
		Obszary dostaw i załadunku	A.11.1.6		A.11.1.6				A.11.1.6				A.11.1.6	
	A.11.2 Sprzęt	Lokalizacja i ochrona sprzętu	A.11.2.1		A.11.2.1				A.11.2.1				A.11.2.1	
		Systemy wspomagające	A.11.2.2		A.11.2.2				A.11.2.2				A.11.2.2	
		Bezpieczeństwo okablowania	A.11.2.3		A.11.2.3				A.11.2.3				A.11.2.3	
		Konserwacja sprzętu	A.11.2.4		A.11.2.4				A.11.2.4				A.11.2.4	
		Wynoszenie aktywów	A.11.2.5		A.11.2.5				A.11.2.5				A.11.2.5	
		Bezpieczeństwo sprzętu i aktywów poza siedzibą	A.11.2.6		A.11.2.6				A.11.2.6				A.11.2.6	
		Bezpieczne zbywanie lub przekazywanie do ponownego użycia	A.11.2.7		A.11.2.7				A.11.2.7				A.11.2.7	
		Pozostawianie sprzętu użytkownika bez opieki	A.11.2.8		A.11.2.8				A.11.2.8				A.11.2.8	

ZABEZPIECZENIE			CERTY-FIKACJA		I AUDIT NADZÓR				II AUDIT NADZÓR				RECERTY-FIKACJA	
ROZDZIAŁ	GRUPA	PODGRUPA	PN	O	PN	O	ZO	KO	PN	O	ZO	KO	PN	O
		Polityka czystego biurka i czystego ekranu	A.11.2.9		A.11.2.9				A.11.2.9				A.11.2.9	
A.12 BEZPIECZEŃA EKSPLOATACJA	A.12.1 Procedury eksploatacyjne i odpowiedzialność	Dokumentowanie procedur eksploatacyjnych	A.12.1.1		A.12.1.1				A.12.1.1				A.12.1.1	
		Zarządzanie zmianami	A.12.1.2		A.12.1.2				A.12.1.2				A.12.1.2	
		Zarządzanie pojemnością	A.12.1.3		A.12.1.3				A.12.1.3				A.12.1.3	
		Oddzielanie środowisk rozwojowych, testowych i produkcyjnych	A.12.1.4		A.12.1.4				A.12.1.4				A.12.1.4	
	A.12.2 Ochrona przed szkodliwym oprogramowaniem	Zabezpieczenia przed szkodliwym oprogramowaniem	A.12.2.1		A.12.2.1				A.12.2.1				A.12.2.1	
	A.12.3 Kopie zapasowe	Zapasowe kopie informacji	A.12.3.1		A.12.3.1				A.12.3.1				A.12.3.1	
	A.12.4 Rejestrowanie zdarzeń i monitorowanie	Rejestrowanie zdarzeń	A.12.4.1		A.12.4.1				A.12.4.1				A.12.4.1	
		Ochrona informacji w dziennikach zdarzeń	A.12.4.2		A.12.4.2				A.12.4.2				A.12.4.2	
		Rejestrowanie działań administratorów i operatorów	A.12.4.3		A.12.4.3				A.12.4.3				A.12.4.3	
		Synchronizacja zegarów	A.12.4.4		A.12.4.4				A.12.4.4				A.12.4.4	
	A.12.5 Nadzór nad oprogramowaniem produkcyjnym	Instalacja oprogramowania w systemach produkcyjnych	A.12.5.1		A.12.5.1				A.12.5.1				A.12.5.1	
	A.12.6 Zarządzanie podatnościami technicznymi	Zarządzanie podatnościami technicznymi	A.12.6.1		A.12.6.1				A.12.6.1				A.12.6.1	
		Ograniczenia w instalowaniu oprogramowania	A.12.6.1		A.12.6.1				A.12.6.1				A.12.6.1	
	A.12.7 Rozważania dotyczące audytu systemów informacyjnych	Zabezpieczenia audytu systemów informacyjnych	A.12.7.1		A.12.7.1				A.12.7.1				A.12.7.1	
A.13 BEZPIECZEŃSTWO KOMUNIKACJI	A.13.1 Zarządzanie bezpieczeństwem sieci	Zabezpieczenia sieci	A.13.1.1		A.13.1.1				A.13.1.1				A.13.1.1	
		Bezpieczeństwo usług sieciowych	A.13.1.2		A.13.1.2				A.13.1.2				A.13.1.2	
		Rozdzielanie sieci	A.13.1.3		A.13.1.3				A.13.1.3				A.13.1.3	
	A.13.2 Przesyłanie informacji	Polityki i procedury przesyłania informacji	A.13.2.1		A.13.2.1				A.13.2.1				A.13.2.1	
		Porozumienia dotyczące przesyłania informacji	A.13.2.2		A.13.2.2				A.13.2.2				A.13.2.2	
		Wiadomości elektroniczne	A.13.2.3		A.13.2.3				A.13.2.3				A.13.2.3	
		Umowy o zachowaniu poufności	A.13.2.4		A.13.2.4				A.13.2.4				A.13.2.4	
A.14 POZYSKIWANIE, ROWÓJ I UTRZYMANIE	A.14.1 Wymagania związane z bezpieczeństwem systemów informacyjnych	Analiza i specyfikacja wymagań bezpieczeństwa informacji	A.14.1.1		A.14.1.1				A.14.1.1				A.14.1.1	
		Zabezpieczanie usług aplikacyjnych w sieciach publicznych	A.14.1.2		A.14.1.2				A.14.1.2				A.14.1.2	
		Ochrona transakcji usług aplikacyjnych	A.14.1.3		A.14.1.3				A.14.1.3				A.14.1.3	

ZABEZPIECZENIE			CERTY-FIKACJA		I AUDIT NADZÓR				II AUDIT NADZÓR				RECERTY-FIKACJA	
ROZDZIAŁ	GRUPA	PODGRUPA	PN	O	PN	O	ZO	KO	PN	O	ZO	KO	PN	O
	A.14.2 Bezpieczeństwo w procesach rozwoju i wsparcia	Polityka bezpieczeństwa prac rozwojowych	A.14.2.1		A.14.2.1				A.14.2.1				A.14.2.1	
		Procedury kontroli zmian w systemach	A.14.2.2		A.14.2.2				A.14.2.2				A.14.2.2	
		Przegląd techniczny aplikacji po zmianach w platformie produkcyjnej	A.14.2.3		A.14.2.3				A.14.2.3				A.14.2.3	
		Ograniczenia dotyczące zmian w pakietach oprogramowania	A.14.2.4		A.14.2.4				A.14.2.4				A.14.2.4	
		Zasady projektowania bezpiecznych systemów	A.14.2.5		A.14.2.5				A.14.2.5				A.14.2.5	
		Bezpieczne środowisko rozwojowe	A.14.2.6		A.14.2.6				A.14.2.6				A.14.2.6	
		Prace rozwojowe zlecane podmiotom zewnętrznym	A.14.2.7		A.14.2.7				A.14.2.7				A.14.2.7	
		Testowanie bezpieczeństwa systemów	A.14.2.8		A.14.2.8				A.14.2.8				A.14.2.8	
		Testy akceptacyjne systemów	A.14.2.9		A.14.2.9				A.14.2.9				A.14.2.9	
	A.14.3 Dane testowe	Ochrona danych testowych	A.14.3.1		A.14.3.1				A.14.3.1				A.14.3.1	
A.15 RELACJE Z DOSTAWCAMI	A.15.1 Bezpieczeństwo informacji w relacji z dostawcami	Polityka bezpieczeństwa informacji w relacjach z dostawcami	A.15.1.1		A.15.1.1				A.15.1.1				A.15.1.1	
		Uwzględnianie bezpieczeństwa w porozumieniach z dostawcami	A.15.1.2		A.15.1.2				A.15.1.2				A.15.1.2	
		Łańcuch dostaw technologii informacyjnych i telekomunikacyjnych	A.15.1.3		A.15.1.3				A.15.1.3				A.15.1.3	
	A.15.2 Zarządzanie usługami świadczonymi przez dostawców	Monitorowanie i przegląd usług świadczonych przez dostawców	A.15.2.1		A.15.2.1				A.15.2.1				A.15.2.1	
		Zarządzenie zmianami w usługach świadczonych przez dostawców	A.15.2.2		A.15.2.2				A.15.2.2				A.15.2.2	
A.16 ZARZĄDZANIE INCYDENTAMI ZWIĄZANYMI	A.16.1 Zarządzanie incydentami związanymi z bezpieczeństwem	Odpowiedzialność i procedury	A.16.1.1		A.16.1.1				A.16.1.1				A.16.1.1	
		Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji	A.16.1.2		A.16.1.2				A.16.1.2				A.16.1.2	
		Zgłaszanie słabości związanych z bezpieczeństwem informacji	A.16.1.3		A.16.1.3				A.16.1.3				A.16.1.3	

ZABEZPIECZENIE			CERTY-FIKACJA		I AUDIT NADZÓR				II AUDIT NADZÓR				RECERTY-FIKACJA	
ROZDZIAŁ	GRUPA	PODGRUPA	PN	O	PN	O	ZO	KO	PN	O	ZO	KO	PN	O
	informacji oraz udoskonaleniami	Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji	A.16.1.4		A.16.1.4				A.16.1.4				A.16.1.4	
		Reagowanie na incydenty związane z bezpieczeństwem informacji	A.16.1.5		A.16.1.5				A.16.1.5				A.16.1.5	
		Wyciąganie wniosków z incydentów związanych z bezpieczeństwem	A.16.1.6		A.16.1.6				A.16.1.6				A.16.1.6	
		Gromadzenie materiału dowodowego	A.16.1.7		A.16.1.7				A.16.1.7				A.16.1.7	
A.17 ASPEKTY BEZP. INFORMACJI W ZARZĄDZANIU CIĄGŁOŚCIĄ DZIAŁANIA	A.17.1 Ciągłość bezpieczeństwa informacji	Planowanie ciągłości bezpieczeństwa informacji	A.17.1.1		A.17.1.1				A.17.1.1				A.17.1.1	
		Wdrożenie ciągłości bezpieczeństwa informacji	A.17.1.2		A.17.1.2				A.17.1.2				A.17.1.2	
		Weryfikowanie, przegląd i ocena ciągłości bezp. informacji	A.17.1.3		A.17.1.3				A.17.1.3				A.17.1.3	
	A.17.2 Nadmiarowość	Dostępność środków przetwarzania informacji	A.17.2.1		A.17.2.1				A.17.2.1				A.17.2.1	
A.18 ZGODNOŚĆ	A.18.1 Zgodność z wymaganiami prawnymi i umowami	Określenie stosownych wymagań prawnych i umownych	A.18.1.1		A.18.1.1				A.18.1.1				A.18.1.1	
		Prawa własności intelektualnej	A.18.1.2		A.18.1.2				A.18.1.2				A.18.1.2	
		Ochrona zapisów	A.18.1.3		A.18.1.3				A.18.1.3				A.18.1.3	
		Prywatność i ochrona danych identyfikujących osobę	A.18.1.4		A.18.1.4				A.18.1.4				A.18.1.4	
		Regulacje dotyczące zabezpieczeń kryptograficznych	A.18.1.5		A.18.1.5				A.18.1.5				A.18.1.5	
	A.18.2 Przegląd bezpieczeństwa informacji	Niezależny przegląd bezpieczeństwa informacji	A.18.2.1		A.18.2.1				A.18.2.1				A.18.2.1	
		Zgodność z politykami bezpieczeństwa i standardami	A.18.2.2		A.18.2.2				A.18.2.2				A.18.2.2	
		Sprawdzanie zgodności technicznej	A.18.2.3		A.18.2.3				A.18.2.3				A.18.2.3	