

Rejestr wymagań prawnych i innych
dot. Systemu Zarządzania Bezpieczeństwem Informacji

L.p.	Wymaganie prawne i inne
1.	Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r. (Dz.U. z 1997, nr 78, poz. 483)
2.	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1 z dnia 4 maja 2016 r.)
3.	Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781 t.j.)
4.	Ustawa z dnia 6 września 2001r. o dostępie do informacji publicznej (Dz.U. z 2022 r. poz. 902 t.j.).
5.	Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. z 2019 r. poz. 730)
6.	Ustawa z dnia 5 września 2016 o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2021 r. poz. 1797 t.j.)
7.	Ustawa z dnia 17 lutego 2005 o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2021 r. poz. 2070 t.j.)
8.	Ustawa z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (Dz.U. z 2022 r. poz. 2240 t.j.)
9.	Ustawa z dnia 5 lipca 20218 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2022 r. poz. 1863)
10.	Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów Publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r. poz. 2247, t.j.)
11.	Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 (Monitor Polski 2019 r. poz. 1037)
12.	Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (Monitor Polski 2019 r. poz. 666)
13.	Zarządzenie nr ON.120.34.2021.PSZ Prezydenta Miasta Bielska-Białej z dnia 23 lutego 2021 r. w sprawie organizacji Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Bielsku-Białej (Manager Bezpieczeństwa)
14.	Zarządzenie nr ON.120.48.2020.ABI Prezydenta Miasta Bielska-Białej z dnia 29 maja 2020 r. w sprawie wyznaczenia Inspektora ochrony danych w Urzędzie Miejskim w Bielsku-Białej (zmienione zarządzeniem nr ON.120.140.2021.IOD Prezydenta Miasta Bielska-Białej z dnia 16 grudnia 2021 r.)
15.	Zarządzenie Nr ON.120.51.2022.IOD Prezydenta Miasta Bielska-Białej z dnia 25 maja 2022 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych Urzędu Miejskiego w Bielsku-Białej
16.	Zarządzenie Nr ON.120.105.2020.IOD Prezydenta Miasta Bielska-Białej z dnia 4 listopada 2020 r. w sprawie wprowadzenia „Regulaminu pracy zdalnej dla pracowników Urzędu Miejskiego w Bielsku-Białej (zmienione zarządzeniem nr ON.120.106.2020.IOD Prezydenta Miasta Bielska-Białej z dnia 6 listopada 2020 r.)
17.	Polska Norma PN-ISO/IEC 27001:2017-06 Technika Informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania (W dn. 25.10.2022 Międzynarodowa Organizacja Normalizacyjna opublikowała nowe wydanie standardu ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Wytyczne dotyczące okresu przejścia znajdują się w dokumencie IAF MD 26:2022 Międzynarodowego Forum Akredytacji (IAF). Zgodnie, z terminami określonymi w ww. dokumencie począwszy od publikacji ISO/IEC 27001:2022: certyfikowane Organizacje mają 36 miesięcy na dokonanie przejścia na nowe wydanie normy. Termin liczony jest od ostatniego dnia miesiąca publikacji ISO/IEC 27001:2022 czyli od 31.10.2022.)
18.	Norma PN-EN ISO/IEC 27002:2017-06 Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zabezpieczania informacji
19.	Norma ISO/IEC 27005:2018 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji
20.	PSZ-1 nadzorowanie i doskonalenie Zintegrowanego Systemu Zarządzania PSZ-1/5 Postępowanie z incydentami, niezgodnościami i działania korygujące Instrukcja ISZ-1/5/1 Instrukcja ISZ-1/5/1 Postępowanie z incydentami związanymi z bezpieczeństwem informacji, cyberbezpieczeństwem oraz naruszeniami ochrony danych osobowych w Urzędzie Miejskim w Bielsku-Białej

L.p.	Wymaganie prawne i inne
	<p>PSZ-4 Nadzorowanie funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji</p> <p>PSZ-4/1 Analiza ryzyka bezpieczeństwa informacji</p> <p>PSZ-4/2/IT Utrzymanie i monitorowanie obszarów bezpieczeństwa informacji – obszar bezpieczeństwa informatycznego</p> <p>Instrukcja ISZ-4/2/IT/1 Zasady bezpiecznego korzystania z systemów informatycznych przez użytkowników</p> <p>PSZ-4/2/BO Utrzymanie i monitorowanie obszarów bezpieczeństwa informacji – obszar bezpieczeństwa osobowego</p> <p>Instrukcja ISZ-4/2/BO/1 Zasady postępowania przy zmianie stanowiska pracy</p> <p>PSZ-4/2/BF Utrzymanie i monitorowanie obszarów bezpieczeństwa informacji – obszar bezpieczeństwa fizycznego</p> <p>Instrukcja ISZ-4/2/BF/1 Zarządzanie dostępem do pomieszczeń</p> <p>Instrukcja ISZ-4/2/BF/2 Zasady pracy w strefach</p> <p>Instrukcja ISZ-4/2/BF/3 Kontrola dostępu przez wykonawców zewnętrznych</p> <p>PSZ-4/3 Zarządzanie ciągłością działania</p> <p>Plan Ciągłości Działania</p>

Data aktualizacji: 7 listopada 2022 r.

Biuro ds. Systemu Zarządzania