POLITYKA BEZPIECZEŃSTWA PRODUKTÓW Z ELEMENTAMI CYFROWYMI WG CRA

Dotyczy Norma	Opracował:	Sprawdził:	Zatwierdził:
CRA (Cyber Resilience Act)	**GFLEAN**	**Pełnomocnik ds. cyberbezpieczeństwa / CISO**	**Prezes Zarządu BRAGER Sp. z o.o. Rafał Urbaniak**

Projekt polityki

POLITYKA BEZPIECZEŃSTWA PRODUKTÓW Z ELEMENTAMI CYFROWYMI WG CRA
BRAGER Sp. z o.o.
Wersja: 1.0
Data wejścia w życie: [30.06.2026]
Właściciel dokumentu: [Pełnomocnik ds. cyberbezpieczeństwa / CISO / Zarząd]
Data przeglądu: [30.06.2027]

Element	Opis
Status dokumentu	Zatwierdzony przez Zarząd BRAGER Sp. z o.o.
Podstawa opracowania	Polityka skoordynowanego ujawniania podatności (CVD) Brager Sp. z o.o. oraz wymagania Rozporządzenia (UE) 2024/2847 (Cyber Resilience Act).
Charakter dokumentu	Dokument nadrzędny systemu bezpieczeństwa produktu; polityka CVD pozostaje dokumentem powiązanym i wykonawczym.

1. Cel

Celem niniejszej Polityki bezpieczeństwa produktów z elementami cyfrowymi jest ustanowienie zasad projektowania, wytwarzania, wprowadzania do obrotu, utrzymywania, aktualizowania oraz monitorowania bezpieczeństwa produktów oferowanych przez BRAGER Sp. z o.o. w sposób zgodny z wymaganiami Cyber Resilience Act (CRA).

Polityka ma zapewnić, że produkty z elementami cyfrowymi są projektowane i utrzymywane tak, aby ograniczać ryzyka naruszenia poufności, integralności, dostępności, autentyczności oraz bezpiecznego działania produktu w przewidywalnych warunkach użytkowania.

- wprowadzenie zasad bezpieczeństwa przez cały cykl życia produktu;
- zapewnienie zarządzania ryzykiem cyberbezpieczeństwa produktu;
- ustanowienie zasad security by design oraz security by default;
- powiązanie bezpieczeństwa produktu z obsługą podatności, aktualizacji i incydentów;
- określenie ról, odpowiedzialności, rejestrów i dowodów wymaganych do wykazania zgodności z CRA;
- zapewnienie spójności z procedurami wewnętrznymi, w szczególności Polityką skoordynowanego ujawniania podatności (CVD).

2. Zakres

Polityka obejmuje wszystkie produkty z elementami cyfrowymi projektowane, rozwijane, produkowane, wprowadzane do obrotu, integrowane lub utrzymywane przez BRAGER Sp. z o.o., a także powiązane usługi zdalnego przetwarzania danych, jeżeli są niezbędne do realizacji funkcji produktu.

- sterowniki lokalne kotłów i instalacji grzewczych;
- sterowniki wyposażone w komunikację zdalną, w tym zestawy typu PELE BORD 890 + Media Bord;
- moduły komunikacyjne Internet/GSM oraz powiązane rozwiązania zdalnego dostępu;
- firmware, aplikacje, konfiguracje, pliki aktualizacyjne i komponenty programowe;
- interfejsy użytkownika, porty serwisowe, interfejsy diagnostyczne i mechanizmy aktualizacji;
- komponenty dostarczane przez podmioty zewnętrzne, o ile są częścią produktu lub wpływają na jego bezpieczeństwo.

Polityka ma zastosowanie do pracowników, współpracowników, dostawców, podwykonawców, instalatorów, serwisu, działów technicznych oraz osób odpowiedzialnych za rozwój, produkcję, obsługę i wsparcie produktów BRAGER Sp. z o.o.

3. Definicje

Termin	Znaczenie
Produkt z elementami cyfrowymi	produkt sprzętowy lub programowy oraz jego rozwiązania zdalnego przetwarzania danych, których cyberbezpieczeństwo może wpływać na jego funkcje, bezpieczeństwo lub użytkownika.
Cyberbezpieczeństwo produktu	stan, w którym produkt jest chroniony przed nieuprawnionym dostępem, nieuprawnioną modyfikacją, utratą danych, zakłóceniem działania oraz wykorzystaniem podatności.
Podatność	słabość, błąd lub niewłaściwa konfiguracja, która może zostać wykorzystana do naruszenia poufności, integralności, dostępności, autentyczności lub bezpieczeństwa produktu.
Incydent	zdarzenie wpływające lub mogące wpływać na bezpieczeństwo produktu z elementami cyfrowymi.
Security by design	uwzględnianie bezpieczeństwa od etapu koncepcji, projektowania i rozwoju produktu.
Security by default	zapewnienie bezpiecznych ustawień domyślnych i minimalizacji funkcji narażających produkt na atak.
Firmware	oprogramowanie wbudowane sterownika lub modułu komunikacyjnego.
Ryzyko resztkowe	ryzyko pozostające po wdrożeniu środków ograniczających ryzyko.
Okres wsparcia	zadeklarowany okres, w którym BRAGER Sp. z o.o. zapewnia aktualizacje, poprawki bezpieczeństwa i obsługę podatności.
SBOM	wykaz komponentów programowych wykorzystywanych w produkcie, jeżeli jest wymagany lub stosowany jako element kontroli łańcucha dostaw.

4. Podstawa prawna i regulacyjna

Niniejsza Polityka realizuje założenia Rozporządzenia (UE) 2024/2847 w sprawie horyzontalnych wymogów cyberbezpieczeństwa dla produktów z elementami cyfrowymi, znanego jako Cyber Resilience Act (CRA).

Polityka uwzględnia w szczególności obowiązki producenta dotyczące:

- prowadzenia oceny ryzyka cyberbezpieczeństwa produktu;
- uwzględnienia cyberbezpieczeństwa w projektowaniu, rozwoju i produkcji;
- zapewnienia bezpiecznej konfiguracji domyślnej;
- zarządzania podatnościami i skoordynowanego ujawniania podatności;
- dostarczania środków naprawczych oraz aktualizacji bezpieczeństwa;
- raportowania aktywnie wykorzystywanych podatności i poważnych incydentów zgodnie z CRA;
- prowadzenia dokumentacji technicznej i dowodów zgodności produktu.

Niniejszy dokument został opracowany z wykorzystaniem podejścia metodycznego właściwego dla norm IEC 62443, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 29147 oraz ISO/IEC 30111.

5. Klasyfikacja produktów i poziomy ryzyka CRA

BRAGER Sp. z o.o. prowadzi wewnętrzną klasyfikację produktów z elementami cyfrowymi w celu określenia wymaganego poziomu oceny zgodności, środków bezpieczeństwa i intensywności nadzoru nad produktem. Klasyfikacja jest potwierdzana w dokumentacji technicznej danego produktu.

Linia	Opis	Poziom ryzyka CRA	Minimalne wymagania kontrolne
Linia A	Sterowniki lokalne bez dostępu zdalnego	Standardowy produkt z elementami cyfrowymi	Ocena ryzyka, bezpieczna konfiguracja, aktualizacje firmware, instrukcja bezpieczeństwa użytkowania.
Linia B	Sterowniki z modułem Internet/GSM, np. PELE BORD 890 + Media Bord	Important Product - Class I (kwalifikacja robocza do potwierdzenia w analizie produktu)	Silniejsze uwierzytelnianie, szyfrowanie komunikacji, logowanie zdarzeń, zarządzanie podatnościami i aktualizacjami.
Linia C	Moduły komunikacyjne i usługi zdalne	Important Product - Class I (kwalifikacja robocza do potwierdzenia w analizie produktu)	Kontrola dostępu, monitoring usług, segmentacja, zabezpieczenia infrastruktury, procedury incydentowe.
Linia D	Firmware i komponenty wspólne	Poziom dziedziczony z produktu docelowego	Bezpieczny cykl rozwoju, kontrola wersji, testy bezpieczeństwa, weryfikacja komponentów zewnętrznych.

Jeżeli konkretny produkt zostanie sklasyfikowany jako produkt ważny lub krytyczny w rozumieniu CRA, właściciel produktu jest zobowiązany do uzupełnienia dokumentacji o szczegółowe uzasadnienie klasyfikacji oraz wymagany tryb oceny zgodności.

6. Zasady ogólne bezpieczeństwa produktu

6.1 Bezpieczeństwo przez cały cykl życia

Bezpieczeństwo produktu jest zarządzane od etapu koncepcji, przez projektowanie, rozwój, produkcję, testy, sprzedaż, instalację, użytkowanie, serwis, aktualizacje, aż do zakończenia wsparcia produktu.

6.2 Security by design

- wymagania bezpieczeństwa są definiowane przed rozpoczęciem projektowania;
- ryzyka cyberbezpieczeństwa są oceniane przed wdrożeniem funkcji;
- funkcje zdalne są projektowane z uwzględnieniem szyfrowania, uwierzytelniania i rejestrowania zdarzeń;
- komponenty zewnętrzne są oceniane pod kątem znanych podatności i utrzymania.

6.3 Security by default

- produkt nie powinien zawierać trwałych, niezmienialnych haseł domyślnych;
- użytkownik powinien zostać zobowiązany do zmiany danych uwierzytelniających przy pierwszym uruchomieniu, jeżeli produkt wykorzystuje logowanie;
- funkcje komunikacji zdalnej powinny być aktywowane wyłącznie wtedy, gdy są potrzebne i skonfigurowane bezpiecznie;
- nieużywane porty, usługi i interfejsy powinny być wyłączone lub odpowiednio ograniczone.

6.4 Minimalizacja powierzchni ataku

BRAGER Sp. z o.o. ogranicza funkcje, interfejsy, uprawnienia i usługi do zakresu niezbędnego do prawidłowego działania produktu. Każde rozszerzenie funkcjonalności produktu powinno być poprzedzone oceną wpływu na bezpieczeństwo.

7. Role i odpowiedzialności

Rola	Odpowiedzialność
Zarząd	Zatwierdza Politykę, zapewnia zasoby, akceptuje ryzyka resztkowe przekraczające ustalony próg akceptacji.
Pełnomocnik ds. cyberbezpieczeństwa / CISO	Nadzoruje system bezpieczeństwa produktu, koordynuje zgodność z CRA, prowadzi przeglądy, nadzoruje rejestry i raportowanie.
R&D / zespół produktowy	Definiuje wymagania bezpieczeństwa, projektuje zabezpieczenia, prowadzi testy i przygotowuje środki naprawcze.
IT / infrastruktura	Utrzymuje zabezpieczenia usług zdalnych, monitoring, dostęp administracyjny i kopie zapasowe systemów wspierających produkt.
Serwis / support	Wspiera użytkowników, przekazuje zalecenia bezpieczeństwa, eskaluje zgłoszenia incydentów i podatności.
Zakupy / właściciel dostawców	Uwzględnia wymagania cyberbezpieczeństwa w relacjach z dostawcami komponentów i usług.
Dział prawny / compliance	Ocena obowiązków regulacyjnych, komunikatów, klauzul umownych i dokumentacji zgodności.
Dostawcy i podwykonawcy	Spełniają wymagania bezpieczeństwa określone w umowach, przekazują informacje o podatnościach i współpracują przy działaniach naprawczych.

8. Zarządzanie ryzykiem cyberbezpieczeństwa produktu

Każdy produkt z elementami cyfrowymi objęty niniejszą Polityką podlega ocenie ryzyka cyberbezpieczeństwa przed wprowadzeniem do obrotu oraz przy istotnych zmianach produktu, oprogramowania, funkcji komunikacyjnych lub środowiska użytkowania.

1. Identyfikacja aktywów, funkcji bezpieczeństwa i przewidywalnego środowiska użytkowania produktu.
2. Identyfikacja zagrożeń, podatności, możliwych scenariuszy nadużyć i skutków dla użytkowników.
3. Ocena prawdopodobieństwa i skutków, w tym wpływu na poufność, integralność, dostępność, autentyczność i bezpieczeństwo działania produktu.
4. Określenie środków minimalizacji ryzyka, odpowiedzialności i terminów realizacji.
5. Ocena ryzyka resztkowego po wdrożeniu zabezpieczeń.
6. Akceptacja ryzyka resztkowego przez uprawnioną osobę lub organ zarządzający.
7. Aktualizacja rejestru ryzyk, rejestru zagrożeń oraz dokumentacji technicznej produktu.

Ryzyka wysokie wymagają działań redukujących przed wprowadzeniem produktu do obrotu lub przed udostępnieniem danej funkcji użytkownikowi. Ryzyka średnie wymagają zabezpieczeń, monitorowania i decyzji właściciela produktu. Ryzyka niskie mogą zostać zaakceptowane, o ile są udokumentowane.

9. Wymagania bezpieczeństwa technicznego

Obszar	Wymaganie
Uwierzytelnianie	Unikanie haseł domyślnych, wymuszenie zmiany hasła, ograniczenie dostępu serwisowego, role i

	uprawnienia.
Autoryzacja	Zasada najmniejszych przywilejów, rozdzielenie ról użytkownika, instalatora, serwisu i administratora.
Komunikacja zdalna	Szyfrowanie transmisji, weryfikacja autentyczności serwera/usługi, brak nieuzasadnionych otwartych portów.
Aktualizacje	Mechanizm bezpiecznej aktualizacji firmware, weryfikacja integralności i autentyczności aktualizacji, ochrona przed nieautoryzowanym kodem.
Konfiguracja	Walidacja parametrów, ograniczenie zakresów krytycznych, możliwość przywrócenia konfiguracji bezpiecznej.
Logowanie zdarzeń	Rejestrowanie dostępu zdalnego, zmian konfiguracji, błędów krytycznych, aktualizacji i zdarzeń serwisowych, jeżeli funkcje produktu to umożliwiają.
Odporność i dostępność	Tryb lokalny lub bezpieczny w przypadku utraty łączności, ograniczenie skutków awarii usług zdalnych.
Ochrona danych	Minimalizacja danych, zabezpieczenie danych konfiguracyjnych i danych transmisyjnych, kontrola dostępu do logów.
Interfejsy fizyczne	Ograniczenie dostępu do portów serwisowych, procedury serwisowe, zabezpieczenie przed nieautoryzowaną ingerencją.

10. Bezpieczny rozwój produktu i oprogramowania

BRAGER Sp. z o.o. utrzymuje proces bezpiecznego rozwoju produktu, obejmujący co najmniej:

- definiowanie wymagań bezpieczeństwa dla nowych produktów i zmian;
- przeglądy architektury i projektu pod kątem bezpieczeństwa;
- kontrolę wersji kodu i dokumentacji technicznej;
- przeglądy kodu, testy funkcjonalne i testy bezpieczeństwa adekwatne do poziomu ryzyka produktu;
- weryfikację komponentów zewnętrznych i bibliotek;
- zarządzanie błędami, podatnościami i poprawkami;
- dokumentowanie decyzji projektowych wpływających na bezpieczeństwo.

Dla produktów z funkcją zdalnego dostępu wymagane jest wykonanie dodatkowej oceny bezpieczeństwa komunikacji, mechanizmów uwierzytelniania, aktualizacji i logowania zdarzeń.

11. Zarządzanie podatnościami i powiązanie z CVD

Polityka skoordynowanego ujawniania podatności (CVD) jest dokumentem wykonawczym wobec niniejszej Polityki. Określa ona zasady przyjmowania, oceny, obsługi, usuwania i ujawniania informacji o podatnościach dotyczących produktów BRAGER Sp. z o.o.

W ramach niniejszej Polityki BRAGER Sp. z o.o. zapewnia:

- publicznie dostępny i użyteczny kanał zgłaszania podatności;
- potwierdzanie i kwalifikację zgłoszeń w terminach określonych w Polityce CVD;
- klasyfikację podatności według wpływu na poufność, integralność, dostępność i autentyczność;
- priorytetową obsługę podatności krytycznych i wysokich;
- opracowanie i przetestowanie środków naprawczych lub ograniczających ryzyko;
- komunikację z użytkownikami i zgłaszającymi w sposób ograniczający ryzyko nadużyć;
- prowadzenie rejestru zgłoszeń podatności, decyzji i działań naprawczych.

Zgłoszenia podatności są obsługiwane z zachowaniem poufności. BRAGER Sp. z o.o. nie podejmuje działań odwetowych wobec zgłaszających działających legalnie, w dobrej wierze i zgodnie z zasadami CVD.

12. Aktualizacje bezpieczeństwa i okres wsparcia

BRAGER Sp. z o.o. określa i komunikuje użytkownikom zasady dostarczania aktualizacji bezpieczeństwa w okresie wsparcia produktu. Aktualizacje powinny być adekwatne do poziomu ryzyka oraz charakteru produktu.

- aktualizacje krytyczne są przygotowywane i udostępniane bez zbędnej zwłoki;
- aktualizacje są testowane przed udostępnieniem użytkownikom;
- użytkownik otrzymuje zrozumiałą informację o celu aktualizacji, ryzyku i sposobie jej wdrożenia;
- mechanizm aktualizacji powinien weryfikować integralność i autentyczność pakietu aktualizacyjnego, jeżeli technicznie jest to możliwe;
- zakończenie okresu wsparcia powinno być komunikowane w sposób przejrzysty.

13. Reagowanie na incydenty i raportowanie CRA

W przypadku podejrzenia lub potwierdzenia incydentu wpływającego na bezpieczeństwo produktu BRAGER Sp. z o.o. uruchamia proces reagowania na incydenty, obejmujący identyfikację, eskalację, analizę, ograniczenie skutków, działania naprawcze, komunikację i dokumentowanie zdarzenia.

Jeżeli incydent lub podatność spełnia kryteria raportowania wynikające z CRA, właściciel procesu bezpieczeństwa uruchamia obowiązkowy tryb raportowania zgodnie z Polityką CVD i właściwymi procedurami wewnętrznymi.

Etap	Opis
Wykrycie / zgłoszenie	Przyjęcie informacji z kanałów wewnętrznych, serwisu, klienta, badacza, dostawcy lub monitoringu.
Eskalacja	Niezwłoczne przekazanie do właściciela procesu bezpieczeństwa oraz zespołu technicznego.
Analiza	Ocena produktu, wersji, skali narażenia, aktywnego wykorzystania i skutków.
Ograniczenie skutków	Tymczasowe obejście, wyłączenie funkcji, zalecenia dla użytkowników, poprawka techniczna.
Raportowanie	Zgłoszenie przez właściwy kanał, jeżeli spełnione są przesłanki CRA.
Zamknięcie i wnioski	Raport końcowy, aktualizacja rejestrów, działania korygujące i zapobiegawcze.

14. Bezpieczeństwo łańcucha dostaw

BRAGER Sp. z o.o. uwzględnia wymagania cyberbezpieczeństwa w doborze, ocenie i nadzorze nad dostawcami komponentów, usług, bibliotek programowych, narzędzi rozwojowych i rozwiązań zdalnych.

- dostawcy powinni przekazywać informacje o znanych podatnościach komponentów;
- umowy z dostawcami powinny zawierać wymagania dotyczące bezpieczeństwa, poufności i współpracy przy incydentach;
- komponenty programowe powinny być identyfikowalne i monitorowane pod kątem znanych podatności;
- zmiana dostawcy lub komponentu krytycznego wymaga oceny wpływu na bezpieczeństwo produktu.

15. Dokumentacja techniczna i dowody zgodności

Dla produktów objętych CRA BRAGER Sp. z o.o. utrzymuje dokumentację techniczną umożliwiającą wykazanie spełnienia wymagań cyberbezpieczeństwa. Dokumentacja jest aktualizowana przy istotnych zmianach produktu oraz udostępniana właściwym organom w zakresie wymaganym prawem.

Dokument / rejestr	Cel
Rejestr produktów objętych CRA	Lista produktów, wersji, wariantów i okresów wsparcia.
Ocena ryzyka produktu	Identyfikacja zagrożeń, ocena ryzyka, działania ograniczające i ryzyko resztkowe.
Rejestr zagrożeń / ryzyk	Zagrożenia, poziomy ryzyka, status działań i właściciele.
Plan minimalizacji ryzyk	Działania techniczne, organizacyjne i proceduralne wraz z terminami.
Rejestr podatności	Zgłoszenia, klasyfikacja, działania naprawcze, komunikacja, zamknięcie.
Rejestr incydentów	Zdarzenia, analiza, eskalacja, raportowanie, działania korygujące.
Dokumentacja aktualizacji	Wersje firmware, poprawki bezpieczeństwa, testy i komunikaty dla użytkowników.
Instrukcje bezpieczeństwa	Zalecenia dla użytkownika, instalatora i serwisu dotyczące bezpiecznej konfiguracji.

16. Komunikacja z użytkownikami i instalatorami

BRAGER Sp. z o.o. zapewnia użytkownikom, instalatorom i serwisowi informacje niezbędne do bezpiecznej instalacji, konfiguracji, użytkowania i aktualizacji produktu.

- instrukcja powinna wskazywać minimalne wymagania bezpieczeństwa dla instalacji i sieci;
- dla produktów z dostępem zdalnym należy opisać bezpieczne uruchomienie usługi zdalnej;
- komunikaty bezpieczeństwa powinny jasno wskazywać produkt, wersję, ryzyko, dostępny środek naprawczy i zalecane działania;
- informacje o podatnościach są ujawniane w sposób skoordynowany, tak aby ograniczać ryzyko nadużyć.

17. Monitorowanie, audyty i przeglądy

Skuteczność niniejszej Polityki podlega okresowemu monitorowaniu i przeglądom. Przegląd odbywa się nie rzadziej niż raz w roku oraz po istotnym incydencie, ujawnieniu podatności krytycznej, zmianie wymagań prawnych, zmianie architektury produktu lub zmianie portfolio produktów.

- wyniki przeglądu są dokumentowane;
- niezgodności i słabości wymagają działań korygujących;
- w razie potrzeby aktualizuje się rejestry, procedury, instrukcje i dokumentację techniczną;
- audyt może obejmować próbki produktów, kodu, dokumentacji, rejestrów podatności i incydentów.

18. Relacja do innych dokumentów

Niniejsza Polityka jest dokumentem nadrzędnym dla systemu bezpieczeństwa produktów z elementami cyfrowymi BRAGER Sp. z o.o. Dokumenty powiązane obejmują w szczególności:

- Politykę skoordynowanego ujawniania podatności (CVD);
- Procedurę zarządzania podatnościami;
- Procedurę reagowania na incydenty cyberbezpieczeństwa produktu;
- Procedurę zarządzania aktualizacjami bezpieczeństwa i firmware;

- Procedurę oceny ryzyka produktu;
- Rejestr produktów objętych CRA;
- Rejestr zagrożeń i ryzyk cyberbezpieczeństwa;
- Plan minimalizacji ryzyk;
- Instrukcję bezpiecznej konfiguracji i użytkowania produktu;
- Politykę retencji dokumentacji technicznej.

19. Postanowienia końcowe

- Polityka wchodzi w życie z dniem zatwierdzenia przez Zarząd BRAGER Sp. z o.o.
- Wszelkie odstępstwa od Polityki wymagają udokumentowania, oceny ryzyka i akceptacji osoby uprawnionej.
- Pracownicy i współpracownicy objęci zakresem Polityki są zobowiązani do jej stosowania.
- Polityka jest dokumentem wewnętrznym. Części przeznaczone dla użytkowników, instalatorów lub badaczy bezpieczeństwa mogą być publikowane zewnętrznie, jeżeli wspierają realizację wymagań CRA.
- Niniejsza Polityka nie zastępuje Polityki CVD, lecz ustanawia dla niej nadrzędne ramy bezpieczeństwa produktu.

Załącznik 1. Mapa powiązania Polityki z wymaganiami CRA

Obszar	Odniesienie w dokumencie
Obszar CRA	Realizacja w niniejszej Polityce
Ocena ryzyka cyberbezpieczeństwa	Rozdział 8; rejestr ryzyk, plan minimalizacji ryzyka, akceptacja ryzyka resztkowego.
Security by design i security by default	Rozdziały 6, 9 i 10; wymagania projektowe, minimalizacja powierzchni ataku, bezpieczne ustawienia domyślne.
Obsługa podatności	Rozdział 11; powiązanie z Polityką CVD, rejestr podatności, działania naprawcze.
Aktualizacje bezpieczeństwa	Rozdział 12; testy, komunikacja, integralność aktualizacji, okres wsparcia.
Reagowanie na incydenty i raportowanie	Rozdział 13; eskalacja, analiza, ograniczenie skutków i raportowanie zgodnie z CRA.
Dokumentacja techniczna	Rozdział 15; wymagane rejestry i dowody zgodności.
Informacje dla użytkowników	Rozdział 16; instrukcje, komunikaty bezpieczeństwa, zalecenia konfiguracji.
Nadzór nad łańcuchem dostaw	Rozdział 14; wymagania dla dostawców i komponentów.

Załącznik 2. Minimalny zakres przeglądu bezpieczeństwa produktu

- Czy produkt znajduje się w rejestrze produktów objętych CRA?
- Czy określono poziom ryzyka CRA i uzasadnienie klasyfikacji?
- Czy wykonano ocenę ryzyka produktu przed wprowadzeniem do obrotu?
- Czy określono okres wsparcia i zasady aktualizacji bezpieczeństwa?
- Czy mechanizmy dostępu są bezpieczne i pozbawione trwałych haseł domyślnych?
- Czy funkcje zdalne wykorzystują bezpieczną komunikację i kontrolę dostępu?
- Czy istnieje rejestr podatności i kanał ich zgłaszania?
- Czy krytyczne podatności i incydenty mają zdefiniowany tryb eskalacji?
- Czy instrukcja użytkownika zawiera zalecenia bezpieczeństwa?

- Czy dostawcy komponentów krytycznych są objęci wymaganiami bezpieczeństwa?
- Czy dokumentacja techniczna zawiera dowody testów, analiz i decyzji bezpieczeństwa?

Opracował	**Sprawdził**	**Zatwierdził**
GFLEAN Data i podpis	Pełnomocnik ds. cyberbezpieczeństwa / CISO Data i podpis	Prezes Zarządu BRAGER Sp. z o.o. Data i podpis