

Zasady bezpieczeństwa w relacjach z dostawcami

Spis treści

Spis treści	1
1 Cel	2
2 Zakres	2
3 Terminologia.....	2
4 Odpowiedzialność i uprawnienia	2
5 Postanowienia ogólne	3
6 Zasady ogólne dotyczące przetwarzania informacji chronionych	3
7 Zgłaszanie incydentu bezpieczeństwa informacji	7

Centralna Komisja Egzaminacyjna		Wersja v102
	Zasady bezpieczeństwa informacji w relacjach z dostawcami	Data wyd.: 26.02.2024

1 Cel

Celem dokumentu jest:

1. Określenie minimalnych wymagań w zakresie bezpieczeństwa informacji dla dostawców, które mają dostęp na mocy zawartych umów do informacji chronionych CKE.
2. Określenie minimalnych wymagań w zakresie zabezpieczeń systemów informatycznych dostawcy.

2 Zakres

Niniejszy dokument stosuje dostawca zgodnie z zawartą umową z Centralną Komisją Egzaminacyjną.

3 Terminologia

1. **Wykonawca, dostawca, podmiot trzeci** – podmiot świadczący lub dostarczający usługi lub produkty dla CKE.
2. **Użytkownik zewnętrzny** – pracownik wykonawcy/dostawcy lub podwykonawca przetwarzający informacje w systemie informatycznym CKE.
3. **Administrator Danych Osobowych (ADO)** – Centralna Komisja Egzaminacyjna w zakresie realizacji zadań dla Centralnej Komisji Egzaminacyjnej, Dyrektor Centralnej Komisji Egzaminacyjnej w zakresie realizowanych zadań dla Dyrektora Centralnej Komisji Egzaminacyjnej – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydujące o celach i środkach przetwarzania danych osobowych.
4. **Aktywo informacyjne, zasób informacyjny, informacje chronione** – wszelkie informacje w formie papierowej, elektronicznej i innej, przetwarzane (w tym zbierane, utrwalane, przechowywane, opracowywane, zmieniane, udostępniane, transmitowane, przekazywane i usuwane) w sposób tradycyjny lub w systemach informatycznych, będące własnością, wykorzystywane, bądź administrowane przez CKE, które posiadają wartość materialną lub prawną.
5. **Incydent** – to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań CKE i zagrażają bezpieczeństwu informacji.
6. **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

4 Odpowiedzialność i uprawnienia

1. Za nadzór nad przestrzeganiem niniejszego dokumentu odpowiedzialni są:
 - a. pracownik CKE odpowiedzialny za koordynację współpracy z dostawcą;
 - b. dostawca, który został zobowiązany do jego przestrzegania w ramach zawartych umów z CKE.

Centralna Komisja Egzaminacyjna		Wersja v102
	Zasady bezpieczeństwa informacji w relacjach z dostawcami	Data wyd.: 26.02.2024

5 Postanowienia ogólne

1. Zasady bezpieczeństwa informacji w relacjach z dostawcami, zwane dalej „Zasadami bezpieczeństwa”, określają zakres obowiązków i odpowiedzialności dostawców w zakresie bezpieczeństwa informacji chronionych CKE. Zasady bezpieczeństwa obejmują swym zakresem wszystkie podmioty, będące dostawcami produktów lub usług, mające dostęp do informacji chronionych CKE.
2. Pracownik CKE odpowiedzialny za sporządzenie umowy z dostawcą, jest każdorazowo zobligowany do uwzględnienia niniejszych Zasad bezpieczeństwa w sposób o którym mowa w ust. 4 poniżej.
3. Dostawca będzie udostępniać na żądanie CKE wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w Zasadach bezpieczeństwa i przepisach prawa powszechnie obowiązującego oraz umożliwi CKE lub audytorowi upoważnionemu przez Dyrektora CKE do przeprowadzenia audytów i inspekcji w tym zakresie. W przypadku stwierdzenia nieprawidłowości podczas audytu lub inspekcji, Dyrektor CKE jest uprawniony do obciążenia tymi kosztami dostawcy.
4. Dostawca spełnia wymagania Zasad bezpieczeństwa przed uzyskaniem dostępu do informacji chronionych CKE, co potwierdzają przedstawiciele dostawcy realizujący zadania na rzecz CKE poprzez złożenie oświadczenia zgodnie ze wzorem stanowiącym załącznik nr 1 do niniejszego dokumentu. Złożenie oświadczenia o którym mowa w zdaniu poprzedzającym nie jest wymagane w przypadku, zobowiązania się dostawcy w umowie zawartej z CKE, do spełnienia wymagań Zasad bezpieczeństwa.
5. Przed rozpoczęciem przetwarzania informacji chronionych, w szczególności danych osobowych, dostawca powinien spełnić następujące warunki:
 - a. zobowiązać się w formie pisemnej do zachowania poufności przetwarzanych informacji chronionych zgodnie z Zasadami bezpieczeństwa;
 - b. jeżeli realizacja umowy związana jest z przetwarzaniem danych osobowych:
 - i. w stosownym przypadku podpisać umowę powierzenia przetwarzania danych osobowych;
 - ii. w stosownym przypadku wydać upoważnienia osobom przetwarzającym powierzone przez CKE dane osobowe.
6. Zasady bezpieczeństwa ujęte w przedmiotowym dokumencie stanowią ogólne i uniwersalne zasady bezpieczeństwa informacji obowiązujące u Zamawiającego, przy czym nie wyłącza to możliwości odmiennego uregulowania zasad bezpieczeństwa w danych obszarach działalności CKE określonych w odrębnych regulacjach wewnętrznych. W takim wypadku zastosowanie mają szczegółowe regulacje obowiązujące u Zamawiającego.

6 Zasady ogólne dotyczące przetwarzania informacji chronionych

6.1 Zasady postępowania dla dokumentów papierowych i danych elektronicznych zawierających informacje chronione CKE

1. Dokumenty papierowe, wydruki komputerowe:
 - a. wydruki zabezpiecza się przed dostępem osób nieupoważnionych;
 - b. wszelkie wydruki zawierające dane osobowe muszą być przechowywane w miejscu niedostępnym dla osób nieupoważnionych;

Centralna Komisja Egzaminacyjna		Wersja v102
	Zasady bezpieczeństwa informacji w relacjach z dostawcami	Data wyd.: 26.02.2024

- c. w przypadku, gdy do pomieszczeń po godzinach pracy mają dostęp osoby nieupoważnione, dokumenty zawierające informacje chronione zabezpiecza się na ten czas w szafach zamykanych na klucz, dotyczy to również kopii dokumentów;
 - d. wydruki zawierające informacje chronione CKE po upływie czasu ich wykorzystania przez dostawcę zgodnie z umową z CKE należy niszczyć przy pomocy niszczarki o skuteczności niszczenia min. P4 zgodnie z normą ISO/IEC 21964-2 lub przechowywać w pojemnikach przeznaczonych do bezpiecznego niszczenia dokumentacji dostarczanych przez upoważniony podmiot;
 - e. po zakończeniu każdego dnia pracy osoby mające dostęp do informacji chronionych stosują zasadę „czystego biurka” w odniesieniu do dokumentów i innych nośników zawierających informacje chronione CKE.
2. Informacje chronione w formie elektronicznej – przechowywanie:
- a. dokumenty i dane muszą być przechowywane na nośnikach zabezpieczonych kryptograficznie za pomocą algorytmu AES o długości klucza min. 128-bit lub równoważnego algorytmu pod względem poziomu bezpieczeństwa;
 - b. dokumenty i dane mogą być przesyłane wyłącznie za pośrednictwem kanałów szyfrowanych, w szczególności VPN, za pomocą algorytmu wskazanego w ppkt a. powyżej;
 - c. dane osobowe szczególnie chronione (zgodne z art. 9 RODO) mogą być przesyłane pocztą elektroniczną wyłącznie w formie zaszyfrowanej za pomocą algorytmu wskazanego w ppkt a. powyżej, natomiast hasło do odszyfrowania należy przestać innym kanałem komunikacji np.: poprzez SMS;
 - d. w sytuacji, kiedy konieczna jest wymiana informacji zawierających dane szczególnie chronione (dane wrażliwe), należy te dane zaszyfrować, a następnie zaleca się udostępnić poprzez usługę sieciową np. Microsoft Teams lub Sharepoint, natomiast hasło do odszyfrowania należy przestać innym kanałem komunikacji np.: poprzez e-mail lub SMS.
3. Zasady postępowania w przypadku korzystania z zewnętrznych nośników elektronicznych (pendrive’y, zewnętrzne dyski magnetyczne, aparaty fotograficzne, dyktafony, kamery i inne) zawierających informacje chronione:
- a. zewnętrzne nośniki elektroniczne zawierające informacje chronione CKE zabezpiecza się przed dostępem osób nieupoważnionych np. poprzez zabezpieczenie w szafie zamykanej na klucz; za bezpieczne przechowywanie tych nośników odpowiedzialni są pracownicy dostawcy;
 - b. przenoszenie informacji chronionych na zewnętrznym nośniku elektronicznym poza siedzibę CKE lub dostawcy może odbywać się tylko zgodnie z zapisami niniejszych Zasad bezpieczeństwa; informacje znajdujące się na takich nośnikach muszą być zaszyfrowane algorytmem wskazanym w pkt 2 ppkt a. niniejszego podrozdziału, za wyjątkiem tych aparatów fotograficznych i kamer, które nie posiadają możliwości szyfrowania nośników – w takim przypadku należy bezwzględnie zabezpieczyć nośniki fizycznie przed dostępem osób nieupoważnionych oraz nadzorować je przez osobę upoważnioną;
 - c. nośniki zewnętrzne z informacjami chronionymi CKE należy przechowywać w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym;
 - d. informacje chronione CKE w postaci elektronicznej należy usuwać z nośnika niezwłocznie po ustaniu ich przydatności, w sposób uniemożliwiający ich ponowne odzyskanie;
 - e. uszkodzone nośniki należy niszczyć zgodnie z poziomem min. 4 wskazanym w normie ISO/IEC 21964-2 dla odpowiedniego rodzaju nośnika, w szczególności H-4 i E-4.

Centralna Komisja Egzaminacyjna		Wersja v102
	Zasady bezpieczeństwa informacji w relacjach z dostawcami	Data wyd.: 26.02.2024

6.2 Zasady haseł użytkowników aplikacji i systemów informatycznych wykorzystywanych do przetwarzania informacji chronionych CKE

1. Hasła muszą podlegać następującym zasadom:
 - a. hasło składa się z minimum 10 znaków;
 - b. hasło musi spełniać warunek złożoności polegający na występowaniu w nim: wielkiej i małej litery, oraz cyfry lub znaku specjalnego (np. !@#);
 - c. w przypadku gdy system umożliwia stosowanie 2FA (dwuskładnikowego uwierzytelnienia) należy je uruchomić;
 - d. kolejne hasła muszą być różne;
 - e. hasła należy przechowywać w sposób gwarantujący ich poufność.
2. Zabrania się udostępniania haseł osobom nieupoważnionym.
3. Zabrania się tworzenia haseł na podstawie:
 - a. cech i numerów osobistych (np. dat urodzenia, imion itp.);
 - b. sekwencji klawiszy klawiatury (np. qwerty, 12qwaszx);
 - c. identyfikatora użytkownika.
4. W przypadku logowania do systemu informatycznego odbywającego się po raz pierwszy, dostawca lub pracownik dostawcy ma obowiązek zmiany hasła tymczasowego na właściwe, na znane tylko dostawcy lub pracownikowi dostawcy.
5. W przypadku systemów informatycznych, które nie wymuszają cyklicznej zmiany hasła oraz nie kontrolują jego złożoności, obowiązkiem dostawcy lub pracownika dostawcy jest samodzielna cykliczna zmiana hasła zgodnie z zasadami określonymi w ust. poprzednich.
6. Dostawca lub pracownik dostawcy ponosi pełną odpowiedzialność za utworzenie hasła i jego bezpieczne przechowywanie.
7. Hasła tworzone przez dostawcę lub pracownika dostawcy nie mogą być ujawniane w sposób celowy lub przypadkowy i mogą być znane wyłącznie dostawcy lub pracownikowi dostawcy.
8. Hasła nie mogą być przechowywane w formie dostępnej dla osób nieupoważnionych:
 - a. w plikach;
 - b. na kartkach w miejscach dostępnych dla osób trzecich;
 - c. w skryptach;
 - d. w innych zapisach elektronicznych i papierowych, które byłyby dostępne dla osób trzecich.
9. W przypadku podejrzenia ujawnienia haseł osobie nieupoważnionej, dostawca lub pracownik dostawcy niezwłocznie zmienia hasło i zgłasza incydent do CKE.
10. Dostawca lub pracownik dostawcy utrzymuje hasło w tajemnicy również po upływie jego ważności.
11. Zabrania się przekazywania hasła za pomocą telefonu, przesyłania z pomocą faksu i poczty e-mail w formie jawnej (niezaszyfrowanej).

Centralna Komisja Egzaminacyjna		Wersja v102
	Zasady bezpieczeństwa informacji w relacjach z dostawcami	Data wyd.: 26.02.2024

6.3 Zasady zabezpieczeń komputerów zawierających informacje chronione CKE

1. Do systemu informatycznego CKE mogą być podłączane wyłącznie komputery i urządzenia zgodne z minimalnymi wymaganiami bezpieczeństwa, w szczególności:
 - a. system antywirusowy jest zainstalowany w systemie operacyjnym i jego sygnatury są aktualne;
 - b. system operacyjny posiada zainstalowane wszystkie dostępne aktualizacje i poprawki zabezpieczeń;
 - c. usunięte lub wyłączone niepotrzebne konta użytkowników (takie jak konta gości i konta administracyjne, które nie będą używane);
 - d. usunięte lub wyłączone niepotrzebne oprogramowanie (w tym aplikacje, narzędzia systemowe i usługi sieciowe);
 - e. wyłączona dowolna funkcja automatycznego uruchamiania, która umożliwia wykonywanie programów bez autoryzacji użytkownika (na przykład podczas pobierania z Internetu);
 - f. uwierzytelnianie użytkowników przy dostępie do Internetu, danych wrażliwych lub osobowych lub danych, które mają kluczowe znaczenie dla CKE.

6.4 Zasady zabezpieczania komputerów przenośnych zawierających informacje chronione CKE

1. Użytkownik komputera przenośnego, zawierającego informacje chronione CKE, zobowiązany jest:
 - a. stosować ochronę kryptograficzną wobec danych przetwarzanych na komputerze przenośnym;
 - b. zabezpieczyć dostęp do komputera na poziomie systemu operacyjnego stosując identyfikator i hasło;
 - c. nie zezwalać na używanie komputera osobom nieupoważnionym;
 - d. zachować szczególną ostrożność przy podłączaniu komputera przenośnego do sieci publicznych poza budynkami i pomieszczeniami CKE lub dostawcy.
2. Komputer przenośny nie może być pozostawiany w miejscu narażającym go na kradzież (np. w otwartym pomieszczeniu, w samochodzie).
3. Zasady opisane w niniejszym podrozdziale stosuje się odpowiednio do tabletów oraz smartfonów.

6.5 Usługi zarządzane zewnętrznymi (w tym cloud)

Dostawca musi być w stanie potwierdzić, że wymagania, które są poza kontrolą dostawcy, są odpowiednio spełniane przez usługodawcę. Można wziąć pod uwagę istniejące dowody takie jak certyfikaty ISO 27001, które obejmują odpowiedni zakres wykorzystywanej przez dostawcę usługi.

6.6 Aplikacje internetowe

1. Komercyjne aplikacje internetowe tworzone przez firmy programistyczne (a nie programistów wewnętrznych) i które są publicznie dostępne z Internetu powinny być chronione za pomocą metod:
 - a. firewall ograniczający komunikację wyłącznie do niezbędnych portów;
 - b. dostęp do interfejsów administracyjnych (np. SSH) powinien być ograniczony wyłącznie do komunikacji chronionej poprzez połączenia VPN.

Centralna Komisja Egzaminacyjna		Wersja v102
	Zasady bezpieczeństwa informacji w relacjach z dostawcami	Data wyd.: 26.02.2024

2. Wymaganiem środkiem zaradczym chroniącym przed lukami w zabezpieczeniach aplikacji internetowych jest opracowywanie i testowanie zgodnie z najlepszymi praktykami komercyjnymi, takimi jak standardy Open Web Application Security Project (OWASP).

6.7 Ochrona sieci

6.7.1 Wymagane jest stosowanie jednej z metod ochrony sieci:

- a. firewall brzegowy, który może ograniczać przychodzący i wychodzący ruch sieciowy do usług w sieci komputerów i urządzeń mobilnych; może pomóc w ochronie przed cyberatakami poprzez wdrożenie ograniczeń, znanych jako "reguły firewall", które mogą zezwalać lub blokować ruch zgodnie z jego źródłem, miejscem docelowym i typem protokołu komunikacyjnego;
- b. jeśli dostawca nie kontroluje sieci za pomocą firewall brzegowego, na urządzeniach wewnątrz sieci musi być skonfigurowana zaporą oparta na hoście; działa to w taki sam sposób, jak firewall brzegowy, ale chroni tylko jedno urządzenie, na którym jest skonfigurowany.

6.7.2 Urządzenia sieciowe (przełączniki, routery, firewall lub równoważne)

1. W przypadku wszystkich firewall sieciowych (lub równoważnych urządzeń sieciowych) dostawca musi:
 - a. zmienić domyślne hasło administracyjne na alternatywne, które jest trudne do odgadnięcia — lub całkowicie wyłączyć zdalny dostęp administracyjny;
 - b. uniemożliwić dostęp do interfejsu administracyjnego (używanego do zarządzania konfiguracją urządzenia) z Internetu, chyba że istnieje jasna i udokumentowana potrzeba, a interfejs jest chroniony przez jedną z następujących metod:
 - i. dostęp tylko poprzez VPN lub
 - ii. drugi składnik uwierzytelniania np. kod jednorazowy lub
 - iii. lista dozwolonych adresów IP, która ogranicza dostęp do niewielkiego zakresu zaufanych adresów;
 - c. domyślnie blokować nieuwierzytelnione połączenia przychodzące;
 - d. zapewnić, że przychodzące reguły firewall są zatwierdzone i udokumentowane przez upoważnioną osobę.

7 Zgłaszanie incydentu bezpieczeństwa informacji

1. Każdy incydent bezpieczeństwa informacji CKE wymaga odpowiedniej reakcji, w tym w szczególności poinformowania o wystąpieniu naruszenia CKE. Obowiązek w tym zakresie spoczywa **na dostawcach**, którzy uzyskali dostęp na mocy zawartej umowy do informacji chronionych CKE.
2. W przypadku powierzenia przez CKE dostawcy do przetwarzania danych osobowych, CKE mając na uwadze potrzebę zachowania gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych przez dostawcę będącym także podmiotem przetwarzającym w świetle RODO zastrzega sobie prawo do weryfikacji dostawcy w obszarze zapewniania przez niego odpowiedniego poziomu bezpieczeństwa i ochrony danych osobowych.
3. W przypadku naruszenia bezpieczeństwa informacji chronionych CKE, dostawca postępuje zgodnie z zapisami umowy zawartej pomiędzy CKE i tym dostawcą.
4. Naruszeniem bezpieczeństwa informacji może być w szczególności:

Centralna Komisja Egzaminacyjna		Wersja v102
	Zasady bezpieczeństwa informacji w relacjach z dostawcami	Data wyd.: 26.02.2024

- a. infekcja złośliwego oprogramowania w systemie informatycznym dostawcy;
- b. ujawnienie osobom nieupoważnionym haseł lub kodów PIN do systemów informatycznych dostawcy;
- c. przełamanie zabezpieczeń informatycznych systemów informatycznych dostawcy;
- d. ujawnienie informacji chronionych, w tym w szczególności danych osobowych osobom nieupoważnionym;
- e. nieuprawniona obserwacja i analiza ruchu w sieci dostawcy;
- f. kradzież lub zagubienie dokumentów lub nośników z informacjami podlegającymi ochronie;
- g. wyciek informacji chronionych, w tym w szczególności danych osobowych;
- h. utrata danych;
- i. nieuprawnione uszkodzenie lub zniszczenie danych.

Centralna Komisja Egzaminacyjna		Wersja v102
	Zasady bezpieczeństwa informacji w relacjach z dostawcami	Data wyd.: 26.02.2024

Załącznik nr 1 - Wzór oświadczenia o zapoznaniu się i zobowiązaniu pracownika dostawcy do stosowania zapisów Zasad bezpieczeństwa informacji w relacjach z dostawcami

Warszawa, dnia.....

.....
Imię i nazwisko

.....
Nazwa (Dostawca)

Oświadczenie

Oświadczam, że zapoznałem/zapoznałam się z treścią i zobowiązuję się do przestrzegania zapisów *Zasad bezpieczeństwa informacji w relacjach z dostawcami*, będących elementem Systemu Zarządzania Bezpieczeństwem Informacji Centralnej Komisji Egzaminacyjnej.

Ponadto, zobowiązuję się do:

1. Zachowania w tajemnicy informacji chronionych, których właścicielem jest Centralna Komisja Egzaminacyjna, w szczególności sposobów ich zabezpieczenia, zarówno w trakcie jak i po zakończeniu wykonywania zadań objętych umową/wykonywanych w celu realizacji umowy nr [...] zawartej dnia [...].
2. Niewykorzystywania żadnych informacji chronionych CKE w celu innym niż wykonywanie ww. zadań.

.....
Podpis