

# Wizja V sp. z o.o.



## BI-03-SZBI PROCEDURA SYSTEMOWA SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Wersja  
**1.0.**

Data wydania:  
**2024-03-04**

### POLITYKA CIĄGŁOŚCI DZIAŁANIA

Strona:

**1 / 6**

Opracował: Michał Mrówka	Data:	Podpis:
Sprawił: Marta Nowacka	Data:	Podpis:
Zatwierdził: Monika Nogala	Data:	Podpis:
Obowiązuje od dnia: 04.03.2024 r.		

## I. CEL PROCEDURY

Celem wprowadzenia w WizjaV Systemu Zarządzania Ciągłością Działania, jest zapewnienie o nieprzerwalności w realizacji zadań statutowych w sposób uporządkowany - w tym usług kluczowych – na wypadek wystąpienia nagłych zdarzeń lub nieszczęśliwych wypadków.

System Zarządzania Ciągłością Działania, ma na celu minimalizację zakłóceń w realizacji działalności statutowej oraz określenie planu postępowania w przypadku zaistnienia zdarzeń mających wpływ (również potencjalny) na bezpieczeństwo informacji oraz ciągłości działania WizjaV.

## II. PRZEDMIOT I ZAKRES PRCEODURY

Na System Zarządzania ciągłością działania, składają się:

- Polityka Ciągłości Działania;
- Plany ciągłości działania.

## III. TERMINOLOGIA I DEFINICJE

Pojęcie	Definicja
<b>Bezpieczeństwo informacji</b>	zachowanie poufności, integralności i dostępności informacji; dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
<b>Centralny Zespół ds. Reagowania na Incydenty (CZRI)</b>	wewnętrzna struktura odpowiedzialna za cyberbezpieczeństwo w WizjaV powołana odrębnym Zarządzeniem Dyrektora WizjaV;
<b>Ciągłość działania</b>	zdolność WizjaV do ciągłego świadczenia usług w akceptowalnych ramach czasowych przy zdefiniowanej wcześniej zdolności do działania w czasie zakłócenia;
<b>Naruszenie bezpieczeństwa informacji</b>	przypadek, w którym użytkownik lub inna osoba pomija lub niszczy ustanowione zabezpieczenia lub środki ochrony w celu pozyskania nieuprawnionego dostępu do informacji lub do pozostałych zasobów systemu informatycznego;
<b>Plan ciągłości działania</b>	udokumentowany zbiór procedur awaryjnych i informacji, które są opracowane, gromadzone i utrzymywane w stanie gotowym do użycia w przypadku wystąpienia incydentu, aby umożliwić WizjaV kontynuowanie wykonywanych działań krytycznych na możliwym do przyjęcia wcześniej określonym poziomie;
<b>Plan odtworzeniowy</b>	dokument zawierający szczegółowy opis postępowania w przypadku wystąpienia określonego zdarzenia (awarii lub katastrofy),

# Wizja V sp. z o.o.

	<b>BI-03-SZBI PROCEDURA SYSTEMOWA</b> <b>SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI</b>	Wersja <b>1.0.</b>	Data wydania: <b>2024-03-04</b>
	<b>POLITYKA CIĄGŁOŚCI DZIAŁANIA</b>	Strona:	<b>2 / 6</b>

	mającego na celu usunięcie skutków lub przyczyn awarii lub katastrofy;
<b>UKSC</b>	ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
<b>Zabezpieczenie</b>	środki służące zarządzaniu ryzykiem, łącznie z politykami, procedurami, zaleceniami, praktyką lub strukturami organizacyjnymi, które mogą mieć naturę administracyjną, techniczną, zarządczą lub prawną;
<b>Zagrożenie</b>	potencjalna przyczyna niepożądanego incydentu, który powoduje, że ryzyko materializuje się w postaci wymiernej straty poprzez wystawienie danych osobowych na utratę, ujawnienie, zniszczenie lub zmianę;
<b>Zagrożenie cyberbezpieczeństwa</b>	potencjalna przyczyna wystąpienia incydentu;
<b>Zarządzanie incydemem</b>	obsługa incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu;
<b>Zarządzanie ryzykiem</b>	skoordynowane działania w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka; systematyczne stosowanie zasad zarządzania, procedur i praktyk na rzecz działań w zakresie informowania, konsultowania, tworzenia kontekstu oraz identyfikowania, analizy, oceny, postępowania z ryzykiem, monitorowania i przeglądania ryzyka związanego z przetwarzaniem informacji;
<b>Zarządzanie ciągłością działania</b>	całościowy proces zarządzania identyfikujący potencjalne zagrożenia i skutki, jakie te zagrożenia mogą wywierać na działalność WizjaV w przypadku ich wystąpienia, który zapewnia kształtowanie odporności WizjaV i umożliwia skuteczną reakcję w celu ochrony interesów kluczowych interesariuszy tj. osób zaangażowanych w działalność WizjaV, reputacji i wizerunku WizjaV;
<b>Zdarzenie związane z bezpieczeństwem informacji</b>	stwierdzone wystąpienie stanu systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji lub błąd zabezpieczenia, lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem informacji;
<b>Zespół ds. Cyberbezpieczeństwa</b>	zespół osób powołany Zarządzeniem Dyrektora WizjaV, realizujący zadania wskazane w art. 8 pkt. 4 i 6, art. 11 ust. 1 pkt. 1-5, art. 12 i art. 13 UKSC;
<b>Zespół ds. Zarządzania Ciągłością Działania</b>	wewnętrzna struktura odpowiedzialna za zarządzanie ciągłością działania w WizjaV powołana odrębnym Zarządzeniem Dyrektora WizjaV.

## IV. ODPOWIEDZIALNOŚCI I UPRAWNIENIA

1. WizjaV jest jednostką, która ma za zadanie w szczególności realizować zadania ustawowe i w związku z realizacją tych zadań jest zobowiązany do zapewnienia poufności, integralności oraz dostępności danych w tym danych osobowych, które przetwarza w wyżej wymienionych celach. Wszystkie czynności przetwarzania, które WizjaV wykonuje, są realizowane w oparciu o wartości będące fundamentem misji oraz celów WizjaV. Zapewnienie ciągłości działania usługi kluczowej polegającej na „udzielaniu świadczeń opieki zdrowotnej przez podmiot leczniczy oraz obrocie i dystrybucji produktów leczniczych” jest wpisane również w strategię WizjaV.

# Wizja V sp. z o.o.

	<b>BI-03-SZBI PROCEDURA SYSTEMOWA</b> <b>SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI</b>	Wersja <b>1.0.</b>	Data wydania: <b>2024-03-04</b>
		Strona:	<b>3 / 6</b>
<b>POLITYKA CIĄGŁOŚCI DZIAŁANIA</b>			

2. Główne cele ciągłości działania obejmują:
  - 1) zapobieganie niezaplanowanym przerwom w realizacja procesów i zadań WizjaV,
  - 2) utrzymywanie właściwej i niezawodnej infrastruktury technicznej niezbędnej do ich realizacji,
  - 3) monitorowanie i ograniczanie potencjalnych zagrożeń w środowisku pracy, w tym identyfikację i ocenę zdarzeń niepewnych, które mogą mieć wpływ na realizowane przez WizjaV zadania,
  - 4) stałe podnoszenie świadomości pracowników w zakresie utrzymania ciągłości działania i ich roli w przypadku wystąpienia sytuacji kryzysowej.
3. WizjaV jako podmiot odpowiedzialny za realizację kluczowej usługi, uwzględniając wymogi prawne zobowiązuje się do:
  - a) przygotowania, utrzymywania, przeglądania i doskonalenia procedur SZCD,
  - b) odtworzenia kluczowych usług w przypadku wystąpienia zakłócenia,
  - c) zapewnienia niezbędnych zasobów do utrzymania SZCD,
  - d) wdrożenia działań zmniejszających ryzyko wystąpienia zakłóceń,
  - e) sprawnego komunikowania niniejszej Polityki Ciągłości Działania oraz aktualnych Planów Ciągłości Działania,
  - f) utrzymania współpracy z dostawcami usług w tym ekspertami technicznymi, którzy są niezbędni dla zapewnienia realizacji Planów Ciągłości Działania.
4. Polityką Ciągłości Działania związany jest cały Personel WizjaV, a także wyznaczeni przez WizjaV dostawcy usług w tym eksperci techniczni.
5. Zespół ds. Zarządzania Ciągłością Działania odpowiada za koordynowanie działań organizacji zarówno w trakcie wystąpienia zakłócenia, jak i w warunkach bieżącej działalności organizacji. Zespół odpowiada także za aktualność wszystkich ustanowionych Planów Ciągłości Działania w tym uczestniczy w przeglądzie zarządzania SZCD.
6. Zespół ds. cyberbezpieczeństwa odpowiada za:
  - 1) identyfikowanie zagrożeń w odniesieniu do systemów informacyjnych WizjaV oraz proponowanie rozwiązań ograniczających ryzyko wynikające z tych zagrożeń,
  - 2) analizowanie oprogramowania szkodliwego i określanie jego wpływu na system informacyjny WizjaV;
  - 3) wykrywanie przełamania lub ominięcia zabezpieczeń systemu informacyjnego WizjaV, prowadzenie analizy powłamaniowej wraz z określeniem działań niezbędnych do przywrócenia sprawności systemu informacyjnego WizjaV,
  - 4) zabezpieczanie informacji potrzebnych do analizy powłamaniowej, pozwalających na określenie wpływu incydentu poważnego na świadczenie usługi kluczowej, w tym informacji dotyczących:
    - a) rodzajów usług kluczowych, na które incydent miał wpływ,
    - b) liczby użytkowników usługi kluczowej, na których incydent miał wpływ,
    - c) momentu wystąpienia i wykrycia incydentu oraz czas jego trwania,
    - d) zasięgu geograficznego obszaru, którego dotyczy incydent poważny,
    - e) wpływu incydentu na świadczenie usługi kluczowej przez innych operatorów usług kluczowych i dostawców usług cyfrowych,
    - f) przyczyny zaistnienia incydentu i sposobu jego przebiegu oraz skutków jego oddziaływania na systemy informacyjne lub świadczone usługi kluczowe na potrzeby postępowań prowadzonych przez organy ścigania.

## Wizja V sp. z o.o.

	<b>BI-03-SZBI PROCEDURA SYSTEMOWA</b> SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI	Wersja <b>1.0.</b>	Data wydania: <b>2024-03-04</b>
		Strona:	<b>4 / 6</b>
<b>POLITYKA CIĄGŁOŚCI DZIAŁANIA</b>			

7. Najwyższe kierownictwo sprawuje nadzór w zakresie funkcjonowania SZCD.
8. Ćwiczenia i testy w omawianym obszarze, przeprowadzane są zgodnie z ustalonym przez WizjaV harmonogramem.
9. Personel WizjaV jest na bieżąco szkolony, w ustalonych odstępach czasu, tak by w sytuacji wystąpienia zakłócenia każdy z Personelu WizjaV, wiedział jaka jest jego rola i odpowiedzialność w SZCD.
10. Polityka Ciągłości Działania jest dostępna dla stron zainteresowanych w udokumentowanej formie, a także jest komunikowana na wszystkich szczeblach struktury WizjaV.

### V. DOKUMENTY ZWIĄZANE:

1. BI-01-SZBI - Polityka bezpieczeństwa informacji;
2. BI-02-SZBI - Polityka ochrony danych osobowych;
3. BI-03-SZBI - Polityka ciągłości działania;
4. BI-04-SZBI - Procedura nadawania upoważnień;
5. BI-05-SZBI - Procedura udostępniania danych;
6. BI-06-SZBI - Procedura powierzenia przetwarzania danych;
7. BI-07-SZBI - Procedura oceny skutków;
8. BI-08-SZBI - Procedura zarządzania ryzykiem bezpieczeństwa informacji;
9. BI-09-SZBI - Procedura zarządzania podatnościami;
10. BI-10-SZBI - Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji;
11. BI-11-SZBI - Procedura użytkowania sieci teleinformatycznej;
12. BI-12-SZBI - Procedura rejestracji i inwentaryzacji oprogramowania i sprzętu komputerowego;
13. BI-13-SZBI - Procedura pracy zdalnej;
14. BI-14-SZBI - Procedura dostępu VPN do zasobów sieci WizjaV;
15. BI-15-SZBI - Procedura przechowywania i przekazywania hasła administratora systemu;
16. BI-16-SZBI - Procedura wykonywania kopii zapasowych;
17. BI-17-SZBI - Procedura rejestracji i inwentaryzacji sprzętu medycznego;
18. BI-18-SZBI - Procedura zarządzania zmianą IT;
19. BI-19-SZBI - Procedura privacy by design, privacy by default;
20. BI-20-SZBI - Procedura zarządzania aktywami informacyjnymi;
21. BI-21-SZBI - Procedura zarządzania bezpieczeństwem zasobów ludzkich;
22. BI-22-SZBI - Procedura bezpieczeństwa fizycznego i środowiskowego;
23. BI-23-SZBI - Procedura zarządzania kluczami;
24. BI-24-SZBI - Procedura zarządzania uprawnieniami w systemie kontroli dostępu;
25. BI-25-SZBI - Procedura dostępu do serwerowni;
26. BI-26-SZBI - Procedura zarządzania systemem monitoringu wizyjnego;
27. BI-27-SZBI - Procedura korzystania z bezprzewodowej sieci dla pracownika;
28. BI-28-SZBI - Procedura korzystania z bezprzewodowej sieci dla gości;

## Wizja V sp. z o.o.

	<b>BI-03-SZBI PROCEDURA SYSTEMOWA</b> SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI	Wersja <b>1.0.</b>	Data wydania: <b>2024-03-04</b>
		Strona:	<b>5 / 6</b>
<b>POLITYKA CIĄGŁOŚCI DZIAŁANIA</b>			

- 29. BI-29-SZBI - Procedura bezpieczeństwa w relacjach z podmiotami zewnętrznymi dla pracowników;
- 30. BI-30-SZBI - Procedura bezpieczeństwa w relacjach z podmiotami zewnętrznymi dla dostawców;
- 31. BI-31-SZBI - Procedura monitorowania i nadzoru nad bezpieczeństwem informacji.

### VI. PODSTAWA PRAWNA:

1. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
2. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
3. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
4. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
5. Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta;
6. Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej;
7. Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia;
8. Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych;
9. Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych;
10. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej;
11. Ustawa z dnia 11 września 2019 r. prawo zamówień publicznych;
12. Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy;
13. Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach;
14. Ustawa z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych;
15. Ustawa z dnia 29 września 1994 roku o rachunkowości;
16. Ustawa z dnia 6 czerwca 1997 r. Kodeks karny;
17. Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia;
18. Ustawa z dnia 27 lipca 2001 roku o ochronie baz danych;
19. Ustawa z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym;
20. Ustawa z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną;
21. Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny;
22. Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych;
23. Rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo;
24. Rozporządzenie Rady Ministrów z dnia 16 października 2028 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;
25. Rozporządzenie Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu;

## Wizja V sp. z o.o.

	<b>BI-03-SZBI PROCEDURA SYSTEMOWA</b> <b>SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI</b>  <b>POLITYKA CIĄGŁOŚCI DZIAŁANIA</b>	Wersja <b>1.0.</b>	Data wydania: <b>2024-03-04</b>
		Strona:	<b>6 / 6</b>

26. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
27. Rozporządzenie Ministra Zdrowia z dnia 8 maja 2018 r. w sprawie rodzajów elektronicznej dokumentacji medycznej;
28. Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania.

### VII. ZAŁĄCZNIK: