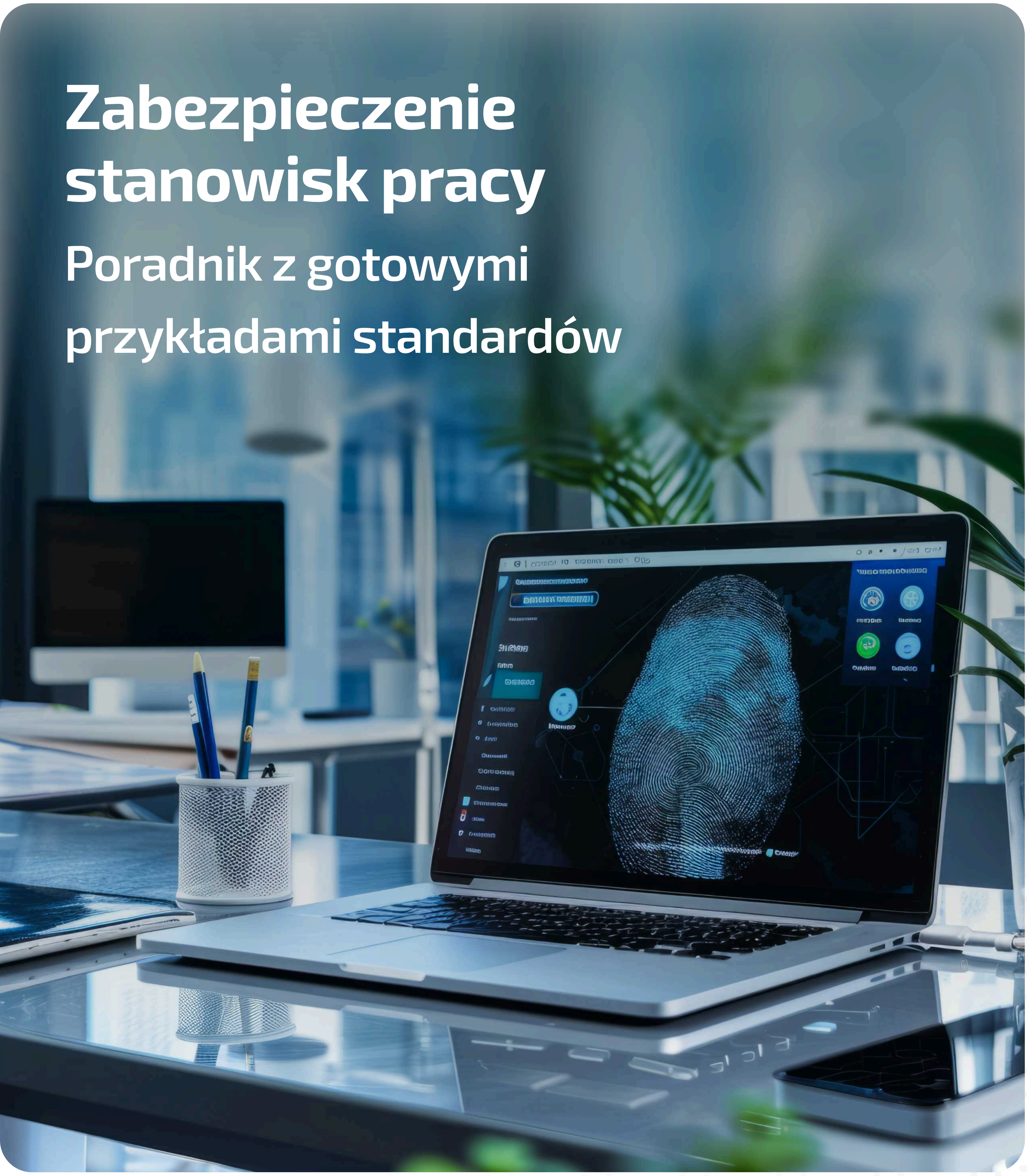
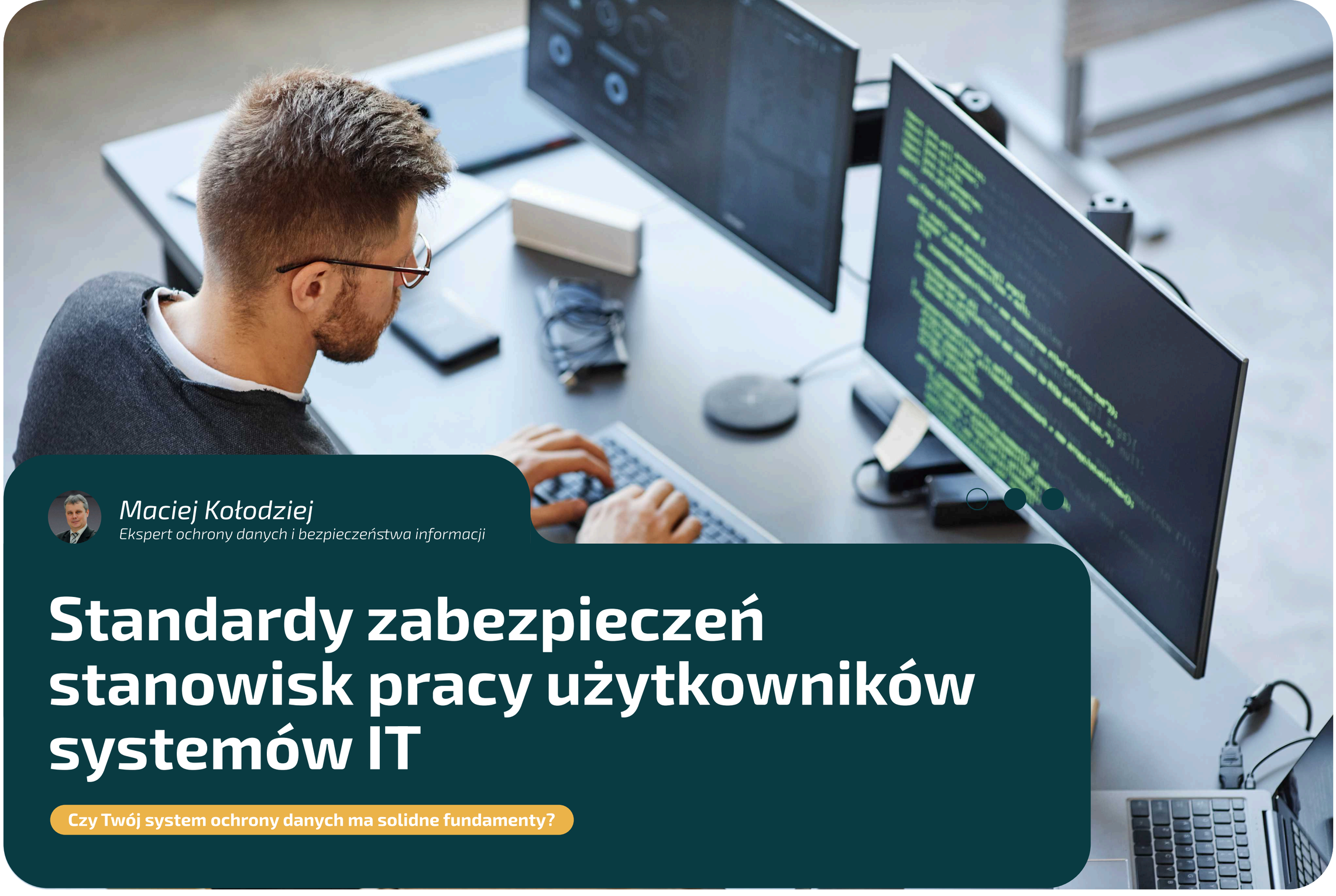
# Zabezpieczenie stanowisk pracy

## Poradnik z gotowymi przykładami standardów



LexDigital

lexdigital.pl






*Maciej Kołodziej*
*Ekspert ochrony danych i bezpieczeństwa informacji*


# Standardy zabezpieczeń stanowisk pracy użytkowników systemów IT

**Czy Twój system ochrony danych ma solidne fundamenty?**

W ostatnich latach, ze względu na rozwój technologii, przejście wielu podmiotów na hybrydowe modele funkcjonowania, upowszechnienie się pracy zdalnej z wykorzystaniem urządzeń służbowych i prywatnych oraz outsourcing operacyjny **pojawiła się konieczność przeglądu stosowanych i zaprojektowania nowych rozwiązań w zakresie bezpieczeństwa teleinformatycznego.** Projektanci i administratorzy systemów IT zapewniają jakość oraz nadzór nad zasobami i konfigurację systemów w skład których wchodzą serwery, infrastruktura, aplikacje i oferowane usługi. Z systemów tych korzystają użytkownicy – zarówno zewnętrzni (klienci), jak i wewnętrzni  (pracownicy i współpracownicy). **Projektanci rozwiązań powinni jednak zadbać także o odpowiedni poziom bezpieczeństwa urządzeń końcowych, które z tych zasobów korzystają, mają dostęp do przetwarzanych informacji i systemów lub są wykorzystywane w procesach wewnętrznych podmiotów.**

Każde stosowane urządzenie końcowe, stacjonarne lub mobilne, np. komputer, tablet, telefon komórkowy oraz urządzenia sieciowe, np. routery wykorzystywane przez użytkowników wewnętrznych, powinno zapewniać ochronę informacji adekwatną do jego roli w infrastrukturze i sposobu przetwarzania danych.

Poziom bezpieczeństwa i stawiane urządzeniom wymagania powinny być zależne od sposobu i celu wykorzystywania oraz jego wpływu na przetwarzane informacje. Podmiot powinien opracować wymagania dotyczące minimalnych standardów zabezpieczeń dla urządzeń końcowych oraz zapewnić kompleksowe wdrożenie i możliwość nadzoru nad ich stosowaniem. Standardy te, w uzasadnionych przypadkach, mogą być uzupełniane o dodatkowe wymagania gwarantujące wyższy poziom ochrony istotnych dla podmiotu urządzeń, zasobów lub osób.

Nie każde urządzenie wykorzystywane w infrastrukturze może być zarządzane przez podmiot i jego własny personel techniczny, gdyż w celu realizacji obowiązków służbowych albo świadczenia usług na rzecz podmiotu używane są również urządzenia prywatne lub należące do innych podmiotów. Dlatego zalecamy, aby obowiązujące standardy bezpieczeństwa stanowiły obowiązkowy element specyfikujący wymagania techniczno-organizacyjne w zawieranych z pracownikami lub podwykonawcami umowach oraz aby stosowanie się do tych standardów mogło być przez zleceniodawcę weryfikowane, w ramach wykonywanych testów lub dzięki otrzymywanym informacji i oświadczeń o ich stosowaniu.

## Podstawy prawne

Wśród istotnych regulacji dotyczących konfiguracji i zabezpieczeń stosowanych w urządzeniach wykorzystywanych do przetwarzania danych wskazać należy:

**Rozporządzenie o ochronie danych osobowych (RODO)**, które w art. 25 i 32 zaleca stosowanie zabezpieczeń adekwatnych do wagi zagrożeń, aby skutecznie chronić dane i zapewnić ich poufność, integralność i dostępność na każdym etapie przetwarzania.

**Dyrektywę NIS2**, drugą odsłonę regulacji unijnej dotyczącej bezpieczeństwa siecii informacji. W motywach preambuły znalazły się między innymi zapisy dotyczące konieczności stosowania odpowiednich zabezpieczeń przed cyberzagrożeniami, podnoszeniu świadomości i czujności personelu w kwestiach dotyczących ochrony informacji oraz odpowiedniej konfiguracji urządzeń, za pomocą których informacja jest przetwarzana.

**Rozporządzenie w sprawie operacyjnej odporności cyfrowej (DORA)**, które określa ramy kompleksowego zarządzania ryzykiem cyfrowym na rynkach finansowych i nakłada obowiązek ochrony urządzeń (sprzętu) jako części zasobów ICT (ang. Information and Communication Technologies). W ramach zarządzania ryzykiem wymagane jest wdrożenie środków technicznych i organizacyjnych, które mają na celu ochronę wszystkich zasobów informacyjnych i ICT, w tym w szczególności przetwarzanych danych i sprzętu (np. serwerów i urządzeń końcowych)

**Rozporządzenie w sprawie Krajowych Ram Interoperacyjności (KRI)**, będące jednym z aktów wykonawczych do Ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, w którym zawarte zostały najważniejsze wymagania stawiane przed podmiotami świadczącymi elektroniczne usługi w przestrzeni publicznej. W Rozdziale 4 powołano minimalne wymagania dla systemów teleinformatycznych, z których część realizowana powinna być poprzez odpowiednią konfigurację urządzeń i stanowisk roboczych.

**Ustawę o Krajowym Systemie Cyberbezpieczeństwa (UKSC)** nakładającą na podmioty objęte krajowym systemem cyberbezpieczeństwa obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych adekwatnych do ryzyka, które mają zapewnić bezpieczeństwo

systemów informacyjnych, (w tym urządzeń ICT). Decyzje o doborze środków podejmuje kierownictwo podmiotu.

**Normy ISO 27001 i 27002**, które przewidują konieczność odpowiedniego przygotowania podmiotu do ochrony informacji, a w klauzulach dotyczących bezpieczeństwa fizycznego (zabezpieczenia w sekcji 7) oraz technologicznego (zabezpieczenia wymienione w sekcji 8) wskazują na konieczność przeprowadzania analiz i stosowania odpowiednich zabezpieczeń w systemach teleinformatycznych, na urządzeniach oraz podczas wykonywania operacji przetwarzania informacji

## Realizacja praktyczna

Analizując rodzaje, cechy i parametry urządzeń wykorzystywanych najczęściej przez użytkowników systemów IT (pracowników, współpracowników, kontraktorów i innych podwykonawców) na stanowiskach pracy należy wskazać na sześć kategorii, które powinny podlegać standaryzacji w zakresie konfiguracji sprzętu i oprogramowania:

**Komputery stacjonarne i przenośne, wyposażone w system operacyjny:**

- Windows
- macOS
- Linux

**Telefony komórkowe oraz tablety, działające pod kontrolą systemu operacyjnego:**

- Android
- iOS

**Urządzenia sieciowe zapewniające dostęp do sieci Internet**

- routery i access pointy WiFi

**Każda z wymienionych kategorii urządzeń powinna zostać przeanalizowana pod kątem oczekiwań funkcjonalnych, wydajności i wymagań w zakresie cyberbezpieczeństwa, ze szczególnym uwzględnieniem:**

- wersji systemu operacyjnego
- szyfrowania nośników danych
- zarządzania kontami użytkowników lokalnych
- ochrony przed złośliwym oprogramowaniem
- zasad instalowania oprogramowania
- komunikacji w sieciach komputerowych
- ochrony dostępu do danych i konsoli urządzenia
- wykonywania niezbędnych kopii zapasowych systemu, konfiguracji i danych,
- zgodności z obowiązującymi przepisami prawa i innymi wymaganiami, do których stosowania podmiot jest zobowiązany

a wyniki powinny zostać uwzględnione w wewnętrznych standardach bezpieczeństwa.

Mając na uwadze konieczność kompleksowego i spójnego nadzoru nad całością infrastruktury podmiotu oraz unifikację procesów bezpieczeństwa systemów zalecamy zobowiązanie wszystkich użytkowników do stosowania opracowanych standardów, wdrażając je na urządzeniach własnych oraz zapewniając ich implementację na pozostałym sprzęcie wykorzystywanym w celach służbowych, który nie jest zarządzany przez personel IT podmiotu.

Na kolejnych stronach przedstawiamy przykładowe zestawy wymagań dla poszczególnych kategorii urządzeń, które mają charakter katalogów otwartych, aby każdy podmiot mógł uwzględnić środki optymalne, wynikające z przeprowadzonej analizy ryzyk oraz potrzeb organizacyjnych i możliwości technicznych.


# 1 Standardowe wymagania bezpieczeństwa dla komputerów działających pod kontrolą systemu operacyjnego Microsoft Windows

## Sprzęt:

- 8GB RAM, procesor zgodny z TPM w wersji 2.0
- BIOS/UEFI: ochrona hasłem administratora, włączona opcja Secure Boot

## System operacyjny:

- Windows 11 lub Windows 10 (zalecana wersja Professional)
- zainstalowane najnowsze aktualizacje i poprawki bezpieczeństwa
- włączona automatyczna aktualizacja systemu
- wsparcie techniczne, aktywny support i aktualizacje dostarczane przez Microsoft

## Ochrona zawartości lokalnych nośników danych

- szyfrowanie dysków i nośników z wykorzystaniem BitLocker, Full Disk Encryption, zachowanie kopii klucza odzyskiwania BitLocker (np. na koncie Microsoft)
- stosowanie VeraCrypt w Windows Home jako alternatywy dla BitLocker, zachowanie kopii haseł do ukrytych partycji lub kontenerów danych
- wykonywanie niezbędnych kopii zapasowych (przez sieć lub na nośniki lokalne)

## Oprogramowanie użytkowe:

- program antywirusowy (+ sieciowa konsola zarządzania, jeśli jest dostępna)
- archiwizator plików (dla kryptograficznej ochrony dokumentów, np. 7-Zip)
- klient VPN zgodny ze standardem organizacji (urządzenia pracujące z zewnątrz)
- bezpieczna konfiguracja aplikacji, aby korzystały tylko z połączeń szyfrowanych
- wymóg instalowania programów z zaufanych źródeł

## Konta użytkowników

- brak lokalnych kont niechronionych hasłem
- osobne konta służbowe i prywatne
- rozdzielenie funkcji użytkownika standardowego i administratora urządzenia
- okresowa zmiana silnych haseł, zgodnie z ustalonymi w organizacji zasadami
- połączenie z usługą katalogową (jeśli to możliwe, np. Active Directory)
- weryfikacja dwuskładnikowa (2FA) dla kont Microsoft (jeśli możliwe)
- zachowanie kopii hasła do konta administratora

## Wygaszacz ekranu:

- blokada po 15 minutach braku aktywności użytkownika
- do odblokowania wymagana autentykacją (PIN, hasło lub biometria)

## Funkcje sieciowe

- skonfigurowany lokalny firewall filtrujący cały ruch wejściowy, z wyjątkami ustalonymi w organizacji
- zalecane korzystanie z zaufanych sieci LAN i WLAN (także z własnego telefonu)

## Inne:

- włączona ochrona korzystania aplikacji z kamery i mikrofonu
- korzystanie z blokady fizycznej urządzeń przenośnych (np. linka zabezpieczająca typu Kensington Lock)

## 2 Standardowe wymagania bezpieczeństwa dla komputerów działających pod kontrolą systemu operacyjnego macOS

### Sprzęt:

- 8GB RAM, procesor Apple Silicon M
- chroniona hasłem sprzętowym blokada dostępu do trybu recoveryOS

### System operacyjny:

- zalecana najnowsza wersja (Sonoma 14 lub Sequoia 15)
- zainstalowane najnowsze aktualizacje i poprawki bezpieczeństwa
- włączona automatyczna lub zarządzana w organizacji aktualizacja systemu
- wsparcie techniczne, aktywny support i aktualizacje dostarczane przez Apple

### Ochrona zawartości lokalnych nośników danych

- szyfrowanie dysków i nośników z wykorzystaniem FileVault, Full Disk Encryption, zachowanie kopii klucza odzyskiwania FileVault (np. w Pęku kluczy Apple)
- stosowanie VeraCrypt jako alternatywy dla FileVault dla nośników zewnętrznych, zachowanie kopii haseł do ukrytych partycji lub kontenerów danych
- wykonywanie niezbędnych kopii zapasowych (przez sieć lub na nośniki lokalne)

### Oprogramowanie użytkowe:

- program antywirusowy (+ sieciowa konsola ochrony dokumentów, np. 7-Zip)
- archiwizator plików (dla kryptograficznej ochrony dokumentów, np. 7-Zip)
- klient VPN zgodny ze standardem organizacji (urządzenia pracujące z zewnątrz)
- bezpieczna konfiguracja aplikacji, aby korzystały tylko z połączeń szyfrowanych
- wymóg instalowania programów z zaufanych źródeł

### Konta użytkowników

- brak lokalnych kont niechronionych hasłem
- osobne konta służbowe i prywatne
- rozdzielenie funkcji użytkownika standardowego i administratora urządzenia
- okresowa zmiana silnych haseł, zgodnie z ustalonymi w organizacji zasadami
- weryfikacja dwuskładnikowa (2FA) dla Apple ID
- zachowanie kopii hasła do konta administratora

### Wygaszacz ekranu:

- blokada po 15 minutach braku aktywności użytkownika
- do odblokowania wymagana autentykacją (hasło lub biometria)

### Funkcje sieciowe

- skonfigurowany lokalny firewall filtrujący cały ruch wejściowy, z wyjątkami ustalonymi w organizacji
- zalecane korzystanie z zaufanych sieci LAN i WLAN (także z własnego telefonu)

### Inne:

- włączona ochrona korzystania aplikacji z kamery i mikrofonu
- korzystanie z blokady fizycznej urządzeń przenośnych (np. linka zabezpieczająca typu CompuLocks)


## 3 Standardowe wymagania bezpieczeństwa dla komputerów działających pod kontrolą systemu operacyjnego Linux

### Sprzęt:

- 4GB RAM, procesor zgodny z TPM
- BIOS/UEFI: ochrona hasłem administratora, włączona opcja Secure Boot

### System operacyjny:

- dystrybucja systemu w stabilnej wersji, obsługiwane, aktualne jądro Linux
- stosowanie zasady minimalizacji dotyczącej instalacji tylko niezbędnego oprogramowania systemowego i użytkowego
- włączona automatyczna lub zarządzana w organizacji aktualizacja systemu
- wdrożenie harmonogramu aktualizacji systemu i oprogramowania
- reagowanie na publikowane, istotne luki w bezpieczeństwie

### Ochrona zawartości lokalnych nośników danych

- szyfrowanie dysków i nośników z wykorzystaniem LUKS (Linux Unified Key Setup), Full Disk Encryption, zachowanie kopii hasła do głównego kontenera, pliku klucza lub kopii nagłówka LUKS
- stosowanie VeraCrypt jako alternatywy dla LUKS dla nośników zewnętrznych, zachowanie kopii haseł do ukrytych partycji lub kontenerów danych
- wykonywanie niezbędnych kopii zapasowych (przez sieć lub na nośniki lokalne)

### Oprogramowanie użytkowe:

- program antywirusowy (+ sieciowa konsola zarządzania, jeśli jest dostępna)
- archiwizator plików (dla kryptograficznej ochrony dokumentów, np. 7-Zip)
- klient VPN zgodny ze standardem organizacji (urządzenia pracujące z zewnątrz)
- bezpieczna konfiguracja aplikacji, aby korzystały tylko z połączeń szyfrowanych
- wymóg instalowania programów z zaufanych źródeł

### Konta użytkowników

- brak lokalnych kont niechronionych hasłem
- osobne konta służbowe i prywatne
- ograniczenie bezpośredniego dostępu do konta administracyjnego root
- rozdzielenie funkcji użytkownika standardowego i administratora
- okresowa zmiana silnych haseł, zgodnie z ustalonymi w organizacji zasadami
- uwierzytelnienie dwuskładnikowe (2FA) dla dostępu administracyjnego
- zachowanie kopii hasła do konta root

### Wygaszacz ekranu:

- blokada po 15 minutach braku aktywności użytkownika
- do odblokowania wymagana autentykacją (PIN, hasło lub biometria)

### Funkcje sieciowe

- skonfigurowany lokalny firewall filtrujący cały ruch wejściowy, z wyjątkami ustalonymi w organizacji
- zalecane korzystanie z zaufanych sieci LAN i WLAN (także z własnego telefonu)

### Inne:

- włączona ochrona korzystania aplikacji z kamery i mikrofonu
- korzystanie z blokady fizycznej urządzeń przenośnych (np. linka zabezpieczająca typu Kensington Lock)


# 4 Standardowe wymagania bezpieczeństwa dla telefonów komórkowych oraz tabletów działających pod kontrolą systemu operacyjnego Android

## Sprzęt:

- Urządzenie oryginalne, niemodyfikowane, bez dostępu użytkownika do konta root

## System operacyjny:

- aktualny system Android (minimum w wersji 13)
- zainstalowane najnowsze aktualizacje i poprawki bezpieczeństwa
- włączona automatyczna aktualizacja systemu
- wsparcie techniczne, aktywny support i aktualizacje dostarczane przez Google

## Ochrona zawartości lokalnych nośników danych

- aktywna blokada ekranu (hasło alfanumeryczne, kod PIN, symbol lub biometria)
- włączone szyfrowanie pamięci wewnętrznej, zachowanie loginu (adres @gmail.com) i hasła konta powiązanego z urządzeniem
- szyfrowanie stosowanych kart pamięci, wykonywanie regularnych kopii danych znajdujących się na kartach pamięci ze względu na szyfrowanie sprzętowe kart, powiązane z konkretnym urządzeniem
- wykonywanie niezbędnych kopii zapasowych (GDisk lub na nośniki lokalne)

## Oprogramowanie użytkowe:

- program antywirusowy (+ sieciowa konsola zarządzania, jeśli jest dostępna)
- archiwizator plików (dla kryptograficznej ochrony dokumentów, np. 7-Zip)
- klient VPN zgodny ze standardem organizacji (urządzenia pracujące z zewnątrz)
- bezpieczna konfiguracja aplikacji, aby korzystały tylko z połączeń szyfrowanych
- wymóg instalowania programów z zaufanych źródeł i potwierdzania instalacji

## Konta użytkowników

- separacja danych służbowych i prywatnych
- zachowanie loginu (adres @gmail.com) i hasła konta powiązanego z urządzeniem

## Wygaszacz ekranu:

- blokada po 5 minutach braku aktywności użytkownika oraz ręczna
- do odblokowania wymagana autentykacją (hasło, PIN, symbol lub biometria)

## Funkcje sieciowe

- zalecane korzystanie z zaufanych sieci WLAN oraz transmisji danych operatora

## Inne:

- włączona ochrona korzystania aplikacji z kamery i mikrofonu
- opcjonalne oprogramowanie typu MDM do zarządzania i ochrony urządzenia
- wyłączenie automatycznej synchronizacji danych służbowych na prywatny GDisk

## 5 Standardowe wymagania bezpieczeństwa dla telefonów komórkowych oraz tabletów działających pod kontrolą systemu operacyjnego iOS

### Sprzęt:

- Urządzenie oryginalne, niemodyfikowane, bez Jailbreak

### System operacyjny:

- aktualny system iOS (minimum w wersji 15, w zależności od wsparcia urządzenia)
- zainstalowane najnowsze aktualizacje i poprawki bezpieczeństwa
- włączona automatyczna aktualizacja systemu
- wsparcie techniczne, aktywny support i aktualizacje dostarczane przez Apple

### Ochrona zawartości lokalnych nośników danych

- aktywna blokada ekranu (silny kod blokady ekranu, FaceID/TouchID)
- włączone szyfrowanie pamięci wewnętrznej, zachowanie loginu (Apple ID) i hasła konta iCloud powiązanego z urządzeniem
- wykonywanie niezbędnych kopii zapasowych (iCloud lub na nośniki lokalne)

### Oprogramowanie użytkowe:

- program antywirusowy (+ sieciowa konsola zarządzania, jeśli jest dostępna)
- archiwizator plików (dla kryptograficznej ochrony dokumentów, np. 7-Zip)
- klient VPN zgodny ze standardem organizacji (urządzenia pracujące z zewnątrz)
- bezpieczna konfiguracja aplikacji, aby korzystały tylko z połączeń szyfrowanych

### Konta użytkowników

- separacja danych służbowych i prywatnych
- zachowanie loginu (Apple ID) i hasła konta iCloud powiązanego z urządzeniem
- aktywna weryfikacja dwuskładnikowa (2FA) dla Apple ID

### Wygaszacz ekranu:

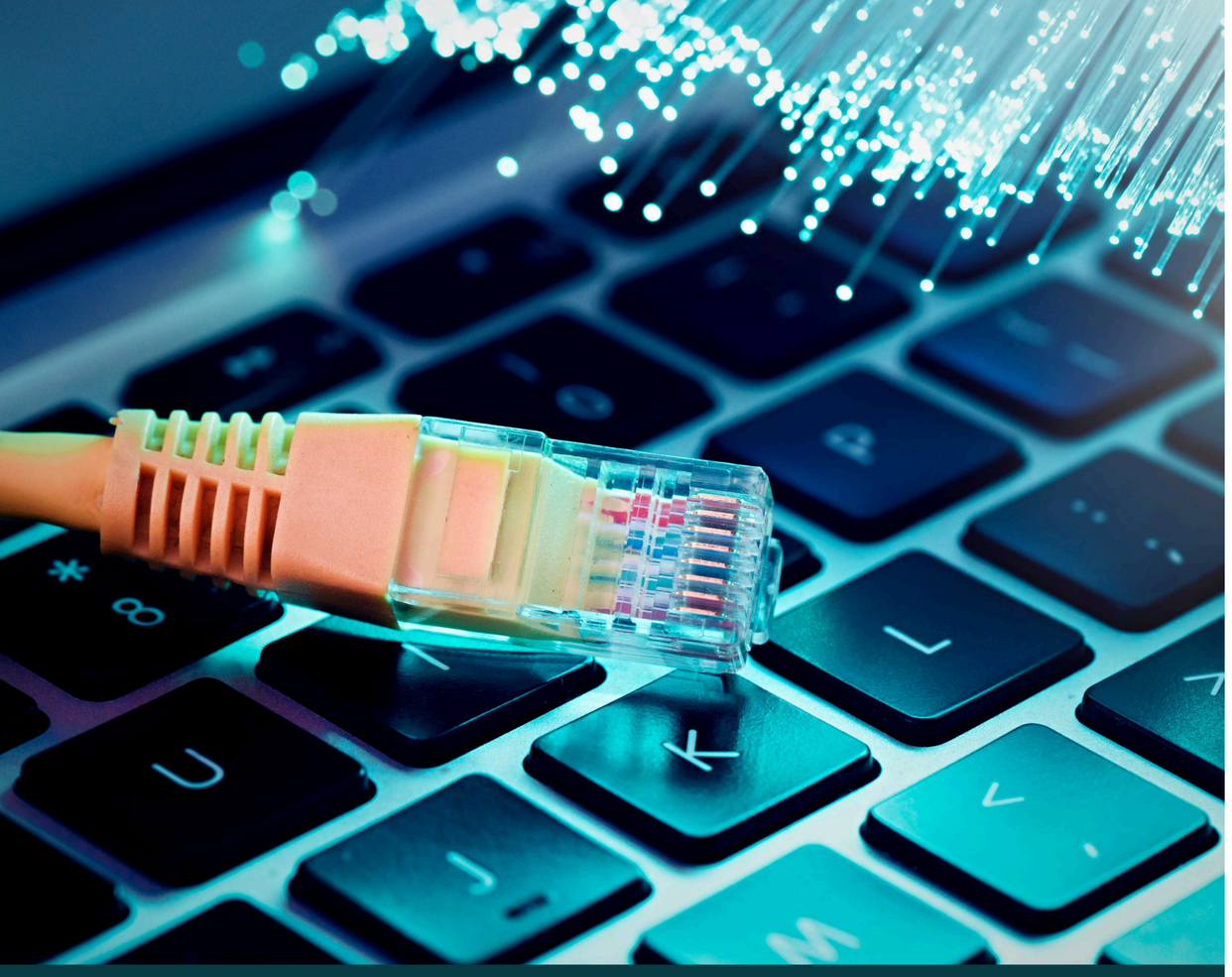
- blokada po 5 minutach braku aktywności użytkownika oraz ręczna
- do odblokowania wymagana autentykacją (kod blokady ekranu, FaceID/TouchID)

### Funkcje sieciowe

- zalecane korzystanie z zaufanych sieci WLAN oraz transmisji danych operatora

### Inne:

- włączona ochrona korzystania aplikacji z kamery i mikrofonu
- opcjonalne oprogramowanie typu MDM do zarządzania i ochrony urządzenia
- wyłączenie automatycznej synchronizacji danych służbowych na prywatny iCloud



## 6 Standardowe wymagania bezpieczeństwa dla urządzeń sieciowych, z których użytkownicy korzystają podczas łączenia z siecią Internet

### Sprzęt:

- [x] korzystanie z routerów i access pointów WiFi zarządzanych przez użytkownika lub na jego polecenie

### System operacyjny:

- [x] najnowszy system operacyjny urządzenia (gdy jest możliwość aktualizacji)
- [x] wykonywanie kopii zapasowych konfiguracji urządzeń

### Konta użytkowników

- [x] zmiana domyślnych haseł do kont administracyjnych urządzeń
- [x] zachowanie kopii haseł do kont administracyjnych

### Funkcje sieciowe

- [x] skonfigurowany na routerach firewall filtrujący cały ruch wejściowy, z wyjątkami ustalonymi w organizacji
- [x] konfiguracja access pointów do bezpiecznej komunikacji WiFi (WPA2-PSK, WPA3-Personal) z silnymi hasłami, rozgłaszanym SSID i ograniczeniem dostępu do wskazanych urządzeń bezprzewodowych

## Podsumowanie:

Bezpieczeństwo systemów IT zależy od wielu czynników i ich elementów. Dbałość o odpowiednią konfigurację, wyposażenie i eksploatację urządzeń końcowych, z których korzystają pracownicy i współpracownicy mający dostęp do aplikacji, repozytoriów danych i komponentów systemowych, pozwala na podniesienie poziomu ochrony informacji oraz zmniejsza ryzyka występowania nieprawidłowości w całym systemie IT.

Zagrożenia pochodzące z urządzeń końcowych mogą mieć istotny wpływ na przetwarzane informacje, doprowadzając do nieprawidłowości w ich treści, powodując wycieki lub utratę kontroli nad danymi, wpływając na ich poufność i dostępność. Aby temu zapobiec konieczne są systematyczne i kompleksowe działania w zakresie cyberbezpieczeństwa i wdrażanie rozwiązań zmniejszających prawdopodobieństwo wystąpienia nieprawidłowości i ewentualnych incydentów. Wprowadzenie spójnych wymagań dotyczących wszystkich, nie tylko firmowych urządzeń mających dostęp do systemów pozwala na podniesienie jakości ochrony i ułatwia zarządzanie infrastrukturą teleinformatyczną całej organizacji.

Postępowanie takie pozwala wykazać podmiotom staranność w działaniu i dbałość o wszystkie elementy systemów oraz wpływa na świadomość cyberbezpieczeństwa użytkowników, dlatego standaryzacja oraz zobowiązanie użytkowników do stosowania obowiązujących wymogów bezpieczeństwa podczas korzystania ze wszystkich rodzajów urządzeń jest praktyką zalecano i przynoszącą wymierne, pozytywne efekty dla ochrony informacji.




# Dziękujemy za przeczytanie naszego newslettera!

Masz pytania?

SKONTAKTUJ SIĘ Z NAMI