Deklaracja stosowania

Wymagania PN-ISO/IEC 27001:2014-12 Załącznik A Wzorcowy wykaz celów stosowania zabepieczeń i zabezpieczenia	Stosowana kontrola			Wybrane zabezpieczenia i powody stosowania zabezpieczeń				Uwagi (w tym odnoszące się dokumenty, procedury i instrukcje)
	wdrożone	planowane wdrażane	wykluczone	wymagania dot. funkcjon. UM	wymagania prawne	dobre praktyki	wyniki analizy ryzyka	
5 Polityki bezpieczeństwa informacji								
5.1 Kierunki bezpieczeństwa informacji określane przez kierownictwo								
5.1.1 Polityki bezpieczeństwa informacji	X			X	X			Polityka Kierownictwa, Dokumentacja Systemu Zarządzania Bezpieczeństwa Informacji, Zasady Systemu Zarządzania Bezpieczeństwem Informacji, Księga ZSZ, Zarządzenie PM ws. wprowadzenia w Urzędzie Miejskim w B-B "Polityki bezpieczeństwa ochrony danych osobowych" oraz zarządzenie w sprawie organizacji ochrony danych osobowych oraz zasad postępowania przy ich przetwarzaniu w Urzędzie Miejskim w Bielsku-Białej
5.1.2 Przegląd polityk bezpieczeństwa informacji	X			X	X			Przeglądy ZSZ
6 Organizacja bezpieczeństwa informacji								
6.1 Organizacja wewnętrzna								
6.1.1 Role i odpowiedzialność za bezpieczeństwo informacji	X			X	X	X		Księga ZSZ, Administratorzy, Pełnomocnik PM ds. ZSZ, Naczelnicy wydziałów - właściciele aktywów, Instrukcja ISZ-4/2/IT/1 Zasady bezpiecznego korzystania z systemów informatycznych przez użytkowników, Zarządzenie PM ws. organizacji ochrony danych osobowych oraz zasad postępowania przy ich przetwarzaniu w UM w B-B, Instrukcja ISZ-4/2/BO/1 Zasady postępowania przy zmianie stanowiska pracy, karty stanowiskowe, Upoważnienie do przetwarzania danych osobowych
6.1.2 Rozdzielanie obowiązków	X			X	X	X		Księga ZSZ, Administratorzy, Pełnomocnik PM ds. ZSZ, Naczelnicy wydziałów - właściciele aktywów, karty urządzeń
6.1.3 Kontakty z organami władzy	X			X	X	X		Telefony alarmowe, ISZ-3/2/3 Instrukcja ewakuacji na wypadek pożaru, Plan ciągłości działania, publikacje w Dzienniku Urzędowym Województwa
6.1.4 Kontakty z grupami zainteresowanych specjalistów	X				X	X		Polskie Towarzystwo Informatyczne, Stowarzyszenie "Miasta w Internecie", konferencje organizowane przez firmy informatyczne, administratorzy systemów korzystają z forów internetowych, Śląskie Centrum Społeczeństwa Informacyjnego - "SEKAP", Centrum Projektów Informatycznych
6.1.5 Bezpieczeństwo informacji w zarządzaniu projektami								Instrukcja INF-1/4/7 Bezpieczeństwo projektów informatycznych
6.2 Urządzenia mobilne i telepraca								
6.2.1 Polityka stosowania urządzeń mobilnych	X			X		X		Konfiguracja, Instrukcje: INF-1/4/2 Bezpieczeństwo komputerów przenośnych, INF-1/4/4 Bezpieczeństwo sieci, INF-1/4/5 Bezpieczeństwo urządzeń mobilnych
6.2.2 Telepraca	X			X		X		Konfiguracja, Instrukcje: INF-1/4/2 Bezpieczeństwo komputerów przenośnych, INF-1/4/4 Bezpieczeństwo sieci, klauzule w umowach z dostawcami oprogramowania, INF-1/4/6 Bezpieczeństwo podczas telepracy

Wymagania PN-ISO/IEC 27001:2014-12 Załącznik A Wzorcowy wykaz celów stosowania zabepieczeń i zabezpieczenia	Stosowana kontrola			Wybrane zabezpieczenia i powody stosowania zabezpieczeń				Uwagi (w tym odnoszące się dokumenty, procedury i instrukcje)
	wdrożone	planowane wdrażane	wykluczone	wymagania dot. funkcjon. UM	wymagania prawne	dobre praktyki	wyniki analizy ryzyka	
7 Bezpieczeństwo zasobów ludzkich								
7.1 Przed zatrudnieniem								
7.1.1 Postępowanie sprawdzające	X				X	X		Instrukcja ISZ-4/2/BO/1 Zasady postępowania przy zmianie stanowiska pracy, karty stanowiskowe, wymagania prawne, konkursy
7.1.2 Warunki zatrudnienia	X			X		X		Instrukcja ISZ-4/2/BO/1 Zasady postępowania przy zmianie stanowiska pracy, umowa z pracownikiem, umowy ze stroną trzecią, Regulamin pracy, Polityka bezpieczeństwa ochrony danych osobowych, wymagania prawne,
7.2 Podczas zatrudnienia								
7.2.1 Odpowiedzialność kierownictwa	X			X	X	X		Instrukcja ISZ-4/2/BO/1 Zasady postępowania przy zmianie stanowiska pracy, szkolenia wstępne, Regulamin pracy, Oświadczenie o zapoznaniu się z treścią Polityki Kierownictwa oraz o sposobie postępowania z informacjami w UM w B-B, Polityka bezpieczeństwa ochrony danych osobowych
7.2.2 Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji	X			X	X			Szkolenia na wszystkich szczeblach, Regulamin pracy, Oświadczenie o zapoznaniu się z treścią Polityki Kierownictwa oraz o sposobie postępowania z informacjami w UM w B-B
7.2.3 Postępowanie dyscyplinarne	X			X	X	X		Regulamin pracy
7.3 Zakończenie i zmiana zatrudnienia								
7.3.1 Zakończenie zatrudnienia lub zmiana zakresu obowiązków	X			X	X	X		Instrukcja ISZ-4/2/BO/1 Zasady postępowania przy zmianie stanowiska pracy, karta obiegowa, Polityka bezpieczeństwa ochrony danych osobowych, INF-1/5/5 Utrzymywanie i kontrola dostępu w systemach informatycznych
8 Zarządzanie aktywami								
8.1 Odpowiedzialność za aktywa								
8.1.1 Inwentaryzacja aktywów	X					X	X	Procedura PSZ-4/1 Analiza ryzyka bezpieczeństwa informacji, klasyfikacja informacji, Programy-środki trwałe, środki nietrwałe i prasa
8.1.2 Własność aktywów	X					X	X	Procedura PSZ-4/1 Analiza ryzyka bezpieczeństwa informacji, klasyfikacja informacji
8.1.3 Akceptowalne użycie aktywów	X			X		X		Procedury BI (postępowanie)
8.1.4 Zwrot aktywów	X			X	X			Instrukcja ISZ-4/2/BO/1 Zasady postępowania przy zmianie stanowiska pracy, karta obiegowa
8.2 Klasyfikacja informacji								
8.2.1 Klasyfikowanie informacji	X			X	X	X	X	Procedury: PSZ-4/1 Analiza ryzyka bezpieczeństwa informacji, PSZ-1/3 Nadzór nad udokumentowaną informacją
8.2.2 Oznaczanie informacji	X			X	X	X	X	Procedury: PSZ-4/1 Analiza ryzyka bezpieczeństwa informacji, PSZ-1/3 Nadzór nad udokumentowaną informacją
8.2.3 Postępowanie z aktywami	X			X	X	X	X	Procedura PSZ-1/3 Nadzór nad udokumentowaną informacją, Upoważnienie do przetwarzania danych osobowych

Wymagania PN-ISO/IEC 27001:2014-12 Załącznik A Wzorcowy wykaz celów stosowania zabepieczeń i zabezpieczenia	Stosowana kontrola			Wybrane zabezpieczenia i powody stosowania zabezpieczeń				Uwagi (w tym odnoszące się dokumenty, procedury i instrukcje)
	wdrożone	planowane wdrażane	wykluczone	wymagania dot. funkcjon. UM	wymagania prawne	dobre praktyki	wyniki analizy ryzyka	
8.3 Postępowanie z nośnikami								
8.3.1 Zarządzanie nośnikami wymiennymi	X			X		X	X	Instrukcje: INF-1/5/2 Przekazywanie urządzeń i nośników do ponownego wykorzystania, zbywania lub wycofania z użycia, INF-1/6/1 Tworzenie i przechowywanie kopii bezpieczeństwa danych, niszczenie i usuwanie danych, rejestr wykorzystywanych nośników informacji
8.3.2 Wycofywanie nośników	X				X	X	X	Instrukcja INF-1/5/2 Przekazywanie urządzeń i nośników do ponownego wykorzystania, zbywania lub wycofania z użycia
8.3.3 Przekazywanie nośników	X			X	X	X		Procedura PSZ-1/3 Nadzór nad udokumentowaną informacją, Instrukcje: INF-1/4/2 Bezpieczeństwo komputerów przenośnych, INF-1/5/2 Przekazywanie urządzeń i nośników do ponownego wykorzystania, zbywania lub wycofania z użycia, INF-1/6/2 Ochrona kryptograficzna, INF-1/6/3 Przekazanie sprzętu do i z eksploatacji, do i z naprawy
9 Kontrola dostępu								
9.1 Wymagania biznesowe wobec kontroli dostępu								
9.1.1 Polityka kontroli dostępu	X			X	X	X	X	Instrukcje: INF-1/4/2 Bezpieczeństwo komputerów przenośnych, INF-1/4/3 Bezpieczeństwo stacji roboczych, INF-1/4/4 Bezpieczeństwo sieci, INF-1/5/3 Dobór haseł, IINF-1/5/4 Bezpieczeństwo oprogramowania, INF-1/5/5 Utrzymanie i kontrola dostępu w systemach informatycznych, INF-1/6/3 Przekazanie sprzętu do i z eksploatacji, do i z naprawy, ISZ-4/2/IT/1 Zasady bezpiecznego korzystania z systemów informatycznych przez użytkowników, ISZ-4/2/BF/1 Zarządzanie dostępem do pomieszczeń, ISZ-4/2/BF/2 Zasady pracy w strefach, ISZ-4/2/BF/3 Kontrola dostępu przez wykonawców zewnętrznych, ISZ-4/2/BO/1 Zasady postępowania przy zmianie stanowiska pracy
9.1.2 Dostęp do sieci i usług sieciowych	X			X	X	X		Instrukcja INF-1/4/4 Bezpieczeństwo sieci
9.2 Zarządzenie dostępem użytkowników								
9.2.1 Rejestrowanie i wyrejestrowywanie użytkowników	X			X	X	X	X	Instrukcje: ISZ-4/2/BF/1 Zarządzanie dostęp do pomieszczeń, ISZ-4/2/BO/1 Zasady postępowania przy zmianie stanowiska pracy, INF-1/5/5 Utrzymanie i kontrola dostępu w systemach informatycznych, Karta użytkownika zasobów informatycznych - stosowanie programu eKarta, Upoważnienie do przetwarzania danych osobowych, podpis użytkownika, Unikalne identyfikatory, konfiguracja, Instrukcja INF-1/5/3 Dobór haseł, autoryzacja AD
9.2.2 Przydzielanie dostępu użytkownikom	X			X	X	X	X	Instrukcje: ISZ-4/2/BF/1 Zarządzanie dostęp do pomieszczeń, ISZ-4/2/BO/1 Zasady postępowania przy zmianie stanowiska pracy, INF-1/5/5 Utrzymanie i kontrola dostępu w systemach informatycznych, Karta użytkownika zasobów informatycznych - stosowanie programu eKarta , Upoważnienie do przetwarzania danych osobowych, podpis użytkownika

Wymagania PN-ISO/IEC 27001:2014-12 Załącznik A Wzorcowy wykaz celów stosowania zabepieczeń i zabezpieczenia	Stosowana kontrola			Wybrane zabezpieczenia i powody stosowania zabezpieczeń				Uwagi (w tym odnoszące się dokumenty, procedury i instrukcje)
	wdrożone	planowane wdrażane	wykluczone	wymagania dot. funkcjon. UM	wymagania prawne	dobre praktyki	wyniki analizy ryzyka	
9.2.3 Zarządzanie prawami uprzywilejowanego dostępu	X			X	X	X	X	Instrukcje: INF-1/4/2 Bezpieczeństwo komputerów przenośnych, INF-1/4/3 Bezpieczeństwo stacji roboczych, INF-1/4/4 Bezpieczeństwo sieci, INF-1/5/3 Dobór haseł, INF-1/5/4 Bezpieczeństwo oprogramowania, ISZ-4/2/BO/1 Zasady postępowania przy zmianie stanowiska pracy - stosowanie programu eKarta, ISZ-4/2/BF/1 Zarządzanie dostępem do pomieszczeń, ISZ-4/2/BF/2 Zasady pracy w strefach, Karta użytkownika zasobów informatycznych, Upoważnienie do przetwarzania danych osobowych
9.2.4 Zarządzanie poufnymi informacjami uwierzytelniającymi	X			X	X	X	X	Instrukcja INF-1/5/3 Dobór haseł, Konfiguracja urządzeń
9.2.5 Przegląd praw dostępu użytkowników	X			X		X	X	Instrukcje: INF-1/5/1 Monitorowanie systemów informatycznych, ISZ-4/2/IT/1 Zasady bezpiecznego korzystania z systemów informatycznych przez użytkowników
9.2.6 Odebranie lub dostosowywanie praw dostępu	X			X	X	X		Instrukcja ISZ-4/2/BO/1 Zasady postępowania przy zmianie stanowiska pracy, karta obiegowa, Polityka bezpieczeństwa ochrony danych osobowych - stosowanie programu eKarta
9.3 Odpowiedzialność użytkowników								
9.3.1 Stosowanie poufnych informacji uwierzytelniających	X			X	X	X	X	Instrukcje: INF-1/5/3 Dobór haseł, ISZ-4/2/IT/1 Zasady bezpiecznego korzystania z systemów informatycznych przez użytkowników
9.4 Kontrola dostępu do systemów i aplikacji								
9.4.1 Ograniczanie dostępu do informacji	X			X	X	X		Procedura PSZ-1/3 Nadzór nad udokumentowaną informacją, Instrukcje: INF-1/4/1 Bezpieczeństwo serwerów, INF-1/4/2 Bezpieczeństwo komputerów przenośnych, INF-1/4/3 Bezpieczeństwo stacji roboczych, Polityka bezpieczeństwa ochrony danych osobowych, Upoważnienie do przetwarzania danych osobowych
9.4.2 Procedury bezpiecznego logowania	X			X	X	X		Konfiguracja dostępu AD, Instrukcja INF-1/5/3 Dobór haseł, Konfiguracja urządzeń, programów i wygaszacza
9.4.3 System zarządzania hasłami	X			X	X	X		Instrukcja INF-1/5/3 Dobór haseł
9.4.4 Użycie uprzywilejowanych programów narzędziowych	X					X		Odebranie praw administracyjnych, karty urządzeń, Instrukcje: INF-1/4/2 Bezpieczeństwo komputerów przenośnych, INF-1/4/3 Bezpieczeństwo stacji roboczych
9.4.5 Kontrola dostępu do kodów źródłowych programów	X					X		Instrukcja INF-1/5/6 Bezpieczeństwo rozwoju oprogramowania, własne - chronione, inne - brak dostępu
10 Kryptografia								
10.1 Zabezpieczenia kryptograficzne								
10.1.1 Polityka stosowania zabezpieczeń kryptograficznych	X			X	X	X		Instrukcja INF-1/6/2 Ochrona kryptograficzna
10.1.2 Zarządzanie kluczami	X			X	X	X		Instrukcja INF-1/6/2 Ochrona kryptograficzna

Wymagania PN-ISO/IEC 27001:2014-12 Załącznik A Wzorcowy wykaz celów stosowania zabepieczeń i zabezpieczenia	Stosowana kontrola			Wybrane zabezpieczenia i powody stosowania zabezpieczeń				Uwagi (w tym odnoszące się dokumenty, procedury i instrukcje)
	wdrożone	planowane wdrażane	wykluczone	wymagania dot. funkcjon. UM	wymagania prawne	dobre praktyki	wyniki analizy ryzyka	
11 Bezpieczeństwo fizyczne i środowiskowe								
11.1 Obszary bezpieczne								
11.1.1 Fizyczna granica obszaru bezpiecznego	X			X		X		Instrukcje: ISZ-4/2/BF/1 Zarządzanie dostępem do pomieszczeń, ISZ-4/2/BF/2 Zasady pracy w strefach, ISZ-4/2/BF/3 Kontrola dostępu przez wykonawców zewnętrznych, Obszary bezpieczne, podział na strefy, drzwi, domofony, elektryczne karty dostępowe
11.1.2 Fizyczne zabezpieczenie wejść	X					X		Instrukcje: ISZ-4/2/BF/1 Zarządzanie dostępem do pomieszczeń, ISZ-4/2/BF/2 Zasady pracy w strefach, ISZ-4/2/BF/3 Kontrola dostępu przez wykonawców zewnętrznych
11.1.3 Zabezpieczenie biur, pomieszczeń i obiektów	X					X		Instrukcje: ISZ-4/2/BF/1 Zarządzanie dostępem do pomieszczeń, ISZ-4/2/BF/2 Zasady pracy w strefach, ISZ-4/2/BF/3 Kontrola dostępu przez wykonawców zewnętrznych
11.1.4 Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi	X					X		Procedura PSZ-3/2 Postępowanie w przypadku nadzwyczajnych zagrożeń i awarii, PSZ-4/3 Zarządzanie ciągłością działania, Plan ciągłości działania,
11.1.5 Praca w obszarach bezpiecznych	X					X		Instrukcje: ISZ-4/2/BF/1 Zarządzanie dostępem do pomieszczeń, ISZ-4/2/BF/2 Zasady pracy w strefach, ISZ-4/2/BF/3 Kontrola dostępu przez wykonawców zewnętrznych
11.1.6 Obszary dostaw i załadunku	X					X		Instrukcje: ISZ-4/2/BF/1 Zarządzanie dostępem do pomieszczeń, ISZ-4/2/BF/2 Zasady pracy w strefach, ISZ-4/2/BF/3 Kontrola dostępu przez wykonawców zewnętrznych
11.2 Sprzęt								
11.2.1 Lokalizacja i ochrona sprzętu	X			X	X	X		Instrukcje: ISZ-4/2/BF/1 Zarządzanie dostępem do pomieszczeń, ISZ-4/2/BF/2 Zasady pracy w strefach, ISZ-4/2/BF/3 Kontrola dostępu przez wykonawców zewnętrznych, INF-1/4/1 Bezpieczeństwo serwerów, INF-1/4/2 Bezpieczeństwo komputerów przenośnych, INF-1/4/3 Bezpieczeństwo stacji roboczych, INF-1/4/4 Bezpieczeństwo sieci
11.2.2 Systemy wspomagające	X			X		X		Zasilanie, UPS, klimatyzacja, Plan ciągłości działania
11.2.3 Bezpieczeństwo okablowania	X			X		X		Przeglądy okablowania, monitorowanie ruchu, Instrukcja INF-1/4/4 Bezpieczeństwo sieci
11.2.4 Konserwacja sprzętu	X			X		X		Instrukcja INF-1/5/2 Przekazywanie urządzeń i nośników do ponownego wykorzystania, zbywania lub wycofania z użycia
11.2.5 Wynoszenie aktywów	X			X		X		Instrukcja INF-1/4/2 Bezpieczeństwo komputerów przenośnych, Regulamin pracy
11.2.6 Bezpieczeństwo sprzętu i aktywów poza siedzibą	X			X		X	X	Instrukcje: INF-1/4/2 Bezpieczeństwo komputerów przenośnych, INF-1/6/3 Przekazanie sprzętu do i z eksploatacji, do i z naprawy
11.2.7 Bezpieczne zbywanie lub przekazywanie do ponownego użycia	X			X		X	X	Instrukcja INF-1/5/2 Przekazywanie urządzeń i nośników do ponownego wykorzystania, zbywania lub wycofania z użycia
11.2.8 Pozostawianie sprzętu użytkownika bez opieki	X			X		X		Instrukcje: ISZ-4/2/IT/1 Zasady bezpiecznego korzystania z systemów informatycznych przez użytkowników, INF-1/5/5 Utrzymanie i kontrola dostępu w systemach informatycznych
11.2.9 Polityka czystego biurka i czystego ekranu	X			X		X		Księga ZSZ, Instrukcja ISZ-4/2/IT/1 Zasady bezpiecznego korzystania z systemów informatycznych przez użytkowników

Wymagania PN-ISO/IEC 27001:2014-12 Załącznik A Wzorcowy wykaz celów stosowania zabepieczeń i zabezpieczenia	Stosowana kontrola			Wybrane zabezpieczenia i powody stosowania zabezpieczeń				Uwagi (w tym odnoszące się dokumenty, procedury i instrukcje)
	wdrożone	planowane wdrażane	wykluczone	wymagania dot. funkcjon. UM	wymagania prawne	dobre praktyki	wyniki analizy ryzyka	
12 Bezpieczna eksploatacja								
12.1 Procedury eksploatacyjne i odpowiedzialność								
12.1.1 Dokumentowanie procedur eksploatacyjnych	X			X	X	X		Instrukcje: INF-1/5/1 Monitorowanie systemów informatycznych, INF-1/5/4 Bezpieczeństwo oprogramowania, ISZ-4/2/BF/2 Zasady pracy w strefach
12.1.2 Zarządzanie zmianami	X			X		X		Instrukcje: INF-1/5/4 Bezpieczeństwo oprogramowania, INF-1/6/3 Przekazanie sprzętu do i z eksploatacji, do i z naprawy, karty urządzeń
12.1.3 Zarządzanie pojemnością	X					X		Umowy z dostawcami, Instrukcje: INF-1/4/1 Bezpieczeństwo serwerów, Instrukcja INF-1/5/1 Monitorowanie systemów informatycznych
12.1.4 Oddzielenie środowisk rozwojowych, testowych i produkcyjnych	X			X		X		Instrukcja INF-1/4/4 Bezpieczeństwo sieci, INF-1/5/6 Bezpieczeństwo rozwoju oprogramowania, zasady zwyczajowo przyjęte
12.2 Ochrona przed szkodliwym oprogramowaniem								
12.2.1 Zabezpieczenia przed szkodliwym oprogramowaniem	X			X	X	X		Instrukcje: INF-1/4/1 Bezpieczeństwo serwerów, INF-1/4/3 Bezpieczeństwo stacji roboczych, INF-1/4/4 Bezpieczeństwo sieci, INF-1/5/4 Bezpieczeństwo oprogramowania
12.3 Kopie zapasowe								
12.3.1 Zapasowe kopie informacji	X			X	X	X	X	Instrukcje INF-1/4/1 Bezpieczeństwo serwerów, INF-1/4/2 Bezpieczeństwo komputerów przenośnych, INF-1/4/3 Bezpieczeństwo stacji roboczych, INF-1/4/4 Bezpieczeństwo sieci, harmonogram backupu, karty urządzeń
12.4 Rejestrowanie zdarzeń i monitorowanie								
12.4.1 Rejestrowanie zdarzeń	X				X	X		Konfiguracja urządzeń, Instrukcje: ISZ-4/2/IT/1 Zasady bezpiecznego korzystania z systemów informatycznych przez użytkowników, INF-1/5/5 Utrzymanie i kontrola dostępu w systemach informatycznych, Instrukcja INF-1/5/1 Monitorowanie systemów informatycznych, Procedura PSZ-1/5 Postępowanie z incydentami, niezgodnościami i działania korygujące
12.4.2 Ochrona informacji w dziennikach zdarzeń	X				X	X		Konfiguracja urządzeń, Instrukcja INF-1/5/1 Monitorowanie systemów informatycznych
12.4.3 Rejestrowanie działań administratorów i operatorów	X				X	X	X	Konfiguracja urządzeń, Instrukcja INF-1/5/1 Monitorowanie systemów informatycznych, ALLOY NAVIGATOR
12.4.4 Synchronizacja zegarów	X				X	X		Synchronizacja urządzeń wzorcem czasu - konfiguracja automatycznej aktualizacji czasu urządzeń
12.5 Nadzór nad oprogramowaniem produkcyjnym								
12.5.1 Instalacja oprogramowania w systemach produkcyjnych	X			X	X	X		Instrukcja INF-1/6/1 Tworzenie i przechowywanie kopii bezpieczeństwa danych, INF-1/5/4 Bezpieczeństwo oprogramowania
12.6 Zarządzanie podatnościami technicznymi								
12.6.1 Zarządzanie podatnościami technicznymi	X			X		X		Instrukcja INF-1/5/1 Monitorowanie systemów informatycznych, WSUS
12.6.2 Ograniczenia w instalowaniu oprogramowania	X			X	X	X	X	Instrukcje INF-1/4/1 Bezpieczeństwo serwerów, INF-1/4/2 Bezpieczeństwo komputerów przenośnych, INF-1/4/3 Bezpieczeństwo stacji roboczych, INF-1/4/4 Bezpieczeństwo sieci, INF-1/4/5 Bezpieczeństwo urządzeń mobilnych

Wymagania PN-ISO/IEC 27001:2014-12 Załącznik A Wzorcowy wykaz celów stosowania zabepieczeń i zabezpieczenia	Stosowana kontrola			Wybrane zabezpieczenia i powody stosowania zabezpieczeń				Uwagi (w tym odnoszące się dokumenty, procedury i instrukcje)
	wdrożone	planowane wdrażane	wykluczone	wymagania dot. funkcjon. UM	wymagania prawne	dobre praktyki	wyniki analizy ryzyka	
12.7 Rozważania dotyczące audytu systemów informacyjnych								
12.7.1 Zabezpieczenia audytu systemów informacyjnych	X			X	X	X		Umowa certyfikacyjna, audyt techniczny
13 Bezpieczeństwo komunikacji								
13.1 Zarządzanie bezpieczeństwem sieci								
13.1.1 Zabezpieczenia sieci	X			X	X		X	Instrukcja INF-1/4/4 Bezpieczeństwo sieci, firewall, router, VLAN
13.1.2 Bezpieczeństwo usług sieciowych	X			X	X		X	INF-14/4/ Bezpieczeństwo sieci, INF INF-1/4/1 Bezpieczeństwo serwerów, ograniczony dostęp do zasobu Internetu, umowy z firmami które są dostawcami dostępu do sieci publicznej.
13.1.3 Rozdzielanie sieci	X			X		X	X	VLAN - stosowanie rozdzielenia sieci na podsieci. Wydzielenie sieci Gość. Schemat sieci LAN/WAN
13.2 Przesyłanie informacji								
13.2.1 Polityki i procedury przesyłania informacji	X			X	X	X		Procedura PSZ-1/3 Nadzór nad udokumentowaną informacją, wytyczne do umów, oprogramowanie antywirusowe, Polityka czystego biurka i ekranu, Księga ZSZ, Regulamin pracy, Raporty z audytów technicznych, AV, Instrukcje: INF-1/4/2 Bezpieczeństwo komputerów przenośnych, INF-1/5/2 Przekazanie urządzeń i nośników do ponownego wykorzystania, zbywania lub wycofania z użycia, INF-1/6/2 Ochrona kryptograficzna, INF-1/6/3 Przekazanie sprzętu do i z eksploatacji, do i naprawy, szkolenia pracowników
13.2.2 Porozumienia dotyczące przesyłania informacji	X			X	X			Instrukcja INF-1/6/2 Ochrona kryptograficzna, Polityki bezpieczeństwa ochrony danych osobowych
13.2.3 Wiadomości elektroniczne	X			X	X			Instrukcja INF-1/6/2 Ochrona kryptograficzna, PSZ-1/3 Nadzór nad udokumentowaną informacją, podpis elektroniczny, ESP, strona www, BIP, komunikatory i sieci społecznościowe
13.2.4 Umowy o zachowaniu poufności	X			X	X	X		Regulamin pracy, Upoważnienie do przetwarzania danych osobowych
14 Pozyskiwanie, rozwój i utrzymanie systemów								
14.1 Wymagania związane z bezpieczeństwem systemów informacyjnych								
14.1.1 Analiza i specyfikacja wymagań bezpieczeństwa informacji	X			X		X		INF-1/2 Zakupy sprzętu komputerowego i akcesoriów, materiałów eksploatacyjnych do drukarek, oprogramowania, usług, Procedury i Instrukcje w procesie PSZ-4 Nadzorowanie funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji
14.1.2 Zabezpieczanie usług aplikacyjnych w sieciach publicznych	X			X	X			Instrukcja INF-1/4/4 Bezpieczeństwo sieci, Zarządzenie PM dot. BIP i publikowania materiałów
14.1.3 Ochrona transakcji usług aplikacyjnych	X			X	X			Bank, Przelewy (Wydział FK) - umowa z bankiem, SSL strona banku, Program MSWiA, CEPiK, Źródło, portal finansowy - chronione zgodnie z wytycznymi ochrony tych aplikacji

Wymagania PN-ISO/IEC 27001:2014-12 Załącznik A Wzorcowy wykaz celów stosowania zabepieczeń i zabezpieczenia	Stosowana kontrola			Wybrane zabezpieczenia i powody stosowania zabezpieczeń				Uwagi (w tym odnoszące się dokumenty, procedury i instrukcje)
	wdrożone	planowane wdrażane	wykluczone	wymagania dot. funkcjon. UM	wymagania prawne	dobre praktyki	wyniki analizy ryzyka	
14.2 Bezpieczeństwo w procesach rozwoju i wsparcia								
14.2.1 Polityka bezpieczeństwa prac rozwojowych	X			X		X		Instrukcja INF-1/5/6 Bezpieczeństwo rozwoju oprogramowania, INF-1/4/7 Bezpieczeństwo projektów informatycznych
14.2.2 Procedury kontroli zmian w systemach	X			X		X		INF-1/5/5 Utrzymanie i kontrola dostępu w systemach informatycznych
14.2.3 Przegląd techniczny aplikacji po zmianach w platformie produkcyjnej	X			X		X		Instrukcja INF-1/5/5 Utrzymanie i kontrola dostępu w systemach informatycznych, karty urządzeń
14.2.4 Ograniczenia dotyczące zmian w pakietach oprogramowania	X			X	X	X		Instrukcje INF-1/4/1 bezpieczeństwo serwerów, INF-1/4/2 bezpieczeństwo komputerów przenośnych, INF-1/4/3 bezpieczeństwo stacji roboczych, INF-1/5/4 bezpieczeństwo oprogramowania, utrzymyweanie elektronicznynego zbioru kart programów dopuszczonych
14.2.5 Zasady projektowania bezpiecznych systemów	X			X		X		Instrukcja INF-1/5/6 Bezpieczeństwo rozwoju oprogramowania, IINF-1/4/7 bezpieczeństwo projektów informatycznych
14.2.6 Bezpieczne środowisko rozwojowe	X			X		X		Instrukcja INF-1/5/6 Bezpieczeństwo rozwoju oprogramowania, IINF-1/4/7 bezpieczeństwo projektów informatycznych
14.2.7 Prace rozwojowe zlecane podmiotom zewnętrznym	X			X		X		Umowy ze stroną trzecią, wytyczne do umów
14.2.8 Testowanie bezpieczeństwa systemów	X			X	X	X		Instrukcja INF-1/5/6 Bezpieczeństwo rozwoju oprogramowania
14.2.9 Testy akceptacyjne systemów	X				X	X		Przekazanie do używania wyposażenia, Instrukcje: INF-1/4/1 Bezpieczeństwo serwerów, INF-1/5/4 Bezpieczeństwo oprogramowania, INF-1/5/6 Bezpieczeństwo rozwoju oprogramowania, INF-1/6/3 Przekazanie sprzętu do i z eksploatacji, do i z naprawy, Umowy ze stroną trzecią
14.3 Dane testowe								
14.3.1 Ochrona danych testowych	X					X		Instrukcja INF-1/6/1 Tworzenie i przechowywanie kopii bezpieczeństwa danych, chroniona jak każda inna baza, wytyczne do umów, przegląd umów
15 Relacje z dostawcami								
15.1 Bezpieczeństwo informacji w relacjach z dostawcami								
15.1.1 Polityka bezpieczeństwa informacji w relacjach z dostawcami	X			X	X	X		Klauzula w umowach o współpracy, wytyczne do umów
15.1.2 Uwzględnianie bezpieczeństwa w porozumieniach z dostawcami	X			X	X	X		Klauzula w umowach o współpracy, wytyczne do umów
15.1.3 Łańcuch dostaw technologii informacyjnych i telekomunikacyjnych	X			X	X	X		Klauzula w umowach o współpracy, wytyczne do umów
15.2 Zarządzanie usługami świadczonymi przez dostawców								
15.2.1 Monitorowanie i przegląd usług świadczonych przez dostawców	X			X		X		Protokół odbioru, karta urządzenia
15.2.2 Zarządzenie zmianami w usługach świadczonych przez dostawców	X			X		X		Umowy SLA, Protokół odbioru, karta urządzenia

Wymagania PN-ISO/IEC 27001:2014-12 Załącznik A Wzorcowy wykaz celów stosowania zabepieczeń i zabezpieczenia	Stosowana kontrola			Wybrane zabezpieczenia i powody stosowania zabezpieczeń				Uwagi (w tym odnoszące się dokumenty, procedury i instrukcje)
	wdrożone	planowane wdrażane	wykluczone	wymagania dot. funkcjon. UM	wymagania prawne	dobre praktyki	wyniki analizy ryzyka	
16 Zarządzanie incydentami związanymi z bezpieczeństwem informacji								
16.1 Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami								
16.1.1 Odpowiedzialność i procedury	X			X		X		Procedura PSZ-1/5 Postępowanie z incydentami, niezgodnościami i działania korygujące
16.1.2 Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji	X			X		X		Procedura PSZ-1/5 Postępowanie z incydentami, niezgodnościami i działania korygujące
16.1.3 Zgłaszanie słabości związanych z bezpieczeństwem informacji	X			X		X		Procedura PSZ-1/5 Postępowanie z incydentami, niezgodnościami i działania korygujące
16.1.4 Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji	X			X		X		Procedura PSZ-1/5 Postępowanie z incydentami, niezgodnościami i działania korygujące
16.1.5 Reagowanie na incydenty związane z bezpieczeństwem informacji	X			X		X		Procedura PSZ-1/5 Postępowanie z incydentami, niezgodnościami i działania korygujące
16.1.6 Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji	X			X		X		Procedura PSZ-1/5 Postępowanie z incydentami, niezgodnościami i działania korygujące
16.1.7 Gromadzenie materiału dowodowego	X			X		X		Procedura PSZ-1/5 Postępowanie z incydentami, niezgodnościami i działania korygujące
17 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania								
17.1 Ciągłość bezpieczeństwia informacji								
17.1.1 Planowanie ciągłości bezpieczeństwa informacji	X			X				Procedury: PSZ-4/1 Analiza ryzyka bezpieczeństwa informacji, PSZ-4/3 Zarządzanie ciągłością działania
17.1.2 Wdrożanie ciągłości bezpieczeństwa informacji	X			X				Procedura PSZ-4/3 Zarządzanie ciągłością działania, Scenariusze awaryjne w Planie ciągłości działania
17.1.3 Weryfikowanie, przegląd i ocena ciągłości bezpieczeństwa informacji	X			X				Procedura PSZ-4/3 Zarządzanie ciągłością działania
17.2 Nadmiarowość								
17.2.1 Dostępność środków przetwarzania informacji	X			X		X		Zapewnienie dostępności zosobów fizycznych, Scenariusze awaryjne w Planie ciągłości działania
18 Zgodność								
18.1 Zgodność z wymaganiami prawnymi i umownymi								
18.1.1 Określenie stosownych wymagań prawnych i umownych	X			X	X			Ustawy, rozporządzenia, uchwały, zarządzenia
18.1.2 Prawa własności intelektualnej	X			X	X			Ustawa o prawie autorskim i prawach pokrewnych
18.1.3 Ochrona zapisów	X				X			Procedura PSZ-1/3 Nadzór nad udokumentowaną informacją
18.1.4 Prywatność i ochrona danych identyfikujących osobę	X				X			Polityka bezpieczeństwa ochrony danych osobowych, Upoważnienie do przetwarzania danych osobowych
18.1.5 Regulacje dotyczące zabezpieczeń kryptograficznych	X			X	X	X		Instrukcja INF-1/6/2 Ochrona kryptograficzna

Wymagania PN-ISO/IEC 27001:2014-12 Załącznik A Wzorcowy wykaz celów stosowania zabepieczeń i zabezpieczenia	Stosowana kontrola			Wybrane zabezpieczenia i powody stosowania zabezpieczeń				Uwagi (w tym odnoszące się dokumenty, procedury i instrukcje)
	wdrożone	planowane wdrażane	wykluczone	wymagania dot. funkcjon. UM	wymagania prawne	dobre praktyki	wyniki analizy ryzyka	
18.2 Przeglądy bezpieczeństwa informacji								
18.2.1 Niezależny przegląd bezpieczeństwa informacji	X				X			Raport z audytu certyfikacyjnego, Raporty z audytów technicznych, klauzule w umowach ze stroną trzecią
18.2.2 Zgodność z politykami bezpieczeństwa i standardami	X			X	X			Audit wewnętrzny w zakresie bezpieczeństwa
18.2.3 Sprawdzanie zgodności technicznej	X			X		X		Audyt techniczny

Bielsko-Biała, dnia 21 czerwca 2018 r.
wersja 7

Zatwierdzam:

Z. up. Prezydenta Miasta
Waldemar Jędrusiński
Zastępca Prezydenta