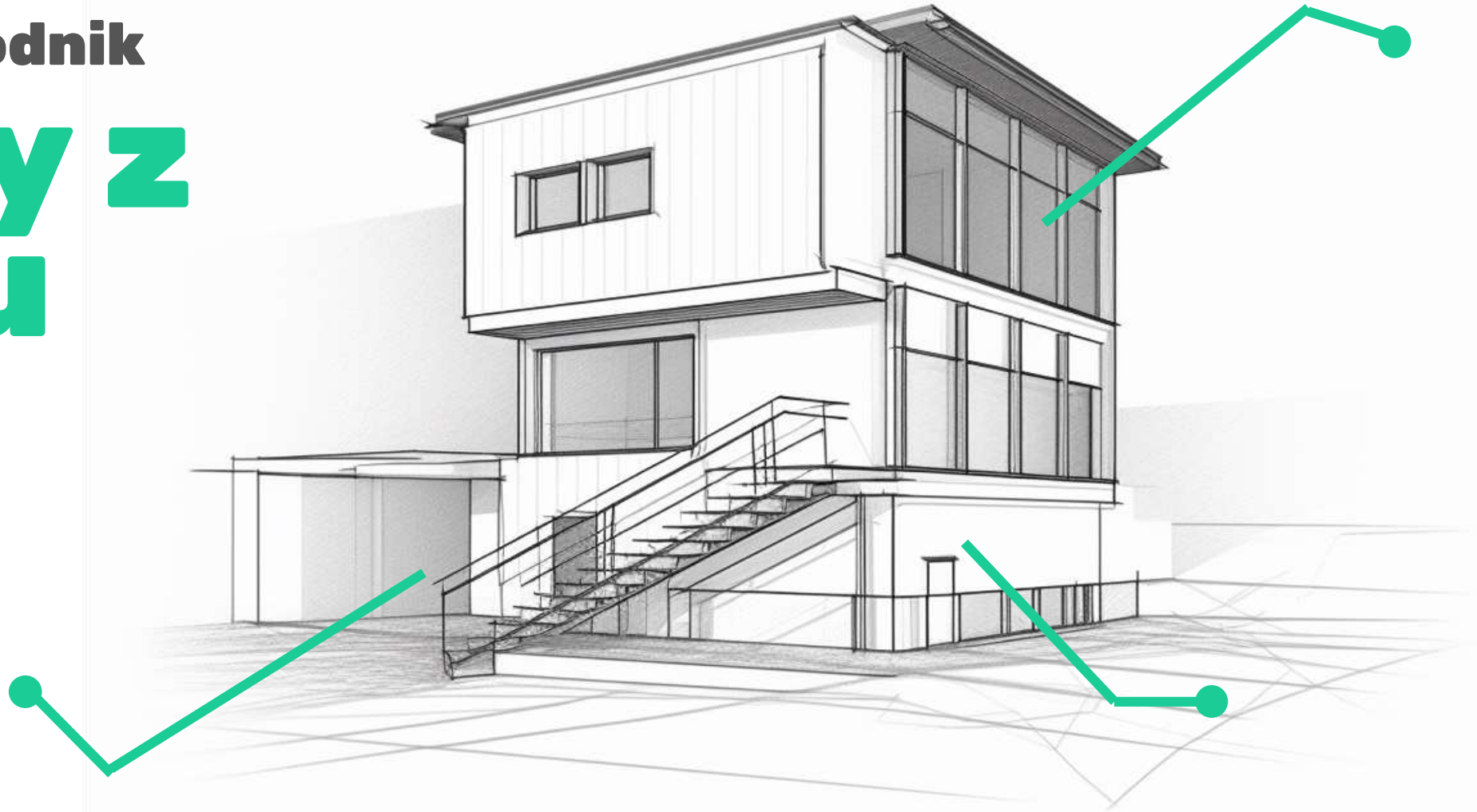
CYBEREADY

Twój przewodnik

pracy z domu



CYBEREADY

Praca zdalna całkowicie redefiniuje krajobraz bezpieczeństwa.
Pokażemy ci, jak zachować bezpieczeństwo w następujących kwestiach:

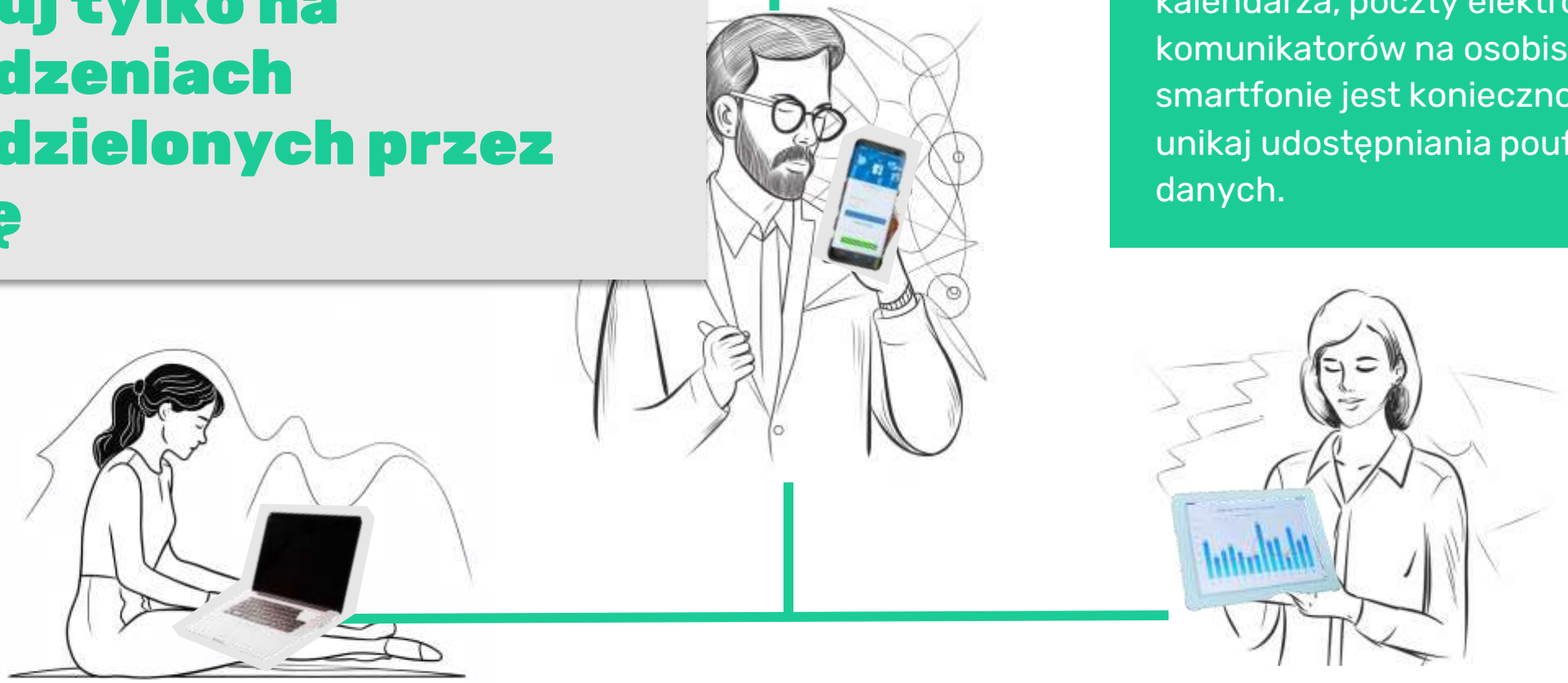
1. Hasło do Wi-Fi
2. Urządzenia
3. Przestrzeńrobocza
4. Podróżowanie
5. Wsparcie techniczne
6. Wsparcie bezpieczeństwa

CYBEREADY

Zrezygnuj z domyślnego hasła do sieci Wi-Fi

Hakerzy mogą łatwo wykorzystać domyślne hasła, przez co router jest narażony na ataki. Pamiętaj, aby ustawić silne hasło składające się z ponad 12 znaków.

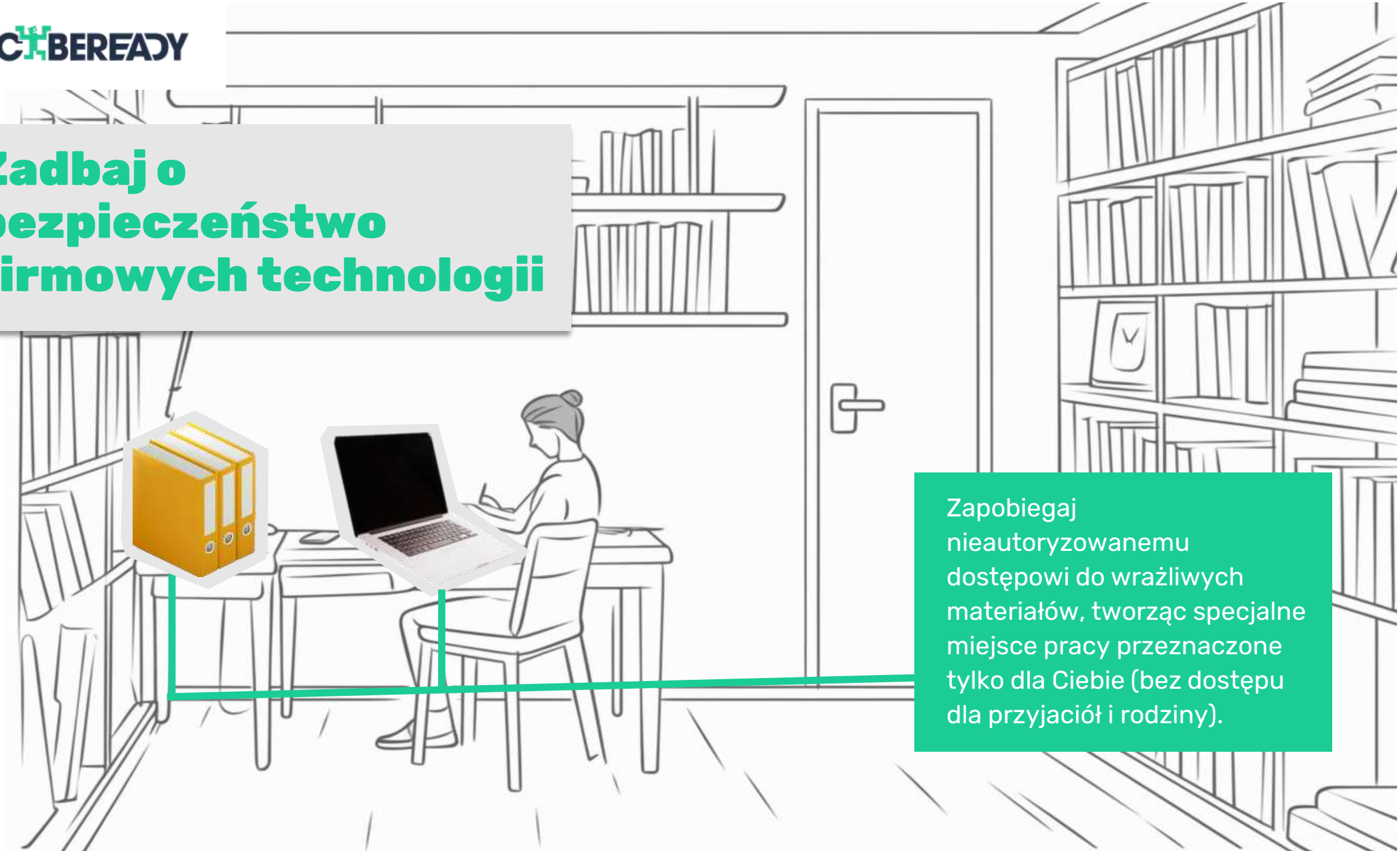
Pracuj tylko na urządzeniach przydzielonych przez firmę



Urządzenia osobiste to nie miejsce na dokumenty związane z pracą! (Zazwyczaj nie mają one solidnych zabezpieczeń). Jeśli dostęp do kalendarza, poczty elektronicznej i komunikatorów na osobistym smartfonie jest koniecznością, unikaj udostępniania poufnych danych.

CYBEREADY

Zadbaj o bezpieczeństwo firmowych technologii

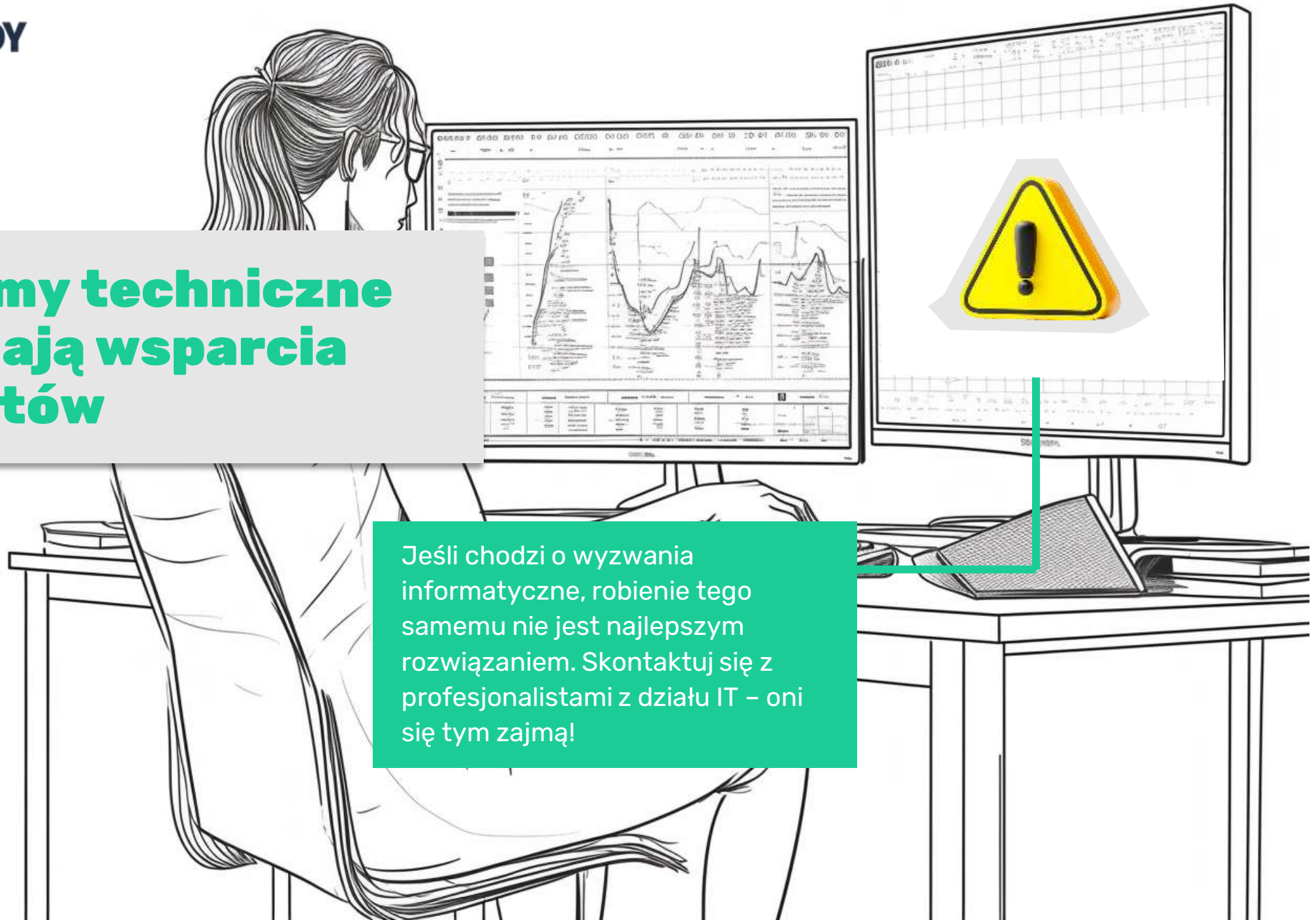


Zapobiegaj nieautoryzowanemu dostępowi do wrażliwych materiałów, tworząc specjalne miejsce pracy przeznaczone tylko dla Ciebie (bez dostępu dla przyjaciół i rodziny).

Chroń swoje urządzenia podczas podróży

Opuszczasz dom na co najmniej 48 godzin? Przechowuj bezpiecznie urządzenia robocze lub zapewnij im ochronę na czas podróży.

Problemy techniczne wymagają wsparcia ekspertów



Jeśli chodzi o wyzwania informatyczne, robienie tego samemu nie jest najlepszym rozwiązaniem. Skontaktuj się z profesjonalistami z działu IT – oni się tym zajmą!

CYBEREADY

Masz obawy o bezpieczeństwo? Skontaktuj się z nami.

Bez obaw! Zespół ds. bezpieczeństwa służy Ci pomocą. Wiemy, jak zabezpieczyć Twoje urządzenia i dane, niezależnie od scenariusza.