

**Dokumentacja techniczna  
cyberbezpieczeństwa  
produktów firmy Mindray**

Listopad 2024

**mindray**

# Spis treści

---

01	STRESZCZENIE	2
----	--------------	---

---

02	NAWIGOWANIE PO CYFRYZACJI OPIEKI ZDROWOTNEJ: DROGA DO BEZPIECZNYCH INNOWACJI	3
----	---	---

---

03	STANOWISKO FIRMY MINDRAY W SPRAWIE CYBERBEZPIECZEŃSTWA	5
----	--	---

---

0	MODEL CYBERBEZPIECZEŃSTWA PRODUKTÓW FIRMY MINDRAY	11
---	---	----

	ZARZĄDZANIE I OCENA RYZYKA	12
--	----------------------------	----

	12	12
--	----	----

	13	13
--	----	----

	13	13
--	----	----

	BEZPIECZNE PROJEKTOWANIE I ROZWÓJ	14
--	-----------------------------------	----

	1	1
--	---	---

	1	1
--	---	---

	1	1
--	---	---

---

---

	ŚRODKI OCHRONNE I KONTROLNE	15
--	-----------------------------	----

	15	15
--	----	----

	1	1
--	---	---

	1	1
--	---	---

	KONSERWACJA I ZARZĄDZANIE CYKLEM ŻYCIA	18
--	--	----

	1	1
--	---	---

	1	1
--	---	---

	ZARZĄDZANIE ZDARZENIAMI	20
--	-------------------------	----

	20	20
--	----	----

	20	20
--	----	----

	OCHRONA DANYCH	21
--	----------------	----

	21	21
--	----	----

	21	21
--	----	----

	22	22
--	----	----

	23	23
--	----	----

---

05	UWAGI KOŃCOWE	24
----	---------------	----

## Streszczenie



## Nawigowanie po cyfryzacji opieki zdrowotnej: droga do bezpiecznych innowacji



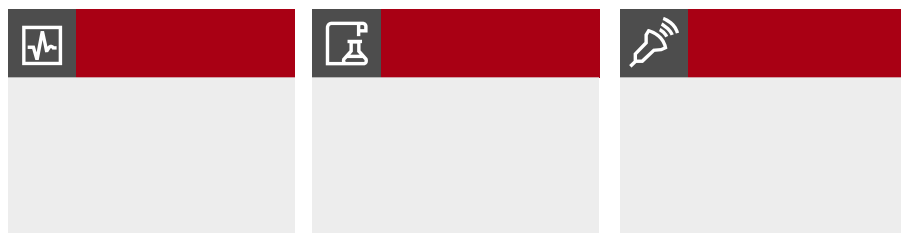
1 // - - - - - / / - - - - -  
- - - - - / - - - - -  
2 // - - - - - / - - - - -  
- - - - - /  
3 // - - - - - / - - - - -  
/2015/02/ - - - - - / - - - - -  
// - - - - - / - - - - -  
5 // - - - - - / - - - - -

# Stanowisko firmy Mindray w sprawie cyberbezpieczeństwa

Uznając rosnące ryzyko zagrożeń cyberbezpieczeństwa, Mindray zobowiązuje się do ciągłego doskonalenia naszych procesów i systemów w celu zintegrowania cyberbezpieczeństwa i ochrony prywatności w każdym aspekcie.

- 
- 
- 
- 
- 





“

“

“





## Zgodność i przestrzeganie standardów

§ 1. Wzrost

§ 2. Wzrost

§ 3. Wzrost

§ 4. Wzrost

§ 5. Wzrost

§ 6. Wzrost

§ 7. Wzrost

§ 8. Wzrost

§ 9. Wzrost

§ 10. Wzrost

§ 11. Wzrost

§ 12. Wzrost

§ 13. Wzrost

§ 14. Wzrost

§ 15. Wzrost

§ 16. Wzrost

§ 17. Wzrost

§ 18. Wzrost

§ 19. Wzrost

§ 20. Wzrost

§ 21. Wzrost

§ 22. Wzrost

§ 23. Wzrost

§ 24. Wzrost

§ 25. Wzrost

§ 26. Wzrost

§ 27. Wzrost

§ 28. Wzrost

§ 29. Wzrost

§ 30. Wzrost

§ 31. Wzrost

§ 32. Wzrost

§ 33. Wzrost

§ 34. Wzrost

§ 35. Wzrost

§ 36. Wzrost

§ 37. Wzrost

§ 38. Wzrost

§ 39. Wzrost

§ 40. Wzrost

§ 41. Wzrost

§ 42. Wzrost

§ 43. Wzrost

§ 44. Wzrost

§ 45. Wzrost

§ 46. Wzrost

§ 47. Wzrost

§ 48. Wzrost

§ 49. Wzrost

§ 50. Wzrost

§ 51. Wzrost

§ 52. Wzrost

§ 53. Wzrost

§ 54. Wzrost

§ 55. Wzrost

§ 56. Wzrost

§ 57. Wzrost

§ 58. Wzrost

§ 59. Wzrost

§ 60. Wzrost

§ 61. Wzrost

§ 62. Wzrost

§ 63. Wzrost

§ 64. Wzrost

§ 65. Wzrost

§ 66. Wzrost

§ 67. Wzrost

§ 68. Wzrost

§ 69. Wzrost

§ 70. Wzrost

§ 71. Wzrost

§ 72. Wzrost

§ 73. Wzrost

§ 74. Wzrost

§ 75. Wzrost

§ 76. Wzrost

§ 77. Wzrost

§ 78. Wzrost

§ 79. Wzrost

§ 80. Wzrost

§ 81. Wzrost

§ 82. Wzrost

§ 83. Wzrost

§ 84. Wzrost

§ 85. Wzrost

§ 86. Wzrost

§ 87. Wzrost

§ 88. Wzrost

§ 89. Wzrost

§ 90. Wzrost

§ 91. Wzrost

§ 92. Wzrost

§ 93. Wzrost

§ 94. Wzrost

§ 95. Wzrost

§ 96. Wzrost

§ 97. Wzrost

§ 98. Wzrost

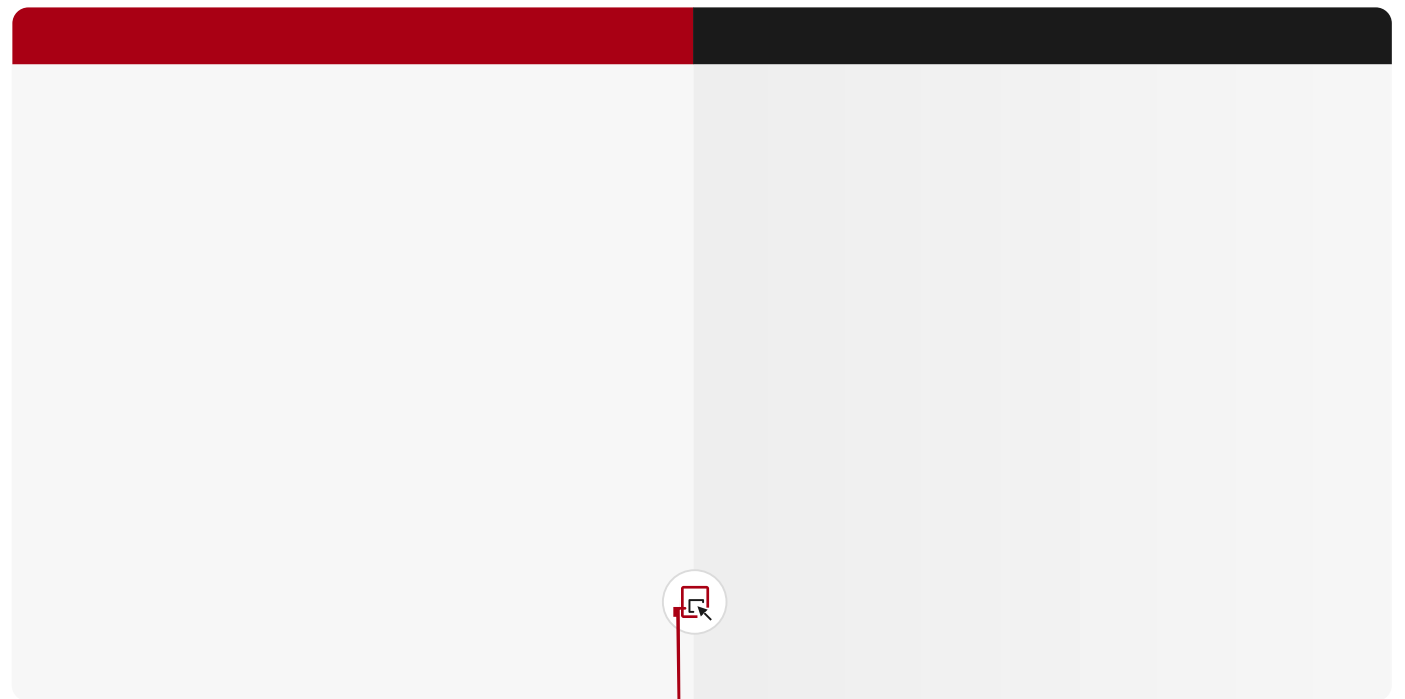
§ 99. Wzrost

§ 100. Wzrost

Nasze zobowiązanie do przestrzegania tych standardów wynika nie tylko z chęci zachowania zgodności z przepisami czy zdobycia certyfikatów, ale przede wszystkim wzbudzenia w naszych klientach i użytkownikach poczucia zaufania i bezpieczeństwa.



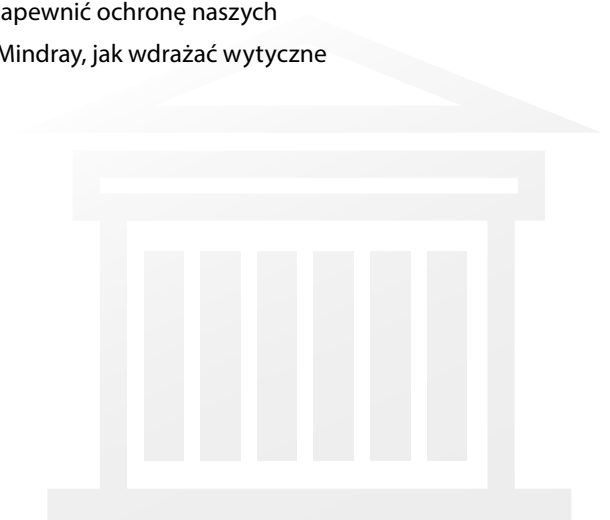
Ochrona w partnerstwie:  
wspólna odpowiedzialność



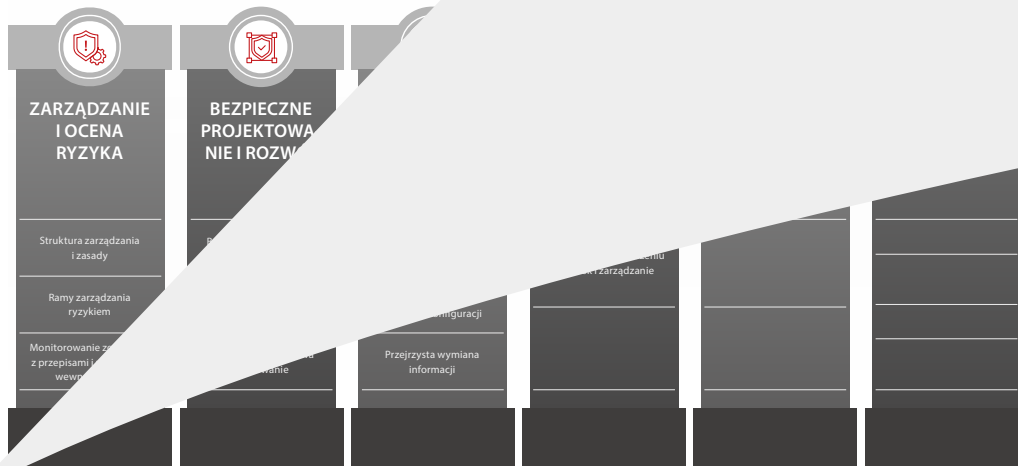
# Model cyberbezpieczeństwa produktów firmy Mindray

Mindray wdraża wewnętrznie opracowane ramy bezpieczeństwa mające zapewnić ochronę naszych urządzeń medycznych, pokazując wszystkim zespołom i oddziałom firmy Mindray, jak wdrażać wytyczne w zakresie cyberbezpieczeństwa.

- 
- 
- 
- 
- 
- 
- 



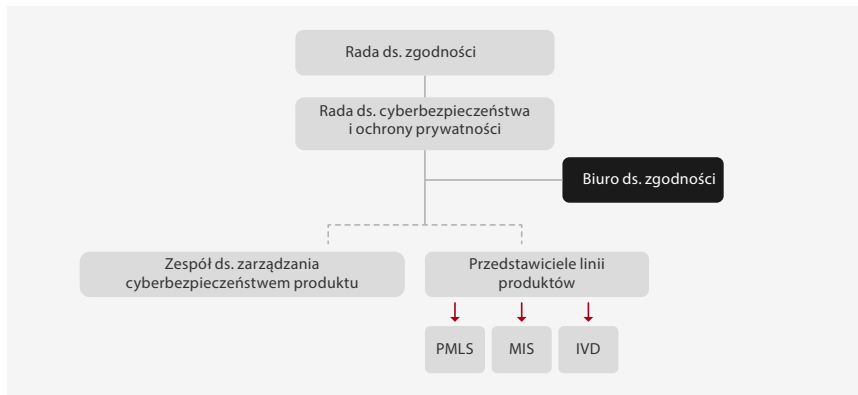
A



# Zarządzanie i ocena ryzyka



## Struktura zarządzania i zasady



**Rada ds. zgodności,** jest to najwyższy organ nadzorczy, który nadzoruje i kieruje działalnością Biura ds. zgodności. Rada ds. zgodności jest odpowiedzialna za nadzór nad systemem zarządzania zgodnością i nadzór nad działalnością Biura ds. zgodności. Rada ds. zgodności jest odpowiedzialna za nadzór nad systemem zarządzania zgodnością i nadzór nad działalnością Biura ds. zgodności.

**Rada ds. cyberbezpieczeństwa i ochrony prywatności** jest to organ nadzorczy, który nadzoruje i kieruje działalnością Biura ds. zgodności. Rada ds. cyberbezpieczeństwa i ochrony prywatności jest odpowiedzialna za nadzór nad systemem zarządzania cyberbezpieczeństwem i nadzór nad działalnością Biura ds. zgodności. Rada ds. cyberbezpieczeństwa i ochrony prywatności jest odpowiedzialna za nadzór nad systemem zarządzania cyberbezpieczeństwem i nadzór nad działalnością Biura ds. zgodności.

## Biuro ds. zgodności

## Zespół ds. zarządzania cyberbezpieczeństwem produktu





eczeństwo  
projektowania

5 5

(1.02) 2(38) 9- . ((.1525 .11 0-52(-)1.522()) .3





## Wzmacnianie systemu i kontrola konfiguracji

Wzmacnianie systemu i kontrola konfiguracji to procesy, które mają na celu zwiększenie odporności systemu operacyjnego na ataki i uszkodzenia, a także zapewnienie, że system jest skonfigurowany zgodnie z najlepszymi praktykami i wymaganiami bezpieczeństwa.

Wytyczne dotyczące zwiększenia odporności systemu operacyjnego

Wytyczne dotyczące zwiększenia odporności systemu operacyjnego to zbiór zasad, które mają na celu zapewnienie, że system jest odporny na ataki i uszkodzenia. Wytyczne te obejmują m.in. regularne aktualizacje systemu operacyjnego i aplikacji, konfigurację systemu operacyjnego zgodnie z najlepszymi praktykami, a także stosowanie zabezpieczeń fizycznych i logicznych.

Białe listy aplikacji i procesów

Białe listy aplikacji i procesów to listy aplikacji i procesów, które są dozwolone na systemie operacyjnym. Białe listy te mają na celu zapewnienie, że tylko te aplikacje i procesy, które są niezbędne do działania systemu, mogą wykonywać swoje zadania. Białe listy te mogą być skonfigurowane na poziomie systemu operacyjnego lub aplikacji.

Programy antywirusowe i zabezpieczające przed złośliwym oprogramowaniem

Programy antywirusowe i zabezpieczające przed złośliwym oprogramowaniem to programy, które mają na celu wykrywanie i usuwanie złośliwego oprogramowania z systemu operacyjnego. Programy te mogą być skonfigurowane na poziomie systemu operacyjnego lub aplikacji. Programy te mogą również wykonywać regularne skanowania systemu operacyjnego i aplikacji w celu wykrywania złośliwego oprogramowania.

Wyłączanie

Wyłączanie to proces, który ma na celu wyłączenie systemu operacyjnego z sieci lub z internetu. Wyłączanie to może być wykonane ręcznie przez użytkownika lub automatycznie przez system operacyjny. Wyłączanie to jest ważnym elementem polityki bezpieczeństwa, który ma na celu zapewnienie, że system operacyjny nie jest dostępny dla atakujących.



## Przejrzysta wymiana informacji

Przejrzysta wymiana informacji jest jednym z najważniejszych elementów, które umożliwiają przedsiębiorcom i konsumentom podejmowanie świadomych decyzji. Dzięki temu można uniknąć problemów związanych z bezpieczeństwem i jakością produktów.

### Dokumentacja dotycząca cyberbezpieczeństwa

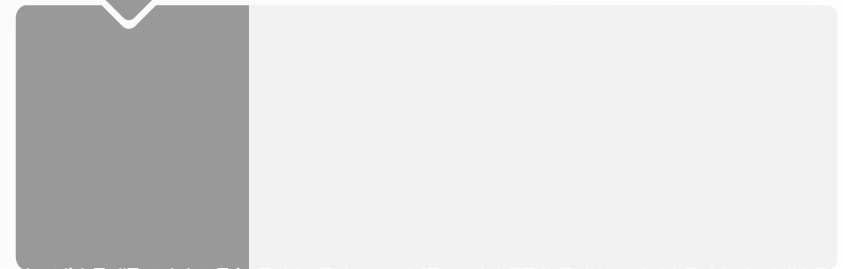
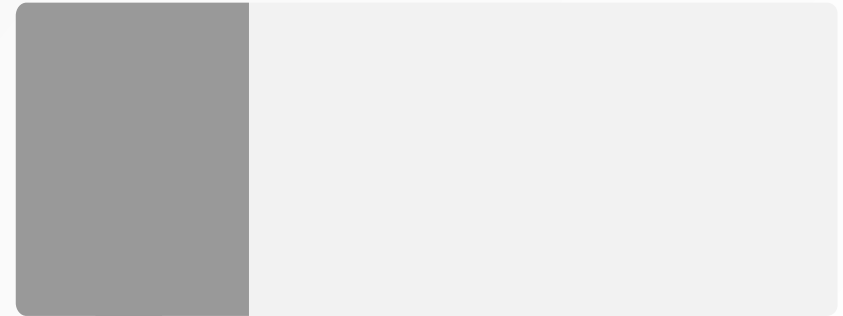
Przedsiębiorcy powinni posiadać dokumentację dotyczącą cyberbezpieczeństwa, która zawiera informacje o sposobie ochrony danych osobowych i innych informacji. Dokumentacja ta powinna być dostępna dla konsumentów i zawierać informacje o sposobie zgłaszania naruszeń bezpieczeństwa.

### Instrukcje obsługi produktów

Przedsiębiorcy powinni posiadać instrukcje obsługi produktów, które są dostępne dla konsumentów. Instrukcje obsługi powinny być jasne i zrozumiałe, a także zawierać informacje o sposobie użytkowania produktu i jego bezpieczeństwie.

### Oświadczenie producenta dotyczące bezpieczeństwa

Przedsiębiorcy powinni posiadać oświadczenie producenta dotyczące bezpieczeństwa, które zawiera informacje o sposobie oceny ryzyka i sposobie zapewnienia bezpieczeństwa produktu. Oświadczenie to powinno być dostępne dla konsumentów i zawierać informacje o sposobie zgłaszania naruszeń bezpieczeństwa.



## Konserwacja i zarządzanie cyklem życia



### Luki w zabezpieczeniach wykryte po wprowadzeniu na rynek i zarządzanie poprawkami

kompleksową strategię zarządzania poprawkami,





## Koniec okresu eksploatacji i wsparcie przy wycofywaniu z eksploatacji

pisma z informacjami o procedurach postępowania w związku ze zbliżającym się końcem okresu eksploatacji produktów.







Mindray dąży do tego, aby ochrona prywatności by02(h) (i80.0x) ..5x (8)1.3 t)8s (8.8 (5 -04.8 (1 t)8w(t)1.8o(y051.0031)-3.0TJ434 c)d-3.0a) (r)-32.0y 2.8 (8031) (ś)-2 (c)4.0i b)







**mindray**