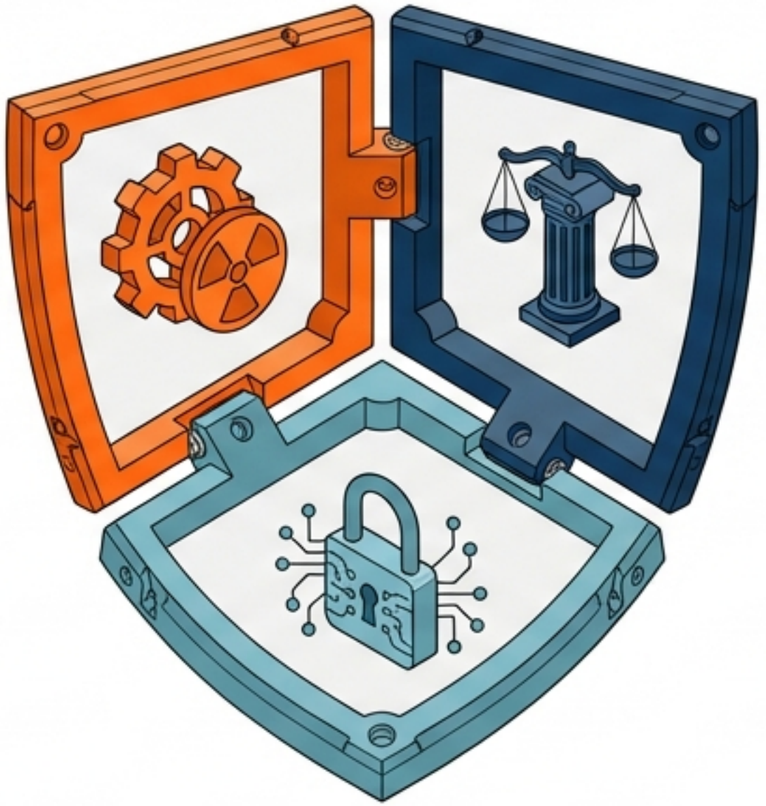
Technical editorial and Swiss International Style



Bezpieczeństwo w Teleinformatyce: Ludzie, Sprzęt i Dane

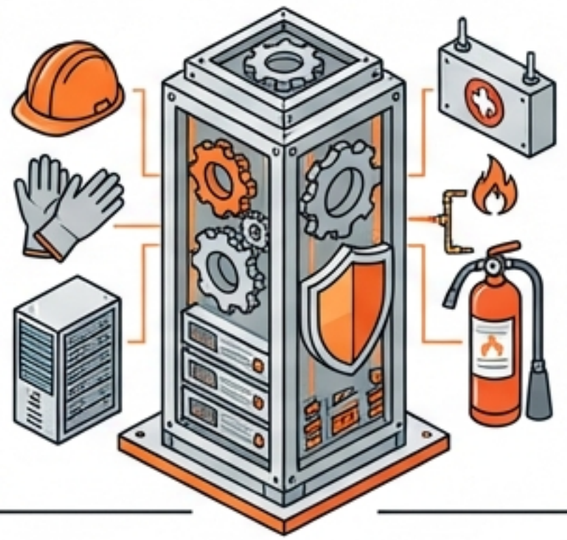
Kompendium wiedzy do egzaminu INF.08 i praktyki zawodowej

Materiał edukacyjny dla przyszlych techników teleinformatyków

Profesjonalny teleinformatyk nie tylko naprawia sprzęt – on zarządza ryzykiem

1. Strefa Fizyczna (BHP)

Ochrona życia, zdrowia i infrastruktury sprzętowej.

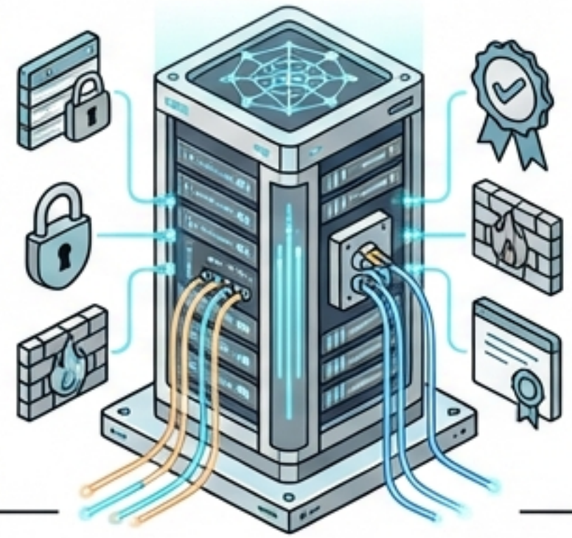


2. Strefa Prawna (Legislacja)

Zgodność z Kodeksem Pracy, RODO i prawem UE.

3. Strefa Systemowa (Standardy)

Wdrażanie norm ISO i procedur cyberbezpieczeństwa.



Bezpieczeństwo to system naczyń połączonych. Zaniedbanie w strefie fizycznej prowadzi do naruszeń w strefie prawnej.

Zagrożenia krytyczne: Prąd i Ogień

Elektryka

- **Zagrożenia:** Uszkodzone przewody, brak uziemienia, zwarcia, wilgoć.
- **Skutki:** Porażenie, oparzenia, trwałe uszkodzenie urządzeń.
- **Profilaktyka:** Kontrola izolacji, wyłączanie zasilania przed pracą, stosowanie zabezpieczeń różnicowoprądowych.

Pożar / Termika

- **Zagrożenia:** Przegrzewanie podzespołów, przeciążenia sieci, złe chłodzenie.
- **Skutki:** Pożar, dym, całkowita utrata infrastruktury i danych.
- **Profilaktyka:** Regularne czyszczenie (kurz), sprawna wentylacja, znajomość procedur ppoż.

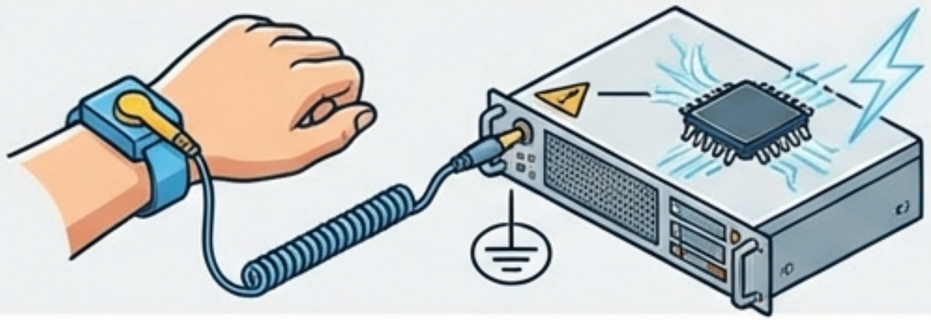
Codzienne ryzyko: Mechanika i Chemia w serwerowni

Zagrożenia mechaniczne (Szafy Rack)

- Ostre krawędzie obudów, ciężkie urządzenia (UPS, serwery), praca na drabinie.
- **Profilaktyka:** Rękawice ochronne, stabilne obuwie, technika bezpiecznego podnoszenia.

Zagrożenia chemiczne

- Kontakt ze środkami czyszczącymi i rozpuszczalnikami.
- **Profilaktyka:** Dobra wentylacja pomieszczenia, stosowanie rękawic, czytelne oznaczenia pojemników.

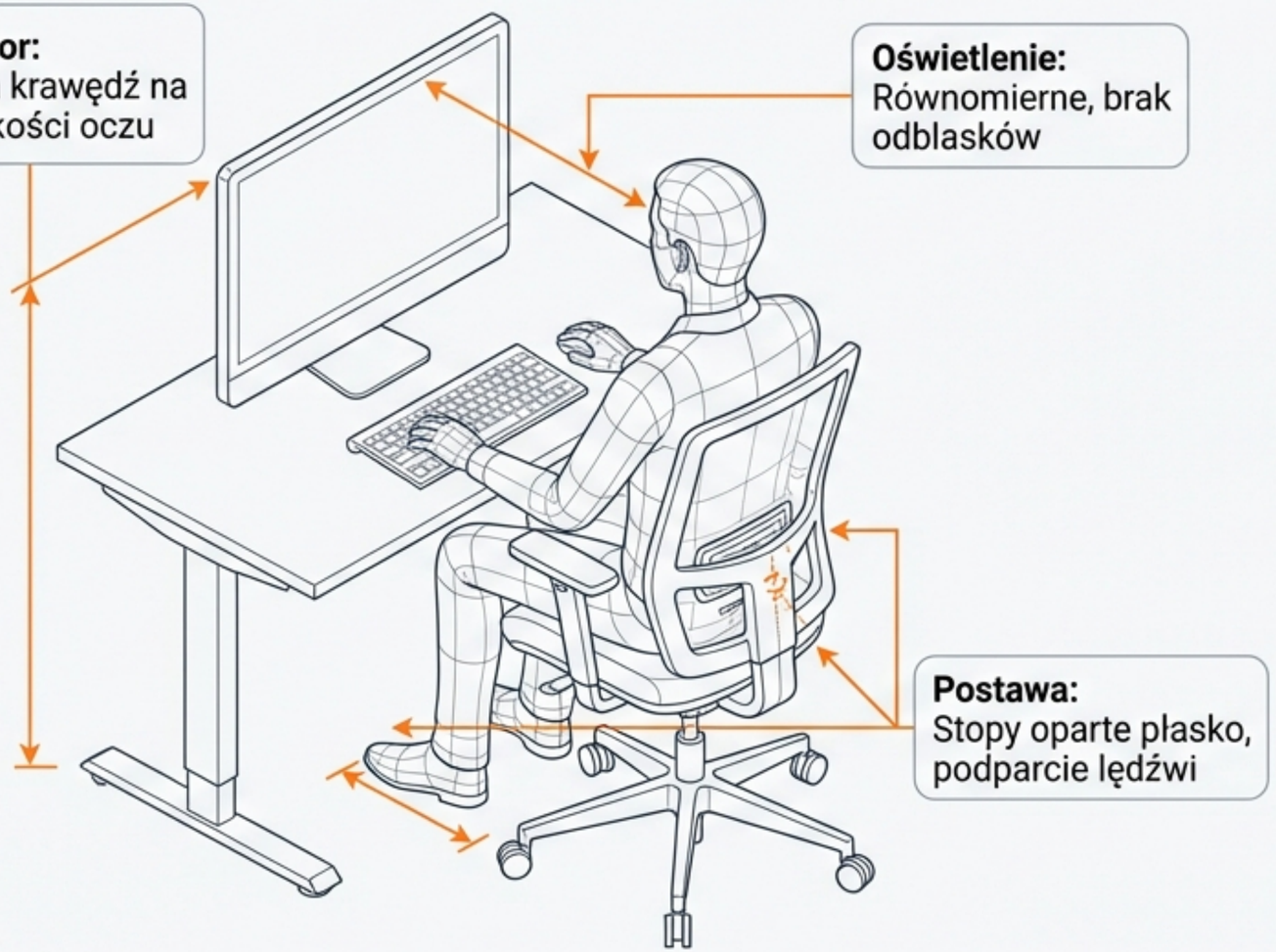


ESD (Wyładowania elektrostatyczne)

- Niewidoczne dla oka, zabójcze dla elektroniki.
- **Ochrona**: Opaski uziemiające, maty antystatyczne.

Czynnik ludzki: Ergonomia i zdrowie długofalowe

Praca teleinformatyka to często godziny spędzone w wymuszonej pozycji.



Czynniki uciążliwe

- Hałas (szum wentylatorów serwerowych)
- Długotrwałe siedzenie (obciążenie kręgosłupa)
- Praca przy monitorze ekranowym (zmęczenie wzroku)

Kodeks Pracy i normy BHP nakładają szczegółowe wymagania dotyczące stanowisk przy monitorach.

Zarządzanie ryzykiem: Uniwersalny proces

Niezależnie czy chronisz człowieka, czy dane, proces jest ten sam.

1. Identyfikacja

Co nam zagraża?

2. Ocena

Prawdopodobieństwo i skutki

3. Profilaktyka

Dobór środków ochrony

Ocena ryzyka zawodowego to obowiązek pracodawcy, ale świadomość ryzyka to obowiązek pracownika.

Fundament Prawny: Kodeks Pracy i obowiązki

Podstawa prawna: **Konstytucja RP** (Art. 66) → **Kodeks Pracy** (Dział X)

Pracodawca

- Zapewnienie bezpiecznych warunków pracy

- Przeprowadzenie oceny ryzyka zawodowego

- Organizacja szkoleń BHP

- Konsultacje z pracownikami

Pracownik

- Prawo do bezpiecznych warunków

- Obowiązek przestrzegania przepisów BHP

- Udział w szkoleniach i instruktażach

Ochrona danych: RODO (GDPR) w praktyce

Bezpośrednio obowiązujące rozporządzenie UE regulujące przetwarzanie danych.

Incydenty

Obowiązek zgłaszania naruszeń w ciągu 72 godzin.

Minimalizacja

Zbieramy tylko te dane, które są niezbędne.

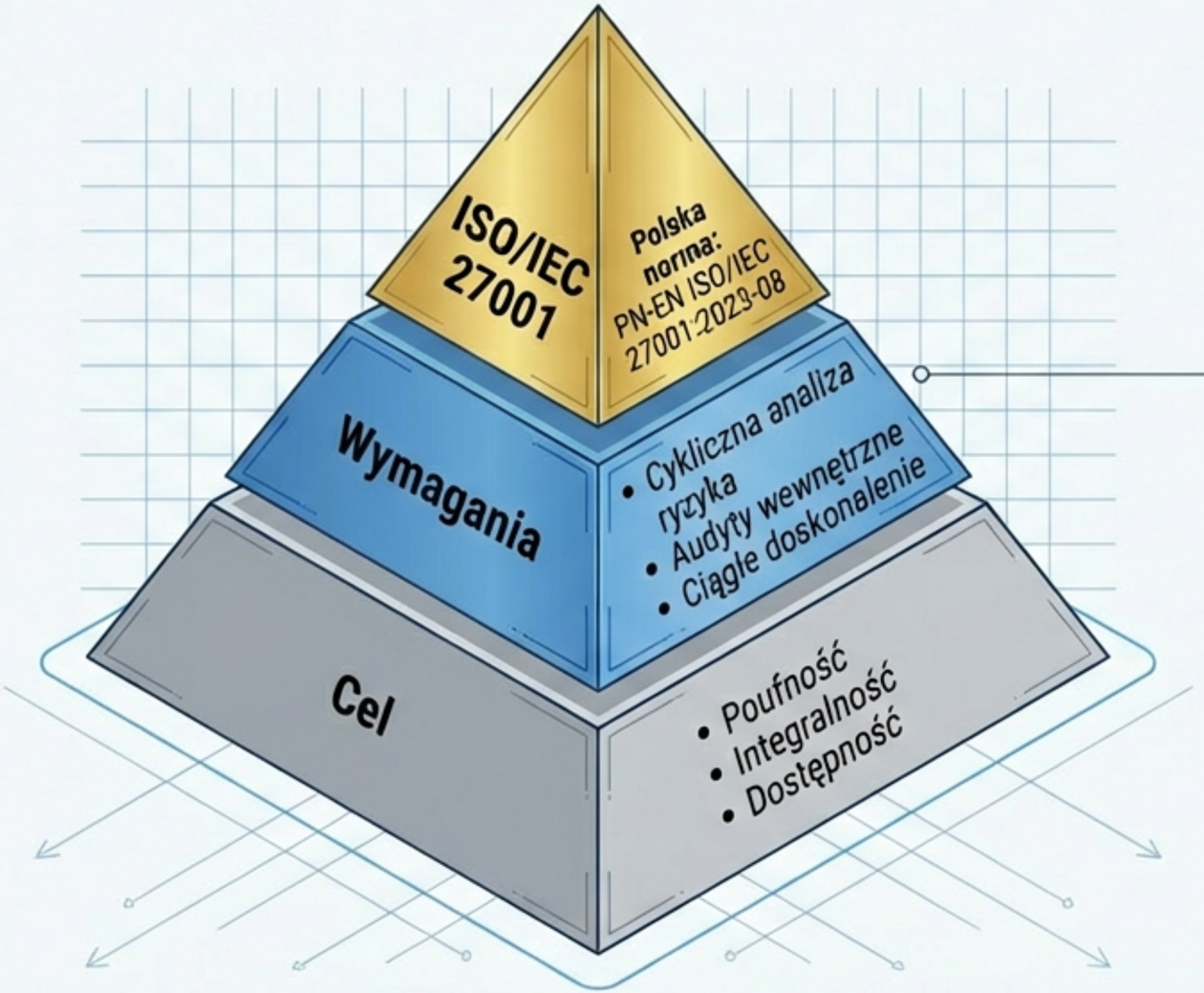
Prawa jednostki

Prawo do wglądu, sprostowania i bycia zapomnianym.

Privacy by Design: Każdy system musi być projektowany z domyślną ochroną prywatności.

Standardy Doskonałości: ISO/IEC 27001

Międzynarodowy standard Systemu Zarządzania Bezpieczeństwem Informacji (ISMS)



Pro Tip:
ISO 27701 to rozszerzenie dedykowane ochronie prywatności.

Ekosystem Cyberbezpieczeństwa: NIS2 i KSC

Dyrektywa NIS2
(EU)

Ustawa o KSC
(Krajowy System Cyberbezpieczeństwa)

Obowiązki operatorów usług kluczowych

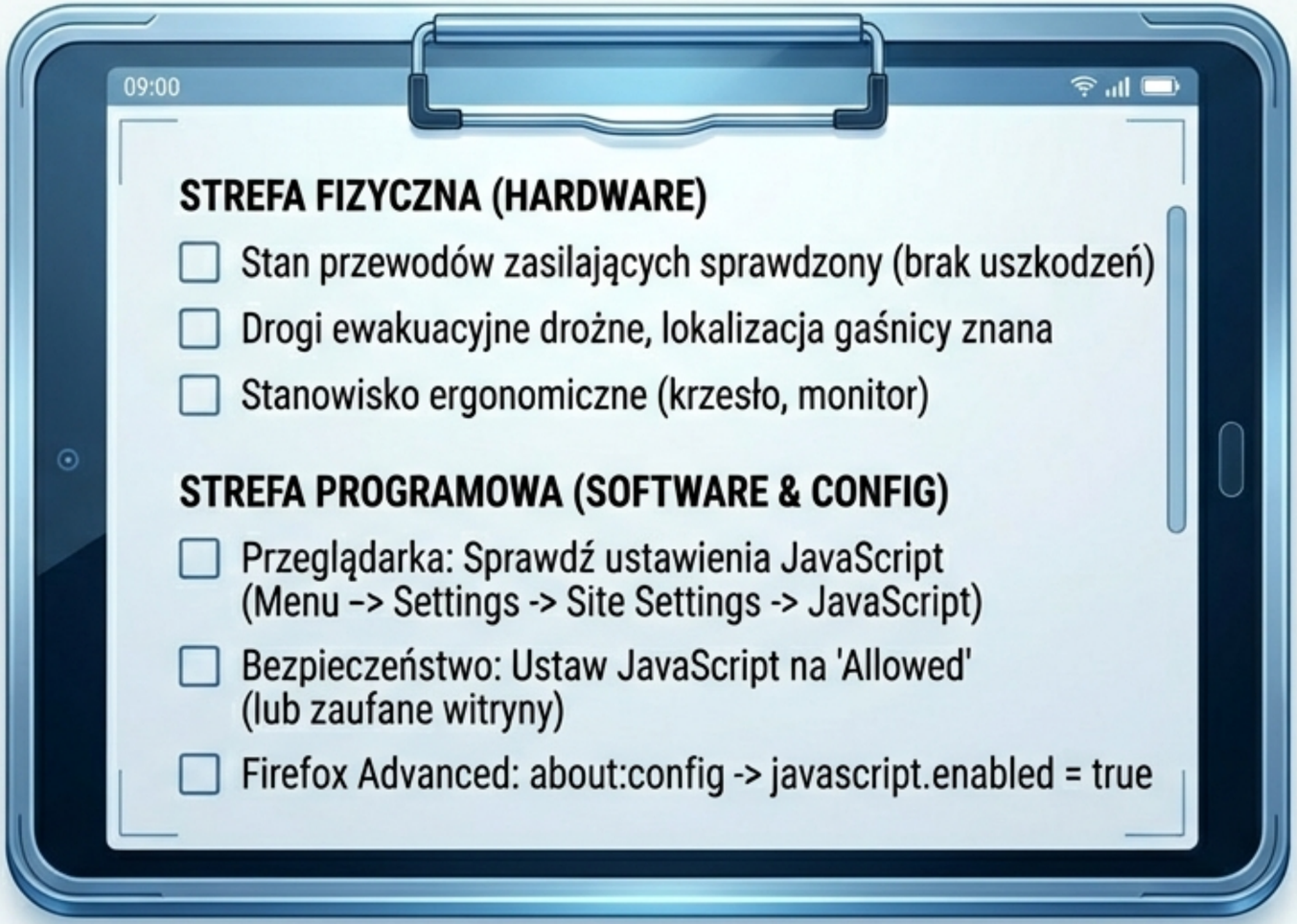
1. Ciągła ocena ryzyka cybernetycznego
2. Obowiązek raportowania incydentów do CSIRT
3. Odpowiedzialność kierownictwa

Synteza: Jak łączą się systemy bezpieczeństwa?

Obszar / Norma	Kluczowe Działanie w Praktyce
BHP (Kodeks Pracy)	Ocena ryzyka zawodowego na stanowisku
Dane Osobowe (RODO)	Zgłaszanie naruszeń i ochrona prywatności
Bezpieczeństwo Info (ISO 27001)	Procedury, polityki i audyty bezpieczeństwa
Cyberbezpieczeństwo (NIS2/KSC)	Raportowanie incydentów krytycznych

Wniosek:
Wszystkie normy opierają się na identyfikacji zagrożeń i procedurach reakcji.

Lista Kontrolna: Gotowość do pracy



Niezbędnik Egzaminacyjny: Słowa Kluczowe

ESD

Electrostatic Discharge – wyładowanie niszczące elektronikę.

ISMS

Information Security Management System (System Zarządzania Bezpieczeństwem Informacji).

KSC

Krajowy System Cyberbezpieczeństwa.

RODO

Rozporządzenie o Ochronie Danych Osobowych (GDPR).

Czynniki uciążliwe

Hałas, oświetlenie, wymuszona pozycja ciała.

PN-EN ISO/IEC 27001

Polska norma zarządzania bezpieczeństwem.

Bezpieczeństwo to proces, nie produkt

1. Bądź świadomy zagrożeń fizycznych.

2. Bądź zgodny z normami prawnymi.

3. Bądź profesjonalny w stosowaniu standardów.

Bezpieczne stanowisko pracy to fundament stabilnej infrastruktury IT.

Materiały dodatkowe i Źródła

- Pełny tekst rozporządzenia BHP
- Film instruktażowy: Bezpieczeństwo w serwerowni
- Checklista stanowiskowa do druku (PDF)
- Ustawienia przeglądarek (Dokumentacja techniczna)
- Tekst jednolity RODO / GDPR