

Zarządzenie nr 1/2026
Dyrektora Okoneckiego Centrum Kultury w Okonku
z dnia 5 marca 2026 roku

w sprawie wprowadzenia Procedury Cyberbezpieczeństwa w Okoneckim Centrum Kultury w Okonku.

Na podstawie art. 17 ustawy z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej (t.j. Dz. U. z 2024 r. poz. 87), art. 22 ust. 1 pkt 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20), § 19 ust. 2 pkt 13 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. z 2024 r. poz. 773), Rozporządzenia (UE) 2016/679 Parlamentu Europejskiego i Rady - RODO oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781 t.j.), zarządza się, co następuje:

§ 1.

Wprowadza się Procedurę Cyberbezpieczeństwa w Okoneckim Centrum Kultury w Okonku, stanowiącą Załącznik do niniejszego zarządzenia.

§ 2.

Wszyscy pracownicy Okoneckiego Centrum Kultury w Okonku zobowiązani są do zapoznania się z treścią Procedury Cyberbezpieczeństwa oraz do przestrzegania jej postanowień. Oświadczenia pracowników o zapoznaniu się z procedurą będą przechowywane w aktach osobowych w części B.

§ 3.

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
OKONECKIEGO CENTRUM KULTURY
Marta Lasota

PROCEDURA CYBERBEZPIECZEŃSTWA

Rozdział I

Cel procedury

1. Zapewnienie bezpiecznego korzystania z technologii informacyjno-komunikacyjnych (TIK), ochrony danych osobowych osób korzystających z usług instytucji i pracowników oraz zapobieganie incydentom cyberbezpieczeństwa na terenie instytucji.

Rozdział II

Zakres stosowania

1. Procedura obowiązuje:
 - a) wszystkich pracowników,
 - b) osoby korzystające z usług instytucji (uczestnicy zajęć, czytelnicy, uczestnicy warsztatów), kontrahentów,
 - c) pracowników w zakresie korzystania z systemów informatycznych,
 - d) podmioty zewnętrzne realizujące usługi informatyczne lub przetwarzające dane instytucji.

Rozdział III

Definicje

1. **Incydent cyberbezpieczeństwa** – zdarzenie powodujące naruszenie poufności, integralności lub dostępności danych, systemów lub sieci.
2. **TIK** – sprzęt, oprogramowanie oraz usługi informatyczne wykorzystywane w instytucji.
3. **Administrator Systemów Informatycznych (ASI)** – osoba odpowiedzialna za infrastrukturę IT jednostki (informatyk / firma IT).
4. **IOD** – Inspektor Ochrony Danych.

Rozdział IV

Obszary zagrożeń

1. Nieuprawniony dostęp do systemu informatycznego i danych osobowych.
2. Cyberprzemoc i zagrożenia internetowe wobec pracowników.
3. Malware, phishing, niebezpieczne załączniki i linki itp.
4. Nieuprawniona instalacja oprogramowania.
5. Utrata danych (brak kopii zapasowych).
6. Niewłaściwe korzystanie z sieci Wi-Fi.

Rozdział V

Zasady bezpieczeństwa technicznego

1. Infrastruktura IT
 - a) Dostęp do komputerów służbowych chroniony hasłem.
 - b) Hasła zmieniane minimum co 90 dni, zgodne z polityką hasel (min. 10-12 znaków tj. duże i małe litery, cyfry, znaki specjalne).
 - c) Automatyczna blokada ekranu po 15 minutach.

- d) Zabroniona instalacja własnych programów.
 - e) Aktualizacje systemów i aplikacji wykonywane na bieżąco przez ASI.
2. Sieć
- a) Sieć Wi-Fi dla pracowników - hasło nieudostępniane innym,
 - b) Osobna sieć Wi-Fi dla osób korzystających z usług instytucji (uczestników zajęć, czytelników, uczestników warsztatów),
 - c) Loginy bezpieczeństwa przechowywane min. 6 miesięcy.
3. Kopie zapasowe
- a) Backup danych prowadzony co najmniej raz w tygodniu,
 - b) Kopie przechowywane w odrębnym miejscu od danych produkcyjnych,
 - c) Raz w roku test odtwarzania danych.

Rozdział VI

Zasady organizacyjne i edukacyjne

1. Pracownicy
- a) Obowiązkowe szkolenie z cyberbezpieczeństwa raz w roku - lista obecności i program szkolenia,
 - b) Korzystanie z poczty służbowej wyłącznie w celach zawodowych,
 - c) Zakaz udostępniania loginów i haseł innym osobom (w tym współpracownikom),
 - d) Sprawdzanie nadawcy i celu korespondencji (szczególnie załączników i linków) - autoryzacja przez inną osobę,
 - e) Odpowiedzialność za bezpieczeństwo kont,
 - f) Obowiązek natychmiastowego zgłoszenia utraty hasła lub podejrzenia włamania.

Rozdział VII

Reagowanie na incydenty cyberbezpieczeństwa

1. Zgłaszanie
- Każda osoba, która podejrzewa incydent, zgłasza go:
- a) Osobie decyzyjnej, IOD,
 - b) ASI lub IOD (w przypadku danych osobowych).
2. Klasyfikacja incyduentu
- a) Niski – np. próba phishingu wykryta przez pracownika,
 - b) Średni – np. blokada komputera, wykrycie wirusa,
 - c) Wysoki – np. wyciek danych osobowych, dostęp osoby nieuprawnionej.
3. Postępowanie
- a) ASI analizuje zdarzenie i zabezpiecza dowody (logi, zrzuty ekranu),
 - b) W przypadku naruszenia danych IOD dokonuje oceny ryzyka i decyduje o zgłoszeniu do UODO w ciągu 72h,
 - c) W razie cyberprzemocy - natychmiastowe działania i zgłoszenie,
 - d) W razie ataku lub próby włamania - blokada kont oraz zmiana haseł,
 - e) Dokumentacja incyduentu przechowywana min. 2 lata.

Rozdział VIII

Profilaktyka i edukacja

1. Szkolenia z cyberbezpieczeństwa - raz w roku.

Rozdział IX
Przegląd i aktualizacja procedury

1. Audyt potwierdzony protokołem KRI - przegląd co 12 miesięcy.
2. Aktualizacja po każdym poważnym incydencie.
3. Dyrektor jest odpowiedzialny za wprowadzenie zmian.

Rozdział X
Załączniki

1. Wzór oświadczenia pracownika o zapoznaniu się z Procedurą Cyberbezpieczeństwa.
2. Wzór karty zgłoszenia incydentu cyberbezpieczeństwa.
3. Wzór powiadomienia o naruszeniu danych osobowych (dla IOD).

Podpis pracodawcy:

D Y R E K T O R
OKONECKIEGO CENTRUM KULTURY
Marta Lasota

OŚWIADCZENIE PRACOWNIKA
o zapoznaniu się z Procedurą Cyberbezpieczeństwa
w Okoneckim Centrum Kultury w Okonku

.....
(imię i nazwisko pracownika)

.....
(stanowisko służbowe)

Oświadczam, że zapoznałem się/zapoznałam się z Procedurą Cyberbezpieczeństwa w Okoneckim Centrum Kultury w Okonku i zobowiązuję się do jej przestrzegania.

....., dnia.....

.....
(podpis pracownika)

**Oświadczenie pracownika o przyjęciu do wiadomości procedury należy przechowywać w ich aktach osobowych część B.*

DYREKTOR
OKONECKIEGO CENTRUM KULTURY
Marta Lasota

KARTA ZGŁOSZENIA INCYDENTU CYBERBEZPIECZEŃSTWA

1. Dane zgłaszającego

- Imię i nazwisko:
- Stanowisko / rola:
- Telefon kontaktowy:
- E-mail:

2. Data i czas wykrycia incydentu

- Data:
- Godzina:

3. Miejsce wystąpienia incydentu

(komputer, pracownia, sala, konto użytkownika, usługa, system itp.)

.....

4. Rodzaj incydentu (zaznaczyć)

- ☐ Podejrzenie włamania
- ☐ Złośliwe oprogramowanie (np. wirus, ransomware, phishing)
- ☐ Ujawnienie lub wyciek danych
- ☐ Nieuprawniony dostęp
- ☐ Uszkodzenie/utrata danych
- ☐ Awarie systemów / niedostępność usług
- ☐ Inny (jaki?):

5. Opis incydentu

(na czym polega, jakie działania lub zdarzenia zauważono, kto brał udział)

.....

.....

.....

6. Zasięg i skutki incydentu

- Jakie systemy/urządzenia zostały dotknięte?
- Jakie dane mogły być zagrożone?

.....

.....

7. Podjęte działania przed zgłoszeniem

(odłączenie od sieci, zmiana hasła, zgłoszenie do administratora, wykonane kopie)

.....

.....

8. Potrzebne działania / uwagi zgłaszającego

.....

.....

9. Osoba przyjmująca zgłoszenie

- Imię i nazwisko:
- Stanowisko:

- Data i godzina przyjęcia zgłoszenia:

10. Dalsze postępowanie (wypełnia administrator / koordynator)

- Ocena incydentu: ☐ zwykły ☐ istotny ☐ krytyczny
- Podjęte działania:
.....
- Konieczność zgłoszenia do CSIRT / organu nadzorczego: ☐ TAK ☐ NIE
- Data zakończenia obsługi incydentu:

Podpis osoby zgłaszającej:

Podpis osoby przyjmującej:

DYREKTOR
OKONECKIEGO CENTRUM KULTURY
Marta Lasota

POWIADOMIENIE O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

1. Dane administratora

Nazwa administratora:

Adres:

Telefon / e-mail:

2. Dane zgłaszającego naruszenie

(Imię i nazwisko, stanowisko lub opis roli w jednostce)

.....

Telefon / e-mail:

3. Data i godzina stwierdzenia naruszenia

Data:

Godzina:

4. Data i godzina wystąpienia incydentu (jeśli znane)

Data:

Godzina:

5. Opis naruszenia ochrony danych

(na czym polegało naruszenie, jak zostało zauważone, jakie działania je spowodowały)

.....

.....

.....

6. Kategoria naruszenia (zaznaczyć właściwe)

- ☐ Utrata danych
- ☐ Ujawnienie danych osobom nieuprawnionym
- ☐ Nieuprawniony dostęp
- ☐ Zniszczenie danych
- ☐ Modyfikacja danych
- ☐ Inne (jakie?):

7. Dotknięte dane osobowe i kategorie osób

- Zakres danych:
- Kategorie osób:
(np. uczestnicy zajęć, rodzice, czytelnicy, pracownicy, petenci)

8. Szacunkowa liczba osób, których dotyczy naruszenie:

.....

9. Ocena możliwych konsekwencji naruszenia

(ryzyko kradzieży tożsamości, szkody majątkowe, szkody niemajątkowe, utrata poufności)

.....

.....

10. Podjęte działania naprawcze i minimalizujące skutki

.....
.....

11. Czy naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych?

- ☐ TAK
- ☐ NIE

Jeśli TAK — konieczne zawiadomienie osób, których dane dotyczą.

12. Czy naruszenie wymaga zgłoszenia do Prezesa UODO (art. 33 RODO)?

- ☐ TAK
- ☐ NIE

Uzasadnienie:

13. Uwagi i zalecenia IOD

.....
.....

14. Podpisy

Zgłaszający: data:

IOD: data:

DYREKTOR
OKONECKIEGO CENTRUM KULTURY
Marta Lasota