**ZARZĄDZENIE NR 76/2026**
**BURMISTRZA MIASTA i GMINY KÓRNIK**
z dnia 2 czerwca 2026 r.

w sprawie wprowadzenia procedury szkoleń pracowników z zakresu cyberbezpieczeństwa

Na podstawie § 19 ust. 2 pkt 6 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2024 poz. 773) (dalej: KRI) oraz w związku z: Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560) (dalej: „uKSC"), Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 (dalej: RODO), Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000), Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2005 nr 64 poz. 565), zarządzam, co następuje:

**§ 1.**

**Cel i podstawa wprowadzenia procedury**

1. Wprowadza się w Urzędzie Miasta i Gminy Kórnik Procedurę szkoleń z zakresu cyberbezpieczeństwa, stanowiącą element systemu zarządzania bezpieczeństwem informacji.
2. Procedura realizuje obowiązki jednostki jako podmiotu publicznego w zakresie:
   1) wdrożenia środków zarządzania ryzykiem w cyberbezpieczeństwie,
   2) zapewnienia regularnych szkoleń pracowników i kadry kierowniczej,
   3) budowania świadomości zagrożeń oraz zdolności reagowania na incydenty.
3. Szkolenia stanowią element środków organizacyjnych wymaganych przez KRI oraz uKSC, w tym w zakresie zarządzania ryzykiem, ciągłości działania oraz reagowania na incydenty.

**§ 2.**

**Postanowienia końcowe**

1. Procedura szkoleń stanowi załącznik nr 1 do niniejszego zarządzenia.
2. Wykonanie zarządzenia powierza się Sekretarzowi Miasta i Gminy Kórnik
3. Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Miasta i Gminy Kórnik

Przemysław Pacholski

**Załącznik nr 1 do**
**zarządzenia nr 76/2026**
**Burmistrza Miasta i Gminy Kórnik**
z dnia 2 czerwca 2026 r.

# PROCEDURA SZKOLEŃ PRACOWNIKÓW Z ZASAD CYBERBEZPIECZEŃSTWA W URZĘDZIE MIASTA I GMINY KÓRNIK

## §1.
## Cel procedury

1. Celem niniejszej procedury jest określenie zasad organizacji, realizacji oraz dokumentowania szkoleń z zakresu cyberbezpieczeństwa dla pracowników Urzędu Miasta i Gminy Kórnik.
2. Procedura ma na celu:
   - podniesienie poziomu świadomości zagrożeń cybernetycznych,
   - zapewnienie zgodności działań jednostki z obowiązującymi przepisami prawa,
   - minimalizację ryzyka incydentów bezpieczeństwa informacji,
   - zapewnienie ciągłości działania systemów teleinformatycznych.

## §3.
## Zakres podmiotowy

1. Obowiązkowi szkoleniowemu podlegają:
   - wszyscy nowo zatrudnieni pracownicy,
   - pracownicy zatrudnieni na stanowiskach kierowniczych,
   - pracownicy mający dostęp do systemów teleinformatycznych,
   - osoby współpracujące na podstawie umów cywilnoprawnych, jeżeli posiadają dostęp do danych lub systemów.
2. Szkolenia mogą być rozszerzone na podmioty zewnętrzne realizujące zadania na rzecz jednostki.

## §4.
## Rodzaje szkoleń

W jednostce wprowadza się następujące rodzaje szkoleń:

**1. Szkolenie wstępne:**
   - realizowane w terminie do 14 dni od rozpoczęcia pracy,
   - obejmuje podstawowe zasady ochrony informacji i korzystania z systemów IT,
   - może mieć formę stacjonarną lub e-learningową,
   - zakończone testem sprawdzającym wiedzę.

**2. Szkolenie okresowe:**
   - realizowane nie rzadziej niż raz na 12 miesięcy,
   - obejmuje aktualne zagrożenia oraz zmiany w przepisach prawa,
   - może mieć formę stacjonarną lub e-learningową.

3. **Szkolenie specjalistyczne:**
   - przeznaczone dla administratorów systemów, kadry kierowniczej oraz pracowników IT,
   - obejmuje zaawansowane zagadnienia techniczne i organizacyjne,
   - organizowane w zależności od potrzeb.
4. **Szkolenie doraźne**
   - realizowane w przypadku wystąpienia incydentu bezpieczeństwa,
   - obejmuje analizę zdarzenia i działania zapobiegawcze.

**§5.**
**Zakres tematyczny szkoleń**

Program szkolenia obejmuje w szczególności:
1. Podstawowe pojęcia z zakresu cyberbezpieczeństwa.
2. Zasady ochrony danych osobowych w kontekście cyberbezpieczeństwa.
3. Identyfikacja na temat szczególnych zagrożeń, w tym:
   - phishing,
   - ransomware,
   - socjotechnika,
   - ataki typu DDoS.
4. Zasady tworzenia i przechowywania haseł.
5. Bezpieczne korzystanie z poczty elektronicznej i Internetu.
6. Zasady bezpieczeństwa w pracy zdalnej.
7. Procedury zgłaszania incydentów bezpieczeństwa.
8. Odpowiedzialność pracowników za naruszenie zasad bezpieczeństwa.

**§6.**
**Organizacja szkoleń**

1. Za organizację szkoleń odpowiada:
   - Administrator Systemów Informatycznych lub
   - Pełnomocnik ds. Bezpieczeństwa Informacji / Inspektor Ochrony Danych.
2. Informacja o szkoleniu przekazywana jest pracownikom drogą elektroniczną z wykorzystaniem służbowej poczty elektronicznej.
3. Szkolenia mogą być prowadzone:
   - przez pracowników jednostki,
   - przez podmioty zewnętrzne posiadające odpowiednie kwalifikacje.

**§7.**
**Dokumentowanie szkoleń**

1. Każde szkolenie dokumentowane jest w formie:
   - listy osób zgłoszonych do przeszkolenia,
   - protokołu szkolenia,
   - testu wiedzy (jeżeli przewidziany).
2. Dokumentacja przechowywana jest przez okres co najmniej 5 lat.
3. Dopuszcza się prowadzenie dokumentacji w formie elektronicznej.

## §8.
## Ocena skuteczności szkoleń

1. Skuteczność szkoleń oceniana jest poprzez:
   - analizę wyników testów,
   - analizę liczby i rodzaju incydentów,
   - okresowe ankiety wśród pracowników.
2. Na podstawie wyników analizy wprowadza się działania korygujące.

## §9.
## Obowiązki pracowników

1. Każdy pracownik zobowiązany jest do:
   - udziału w obowiązkowych szkoleniach,
   - przestrzegania zasad bezpieczeństwa informacji,
   - niezwłocznego zgłaszania incydentów.
2. Nieuczestniczenie w szkoleniu bez uzasadnionej przyczyny może skutkować konsekwencjami służbowymi.

## §10.
## Postanowienia końcowe

1. Procedura wchodzi w życie z dniem podpisania przez Kierownika Jednostki.
2. Za nadzór nad realizacją procedury odpowiada Sekretarz Miasta i Gminy Kórnik.
3. Procedura podlega przeglądowi nie rzadziej niż raz w roku lub w przypadku zmiany przepisów prawa.

Załączniki do procedury:

- Nr 1 - Lista osób zgłoszonych do przeszkolenia,
- Nr 2 - Protokołu szkolenia.

Załącznik Nr 1
do procedury szkoleń pracowników
z zakresu cyberbezpieczeństwa

## LISTA OSÓB ZGŁOSZONYCH DO PRZESZKOLENIA

**Data zgłoszenia do szkolenia:**

.....

**Nazwa podmiotu zgłaszającego:**

.....

**Imię i nazwisko zgłaszającego:**

.....

**Prowadzący szkolenie:**

.....

**Temat szkolenia:**
Zasady cyberbezpieczeństwa w administracji publicznej

**Lista osób zgłoszonych do przeszkolenia**

| Lp. | Nazwisko i imię | Adres email |
|---|---|---|
| 1. | | |
| 2. | | |
| 3. | | |
| 4. | | |
| 5. | | |
| 6. | | |
| 7. | | |
| 8. | | |
| 9. | | |
| 10. | | |

Załącznik Nr 2
do procedury szkoleń pracowników
z zakresu cyberbezpieczeństwa –

## PROTOKÓŁ SZKOLENIA

| Lp. | Sygnatura czasowa | Wynik testu | Imię i nazwisko | Miejscowość | Nazwa instytucji |
|---|---|---|---|---|---|
| 1. | | | | | |
| 2. | | | | | |
| 3. | | | | | |
| 4. | | | | | |
| 5. | | | | | |
| 6. | | | | | |
| 7. | | | | | |
| 8. | | | | | |
| 9. | | | | | |
| 10. | | | | | |