

	Edycja	5
	Strona/ stron	1 z 5
<b>ZAŁĄCZNIK NR 2 DO POLITYKI BEZPIECZEŃSTWA INFORMACJI</b>	Data edycji załącznika	10.10.2024

## INFORMATOR BEZPIECZEŃSTWA INFORMACJI

(zbiór zasad regulujących działania innych niż *Pracownicy* podmiotów/osób uzyskującym dostęp do *Zasobów informacyjnych UCK*)

### § 1

#### Podstawowe obowiązki podmiotu zewnętrznego

1. Każda osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, uzyskująca dostęp do *Zasobów informacyjnych UCK* oraz środków ich przetwarzania na podstawie umów, porozumień lub innych stosunków prawnych, a zwłaszcza współpracujący z UCK *Podmiot zewnętrzny*, zobowiązany jest do przestrzegania określonych w niniejszym dokumencie zasad.
2. Obowiązek, o którym mowa w ust. 1, dotyczy zarówno przypadków przetwarzania *Informacji* na terenie UCK, jak i poza jego siedzibą, w tym zdalnego dostępu do *Systemu teleinformatycznego UCK* lub przetwarzanych w nim danych. Nie ma przy tym znaczenia czy urządzenia, na których się to odbywa, są prywatne czy powierzone przez UCK.
3. W przypadku *Systemów informacyjnych* udostępnianych pacjentom – informacje o *Zagrożeniach* związanych z *Cyberbezpieczeństwem* są opublikowane na stronie internetowej pod adresem <https://uck.pl/nasz-szpital/bezpieczenstwo-informacji/podstawowe-informacje.html>.
4. Wszystkie udostępnione *Zasoby informacje UCK*, w tym *Informacje wrażliwe* i środki służące do ich przetwarzania, będące własnością UCK lub przez niego wykorzystywane, podlegają ochronie. O zakresie i zasadach tej ochrony UCK informuje przy ich udostępnianiu do używania – w przekazanej instrukcji lub informacji umieszczonej przy urządzeniu, zawartej umowie, regulaminie korzystania lub opublikowanej na stronie internetowej [uck.gda.pl](https://uck.gda.pl).
5. Do *Informacji wrażliwych* w UCK zalicza się, w szczególności:
  - a) *Dane osobowe* i *Informacje* zawierające *Tajemnicę skarbową, bankową*,
  - b) dokumentację techniczną *Systemów teleinformatycznych*, systemów *Zabezpieczeń fizycznych i logicznych*, w tym kody źródłowe *Aplikacji* oraz procedury bezpieczeństwa na poziomie technologicznym,
  - c) raporty z *Audytu* i kontroli,
  - d) *Informacje* przekazywane UCK przez *Podmiot zewnętrzny* w wyniku realizacji umowy, o ile *Podmiot zewnętrzny* wskaże konieczność ochrony takich *Informacji* w treści umowy lub w dokumentach odnoszących się do realizacji umowy,
  - e) inne *Informacje*, których udostępnienie osobie nieuprawnionej lub podmiotowi nieuprawnionemu w ocenie *Właściciela zasobu* mogłoby spowodować szkodę dla UCK lub naruszyć prawnie chroniony interes innych osób lub podmiotów.
6. Ochronie podlegają również:
  - a) oprogramowanie i urządzenia służące do przetwarzania ww. *Informacji*,
  - b) pozostałe *Środki przetwarzania informacji*,
7. Osoba/podmiot, o którym mowa w par. 1 ust. 1, zobowiązana/y jest, w szczególności do:

- a) przestrzegania przepisów prawa powszechnie obowiązującego w zakresie *Bezpieczeństwa informacji*, w tym przepisów o ochronie *Danych osobowych* oraz innych *Tajemnic* prawnie chronionych, a także niezbędnych dla realizacji umowy - obowiązujących w UCK - zasad ochrony tych *Informacji*,
  - b) zapewnienia bezpieczeństwa przetwarzanych *Informacji* poprzez ich ochronę przed niepożądanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem, w tym do przeciwdziałania próbom naruszenia ich bezpieczeństwa,
  - c) niepodejmowania działań, które mogłyby prowadzić do naruszenia *Cyberbezpieczeństwa w Systemach informacyjnych* jakie udostępnia UCK,
  - d) zachowania w *Poufności* wszelkich udostępnionych przez UCK *Informacji*, w tym *Informacji wrażliwych*, do których uzyska dostęp w związku z wykonywaniem obowiązków / świadczeniem usług, a zwłaszcza *Danych osobowych* oraz innych *Informacji* prawnie chronionych, a także *Informacji* na temat sposobów ich zabezpieczania. Obowiązek powyższy obejmuje w szczególności:
    - nieujawnianie danych zawartych w eksploatowanych w UCK *Systemach teleinformatycznych*,
    - nieujawnianie szczegółów technologicznych używanych w *Systemach teleinformatycznych* UCK oraz *Informacji* na temat eksploatowanego przez UCK oprogramowania,
    - nieudostępnianie osobom nieuprawnionym *Nośników informacji* zawierających *Informacje wrażliwe*, w tym wydruków komputerowych,
  - e) *Przetwarzania danych* wyłącznie w sposób dopuszczony przez UCK, w tym:
    - niewykorzystywania udostępnionych *Informacji* dla celów innych niż określone w łączącej strony umowie,
    - nietworzenia i nieposiadania jakichkolwiek kopii *Informacji* zawierających *Informacje wrażliwe*, w tym formularzy zawierających *Dane osobowe* lub baz danych zapisanych w postaci dokumentów papierowych lub elektronicznych, a w szczególności w poczcie elektronicznej, na dyskach komputerowych i arkuszach kalkulacyjnych innych niż niezbędne do realizacji łączącej strony umowy,
    - niewynoszenia *Informacji* poza obszar ich przetwarzania (chyba, że inaczej określono w łączącej strony umowie),
  - f) przestrzegania przepisów bhp oraz przepisów bezpieczeństwa przeciwpożarowego,
  - g) zaangażowania w doskonalenie *SZBI* UCK przez zgłaszanie wszelkich nieprawidłowości lub *Zagrożeń* związanych z ochroną *Informacji* lub *Systemów informacyjnych* (w tym np. urządzeń, oprogramowania, sieci)
8. Osoba/podmiot, o którym mowa w par. 1 ust. 1, zobowiązuje się do przeszkolenia swoich *Pracowników* oraz pozostałych osób (np. podwykonawców) realizujących w jego imieniu objęte umową zadania, w zakresie zachowania zasad *Bezpieczeństwa informacji* zawartych w niniejszym dokumencie oraz innych niezbędnych dla realizacji umowy zasad *Bezpieczeństwa informacji*.
9. Osoba/podmiot, o którym mowa w par. 1 ust. 1, zobowiązuje się do nadzorowania swoich *Pracowników* oraz pozostałych osób (np. podwykonawców) realizujących w jego imieniu objęte umową zadania, w zakresie przestrzegania zasad *Bezpieczeństwa informacji*, w tym zabezpieczenia *Aktywów informacyjnych* UCK, do których uzyskał dostęp.

10. Osoba/podmiot, o którym mowa w par. 1 ust. 1, zobowiązuje się, iż niezwłocznie, nie później jednak niż w terminie 14 dni po rozwiązaniu Umowy / zakończeniu świadczenia usług, a także na każde żądanie UCK, o ile nie naruszy to postanowień prawa powszechnie obowiązującego, zwróci lub zniszczy w sposób trwały, uniemożliwiający odczyt, udostępnione uprzednio przez UCK informacje, w tym *Informacje wrażliwe*. Jednocześnie przekaże UCK pisemne oświadczenie, w którym potwierdzi, że nie posiada już żadnych *Informacji*, w tym *Informacji wrażliwych*, do których dostęp uzyskał na podstawie łączącej strony umowy. Zwrot lub zniszczenie nastąpi według wyboru UCK. W przypadku braku oświadczenia ze strony UCK, osoba/podmiot, o którym mowa w par. 1 ust. 1, zwróci się zapytaniem do UCK czy dane winny być zwrócone czy trwale zniszczone.

## § 2

### Bezpieczeństwo fizyczne i środowiskowe

1. UCK objęło ochroną teren, budynki oraz pomieszczenia należące do UCK (*Obszar bezpieczny*).
2. W ramach *Obszaru bezpiecznego* wydzielone zostały trzy *Strefy bezpieczeństwa* (I, II, III), w których obowiązują indywidualne reguły bezpieczeństwa, a także w ich ramach wyodrębniony został *Obszar przetwarzania danych osobowych*. W ramach strefy II wyodrębniona została również strefa obsługi klienta.
3. Dostęp do poszczególnych pomieszczeń należących do *Obszaru bezpiecznego* uzależniony jest od poziomu uprawnień związanych z wykonywanymi obowiązkami.
4. W objętych ochroną pomieszczeniach należących do strefy II, osoby nieuprawnione do przetwarzania *Informacji* nie mogą zostać pozostawione bez nadzoru osoby uprawnionej. Dostęp personelu technicznego zajmującego się konserwacją sprzętu, partnerów handlowych, pacjentów oraz innych osób do ww. pomieszczeń, w tym zwłaszcza sekretariatów i innych pomieszczeń administracyjnych, dyżurek lekarskich i pielęgniarskich, gabinetów zabiegowych, a także magazynów i biur, powinien być nadzorowany przez *Pracowników UCK*.
5. Dostęp do pomieszczeń należących do strefy I mają wyłącznie określone osoby, w tym osoby uprawnione do tego dostępu w związku z wykonywaniem czynności związanych z przechowywaniem i zabezpieczeniem przetwarzanych w tych pomieszczeniach *Informacji*.
6. *Informacje* winny być przetwarzane wyłącznie w przeznaczonych do tego pomieszczeniach, w warunkach zabezpieczających je przed dostępem do nich osób nieuprawnionych.
7. Zabrania się opuszczania obszaru przetwarzania *Informacji* bez jego odpowiedniego zabezpieczenia oraz bez odpowiedniego zabezpieczenia znajdujących się w nim *Informacji* i środków służących do ich przetwarzania.
8. Wszyscy *Pracownicy* osób/podmiotów, o których mowa w par. 1 ust. 1, winni nosić na terenie UCK identyfikatory w widocznym miejscu.
9. Ciągi komunikacyjne obiektów są zaopatrzone w tabliczki informujące o kierunku ewakuacji i w miarę potrzeby wyposażone w oświetlenie awaryjne. Zgodnie z przepisami prawa opracowane są Instrukcje Bezpieczeństwa Pożarowego.

## § 3

### Postępowanie z incydentami

1. Osoba/podmiot, o którym mowa w par. 1 ust. 1, ma obowiązek informowania o wystąpieniu *Incydentu związanego z bezpieczeństwem informacji* oraz o wszelkich zidentyfikowanych słabościach SZBI / *Zdarzeniach związanych z bezpieczeństwem informacji*.
2. O *Incydencie* należy niezwłocznie poinformować Pełnomocnika Dyrektora Naczelnego ds. Systemu Zarządzania Bezpieczeństwa Informacji (Pełnomocnika DN ds. SZNI), a w przypadku jego nieobecności niezwłocznie powiadomić Dyrektora Naczelnego.

3. O innych zdarzeniach należy poinformować właściwą *Komórkę organizacyjną* UCK ustalonymi źródłami komunikacji *Zintegrowanego Systemu Zarządzania (ZSZ)* lub zgodnie z postanowieniami umownymi.
4. Za naruszenie *Bezpieczeństwa informacji* uważa się, w szczególności:
  - a) naruszenie lub próbę naruszenia *Integralności Systemu informacyjnego* przeznaczonego do *Przetwarzania informacji*,
  - b) naruszenie lub próbę naruszenia *Integralności Informacji* w systemie przeznaczonym do ich przetwarzania – wszelkie modyfikacje (dodanie, zmiana, usunięcie), zniszczenie lub próby ich dokonania przez osoby nieuprawnione lub uprawnione działające w złej wierze lub jako błąd osoby uprawnionej (np. zmiana zawartości danych, utrata całości lub części danych),
  - c) naruszenie *Poufności* poprzez celowe lub nieświadome przekazanie *Informacji* osobie nieuprawnionej do ich otrzymania,
  - d) naruszenie ochrony *Informacji* w systemie (np. nieautoryzowane logowanie do systemu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu z zewnątrz),
  - e) nieuprawniony dostęp lub próba dostępu do pomieszczeń, gdzie przetwarza się *Informacje*,
  - f) ujawnienie indywidualnych *Haseł Użytkowników* do systemu przetwarzającego *Informacje*,
  - g) wykonanie nieuprawnionych kopii *Informacji* lub innego przetwarzania, które wykracza poza dozwolony zakres lub odbywa się niezgodnie z określonymi przez UCK zasadami,
  - h) zmianę lub usunięcie *Informacji* zapisanych na *Kopiach bezpieczeństwa* lub *Kopiach archiwalnych*,
  - i) zamierzoną lub niezamierzoną utratę *Poufności* danych poprzez utratę sprzętu mobilnego, klucza do podpisu elektronicznego, *Kopii bezpieczeństwa*, *Nośnika informacji* lub innego składnika *Systemu teleinformatycznego* UCK (w tym na skutek kradzieży),
  - j) zamierzoną lub niezamierzoną utratę *Dostępności Informacji*, w tym np. utratę *Nośnika informacji* (np. na skutek kradzieży/zgubienia wydruku, *Kopii bezpieczeństwa*, komputerowego sprzętu przenośnego czy wymiennego *Nośnika informacji*, takiego jak np. dyskietki czy dysku), a także brak dostępu uprawnionych osób do *Informacji*, do których dostęp winien być zapewniony,
  - k) niewłaściwe niszczenie *Nośników informacji* (np. wydruków, pamięci zewnętrznych, płyt CD),
  - l) pozbawienie *Informacji* lub *Systemów informacyjnych* ich *Autentyczności* (przerabianie, podrabianie, posługiwanie się danymi identyfikującymi innej osoby do przetwarzania *Informacji* lub w celu uzyskania dostępu do *Systemów informacyjnych*).

#### § 4

##### **Obowiązek informacyjny, prawo kontroli**

1. Osoba/podmiot, o którym mowa w par. 1 ust. 1, zobowiązuje się do niezwłocznego udzielenia UCK, na każde jego żądanie, *Informacji* na temat przetwarzania udostępnionych do przetwarzania *Informacji wrażliwych*, w tym na temat zastosowanych przy przetwarzaniu środków technicznych i organizacyjnych. Udzielenie *Informacji* nastąpi w sposób wybrany przez UCK – w formie pisemnej lub ustnej.
2. Osoba/podmiot, o którym mowa w par. 1 ust. 1, umożliwi UCK lub podmiotowi przez niego upoważnionemu dokonywanie kontroli zgodności przetwarzania udostępnionych do przetwarzania *Informacji wrażliwych* zgodnie z wymaganiami prawa, umową oraz regulacjami *Systemu Zarządzania Bezpieczeństwem Informacji* – w miejscach, w których są one przetwarzane. Pisemne zawiadomienie

o zamiarze przeprowadzenia kontroli powinno być przekazane osobie/podmiotowi, o którym mowa w par. 1 ust. 1, co najmniej na 3 dni kalendarzowe przed dniem rozpoczęcia kontroli.

3. Osoba/podmiot, o którym mowa w par. 1 ust. 1, umożliwi UCK lub podmiotowi przez niego upoważnionemu dokonanie kontroli, o której mowa w ust. 2, w trybie niezwłocznym, bez konieczności przedstawienia zawiadomienia, o którym mowa w ust. 2, w przypadku wystąpienia *Incydentu* związanego z naruszeniem przepisów prawa powszechnie obowiązującego, umowy oraz regulacji *Systemu Zarządzania Bezpieczeństwem Informacji*.
4. Osoba/podmiot, o którym mowa w par. 1 ust. 1, zobowiązany jest zastosować się do zaleceń UCK, dotyczących poprawy jakości zabezpieczenia udostępnionych do przetwarzania *Informacji*, w tym *Informacji wrażliwych* oraz sposobu ich przetwarzania, wynikających z przeprowadzonych kontroli.

## § 5

### Postanowienia końcowe

Naruszenie świadome bądź przypadkowe przez osobę/podmiot, o którym mowa w par. 1 ust. 1, przepisów prawa powszechnie obowiązującego i/lub innych postanowień, do których przestrzegania się zobowiązał, stanowi podstawę do wypowiedzenia przez UCK bez zachowania okresu wypowiedzenia i żądania pokrycia powstałej szkody lub zapłaty kary umownej, jeżeli taki obowiązek wynika z zawartej umowy.