Zasady Akceptowalnego Użytkowania dla Przyjmującego zamówienie na podstawie umowy cywilno – prawnej w Centrum Onkologii

1. CEL DOKUMENTU

Celem niniejszej załącznika do umowy cywilno – prawnej jest określenie zasad dotyczących bezpiecznego i odpowiedzialnego korzystania z aktywów informatycznych Centrum Onkologii im. prof. F. Łukaszczyk w Bydgoszczy (zwanego dalej Centrum), w tym laptopów, systemów informacyjnych zawierających dane medyczne oraz infrastruktury IT.

2. WYMAGANIA SZCZEGÓŁOWE

2.1 Dozwolone użytkowanie

Przyjmujący zamówienie może korzystać z aktywów informatycznych wyłącznie do celów służbowych związanych z działalnością Centrum. Przyjmujący zamówienie jest zobowiązany do:

- Korzystania z danych medycznych wyłącznie w celu leczenia pacjentów i zgodnie z obecnymi przepisami prawa.
- Używania zasobów technicznych, w tym laptopów i systemów informatycznych, tylko w sposób zgodny z wewnętrznymi przepisami Centrum.

Przyjmujący zamówienie ma prawo:

- Do zaimportowania do zasobów udostępnionych mu przez Centrum certyfikatu ZUS w okresie obowiązywania umowy. Certyfikat będący własnością Przyjmującego zamówienie powinien zostać usunięty z zasobów informatycznych w chwili rozwiązania umowy.

2.2 Zabronione działania

Zabrania się Przyjmującemu zamówienie:

- Udostępniania kart kryptograficznych oraz kodów PIN do nich osobom trzecim.
- Ujawniania lub przekazywania danych dostępowych do systemów informatycznych innym osobom.
- Używania służbowego konta e-mail w celach prywatnych.
- Przechowywania danych medycznych na zewnętrznych nośnikach bez zgody przełożonych.
- Modyfikacji konfiguracji, w tym zabezpieczeń oraz instalowania na służbowych komputerach oprogramowania bez autoryzacji działu IT.

2.3 Logowanie i zabezpieczenia dostępu

Przyjmujący zamówienie powinien:

- Korzystać z kart kryptograficznych do logowania do systemów Centrum. Karty te są osobiste i nie mogą być udostępniane do użytkowania innym osobom.
- Przechowywać karty kryptograficzne w bezpiecznym miejscu i chronić je przed kradzieżą lub zgubieniem.
- Używać haseł do logowania się do systemów Centrum spełniających następujące kryteria:
    - Co najmniej 12 znaków,
    - Zawierających co najmniej jedną wielką literę, cyfrę oraz znak specjalny.
- Regularnie zmieniać hasła zgodnie z polityką haseł Centrum

- Niezwłocznie zmienić hasło dostępowe do systemu Centrum, jeśli zaistniało podejrzenie ujawnienia danych dostępowych do tego systemu.
- Unikać zapamiętywania haseł w przeglądarkach internetowych.
- Stosować zasadę jedno hasło – jedno konto i bezwzględnie unikać używania haseł wykorzystywanych w celach służbowych do kont prywatnych.

2.4 E-mail służbowy

Służbowe konto e-mail jest przeznaczone wyłącznie do celów związanych z pracą w Centrum. Przyjmujący zamówienie powinien:

- Korzystać z e-maila wyłącznie do komunikacji związanej z działalnością zawodową.
- Unikać otwierania podejrzanych maili, z nieznanych źródeł, które mogą stanowić potencjalne zagrożenie dla bezpieczeństwa systemu Centrum.
- Odpowiednio dbać o zabezpieczenie poczty e-mail hasłem spełniającym kryteria opisane w pkt 2.3 niniejszego załącznika.

2.5 Ochrona danych i klasyfikacja informacji

Przyjmujący zamówienie ma obowiązek przestrzegać zasad obejmujących klasyfikację informacji zgodnie z dokumentami wewnętrznymi Centrum. Wszystkie dane medyczne są klasyfikowane jako informacje szczególnie chronione i muszą być zabezpieczone w sposób adekwatny do ich wrażliwości. Należy:

- Przechowywać dane pacjentów wyłącznie w zatwierdzonych systemach medycznych Centrum
- Nie przesyłać danych medycznych poza zatwierdzone systemy komunikacyjne Centrum a wszelkie inne dane przed ich przesłaniem zabezpieczyć zgodnie z obowiązującym w Centrum dokumentem tworzenia bezpiecznego archiwum danych.
- Bezwzględnie unikać przesyłania i przechowywania wszelkich danych w publicznych zasobach chmurowych.

2.6 Poufność i dostęp do danych

- Przyjmujący zamówienie zobowiązany jest do regularnego uczestniczenia w szkoleniach wewnętrznych organizowanych w Centrum w tym z zakresu ochrony danych.
- Przyjmujący zamówienie zobowiązany jest do przestrzegania zapisów podpisanej umowy o zachowaniu poufności, dotyczącej danych pacjentów i informacji służbowych.
- Dostęp do zasobów informatycznych oraz systemów zawierających dane pacjentów przyznawany jest Przyjmującemu zamówienie wyłącznie na czas trwania umowy i w zakresie niezbędnym do wykonywania jego obowiązków.

2.7 Monitoring

Centrum zastrzega sobie prawo do monitorowania korzystania z aktywów informatycznych, w celu zapewnienia zgodności z niniejszym załącznikiem oraz obowiązującymi w Centrum Politykami Bezpieczeństwa.

2.8 Zgłaszanie incydentów

Każde podejrzenie naruszenia bezpieczeństwa, w tym ujawnienie używanego hasła, utraty karty kryptograficznej lub innych aktywów (np. nośnik zewnętrzny, laptop lub inne będące własnością Centrum), należy niezwłocznie zgłosić do Działu Zarządzania i Informatyzacji.

2.9 Praca zdalna

W przypadku wystąpienia konieczności pracy zdalnej, Przyjmujący zamówienie zobowiązany jest przestrzegać następujących zasad w celu zapewnienia bezpieczeństwa danych oraz aktywów informatycznych:

1. **Bezpieczne połączenie**:
    - W celu realizacji pracy zdalnej Przyjmujący zamówienie korzysta wyłącznie z zasobów informatycznych udostępnionych przez Centrum, wyposażonych w odpowiednio skonfigurowane oprogramowanie, w tym połączenie VPN, które zapewnia bezpieczny dostęp do systemów informatycznych.
    - Niedozwolone jest korzystanie z prywatnych urządzeń do uzyskiwania dostępu do systemów informatycznych Centrum.
2. **Ochrona sprzętu i danych**:
    - Przyjmujący zamówienie ponosi pełną odpowiedzialność za bezpieczeństwo zasobów, które na potrzeby realizacji pracy zdalnej zostały mu udostępnione oraz innych zasobów informatycznych, z których korzysta podczas pracy zdalnej. Sprzęt musi być zawsze przechowywany w bezpiecznym miejscu, aby zapobiec jego kradzieży lub uszkodzeniu.
    - Zabronione jest pozostawianie sprzętu bez nadzoru w miejscach publicznych lub łatwo dostępnych dla osób trzecich.
    - Zabronione jest modyfikowanie konfiguracji, instalowanie oprogramowania oraz wyłączanie zabezpieczeń zainstalowanych na udostępnionym urządzeniu.
3. **Bezpieczeństwo danych**:
    - Podczas pracy zdalnej Przyjmujący zamówienie zobowiązany jest dbać o poufność danych medycznych, zgodnie z obowiązującymi przepisami prawa oraz klasyfikacją informacji w Centrum.
    - Przyjmujący zamówienie zobowiązany jest do pracy w bezpiecznym otoczeniu, unikając dostępu osób postronnych do ekranu laptopa lub materiałów zawierających dane wrażliwe.
4. **Zasady dotyczące haseł i kart kryptograficznych**:
    - Podczas pracy zdalnej obowiązują te same zasady dotyczące ochrony haseł oraz kart kryptograficznych. Przyjmujący zamówienie zobowiązany jest upewnić się, że nikt inny nie ma dostępu do ich danych logowania ani kart kryptograficznych, które służą do autoryzacji w systemach Centrum.
5. **Zgłaszanie incydentów**:
    - W przypadku utraty sprzętu, naruszenia bezpieczeństwa danych lub podejrzenia incydentu, Przyjmujący zamówienie zobowiązany jest niezwłocznie zgłosić ten fakt Kierownikowi Działu Zarządzania i Informatyzacji lub zgłosić incydent zawierający opis i datę zdarzenia na adres e-mail: cyberincydent@co.bydgoszcz.pl

2.10 Rozliczenie w przypadku rozwiązania lub wygaśnięcia umowy

W przypadku rozwiązania umowy, niezależnie od powodu, lub jej wygaśnięcia, Przyjmujący zamówienie jest zobowiązany do przestrzegania następujących zasad dotyczących zwrotu aktywów i zarządzania danymi:

1. **Zwrot aktywów:**
    - Przyjmujący zamówienie jest zobowiązany do niezwłocznego zwrotu wszystkich aktywów przekazanych mu przez Centrum, w tym:
        - Urządzeń komputerowych wraz z komponentami,
        - Karty kryptograficznej,
        - Nośników danych (pendrive'ów, dysków zewnętrznych itp.),
        - Innych urządzeń lub zasobów przekazanych na czas trwania umowy.
    - Zwrot aktywów musi nastąpić najpóźniej w dniu rozwiązania lub wygaśnięcia umowy, o ile strony nie ustalą inaczej.
2. **Postępowanie z danymi:**
    - Przyjmujący zamówienie jest zobowiązany do zabezpieczenia i przekazania wszystkich danych zgromadzonych na użytkowanych zasobach, np. z urządzeń komputerowych i nośników danych, które stanowią własność Centrum.
    - Centrum przeprowadzi proces bezpiecznego usunięcia wszystkich danych z nośników zwróconych przez Przyjmującego zamówienie, zgodnie z wewnętrznymi procedurami, bez możliwości ich odzyskania.
    - Przyjmujący zamówienie zrzeka się wszelkich roszczeń związanych z usunięciem wszystkich danych, które pozostały na urządzeniach po ich zwrocie, w tym np. plików, , dokumentów, zdjęć, prezentacji itp. Centrum nie ponosi odpowiedzialności za jakiekolwiek dane, które zostaną usunięte w ramach procedur bezpiecznego usunięcia informacji oraz przygotowania sprzętu do ponownego użytku.
3. **Postępowanie z kontem i usunięcie uprawnień:**
    - Z dniem rozwiązania lub wygaśnięcia umowy, wszystkie konta Przyjmującego zamówienie w systemach Centrum zostają niezwłocznie dezaktywowane.
    - Konta użytkowników nie są fizycznie usuwane, lecz pozostają dezaktywowane, aby zapewnić możliwość weryfikacji i ewentualnego audytu działań użytkownika, zgodnie z zasadami zachowania rozliczalności.
    - Wszystkie uprawnienia dostępu do systemów Centrum zostają usunięte z chwilą zakończenia umowy.

2.11 Konsekwencje naruszeń

Przyjmujący zamówienie pozostaje odpowiedzialny za bezpieczeństwo i integralność przekazanego przez Centrum sprzętu oraz danych od chwili ich otrzymania do momentu formalnego zwrotu i dezaktywacji konta.

Naruszenie zasad określonych w niniejszej polityce może skutkować:

- Natychmiastowym cofnięciem dostępu do systemów informatycznych Centrum,
- Sankcjami zgodnymi z zawartą umową cywilno – prawną,
- Sankcjami wynikającymi z przepisów prawa,
- Zgłoszeniem incydentu do odpowiednich organów prawnych.