



Załącznik nr 1: Szczegółowy opis parametrów technicznych i funkcjonalności

1. Przedmiotem zamówienia jest zakup i dostawa 100 sztuk fabrycznie nowych, nieużywanych, wolnych od wad fizycznych szyfrowanych nośników danych.
2. Wykonawca zrealizuje przedmiot zamówienia w terminie **do 30 listopada 2026 roku**.
3. Wykonawca zobowiązuje się realizować przedmiot zamówienia zgodnie z zasadą Do No Significant Harm (DNHS), o której mowa w art. 17 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2020/852 Zamawiający zobowiązuje Wykonawcę do postępowania zgodnie z zasadą DNSH (z ang. „Do No Significant Harm” – tzn. Nie Czyń Znaczącej Szkody) dot. niewspierania ani nieprowadzenia działalności gospodarczej, która czyni znaczące szkody dla któregośkolwiek z celów środowiskowych, w rozumieniu art. 17 rozporządzenia (UE) 2020/852 (Rozporządzenie PE i Rady UE 2020/852 z dnia 18 czerwca 2020 r. – tzw. Taksonomii), a także wymaganiami stawianymi w ramach realizacji Krajowego Planu Odbudowy i Zwiększania Odporności.
4. Wykonawca realizując przedmiot zamówienia, zobowiązuje się do postępowania z odpadami, w tym zużytym sprzętem elektronicznym, zgodnie z obowiązującymi przepisami prawa.
5. Szczegółowy opis parametrów technicznych i funkcjonalności:

Lp.	Parametr	Wymaganie minimalne
1.	Pojemność i Nośnik	Minimum 2 TB, technologia półprzewodnikowa SSD.
2.	Szyfrowanie	Sprzętowe szyfrowanie danych min. AES-XTS 256-bit z koprocesorem.
3.	Certyfikacja bezpieczeństwa	Minimum FIPS 140-2 Level 3, FIPS 140-3 Level 3 lub FIPS 197 .
4.	Sposób Autoryzacji	Odblokowanie (autoryzacja) realizowane przez: - fizyczną klawiaturę numeryczną na obudowie, LUB - wbudowany ekran dotykowy, LUB - czytnik biometryczny, LUB - dedykowaną aplikację producenta (OS Windows/macOS).



5.	Ochrona (IP)	Odporność środowiskowa minimum IP67 (dopuszcza się certyfikaty IP54/IP57/IP64 pod warunkiem dołączenia do zestawu ochronnego, dedykowanego etui pancernego/silikonowego).
6.	Anti-Brute Force	Automatyczne wymazanie klucza szyfrującego (Crypto-Erase) po maks. 15 błędnych próbach logowania.
7.	Zabezpieczenie fizyczne (Tamper-proof)	Płytką drukowaną zalaną twardą żywicą epoksydową lub zastosowanie obudowy ze śladami ingerencji uniemożliwiającej ukryte otwarcie urządzenia.
8.	Kompatybilność	Wsparcie i prawidłowe działanie dla systemów operacyjnych Windows 11 oraz macOS .
9.	Gwarancja	Minimum 5 lat

6. Produkt musi pochodzić z oficjalnego kanału dystrybucji producenta na rynek Unii Europejskiej. Dostarczony sprzęt musi posiadać oznaczenie CE. Sprzęt musi być dostarczony w oryginalnym, fabrycznie zamkniętym opakowaniu producenta.

Zamówienie dofinansowane ze środków Unii Europejskiej, Krajowego Planu Odbudowy i Zwiększania Odporności finansowanego ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności; Inwestycja: C3.1.1.

Cyberbezpieczeństwo - CyberPL , infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo; Cyberbezpieczeństwo - Cyberbezpieczny Rząd – w ramach projektu pn. „Cyberbezpieczeństwo w PIP”, na podstawie porozumienia o powierzenie grantu o numerze KPOD.05.10- CR.01-001/24/0036/KPOD.05.10-CR.01-001/25/2025