

## 8. Polityka bezpieczeństwa informacji – podstawa kontroli nad urządzeniami i oprogramowaniem



*W średniej wielkości firmie usługowej doszło do incydentu – pracownik zainstalował na służbowym laptopie darmowy program do edycji PDF-ów. Oprogramowanie okazało się zawierać złośliwy kod, który rozprzestrzenił się po sieci, szyfrując dane na serwerze plików. Problem ujawnił brak jakichkolwiek procedur – firma nie miała polityki instalacji oprogramowania, nikt nie kontrolował używanych aplikacji, a dostęp do konta administratora miał każdy. Koszt przywrócenia danych z kopii zapasowej i przestoju operacyjnego przekroczył 300 000 zł. Po incydencie zarząd wdrożył politykę bezpieczeństwa informacji – kilkustronicowy dokument, który mógł wcześniej zapobiec stratom.*

### Dlaczego każda firma potrzebuje polityki bezpieczeństwa?

**Polityka bezpieczeństwa informacji (PBI)** to formalny dokument określający zasady ochrony danych, systemów, urządzeń oraz użytkowników w firmie. Jej brak oznacza brak kontroli – każdy pracownik działa według własnego uznania, co prowadzi do chaosu i znacznie podnosi ryzyko wystąpienia incydentów bezpieczeństwa.

### Podstawa prawna

Tworzenie polityki bezpieczeństwa informacji nie jest tylko dobrą praktyką – w wielu przypadkach to **wymóg prawny**. W szczególności:

- RODO – nakłada obowiązek wdrażania odpowiednich środków technicznych i organizacyjnych w celu ochrony danych osobowych, w tym m.in. zabezpieczenia urządzeń, kontroli dostępu i szyfrowania.
- Ustawa o krajowym systemie cyberbezpieczeństwa – dla objętych nią podmiotów wymaga wprowadzenia mechanizmów zarządzania ryzykiem.
- Kodeks pracy – reguluje kwestie monitorowania sprzętu służbowego i prywatności pracownika.
- Normy ISO/IEC 27001 – nieobowiązkowe, ale powszechnie uznawane i wdrażane standardy zarządzania bezpieczeństwem informacji, w tym w zakresie sprzętu i systemów.

### Wdrożenie polityki bezpieczeństwa urządzeń w firmie

Wdrożenie takiego dokumentu w organizacji ma na celu:

- ochronę danych i infrastruktury IT firmy,
- ujednolicenie zasad postępowania z urządzeniami,
- określenie obowiązków pracowników i administratorów,
- minimalizację ryzyka związanego z cyberatakami i utratą kontroli nad sprzętem.

Polityka ta powinna być zrozumiała, dostosowana do wielkości firmy i regularnie aktualizowana.



## Etapy wdrażania polityki

Wdrożenie skutecznej polityki bezpieczeństwa w kontekście urządzeń składa się z kilku kroków:

1. identyfikacja zasobów – określenie, jakie urządzenia podlegają polityce;
2. konsultacja z działami – uwzględnienie potrzeb użytkowników i zespołu IT;
3. opracowanie zasad zgodnych z przepisami prawa (RODO, Kodeks pracy);
4. komunikacja – przekazanie dokumentu pracownikom i zebranie podpisów;
5. monitorowanie i egzekwowanie – bieżące kontrole zgodności;
6. aktualizacja – przynajmniej raz w roku lub po incydencie.

Proces ten może być wsparty przez konsultanta ds. bezpieczeństwa.

## Kluczowe aspekty SZBI (Systemu Zarządzania Bezpieczeństwem Informacji) w kontekście bezpieczeństwa urządzeń

- **Identyfikacja i klasyfikacja zasobów.** W pierwszym kroku należy zidentyfikować wszystkie urządzenia, które przechowują lub przetwarzają informacje, a następnie sklasyfikować je w zależności od ich wrażliwości.
- **Ocena ryzyka.** Należy przeprowadzić analizę zagrożeń i ryzyka związanego z każdym urządzeniem, biorąc pod uwagę np. możliwość uszkodzenia, utraty w wyniku przestępstwa czy nieuprawnionego dostępu.
- **Wdrożenie zabezpieczeń.** Na podstawie oceny ryzyka wdraża się odpowiednie zabezpieczenia. Mogą to być rozwiązania techniczne (np. szyfrowanie, zapory sieciowe) i organizacyjne (np. polityki dostępu, procedury postępowania w przypadku incydentu).
- **Ciągłe doskonalenie.** Utrzymanie bezpieczeństwa informacji jest procesem ciągłym. Oznacza to, że system wymaga stałego monitorowania, regularnych audytów i aktualizacji w celu dostosowania do zmieniających się zagrożeń i potrzeb firmy.
- **Szkolenia i świadomość pracowników.** Kluczowym elementem jest edukacja pracowników na temat zasad bezpiecznego korzystania z urządzeń firmowych i potencjalnych zagrożeń

Niemal każdego dnia pracownicy firmy używają laptopów, komputerów stacjonarnych lub urządzeń mobilnych, za pośrednictwem których wykonują swoją pracę. Używając ich, mają dostęp do różnych systemów i aplikacji, przetwarzają za ich pośrednictwem dane osobowe oraz dane wrażliwe biznesowo i ważne dla firmy. Zapewnienie bezpieczeństwa, niezawodności oraz ciągłości pracy urządzeń jest niezbędne dla utrzymania stabilności i efektywności działania przedsiębiorstwa.



## Polityka bezpieczeństwa informacji. Najważniejsze zasady

- Pracownicy korzystają wyłącznie z zatwierdzonego, służbowego sprzętu.
- Na urządzeniach firmowych należy instalować tylko oprogramowanie zaakceptowane przez dział IT.
- Wszystkie urządzenia muszą być zabezpieczone (np. hasłem, tokenem, biometrią), a dyski – zaszyfrowane.
- Regularne aktualizacje systemów i aplikacji są obowiązkowe.
- Użytkownicy nie mają uprawnień administracyjnych, chyba że jest to uzasadnione.
- W przypadku podejrzenia cyberataku lub utraty urządzenia w wyniku przestępstwa – pracownik natychmiast zgłasza to przełożonemu i personelowi IT.
- Co najmniej raz w roku polityka powinna być przeglądana i aktualizowana.



### Pytania kontrolne



Czy Twoja firma ma formalnie spisaną politykę bezpieczeństwa informacji?



Czy polityka reguluje przydzielanie i użytkowanie sprzętu służbowego?



Czy zawiera zasady dotyczące instalacji i aktualizacji oprogramowania?



Czy obejmuje wymagania dotyczące haseł, szyfrowania i blokowania ekranów?



Czy procedury zgłaszania incydentów są jasno określone?



Czy pracownicy zostali zapoznani z polityką bezpieczeństwa i/lub z niej przeszkoleni?



Czy dokument był aktualizowany w ciągu ostatnich 12 miesięcy?