Spis treści:

Opracował: **Specjalista ds. Informatycznych** **Andrzej Zgódka**	**Lider procesu:** **inż. Piotr Pawłowicz**	**Sprawdził pod względem merytorycznym:** **mgr Milena Witczak**
Data: 10.09.2019	Data: 12.09.2019	Data: 13.09.2019
Podpis: Azgódka	Podpis: KOORDYNATOR DS. SYSTEMÓW INFORMATYCZNYCH Centrum Onkologii-Instytutu im. Marii Skłodowskiej-Curie Piotr Pawłowicz	Podpis:
Weryfikował: Kierownik DSZ **Małgorzata Hołówek**	Data: 16.09.2019	Podpis:
Zatwierdził: **Dyrektor Centrum Onkologii** **prof. dr hab. n. med.** **Jan Walewski**	Data: 2019 WRZ. 16	Podpis: z up. DYREKTORA Centrum Onkologii-Instytutu im. Marii Skłodowskiej-Curie Zastępca Dyrektora ds. Klinicznych prof. dr hab. n. med. Andrzej Kawecki
EGZEMPLARZ ☐ Rejestrowany Nr_____ (podlega aktualizacji) ☒ Informacyjny (nie podlega aktualizacji)		

1. Cel instrukcji

Określenie czytelnych i zrozumiałych zasad zapewnienia bezpieczeństwa systemów informatycznych Centrum Onkologii w Warszawie.

2. Przedmiot instrukcji

2.1 Instrukcja bezpieczeństwa systemów IT określa obszary organizacyjne i techniczne służące zapewnieniu bezpieczeństwa systemów informatycznych użytkowanych w COI.

2.2 Obejmuje wszystkich pracowników i współpracowników COI.

3. Zakres instrukcji

Instrukcja bezpieczeństwa systemów IT określa zasady i wymogi bezpiecznego korzystania z zasobów informatycznych Centrum Onkologii w Warszawie oraz podmiotów współpracujących przez pracowników COI i szeroki krąg współpracowników COI.

4. Opis postępowania

W celu zapewnienia bezpieczeństwa zasobów informatycznych Centrum Onkologii w Warszawie należy:

a. stosować zasadę minimalnych uprawień

W ramach przydzielania uprawień do system informatycznych należy przyznać minimum praw dostępu do danych i funkcjonalności umożlwiających wykonywanie obowiązków na danym stanowisku pracy.

b. stosować zasadę wielopoziomowych zabezpieczeń

W ramach stosowanych rozwiązań informatycznych systemy informatyczne COI powinny być chronione równolegle na wielu poziomach.

c. stosować zasadę domyślnego brak dostępu

Domyślnymi uprawnieniami w systemach informatycznych powinno być zabronienie dostępu. Dopiero w przypadku zaistnienia odpowiedniej potrzeby, administrator przyznaje stosowne uprawnienia, adekwatne do wyznaczonych zdań dla pracownika.

d. stosować zasadę gromadzenia istotnych danych informatycznych na serwerach i macierzach dyskowych

Istotne dla COI dane informatyczne są gromadzone na serwerach i macierzach dyskowych, czyli urządzeniach zapewniających: większą odporność na uszkodzenie pojedynczego dysku twardego niż na zwykłych komputerach, lepszą kontrolę dostępu do danych (autoryzacja), dokładniejszy zapisy kto miał dostęp do danych.

e. stosować trudne do złamania hasła oraz regularnie je zmieniać

f. stosować co najmniej podstawowe zabezpieczenia stacji roboczych (komputerów) pracowników

g. stosować monitoring bezpieczeństwa infrastruktury informatycznej

h. prowadzić działania zmierzające do podniesienia świadomości zagrożeń informatycznych oraz sposobów zapobiegania im.

i. stosować zaawansowane zabezpieczenia serwerów i macierzy dyskowej oraz regularne wykonywać kopie bezpieczeństwa zgromadzonych na nich zasobów,

j. stosować zasadę zablokowania dostępu do kont po wygaśnięciu umów o zatrudnienie/współpracę.

W celu spełnienia wyżej wymienionych wymogów wprowadza się szczegółowe regulaminy korzystania z kluczowych usług i dostępów:

Zadanie	Opis	Zapis
4.1	Zapewnienie bezpiecznego korzystania z dostępu do Internetu	Regulamin korzystania z dostępu do Internetu
4.2	Zapewnienie bezpiecznego korzystania z dostępu do sieci lokalnej	Regulamin korzystania z dostępu do sieci lokalnej
4.3	Zapewnienie bezpiecznego korzystania z dostępu poprzez VPN	Regulamin korzystania z usługi dostępu VPN
4.4	Zapewnienie bezpiecznego korzystania z dostępu do medycznych i naukowych baz danych	Regulamin korzystania z dostępu do medycznych i naukowych baz danych
4.5	Zasady bezpieczeństwa informacji medycznej	Zasady bezpieczeństwa informacji medycznej (regulamin)
4.6	Zasady zabezpieczenia danych w trakcie napraw serwisowych sprzętu w serwisie zewnętrznym lub przez serwisantów z firm zewnętrznych w siedzibie COI	Wytyczne w zakresie napraw sprzętu w serwisie zewnętrznym lub z udziałem serwisu zewnętrznego (regulamin)
4.7	Zasady obowiązujące przy nadawaniu uprawnień do przetwarzania danych	Wytyczne w zakresie nadawania uprawnień do przetwarzania danych (regulamin)
4.8	Wytyczne w zakresie metod i środków uwierzytelnienia (polityka haseł)	Wytyczne w zakresie metod i środków uwierzytelnienia (polityka haseł) (regulamin)
4.9	Wytyczne w zakresie niszczenia danych i ich nośników	Wytyczne w zakresie niszczenia danych i ich nośników (regulamin)

Integralną częścią niniejszej instrukcji są następujące opisy:

1. Opis systemu zabezpieczeń informatycznych w Centrum Onkologii w Warszawie.

Załączniki:

1. PR60.5_P1_IR2_Z1 Regulamin korzystania z dostępu do Internetu
2. PR60.5_P1_IR2_Z2 Regulamin korzystania z dostępu do sieci lokalnej
3. PR60.5_P1_IR2_Z3 Regulamin korzystania z usługi dostępu VPN
4. PR60.5_P1_IR2_Z4 Regulamin korzystania z dostępu do medycznych i naukowych baz danych

5. PR60.5_P1_IR2_Z5 Zasady bezpieczeństwa informacji medycznej (regulamin)
6. PR60.5_P1_IR2_Z6 Opis systemu zabezpieczeń informatycznych w Centrum Onkologii w Warszawie
7. PR60.5_P1_IR2_Z7 Wytyczne w zakresie napraw sprzętu w serwisie zewnętrznym lub z udziałem serwisu zewnętrznego (regulamin).
8. PR60.5_P1_IR2_Z8 Wytyczne w zakresie nadawania uprawnień do przetwarzania danych (regulamin)
9. PR60.5_P1_IR2_Z9 Wytyczne w zakresie metod i środków uwierzytelnienia (polityka haseł) (regulamin)
10. PR60.5_P1_IR2_Z10 Wytyczne w zakresie niszczenia danych i ich nośników (regulamin).