I. Wstęp

Mając świadomość znaczenia wartości informacji dla realizacji celów Centrum Rehabilitacji Rolników KRUS w Iwoniczu-Zdroju, został wdrożony, jest utrzymywany i cyklicznie doskonalony system Zarządzania bezpieczeństwem informacji stanowiący integralną część Zintegrowanego Systemu Zarządzania. System bezpieczeństwa informacji jest zgodny z wymaganiami normy ISO/IEC 27001:2023-08 .
Najwyższe kierownictwo zobowiązuje się do spełnienia wymagań dotyczących bezpieczeństwa informacji mających zastosowanie w funkcjonującym ZSZ oraz zobowiązuje się do zapewniania zasobów niezbędnych do funkcjonowania systemu i jego ciągłego doskonalenia.
Skróty :
ZBI- Zarządzanie bezpieczeństwem Informacji
Centrum – Centrum Rehabilitacji Rolników KRUS w Iwoniczu-Zdroju
ZSZ- Zintegrowany System Zarządzania

II. Zakres systemu ZBI.

1. System zarządzania bezpieczeństwem informacji obejmuje swoim zakresem usługi związane ze udzielaniem świadczeń zdrowotnych czyli wypełnianiem statutowych zadań Centrum, opisanych w Księdze ZSZ.
2. Bezpieczeństwo informacji rozumiane jest jako zabezpieczenie przed nieautoryzowanym dostępem, naruszeniem integralności informacji oraz ograniczeniem dostępu do zasobów biorących udział w przetwarzaniu informacji lub ich utratą. Środki stosowane do ochrony zasobów oraz zakres ochrony są odpowiednio dobrane do zakresu przetwarzanych informacji i danych.
3. Bezpieczeństwo i ochrona danych osobowych, która stanowi podstawową i integralną część bezpieczeństwa informacji została opisana w następujących dokumentach :
   a. „Polityka bezpieczeństwa w zakresie ochrony danych osobowych”
   b. „Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych”.

III. Główne cele ZBI.

1. Zabezpieczenie informacji niezależnie od jej postaci, przed utratą, uszkodzeniem, zniszczeniem, kradzież, nieuprawnioną modyfikacją lub niepożądanym udostępnieniem osobom nieuprawnionym.
2. Zagwarantowanie poufności, integralności i dostępności przetwarzanych informacji.
3. Zapewnienie bezpieczeństwa świadczonych usług.
4. Wdrożenie skutecznych technologii informatycznych w celu ochrony informacji.
5. Nadzór nad udokumentowana informacją

6. Identyfikacja i minimalizowanie ryzyka utraty bezpieczeństwa informacji i utrzymanie go w możliwie najniższym, akceptowalnym poziomie oraz ograniczenie skutków utraty bezpieczeństwa informacji.
7. Zaangażowanie wszystkich pracowników w ochronę informacji oraz stałe podnoszenie ich świadomości.

IV. Zasady ZBI

1. Określenie najważniejszych zagrożeń dla bezpieczeństwa informacji w Centrum odbywa się na podstawie analizy ryzyka przeprowadzanej przez Zespół ds. bezpieczeństwa informacji zgodnie z obowiązującą ZBI-01 Procedura zarządzania ryzykiem utraty bezpieczeństwa informacji oraz według ZBI-03 Metodyką analizy ryzyka utraty bezpieczeństwa informacji.
2. Zarządzanie bezpieczeństwem informacji ma charakter proaktywny i zapewnia utrzymanie optymalnych poziomów bezpieczeństwa informacji we wszystkich obszarach funkcjonowania Centrum objętych zakresem funkcjonowania procesu ZBI, poprzez stosowanie zabezpieczeń, zasad oraz procedur. Cele stosowania zabezpieczeń i zabezpieczenia wykorzystane w procesie ZBI zostały zawarte w dokumencie : KS-01-1 Deklaracja stosowania.
3. Wobec obszarów wysokiego ryzyka prowadzone są działania zapobiegawcze w celu wyeliminowania możliwości występowania niepożądanych zdarzeń lub złagodzenia ich ewentualnych skutków. Obszary akceptowalnego ryzyka w celu zapobieżenia jego wzrostowi są stale monitorowane i nadzorowane.
4. Dla osiągnięcia i zachowania akceptowalnych poziomów ryzyka są przeprowadzane audyty wewnętrzne ZSZ i przeglądy bezpieczeństwa oraz mierzona jest skuteczność stosowanych zabezpieczeń zgodnie z Instrukcją pomiaru skuteczności zabezpieczeń i sporządzany jest odpowiedni protokół.
5. Celem tych działań jest potwierdzenie zgodności procesu ZBI z przyjętą Polityką ZSZ, jak również zapewnienie, że procedury są realizowane, a ryzyka są regularnie identyfikowane i właściwie zarządzane.
6. Szczegółowe metody postępowania z informacjami zawarte są w dokumentacji ZSZ.
7. Zasady dotyczące bezpieczeństwa informacji przetwarzanych w systemach informatycznych (w tym między innymi zasady logowania do systemów informatycznych, tworzenie kopii zapasowych, ochrona antywirusowa, aktualizacje oprogramowania, nadawanie uprawnień) zostały szczegółowo opisane w „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych”, która opisuje sposób postępowania ze wszystkimi informacjami, a w szczególności w odniesieniu do danych osobowych.

V. Struktura systemu ZBI i odpowiedzialności.

1. Osobą odpowiedzialną za procesy zabezpieczenia i ochrony informacji jest Dyrektor Centrum, który zapewnia odpowiednie zasoby wymagane do utrzymywania i doskonalenia procesu ZBI.
2. W celu skutecznego funkcjonowania procesu ZBI powołano Zespół ds. bezpieczeństwa informacji, który odpowiada za :

- identyfikowanie ryzyk związanych z bezpieczeństwem informacji,
- przeprowadzanie wspólnie z Pełnomocnikiem ds. ZSZ systematycznej analizy i oceny ryzyka bezpieczeństwa informacji, w tym opracowywanie planów postępowania z ryzykiem,
- zapewnianie, że zadania związane z bezpieczeństwem informacji są realizowane zgodnie z obowiązującą polityką bezpieczeństwa informacji,
- identyfikowanie zagrożeń i stopni narażenia informacji lub środków służących do przetwarzania informacji na zagrożenia,
- szacowanie adekwatności wdrożonych zabezpieczeń,
- koordynowanie wdrażania zabezpieczeń,
- promowanie w Centrum kształcenia, szkolenia i uświadamiania w zakresie bezpieczeństwa informacji.

3. Odpowiedzialność za sieć i systemy informatyczne przypisano Administratorowi Sieci/Systemów informatycznych.
4. System ZBI jest zintegrowany z innymi systemami zarządzania wdrożonymi w Centrum w ramach Zintegrowanego Systemu Zarządzania. Za skuteczną i efektywną integrację systemów odpowiada Pełnomocnik ds. ZSZ.
5. Szczegółowe zakresy odpowiedzialności i uprawnień w ZSZ zostały opisane w „Księdze jakości ZSZ" oraz w „Polityce bezpieczeństwa w zakresie ochrony danych osobowych".

VI. Świadomość.

1. Każdy pracownik Centrum jest odpowiednio przeszkolony i posiada odpowiednią wiedzę w zakresie ochrony informacji.
2. Świadomość bezpieczeństwa informacji jest stale podnoszona i promowana w celu ujawnienia wszelkich zagrożeń i podatności oraz motywowania wszystkich pracowników do działań mających na celu ciągła poprawę poziomu bezpieczeństwa informacji.
3. Wszyscy pracownicy zobowiązani są do aktywnego udziału w utrzymywaniu i doskonaleniu ZSZ w tym ZBI oraz stosowania przyjętych zasad postępowania.

VII. Dokumenty powiązane

PN-EN ISO/IEC 27001:2023-08 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności. Systemy zarządzania bezpieczeństwem informacji. Wymagania. Załącznik A –Wzorcowy wykaz zabezpieczeń informacji.
KS-01 Księga ZSZ
KS-01-1 – Deklaracja stosowania
„Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych".
„Polityka bezpieczeństwa w zakresie ochrony danych osobowych".