BEZPIECZNE DANE SP. Z O. O.
ochrona prywatności

PORADNIK UCZESTNIKA · BEZPŁATNY FRAGMENT

Bezpieczeństwo informacji w urzędzie

System zarządzania bezpieczeństwem informacji — kurs dla pracowników

Fragment: rozdział 1 z 13

Pełny poradnik: 46 stron, listy kontrolne, słowniczek

Podstawa: § 19 rozporządzenia KRI (Dz.U. 2024 poz. 773), RODO



> **To jest bezpłatny fragment poradnika.** Pełny poradnik w formacie PDF jest dołączany bezpłatnie do każdego kursu i udostępniany do pobrania po wykupieniu dostępu.

Dla kogo. Dla każdej osoby zatrudnionej w jednostce publicznej, niezależnie od stanowiska: dla kierownika, dla księgowości, dla kadr, dla wydziału merytorycznego i dla osoby, która rano otwiera kancelarię i przyjmuje korespondencję. Poradnik nie zakłada przygotowania informatycznego — każde pojęcie techniczne jest wyjaśnione tam, gdzie pojawia się po raz pierwszy.

Podstawa prawna szkolenia. Obowiązek szkolenia osób zaangażowanych w przetwarzanie informacji wynika z § 19 ust. 2 pkt 6 rozporządzenia Rady Ministrów z 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (Dz.U. 2024 poz. 773). Ten sam paragraf w ust. 1 nakłada na kierownictwo obowiązek ustanowienia, wdrożenia, eksploatacji i doskonalenia systemu zarządzania bezpieczeństwem informacji, a w ust. 2 pkt 14 — sprawdzania zgodności w drodze audytu nie rzadziej niż raz na rok. Drugim filarem są przepisy o ochronie danych osobowych: art. 32 RODO (środki techniczne i organizacyjne) oraz art. 29 RODO (przetwarzanie wyłącznie na polecenie administratora).

Czas. Kurs liczy 13 lekcji, łącznie około 2 godzin i 20 minut nagrania.

Drugie zastosowanie. Poradnik pełni również rolę dowodu w audycie: pokazuje kontrolerowi pełny zakres merytoryczny szkolenia bez konieczności odtwarzania nagrań.

Jak korzystać z tego poradnika

Poradnik jest pomyślany jako materiał czytany równolegle z odtwarzanym nagraniem, najlepiej w drugim oknie obok odtwarzacza. Nie jest transkrypcją: zawiera to, czego z nagrania nie da się wygodnie przepisać — progi liczbowe, nazwy dokumentów, jednostki redakcyjne przepisów i gotowe listy czynności. Każdy rozdział jest samodzielny, więc mogą Państwo przeczytać wyłącznie ten, który odpowiada właśnie oglądanej lekcji. Sekcje „Konkrety do zapamiętania” i „Lista kontrolna” warto wydrukować i mieć przy biurku. Sekcja „Sprawdź się” nie jest testem zaliczeniowym — to trzy pytania, które warto odnieść do własnego stanowiska pracy. Na końcu znajdą Państwo słowniczek, zestawienie przywołanych podstaw prawnych oraz miejsce na notatki.

Rozdział 1. Podstawy prawne i odpowiedzialność

> **Lekcja w kursie:** Podstawy prawne i odpowiedzialność · **Czas nagrania:** 11 min

W SKRÓCIE

Dbanie o bezpieczeństwo informacji w jednostce publicznej nie jest kwestią dobrej woli ani decyzji informatyka — to obowiązek wynikający wprost z przepisów i dotyczący każdego stanowiska. Stoją za nim dwa filary: przepisy o ochronie danych osobowych oraz rozporządzenie o Krajowych Ramach Interoperacyjności. Chronimy trzy atrybuty informacji: poufność, integralność i dostępność. Obowiązuje przy tym zasada rozliczalności — każde działanie przypisuje się do konkretnej osoby, a nie do stanowiska.

CO TRZEBA WIEDZIEĆ

Dwa filary obowiązku

Filar pierwszy to RODO. Art. 32 nakłada na jednostkę obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych. Art. 29 stanowi, że osoba działająca z upoważnienia administratora przetwarza dane wyłącznie na jego polecenie. To, co Państwo robią z danymi, ma więc wynikać z polecenia i procedury, a nie z własnej inicjatywy.

Filar drugi to rozporządzenie KRI. Aktualne jest rozporządzenie Rady Ministrów z 21 maja 2024 r. (Dz.U. 2024 poz. 773); starsze, z 2012 r., zostało zastąpione. Treść i numeracja § 19 pozostały bez zmian, ale powoływanie się w dokumentacji na akt, który już nie obowiązuje, to prosta droga do uwagi audytora.

Norma ISO/IEC 27001 opisuje, jak zbudować taki system. Norma nie jest ustawą: obowiązuje wtedy, gdy jednostka sama zdecydowała się ją wdrożyć, uzyskała certyfikat albo zobowiązała się do niej w umowie.

Trzy atrybuty — co konkretnie chronimy

Atrybut	Znaczenie	Przykład naruszenia
Poufność	Informację widzi wyłącznie osoba z upoważnieniem	Na monitorze przy okienku wciąż otwarta sprawa poprzedniego interesanta
Integralność	Dane nie zostały nieuprawnienie zmienione ani zniszczone	Pomylona cyfra w numerze działki albo w kwocie podatku
Dostępność	Informacja jest pod ręką, gdy jest potrzebna	Awaria systemu, zagubiony dokument, zaszyfrowany przez przestępców dysk

Poufność nie dotyczy wyłącznie osób z zewnątrz — dotyczy także koleżanki z sąsiedniego pokoju, która danej sprawy nie prowadzi. Każda z Państwa procedur służy któremuś z tych trzech atrybutów.

Czym naprawdę jest SZBI

System zarządzania bezpieczeństwem informacji to nie program antywirusowy ani urządzenie w serwerowni. To trzy połączone elementy: dokumenty (polityki i procedury), technika (systemy i zabezpieczenia) oraz ludzie (Państwa codzienne nawyki). System chroni informację w postaci elektronicznej, papierowej i **ustnej** — czyli także to, o czym rozmawiamy przez telefon, na korytarzu albo przy kawie. Rozmowy o mieszkańcu prowadzonej przy otwartych drzwiach nie zatrzyma żadna zapora sieciowa.

Rozliczalność i konsekwencje

Rozliczalność oznacza, że każde działanie — wprowadzenie danych, zmiana, usunięcie, wydruk, wejście do pomieszczenia — daje się przypisać do konkretnego człowieka. Dlatego każdy ma własny login i hasło i dlatego obowiązuje bezwzględny zakaz ich udostępniania: także zastępstwu, także przełożonemu. Hasło jest jak podpis, a podpisu się nie pożycza.

Konsekwencje układają się w trzy poziomy. Pracownicze — od upomnienia i nagany po rozwiązanie umowy, także w trybie dyscyplinarnym. Finansowe dla jednostki — dla jednostek sektora finansów publicznych limit kary pieniężnej wynosi 100 000 zł. Karne i cywilne — grzywna, w skrajnych przypadkach kara pozbawienia wolności, a także roszczenie o naprawienie szkody.

KONKRETY DO ZAPAMIĘTANIA

Rzecz	Wartość
Aktualne rozporządzenie KRI	Rozporządzenie RM z 21.05.2024, Dz.U. 2024 poz. 773
Obowiązek SZBI i szkoleń	§ 19 ust. 1 oraz § 19 ust. 2 pkt 6
Częstotliwość audytu zgodności	Nie rzadziej niż raz na rok (§ 19 ust. 2 pkt 14)
Przetwarzanie tylko na polecenie	art. 29 RODO
Limit kary dla jednostki sektora finansów publicznych	100 000 zł

LISTA KONTROLNA — DO ZASTOSOWANIA OD JUTRA

- [ ] Sprawdzić, na które rozporządzenie KRI powołuje się polityka bezpieczeństwa w Państwa jednostce.
- [ ] Wstając od biurka, spojrzeć na blat i monitor oczami osoby przechodzącej korytarzem.
- [ ] Sprawdzić, czy hasło nie jest zapisane w szufladzie, pod klawiaturą ani na ramce monitora.
- [ ] Przy najbliższej prośbie o udostępnienie loginu odmówić i wskazać drogę wniosku o uprawnienia.
- [ ] Zamknąć drzwi pokoju przed rozmową telefoniczną dotyczącą konkretnego mieszkańca.

NAJCZĘSTSZY BŁĄD

Powszechne jest przekonanie, że bezpieczeństwo informacji to sprawa działu informatyki, bo to on ma programy, zapory i serwery. Technika zabezpiecza jednak wyłącznie tę część informacji, która przechodzi przez system

teleinformatyczny. Nie zabezpiecza teczki na parapecie, rozmowy przy otwartych drzwiach ani hasła podanego z uprzejmości. Odpowiedzialność jest więc rozdzielona odwrotnie, niż podpowiada intuicja: im bliżej biurka, tym bardziej osobista.

SPRAWDŹ SIĘ

1. Co dziś na Państwa biurku albo ekranie zobaczyłaby osoba, która nie powinna tego widzieć?
2. Który z trzech atrybutów jest najbardziej narażony na Państwa stanowisku i dlaczego?
3. Jak brzmiałaby Państwa odpowiedź, gdyby przełożony poprosił o hasło „tylko na chwilę”?

Dalsza część poradnika

To jest bezpłatny fragment. Pełny poradnik obejmuje jeszcze:

- Rozdział 2. Rola pracownika w systemie: od zatrudnienia do rozstania
- Rozdział 3. Fizyczne bezpieczeństwo biura
- Rozdział 4. Polityka czystego biurka i czystego ekranu
- Rozdział 5. Dokumenty papierowe: tworzenie, przechowywanie i niszczenie
- Rozdział 6. Hasła i dostęp do systemu
- Rozdział 7. Poczta służbowa i Internet
- Rozdział 8. Sprzęt służbowy i instalowanie oprogramowania
- Rozdział 9. Praca zdalna i mobilna
- Rozdział 10. Incydenty bezpieczeństwa: co to jest i jak je rozpoznać
- Rozdział 11. Zgłaszanie incydentów: karta alarmowa
- Rozdział 12. Konsekwencje służbowe i prawne naruszenia bezpieczeństwa informacji
- Rozdział 13. Bezpieczeństwo informacji to proces, nie produkt
- Słowniczek
- Podstawy prawne przywołane w kursie
- Notatki własne

Pełną wersję — wraz z listami kontrolnymi, słowniczkiem i wykazem podstaw prawnych — otrzymują Państwo bezpłatnie po wykupieniu dostępu do kursu.