# Przegląd
# Wytyczne OECD w zakresie bezpieczeństwa systemów i sieci informatycznych: W kierunku kultury bezpieczeństwa

## Overview
## OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security
## Polish translation




**ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT**

**ORGANIZACJA WSPÓŁPRACY GOSPODARCZEJ I ROZWOJU**

# Przedmowa

Wykorzystanie systemów i sieci informatycznych oraz cała technologia środowiska informatycznego zasadniczo się zmieniły od momentu ogłoszenia przez OECD *Wytycznych w zakresie bezpieczeństwa systemów informatycznych* w 1992 r. Te ciągłe zmiany są źródłem znaczących korzyści, choć jednocześnie wymagają położenia dużo większego nacisku na kwestie bezpieczeństwa przez rządy, przedsiębiorstwa, inne organizacje oraz indywidualnych użytkowników (wszyscy są dalej zwani « uczestnikami »), którzy rozwijają, posiadają, obsługują i użytkują systemy i sieci informatyczne oraz świadczą usługi z nimi związane.

Coraz wydajniejsze komputery osobiste, rozwiązania na styku rożnych technologii i powszechne użycie Internetu wyparły proste, niezintegrowane systemy, działające w zamkniętych przeważnie sieciach. Dzisiaj ilość połączeń między uczestnikami nieustannie wzrasta, a same połączenia przekraczają granice państwowe. Co więcej, Internet wspomaga strategiczne infrastruktury - energetyczną, transportową czy finansową - oraz odgrywa dużą rolę w procesie funkcjonowania przedsiębiorstw, świadczeniu przez państwo usług na rzecz obywateli i przedsiębiorstw oraz komunikacji i wymianie informacji między obywatelami. Znaczącej zmianie uległa także istota i rodzaj infrastruktury komunikacyjnej i informatycznej. Zwielokrotniła się liczba i rodzaje urządzeń dostępowych, obejmując jednostki stałe, przenośne i bezprzewodowe, a coraz większa ilość połączeń jest realizowana przy wykorzystaniu łączy stałych. Doprowadziło to do istotnego zwiększenia ilości rodzajów przesyłanych danych, ich objętości oraz wrażliwości na różne rodzaje zagrożeń.

W wyniku rosnącej ilości połączeń systemy i sieci informatyczne są dziś narażone na coraz większą liczbę różnych niebezpieczeństw i są coraz bardziej podatne na awarie. Powoduje to powstawanie nowych wyzwań w zakresie bezpieczeństwa. Dlatego też niniejsze Wytyczne dotyczą wszystkich uczestników nowego społeczeństwa informatycznego i zasugerowano w nich potrzebę większej świadomości i zrozumienia kwestii związanych z bezpieczeństwem oraz potrzebę rozwoju “kultury bezpieczeństwa”.

# I. W kierunku kultury bezpieczeństwa

Odpowiedzią niniejszych Wytycznych na ciągłe zmiany w dziedzinach związanych z bezpieczeństwem jest promowanie tworzenia kultury bezpieczeństwa. Jest ona rozumiana jako skoncentrowanie się na bezpieczeństwie podczas tworzenia systemów i sieci informatycznych oraz przyjęcie nowych sposobów myślenia i postępowania w trakcie ich użytkowania oraz komunikacji przy ich pomocy. Wytyczne stanowczo odcinają się od czasów, kiedy o bezpiecznym projektowaniu i korzystaniu z sieci i systemów zbyt często przypominano sobie dopiero po zakończeniu prac. Uzależnienie uczestników od systemów informatycznych, sieci i powiązanych z nimi usług wzrasta, od wszystkich tych elementów wymaga się niezawodności i bezpieczeństwa. Skuteczny poziom bezpieczeństwa może zapewnić tylko podejście, które przykłada należną wagę do potrzeb wszystkich użytkowników, istoty systemów, sieci i usług pochodnych.

Każdy uczestnik jest ważnym elementem procesu zapewniania bezpieczeństwa. Stosownie do pełnionych przez siebie ról, uczestnicy powinni być świadomi możliwych zagrożeń bezpieczeństwa i działań prewencyjnych, powinni wziąć na siebie odpowiedzialność i podjąć kroki w celu podwyższania poziomu bezpieczeństwa systemów i sieci informatycznych.

Krzewienie kultury bezpieczeństwa będzie wymagać kierowniczego i zarazem szeroko zakrojonego uczestnictwa. Powinno przynieść podwyższenie priorytetu planowania i zarządzania bezpieczeństwem oraz zrozumienie potrzeby bezpieczeństwa wśród wszystkich uczestników. Kwestie bezpieczeństwa powinny być przedmiotem troski i odpowiedzialności na wszystkich poziomach administracji państwowej, sektora prywatnego i dla wszystkich uczestników. Wytyczne formułują założenia pracy mającej na celu tworzenie kultury bezpieczeństwa w społeczeństwie. Mają umożliwić uczestnikom włączenie kwestii bezpieczeństwa do procesów projektowania i użytkowania wszystkich systemów i sieci informatycznych. Proponują przyjęcie i promowanie przez wszystkich uczestników kultury bezpieczeństwa jako sposobu myślenia o funkcjonowaniu infrastruktury informatycznej, jej oceny i użytkowania.

# II. Cele

Cele Wytycznych są następujące:

- Promowanie wśród uczestników kultury bezpieczeństwa jako sposobu ochrony systemów i sieci informatycznych.
- Poszerzanie świadomości ryzyka związanego z systemami i sieciami informatycznymi; świadomości polityk, praktyk, środków i procedur dostępnych wobec tego ryzyka; świadomości potrzeby ich przyjęcia i wdrożenia.

- Zwiększanie zaufania uczestników do systemów i sieci, sposobu ich użytkowania i dostarczania.
- Stworzenie schematu odniesienia, który pomoże uczestnikom zrozumieć kwestie bezpieczeństwa i przestrzegać normy etyczne podczas tworzenia i wdrażania spójnych polityk, praktyk, środków i procedur związanych z zapewnieniem bezpieczeństwa sieci i systemów informatycznych.
- Promowanie należytej współpracy i wymiany informacji pomiędzy wszystkimi uczestnikami w dziedzinach rozwijania i wdrażania polityk, praktyk, środków i procedur bezpieczeństwa.
- Promowanie względów bezpieczeństwa jako istotnego celu wśród wszystkich uczestników zaangażowanych w tworzenie i wdrażanie standardów.

## III. Zasady

Dziewięć poniższych zasad uzupełnia się nawzajem i powinny one być traktowane łącznie. Odnoszą się do uczestników na wszystkich poziomach, włącznie z poziomem ustalania polityki i poziomem operacyjnym. Zgodnie z niniejszymi Wytycznymi odpowiedzialność uczestników zależy od pełnionych przez nich ról. Wszyscy uczestnicy będą wspomagani wiedzą, wykształceniem, wymianą informacji i szkoleniami, które to elementy będą prowadziły do poprawy zrozumienia kwestii bezpieczeństwa i lepszych praktyk postępowania. Działania zmierzające do poprawy bezpieczeństwa systemów i sieci informatycznych powinny współgrać z wartościami demokratycznego społeczeństwa, szczególnie z potrzebą otwartego i wolnego obiegu informacji oraz podstawowym szacunkiem dla ochrony danych osobowych.[1]

### *1) Świadomość*

***Uczestnicy powinni być świadomi potrzeby bezpieczeństwa systemów i sieci informatycznych oraz kroków, jakie mogą podjąć w celu poprawy bezpieczeństwa.***

Świadomość zagrożeń i dostępnych zabezpieczeń stanowi pierwszą linię obrony w bezpieczeństwie systemów i sieci informatycznych. Infrastrukturze informatycznej zagrażają ryzyka pochodzenia zarówno wewnętrznego, jak i zewnętrznego. Uczestnicy powinni rozumieć, że awarie zabezpieczeń mogą poważnie uszkadzać systemy i sieci przez nich zarządzane. Powinni być również świadomi możliwości wyrządzenia szkód innym ze względu na połączenia i współzależności sieciowe. Uczestnicy powinni znać konfigurację i dostępne uaktualnienia do posiadanego systemu, jego rolę w sieci, dobre praktyki umożliwiające zwiększenie bezpieczeństwa oraz potrzeby innych uczestników.

[1] Jako dodatek do niniejszych Wytycznych w zakresie bezpieczeństwa, OECD opracowała uzupełniające zalecenia dotyczące wytycznych w innych kwestiach ważnych dla światowego społeczeństwa informatycznego. Odnoszą się one do ochrony danych osobowych (*OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 1980) i kryptografii (*OECD Guidelines for Cryptography Policy*, 1997). Niniejsze Wytyczne powinny interpretowane razem z nimi.

## *2) Odpowiedzialność*

***Wszyscy uczestnicy są odpowiedzialni za bezpieczeństwo systemów i sieci.***

Uczestnicy są zależni od połączonych lokalnych oraz globalnych systemów i sieci informacyjnych, powinni więc zdawać sobie sprawę ze swojej odpowiedzialności za ich bezpieczeństwo. Odpowiedzialność winna być adekwatna do roli konkretnego uczestnika. Uczestnicy powinni systematycznie badać swoje polityki, praktyki, środki oraz procedury i oceniać, czy są odpowiednie do ich środowiska. Podmioty tworzące, projektujące i dostarczające produkty i usługi powinny wziąć pod uwagę bezpieczeństwo sieci i rozpowszechniać odpowiednie informacje, wraz z systematycznymi, okresowymi aktualizacjami, aby użytkownicy lepiej rozumieli związaną z bezpieczeństwem funkcjonalność produktów i usług, jak również własną odpowiedzialność w dziedzinie bezpieczeństwa.

## *3) Reakcja*

***Uczestnicy powinni działać bez zwłoki i współpracować ze sobą w celu zapobiegania, wykrywania i reagowania na naruszenia bezpieczeństwa***.

Rozumiejąc specyfikę powiązań systemów i sieci informatycznych oraz ich podatność na powstawanie nagłych i rozległych uszkodzeń, uczestnicy powinni wspólnie i bezzwłocznie reagować w przypadkach naruszenia bezpieczeństwa. Powinni wymieniać się odpowiednimi informacjami o zagrożeniach i lukach w zabezpieczeniach, a także wdrożyć procedury szybkiej i skutecznej współpracy, mającej na celu zapobieganie, wykrywanie i reagowanie na naruszenia bezpieczeństwa. Jeżeli jest to dopuszczalne, współpraca i wymiana informacji mogą mieć charakter ponadnarodowy.

## *4) Etyka*

***Uczestnicy powinni szanować uzasadnione dobra innych.***

Biorąc pod uwagę powszechność systemów i sieci informatycznych w naszych społecznościach, uczestnicy powinni rozumieć, że ich działanie lub jego brak może narazić na szkodę innych. Postępowanie etyczne ma zatem wartość kluczową, a uczestnicy powinni starać się rozwijać i wdrażać najlepsze praktyki postępowania, promować zachowania uwzględniające wymagania bezpieczeństwa i poszanowanie dla cudzych praw.

## *5) Demokracja*

***Bezpieczeństwo systemów i sieci informatycznych powinno być zgodne z podstawowymi wartościami społeczeństwa demokratycznego.***

Rozwiązania z zakresu bezpieczeństwa powinny być wdrażane w sposób korespondujący z wartościami uznawanymi przez społeczeństwa demokratyczne, w tym wolność wymiany myśli i poglądów, swobodny przepływ informacji, poufność informacji i komunikacji, odpowiednią ochronę danych osobowych, otwartość i przejrzystość.

## *6) Ocena ryzyka*

***Uczestnicy powinni przeprowadzać oceny ryzyka.***

Ocena ryzyka identyfikuje zagrożenia oraz luki w zabezpieczeniach. Powinna być oparta na wystarczająco szerokich podstawach, żeby objąć kluczowe czynniki wewnętrzne i zewnętrzne, takie jak technologia, czynniki fizyczne, czynniki ludzkie, polityki postępowania, wpływające na bezpieczeństwo usługi świadczone przez jednostki zewnętrzne. Ocena ryzyka pozwoli na określenie akceptowalnego poziomu ryzyka i pomoże wybrać odpowiednich narzędzi zarządzania ryzykiem uszkodzenia systemów i sieci informatycznych, uwzględniając rodzaj i ważność chronionych informacji. Z powodu rosnących współzależności sieciowych pomiędzy systemami informatycznymi, ocena ryzyka powinna uwzględniać potencjalne szkody powodowane przez jednostki zewnętrzne, bądź też im wyrządzone.

## *7) Projektowanie i wdrażanie rozwiązań z zakresu bezpieczeństwa*

***Uczestnicy powinni włączać rozwiązania z zakresu bezpieczeństwa do systemów i sieci informatycznych jako elementy kluczowe.***

W celu optymalizacji bezpieczeństwa systemy, sieci i polityki powinny być odpowiednio projektowane, wdrażane i zsynchronizowane. Powyższe działania koncentrują się głównie (choć nie wyłącznie) na projektowaniu i stosowaniu odpowiednich zabezpieczeń i rozwiązań w celu uniknięcia lub ograniczenia szkód wywołanych przez zidentyfikowane zagrożenia i luki w zabezpieczeniach. Wymagane są zarówno zabezpieczenia techniczne, jak i nietechniczne, i powinny być one dostosowane do wartości informacji przechowywanych w systemach i sieciach organizacji. Zapewnianie bezpieczeństwa powinno być podstawowym elementem wszystkich produktów, usług, systemów i sieci oraz stanowić integralną część projektu i infrastruktury systemu. Na planowanie i wdrażanie rozwiązań z zakresu bezpieczeństwa przez użytkowników końcowych składa się głównie wybór i konfiguracja produktów i usług przeznaczonych dla ich systemów.

## *8) Zarządzanie bezpieczeństwem*

***Uczestnicy powinni przyjąć całościowe podejście do zarządzania bezpieczeństwem.***

Zarządzanie bezpieczeństwem powinno być oparte na ocenie ryzyka, stanowić proces dynamiczny, obejmować wszystkie poziomy działalności uczestnika i wszystkie aspekty jego funkcjonowania. Powinno przewidywać odpowiedzi na nowo pojawiające się zagrożenia, zajmować się zapobieganiem, wykrywaniem zagrożeń i reagowaniem na nie, przywracaniem systemów, ich bieżącą konserwacją, aktualizacją i audytem. Polityki bezpieczeństwa, praktyki, środki i procedury związane z systemami i sieciami informatycznymi powinny być zintegrowane i tworzyć spójny system bezpieczeństwa. Wymagania w stosunku do zarządzania bezpieczeństwem zależą od stopnia zaangażowania, roli pełnionej przez uczestnika, istniejącego ryzyka oraz od wymagań systemowych.

## *9) Przegląd*

***Użytkownicy powinni dokonywać przeglądów i ocen bezpieczeństwa systemów i sieci informatycznych oraz wprowadzać niezbędne zmiany do polityk, praktyk, środków i procedur dotyczących bezpieczeństwa.***

Wciąż odkrywane są nowe, zmieniające się zagrożenia i luki zabezpieczeń. Uczestnicy powinni w sposób ciągły badać, oceniać i modyfikować wszystkie aspekty swojej polityki bezpieczeństwa, aby stawić czoła nowym zagrożeniom.

# Zalecenia Rady Dotyczące Wytycznych w Zakresie Systemów i Sieci Informatycznych

## *W Kierunku Kultury Bezpieczeństwa*

RADA,

uwzględniając Konwencję o Organizacji Współpracy Gospodarczej i Rozwoju z 14 grudnia 1960 r., a w szczególności jej artykuły 1b), 1c), 3a) i 5b),

uwzględniając zalecenie Rady z dnia 23 września 1980 r. w sprawie Wytycznych dotyczących ochrony danych osobowych i transgranicznego przepływu danych osobowych [C(80)58(Final)],

uwzględniając Deklarację o transgranicznym przepływie danych przyjętą przez rządy Członków OECD 11 kwietnia 1985 [Załącznik do C(85)139],

uwzględniając Zalecenie Rady z dnia 27 marca 1997 r. w sprawie Wytycznych dotyczących kryptografii [C(97)62/FINAL],

uwzględniając deklarację Rady Ministerialnej z dn. 7-9 grudnia 1998 r. w sprawie Ochrony danych osobowych w sieciach globalnych [Załącznik do C(98)177/FINAL],

uwzględniając deklarację Rady Ministerialnej z dn. 7-9 grudnia 1998 r. w sprawie Uwierzytelniania w handlu elektronicznym [Załącznik do C(98)177/FINAL],

uznając, że systemy i sieci informatyczne są coraz bardziej użyteczne i cenne dla rządów, przedsiębiorstw, innych organizacji i użytkowników indywidualnych,

uznając, że rosnące znaczenie systemów i sieci informatycznych, rosnąca zależność od nich stabilnych i wydajnych gospodarek narodowych, handlu międzynarodowego, życia społecznego, kulturalnego i politycznego, wymaga szczególnych wysiłków zmierzających do ochrony i wspomagania pokładanego w nich zaufania,

uznając, że systemom i sieciom informatycznym oraz ich globalnemu rozpowszechnieniu towarzyszą nowe i nasilające się zagrożenia,

uznając, że dane i informacje zapisane i przesyłane przy użyciu systemów i sieci informatycznych są narażone na różnego rodzaju akty nieupoważnionego dostępu, użycia, nadużycia, modyfikacji, przesyłanie szkodliwych programów, ataki typu "denial of service" oraz zniszczenie i że wymagają odpowiednich zabezpieczeń,

uznając potrzebę upowszechniania wiedzy o zagrożeniach, jakim podlegają systemy i sieci informatyczne, o politykach, praktykach, środkach i procedurach przeciwdziałania im oraz potrzebę promowania odpowiednich zachowań - za kluczowy krok w kierunku tworzenia kultury bezpieczeństwa,

uznając potrzebę uaktualnienia obecnych polityk, praktyk, środków i procedur w celu zapewnienia ich skuteczności wobec nowych wyzwań związanych z zagrożeniami systemów i sieci informatycznych,

uznając istnienie wspólnego interesu w propagowaniu bezpieczeństwa systemów i sieci informatycznych przez tworzenie kultury bezpieczeństwa, która wspomoże międzynarodową koordynację i współpracę w odpowiedzi na potencjalność szkód dla gospodarek narodowych, handlu międzynarodowego oraz życia społecznego, kulturalnego i politycznego,

a także uznając, że *Wytyczne w zakresie bezpieczeństwa systemów i sieci informatycznych: W kierunku kultury bezpieczeństwa* zawarte w załączniku do niniejszego zalecenia mają charakter fakultatywny i nie wpływają na suwerenne prawa państw,

i uznając, że celem niniejszych wytycznych nie jest sugerowanie istnienia tylko jednego, adekwatnego do wszystkich sytuacji, rozwiązania w kwestiach polityk, praktyk, środków i procedur bezpieczeństwa, lecz ustalenie zbioru ogólnych zasad promujących lepsze zrozumienie sposobu, w jaki uczestnicy mogą odnieść korzyści z rozwijania kultury bezpieczeństwa oraz jak mogą się do jej rozwoju przyczynić;

POLECA niniejsze *Wytyczne w zakresie bezpieczeństwa systemów i sieci informatycznych: W kierunku kultury bezpieczeństwa* rządom, przedsiębiorstwom, innym organizacjom oraz użytkownikom indywidualnym, którzy tworzą, posiadają, dostarczają, kierują, obsługują i używają systemów i sieci informatycznych;

ZALECA Państwom Członkowskim:

stworzenie nowych lub poprawienie obecnych polityk, praktyk, środków i procedur zgodnie z i biorąc pod uwagę *Wytyczne w zakresie bezpieczeństwa systemów i sieci informatycznych: W kierunku kultury bezpieczeństwa*, przyjmując i propagując opisaną w tych wytycznych kulturę bezpieczeństwa;

konsultacje, koordynację i współpracę na poziomie państwowym i międzynarodowym przy wdrażaniu niniejszych wytycznych;

upowszechnianie niniejszych wytycznych w sektorze publicznym i prywatnym, włączając w to administrację rządową, przedsiębiorstwa, inne organizacje oraz użytkowników indywidualnych, promując w ten sposób kulturę bezpieczeństwa, zachęcając wszystkie zainteresowane strony do odpowiedzialnego podjęcia niezbędnych kroków w celu wdrożenia wytycznych w sposób odpowiedni do pełnionych przez nie ról;

udostępnianie niniejszych wytycznych krajom spoza OECD, bez zwłoki i w odpowiedni sposób;

analizę wytycznych odbywającą się co pięć lat, co ma na celu wsparcie międzynarodowej współpracy w dziedzinie bezpieczeństwa systemów i sieci informatycznych;

ZLECA Komisji ds. Polityki Informatycznej, Komputerowej i Komunikacyjnej OECD (Committee for Information, Computer and Communications Policy) promowanie wdrażania niniejszych wytycznych.

To zalecenie zastępuje zalecenie Rady z dn. 26 listopada 1992 r. w sprawie Wytycznych w zakresie bezpieczeństwa systemów informatycznych [C(92)188/FINAL].

# Historia zmian

Wytyczne w zakresie bezpieczeństwa wydano po raz pierwszy w 1992 r. i zaktualizowano w 1997 r. Obecną aktualizację wykonała Grupa Robocza ds. Bezpieczeństwa Informatycznego i Danych Osobowych (Working Party on Information Security and Privacy - WPISP) na mocy polecenia Komisji ds. Polityki Informatycznej, Komputerowej i Komunikacyjnej OECD, a prace uległy przyspieszeniu po tragedii 11 września.

Prace projektowe zostały podjęte przez grupę ekspercką WPISP, która zebrała się w dn.10-11 marca 2001 r. w Waszyngtonie, 12-13 lutego 2002 r. w Sydney i 4 oraz 6 marca 2002 w Paryżu. Członkowie WPISP spotkali się w Paryżu w dn. 5-6 marca 2002, 22-23 kwietnia 2002 oraz 25-26 czerwca 2002.

Niniejsze *Wytyczne OECD w zakresie bezpieczeństwa systemów i sieci informatycznych: W kierunku kultury bezpieczeństwa* zostały przyjęte jako Zalecenie Rady OECD na 1037. sesji, 25 lipca 2002 r.

## Spis treści oryginalnej angielskiej wersji niniejszej publikacji

*(bez załączników, listy pól, tabel i wykresów):*

**Niniejszy *Przegląd* stanowi tłumaczenie fragmentów poniższych dokumentów OECD pierwotnie opublikowanych pod następującymi tytułami, angielskim i francuskim:**

**OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security**

**Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information: Vers une culture de la sécurité**



Publikacje OECD oraz egzemplarze *Przeglądów* dostępne są w księgarni internetowej OECD pod adresem www.oecd.org/bookshop/

*Należy wpisać „overview" (przegląd) w polu „Title search" na stronie księgarni internetowej lub wpisać tytuł angielski publikacji*

*(Przeglądy są powiązane z oryginalnymi publikacjami w języku angielskim).*

Za przygotowanie *Przeglądu* odpowiada dział Praw Autorskich i Tłumaczeń,
Dyrektoriat ds. Spraw Publicznych i Komunikacji
email : rights@oecd.org / Fax: +33 1 45 24 13 91