I. Obowiązki i uprawnienia Właściciela biznesowego Systemu informatycznego (WBSI)

1. Do obowiązków WBSI należy:
   1) koordynowanie przygotowania wymagań funkcjonalnych SI oraz ich zatwierdzanie,
   2) nadzorowanie zapewnienia poprawności i kompletności danych wprowadzanych do SI,
   3) ustalenie i zapewnienie posiadania procedur nadawania uprawnień w SI skutkujących posiadaniem ewidencji uprawnień w postaci informacji takich jak: imię i nazwisko Użytkownika, datę nadania i odebrania oraz zakres uprawnień, nazwę jednostki Uczelni, identyfikator Użytkownika,
   4) zapewnienie rejestracji w ramach SI wszystkich czynności skutkujących zmianą lub podjętą decyzją w ramach obsługiwanego procesu biznesowego,
   5) przeprowadzanie lub koordynacja i nadzór nad kontrolą uprawnień do SI nie rzadziej niż co pół roku,
   6) występowanie o środki niezbędne do zapewnienia prawidłowego utrzymania i rozwoju SI, w tym zapewniające odpowiedni poziom Bezpieczeństwa Informacji na podstawie potrzeb oraz opinii pozyskanych od ABSI/ATSI w ramach obowiązującej procedury budżetowej,
   7) ocena i rekomendacja działań w zakresie efektywności biznesowej utrzymywania i rozwoju SI oraz potrzeb z tym związanych,
   8) podejmowanie niezwłocznych i odpowiednich działań w przypadku naruszeń Bezpieczeństwa Informacji oraz współpraca celem ich wyjaśniania i obsługi.
   9) nadzór nad realizacją obowiązków WBSI wynikających z ZBI delegowanych na podległych Pracowników,
   10) współpraca z innymi Kierownikami jednostek w zakresie określania zasad użytkowania SI / kontroli nadawania uprawnień oraz pozyskiwania wymagań funkcjonalnych.

2. WBSI ma prawo do:
   1) określania zakresu i sposobu wykorzystania przetwarzanych Danych w SI,
   2) podejmowania decyzji o zakresie wykorzystania SI przez inne Jednostki,
   3) akceptowania lub odrzucania wniosków o udzielenie dostępu do SI,
   4) zgłaszania potrzeb w zakresie innych SI wspierających działanie własnego SI,
   5) nakładanie na Użytkowników SI obowiązków, w szczególności odnośnie sposobu obsługi SI oraz zgłaszania naruszeń Bezpieczeństwa Informacji,
   6) delegowania obowiązków lub uprawnień wynikających z ZBI na podległych Pracowników lub na Kierowników jednostek wykorzystujących SI do wsparcia swoich procesów biznesowych w zakresie objętym ZBI,
   7) uczestnictwa w procesie zawierania umowy o powierzenie przetwarzania danych osobowych podmiotowi trzeciemu oraz do nadzorowania realizacji tej umowy.

8) pozyskania informacji w zakresie zgodności SI z regulacjami zewnętrznymi SI poprzez zwrócenie się do ABSI i/lub ATSI celem uzyskania opinii w zakresie za jaki odpowiadają oraz dokonania własnej oceny w tym zakresie.
9) udziału w ocenie ryzyka związanego z przetwarzaniem Danych w ramach swojego SI.

II. Obowiązki i uprawnienia Administratora Biznesowego SI (ABSI)

1. Do obowiązków ABSI należy:
   1) zapewnienie prawidłowego funkcjonowania SI w obszarze funkcjonalnym SI wraz z jego interfejsami,
   2) zapewnienie poprawności merytorycznej przetwarzania Danych przez SI,
   3) zapewnienie identyfikowania ewentualnych zakłóceń oraz identyfikowanie ryzyk mających wpływ na Bezpieczeństwo Informacji w obszarze funkcjonalnym, przetwarzanych w ramach SI oraz zapewnienie powiadamiania o naruszeniach,
   4) udział w opiniowaniu zmian w ramach SI w obszarze funkcjonalnym,
   5) nadzór nad prawidłową współpracą z dostawcami SI w zakresie obowiązujących umów serwisowych i wdrożeniowych,
   6) zapewnienie odpowiednich zasobów do rozwiązywania problemów związanych z funkcjonalnościami SI,
   7) zapewnienie zasobów do utrzymywania i opiniowania dokumentacji funkcjonalnej oraz aktualizacja instrukcji użytkowania funkcjonalności SI,
   8) zapewnienie zasobów do opracowywania wymagań funkcjonalnych w zakresie utrzymania i rozwoju SI,
   9) prowadzenie analiz oraz projektowania architektury przetwarzania oraz przepływu Danych w ramach SI,
   10) monitorowanie prawidłowości funkcjonowania SI,
   11) współpraca z WBSI w zakresie rozwiązywania incydentów Bezpieczeństwa Informacji w obszarze funkcjonalnym,
   12) określanie niezbędnych wymagań organizacyjnych, jakie muszą być zapewnione podczas użytkowania SI z uwzględnieniem wymaganego poziomu Bezpieczeństwa Informacji,
   13) ustalanie i nadzór nad realizacją polityki jakości Danych przetwarzanych w ramach SI oraz zapewnienie realizacji testów jakości tych Danych,
   14) w porozumieniu z WBSI / ATSI, dokonywanie okresowej analizy ryzyk związanych z wykorzystaniem SI, w tym także analizy adekwatności zastosowanych w SI środków Bezpieczeństwa Informacji oraz inicjowanie działań zmierzających do utrzymywania tego ryzyka na akceptowalnym poziomie.
   15) zapewnienie administracji biznesowej SI, parametryzacja oraz planowanie zmian, wdrażanie i modyfikacja funkcjonalności biznesowych SI,
   16) zatwierdzanie i zlecanie uzgodnionych z WBSI modyfikacji funkcjonalnych SI do ATSI,
   17) organizacja testowania funkcjonalności SI oraz współpraca z dostawcami SI (obiór i akceptacja) w zakresie dostarczania poprawek funkcjonalnych,

18) nadawanie, odbieranie, modyfikowanie, profilowanie, standaryzacja uprawnień w SI lub nadzorowanie tego procesu zgodnie z obowiązującą procedurą nadawania uprawnień w ramach SI oraz zapewnienie kontroli dostępu Użytkowników,
19) konfiguracja funkcjonalna oraz parametryzacja SI zgodnie z potrzebami i celami biznesowymi,
20) współpraca z WBSI w zakresie realizowanych kontroli uprawnień w ramach SI,
21) zapewnienie szkoleń dla Użytkowników w całym okresie życia SI zgodnie z wymaganiami SI w celu jego prawidłowej obsługi,
22) współpraca z WBSI w zakresie realizacji okresowych ocen ryzyka związanych z eksploatacją SI w tym w zakresie zgodności z obowiązującym przepisami,
23) zapewnienie realizacji przygotowywania raportów z SI,
24) zapewnienie prawidłowego procesu zasilania i przepływu Danych w ramach SI oraz jego interfejsów,
25) zapewnienie obsługa zgłoszeń błędów przez Użytkowników SI,
26) zapewnienie obsługa rozliczeń związanych z utrzymaniem SI, wsparcie WBSI przy budżetowaniu kosztów i nakładów niezbędnych do utrzymania i rozwoju SI,
27) zapewnienie by dziennik eksploatacji SI był prowadzony sumiennie.

2. ABSI ma prawo do:
   1) wnioskowania o wprowadzenie zmian w SI związanych ze zidentyfikowanymi zagrożeniami dla prawidłowego funkcjonalnymi, brakiem zgodności SI z obowiązującymi przepisami,
   2) wnioskowania o modyfikację regulacji wewnętrznych dotyczących zarządzania SI,
   3) delegowania obowiązków ABSI na Pracowników, odpowiedzialnych za dany obszar funkcjonalny działania SI (np. zasilanie, nadawanie uprawnień, raportowanie, analityka biznesowa, zgodność z przepisami itd.).

III. Obowiązki i uprawnienia Administratora Technicznego SI (ATSI)

1. Do obowiązków ATSI należy:
   1) zapewnienie prawidłowego funkcjonowania SI w obszarze technicznym wraz z jego interfejsami,
   1) zapewnienie identyfikowania ewentualnych zakłóceń oraz identyfikowanie ryzyk mających wpływ na Bezpieczeństwo Informacji w obszarze teleinformatycznym, przetwarzanych w ramach SI oraz zapewnienie powiadamiania o naruszeniach,
   2) udział w opiniowaniu zmian w ramach SI w obszarze technicznym,
   3) udział w prowadzonych analizach związanych z ryzykiem technicznym w ramach SI,
   4) zapewnienie prawidłowego wdrażania zleconych modyfikacji SI,
   5) nadzór nad prawidłową współpracą z dostawcami SI w zakresie obowiązujących umów serwisowych i wdrożeniowych,
   6) zapewnienie odpowiednich zasobów do rozwiązywania problemów technicznych oraz aktualizacja elementów SI,

7) organizacja skutecznego nadzorowania Osób zewnętrznych w zakresie wykonywanych prac technicznych w ramach SI,
8) zapewnienie zasobów do utrzymywania i opiniowania dokumentacji technicznej oraz aktualizacji Kart Technicznych SI,
9) zapewnienie zasobów do opracowywania wymagań technicznych w zakresie utrzymania i rozwoju SI,
10) prowadzenie analiz oraz projektowania architektury teleinformatycznej SI,
11) monitorowanie dostępności usług informatycznych SI,
12) współpraca z WBSI w zakresie rozwiązywania incydentów Bezpieczeństwa Informacji w obszarze teleinformatycznym,
13) określanie niezbędnych wymagań bezpieczeństwa teleinformatycznego, jakie muszą być zapewnione podczas eksploatacji SI z uwzględnieniem wymaganego poziomu Bezpieczeństwa Informacji,
14) ustalanie i nadzór nad realizacją polityki wykonywania kopii bezpieczeństwa SI oraz zapewnienie realizacji testów ich odtwarzania oraz testów UCB,
15) w porozumieniu z WBSI / ABSI, dokonywanie okresowej analizy ryzyk związanych z wykorzystaniem SI, w tym także analizy adekwatności zastosowanych w SI środków Bezpieczeństwa Informacji oraz inicjowanie działań zmierzających do utrzymywania tego ryzyka na akceptowalnym poziomie.

2. ATSI ma prawo do:
1) wnioskowania o wprowadzenie zmian w SI związanych z Bezpieczeństwem Informacji oraz ze zidentyfikowanymi zagrożeniami dla prawidłowego funkcjonowania SI,
1) wnioskowania o modyfikację regulacji wewnętrznych dotyczących zarządzania SI,
2) delegowania obowiązków ATSI na Pracowników podwładnych, odpowiedzialnych za dany obszar techniczny działania SI (np. baza danych, aplikacja, separacja sieciowa, storage, system operacyjny itd.).

IV. Obowiązki i uprawnienia Właściciela InT (WInT)

1. Do obowiązków WInT należy:
1) zapewnienie dostępności i pojemności usług InT niezbędnych do prawidłowego funkcjonowania SI oraz zapewniały wymagane parametry dostępności w tym RPO i RTO,
2) optymalizacja zasobów realizujących usługi InT,
3) opiniowanie umów uwzględniających przetwarzanie Danych przez podmioty zewnętrze celem zapewnienie im właściwej ochrony,
4) zapewnienie realizacji uzgodnionych planów ciągłości działania z WBSI/ATSI w obszarze zapewnienia odpowiedniego poziomu dostępności i wydajności InT,
5) zapewnienie zarządzania uprawnieniami Użytkowników uprzywilejowanych administrujących elementami InT,

6) zapewnienie możliwości nadzoru nad działaniami Użytkowników w ramach SI oraz Użytkowników uprzywilejowanych w ramach administracji technicznej InT,
7) zapewnienie prawidłowej realizacji procesu kontroli uprawnień w ramach Użytkowników uprzywilejowanych w ramach InT,
8) opiniowanie zmian oraz udział w procesie podejmowania decyzji w zakresie utrzymywania i rozwoju InT,
9) zapewnienie utrzymywania wymaganej dokumentacji technicznej dla InT oraz jej aktualizacji,
10) zapewnienie utrzymywania wymaganej dokumentacji technicznej dla InT oraz jej aktualizacji,
11) zapewnienia logowania na poziomie technicznym umożliwiającym identyfikację czynności przez danego Pracownika administrującego elementami InT,
12) zapewnienie informowania WBSI/ABSI o planach oraz działaniach mających wpływ na funkcjonowania SI poza uzgodnionymi poziomami usług InT oraz realizacji istotnych z jego punktu widzenia SI projektów związanych z InT,
13) zapewnienie by Pracownicy zajmujący się obszarem bezpieczeństwa teleinformatycznego mogli realizować swoje obowiązki w sposób niezależny od czynności realizowanych przez Pracowników zajmujących się administracją techniczną elementami InT oraz by realizowane przez nich kontrole uprawnień i/lub kontrole / testowanie zabezpieczeń w zakresie bezpieczeństwa teleinformatycznego InT prowadzone były w sposób niezależny od subiektywnej oceny stanu bezpieczeństwa teleinformatycznego pozostałych Pracowników,
14) zapewnienie monitorowania i wykrywanie nieprawidłowości, zakłócenia dostępności kluczowych elementów InT,
15) zapewnienie utrzymywania stałego procesu monitorowanie zagrożeń i podatności elementów InT, reagowania adekwatnie do zidentyfikowanego poziomu ryzyka oraz regularnie dokonywać przeglądu zidentyfikowanych ryzyka, które mają negatywny wpływ na Bezpieczeństwo Informacji,
16) zapewnienie planowania i realizacji planów audytów w obszarze InT zgodnie z obowiązującymi regulacjami oraz realizacji formalnego procesu działań następczych, w tym terminowej weryfikacji działań naprawczych w odniesieniu do najważniejszych ustaleń w wyniku realizacji tych audytów.
17) zapewnienie identyfikacji potencjalnych podatności w ramach InT, które należy oceniać i naprawiać poprzez zapewnienie aktualizacji oprogramowania i oprogramowania firmware, włączając w to oprogramowanie zapewniane przez instytucje finansowe użytkownikom wewnętrznym i zewnętrznym, poprzez wprowadzanie krytycznych poprawek zabezpieczeń oraz poprzez wdrażanie kompensacyjnych środków kontroli,
18) zapewnienie standaryzacji konfiguracji bezpieczeństwa dla wszystkich elementów InT w obszarze sieciowym,
19) zapewnienie odpowiedniej segmentacji sieci i elementów SI oraz zapobiegania utracie Danych,

20) zapewnienie odpowiednio do klasyfikacji Danych odpowiedniego poziomu ich szyfrowania zarówno podczas przetwarzania, przesyłania jak i przechowywania,
21) zapewnienie ochrony punktów końcowych, w tym Sprzętu komputerowego oraz stosowania adekwatnych mechanizmów ochrony do zidentyfikowanego ryzyka,
22) zapewnienie mechanizmów służących weryfikowaniu integralności oprogramowania, oprogramowania firmware i danych,
23) zapewnienie realizacji formalnego procesu zarządzania zmianą, który powinien zapewnić odpowiednie planowanie, testowanie, dokumentowanie, zatwierdzanie i wdrażanie zmian w zakresie InT,
24) zapewnienie prowadzenia aktualnych spisów elementów InT (w tym Sprzętu komputerowego, urządzeń sieciowych, baz danych itp.). Spis elementów InT powinien zawierać ich konfigurację oraz powiązania i wzajemne zależności między innymi elementami InT, aby umożliwić właściwą konfigurację i proces zarządzania zmianą.
25) zapewnienie by procedury tworzenia kopii zapasowych i przywracania danych oraz SI były zoptymalizowane pod kątem zapewnienia ich możliwie szybkiego odtworzenia i były one testowane okresowo,
26) podejmowanie odpowiednich środków przewidzianych umowami w przypadku stwierdzenia niedociągnięć w zakresie realizowanych czynności zleconych w ramach umów outsourcingowych.

2. WInT ma prawo do:
    1) realizacji zmian w ramach InT, które nie wpływają negatywnie na SI,
    2) opiniowanie i wnioskowanie zmian w ramach regulacji wewnętrznych opisujących współpracę z obszarem biznesowym w tym z WBSI/ABSI,
    3) zgłaszanie inicjatyw oraz potrzeb związanych z optymalizacją, utrzymaniem i rozwojem InT mających wpływ na SI,
    4) uczestniczenie w procesie planowania strategii oraz oceny ryzyka związanego z utrzymaniem i rozwojem SI oraz InT.