Zasady bezpieczeństwa informacji w relacjach z dostawcami

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 NID.
2. Określenie minimalnych wymagań w zakresie zabezpieczeń systemów informatycznych dostawcy.

2 Zakres

Niniejszy dokument stosuje dostawca zgodnie z zawartą umową z Narodowym Instytutem Dziedzictwa.

3 Terminologia

1. **Dostawca –** oznacza podmiot świadczący usługi na rzecz Narodowego Instytutu Dziedzictwa na podstawie odrębnych umów lub porozumień, którego pracownicy uzyskują dostęp do aktywów informacyjnych NID w związku z realizacją przedmiotu umowy.
2. **Użytkownik zewnętrzny –** pracownik lub podwykonawca dostawcy przetwarzający informacje w systemie informatycznym NID**.**
3. **Administrator Danych Osobowych (ADO) –** Dyrektor Narodowego Instytutu Dziedzictwa – 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 NID, które posiadają wartość materialną lub prawną.
5. **Autoryzacja –** potwierdzenie czy uwierzytelniony podmiot jest uprawniony do korzystania z danego zasobu.
6. **Dane osobowe –** informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Dane osobowe dzieli się na dane zwykłe i dane wrażliwe.
7. **Incydent –** zdarzenie, które ma lub może mieć niekorzystny wpływ na Aktywo informacyjne, powoduje lub może spowodować obniżenie jakości lub przerwanie świadczenia usług przez NID;
8. **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 NID odpowiedzialny za koordynację współpracy z dostawcą;
   b. dostawca, który został zobowiązany do jego przestrzegania w ramach zawartych umów z NID.

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 NID. Zasady bezpieczeństwa obejmują swym zakresem wszystkie podmioty, będące dostawcami produktów lub usług, mające dostęp do informacji chronionych NID. Zasady bezpieczeństwa są syntezą wymagań zawartych w dokumentacji Systemu Zarządzania Bezpieczeństwa Informacji, dotyczących bezpieczeństwa informacji NID.
2. Pracownik NID odpowiedzialny za sporządzenie umowy/porozumienia z dostawcą, jest każdorazowo zobligowany do uwzględnienia niniejszych Zasad bezpieczeństwa.
3. Dostawca będzie udostępniać NID wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w Zasadach bezpieczeństwa i przepisach prawa powszechnie obowiązującego oraz umożliwi NID lub audytorowi upoważnionemu przez Dyrektora NID do przeprowadzenie audytów i inspekcji w tym zakresie. W przypadku stwierdzenia nieprawidłowości podczas audytu lub inspekcji, ich uzasadnione koszty ponosi dostawca.
4. Dostawca spełnia wymagania Zasad bezpieczeństwa przed uzyskaniem dostępu do informacji chronionych NID.
5. Przed rozpoczęciem przetwarzania informacji chronionych, w szczególności danych osobowych, dostawca powinien spełnić następujące warunki:
   a. podpisać zobowiązanie do zachowania poufności przetwarzanych informacji na wzorze obowiązującym w NID;
   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 NID dane osobowe.

6 Zasady ogólne dotyczące przetwarzania informacji chronionych

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

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,

c. w przypadku, gdy do pomieszczeń dostawcy 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 NID po upływie czasu ich wykorzystania przez dostawcę zgodnie z umową z NID 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 NID.

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. 256-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. w przypadku przesyłania informacji chronionych pocztą elektroniczną wymagane jest stosowanie formy zaszyfrowanej za pomocą algorytmu wskazanego w ppkt a. powyżej, natomiast hasło do odszyfrowania należy przesłać 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 przesłać innym kanałem komunikacji np.: poprzez SMS. W stosowanym wypadku należy ustawić okres wygasania udostępnienia na nie dłuższy niż 14 dni.

e. dostawca nie może stosować innych kanałów wymiany informacji niż zaakceptowane przez NID.

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 NID 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 NID 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 przed dostępem osób nieupoważnionych,

c. nośniki zewnętrzne z informacjami chronionymi NID należy przechowywać w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym,

d. informacje chronione NID 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.

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

1. Hasła muszą podlegać następującym zasadom:
   a. hasło składa się z minimum 12 znaków;
   b. hasło musi spełniać warunek złożoności polegający na występowaniu w nim: wielkiej i małej litery, oraz cyfry lub znaku specjalnego (np. !@#);
   c. hasła należy przechowywać w sposób gwarantujący ich poufność.
2. Zabrania się udostępniania haseł osobom nieupoważnionym.
3. Należy stosować dwuskładnikowe uwierzytelnienie w sytuacji, gdy system posiada taką funkcjonalność.
4. 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,
5. Zabrania się tworzenia haseł łatwych do odgadnięcia.
6. W przypadku logowania do systemu informatycznego odbywającego się po raz pierwszy, pracownik dostawcy ma obowiązek zmiany hasła tymczasowego na właściwe, na znane tylko pracownikowi dostawcy:
7. W przypadku systemów informatycznych, które nie wymuszają stosowania zgodnej z pkt powyżej polityki haseł, obowiązkiem pracownika dostawcy jest zapewnienie zgodności z zasadami określonymi w ust. poprzednich.
8. Pracownik dostawcy ponosi pełną odpowiedzialność za utworzenie hasła i jego bezpieczne przechowywanie.
9. Hasła tworzone przez pracownika dostawcy nie mogą być ujawniane w sposób celowy lub przypadkowy i mogą być znane wyłącznie pracownikowi dostawcy.
10. 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.
11. W przypadku podejrzenia ujawnienia haseł osobie nieupoważnionej, pracownik dostawcy niezwłocznie zmienia hasło i zgłasza incydent do NID.
12. Pracownik dostawcy utrzymuje hasło w tajemnicy również po upływie jego ważności.

6.3 Zasady zabezpieczeń komputerów zawierających informacje chronione NID

1. Do systemu informatycznego NID 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. Wyłączona dowolna funkcja automatycznego uruchamiania, która umożliwia wykonywanie programów bez autoryzacji użytkownika (na przykład podczas pobierania z Internetu);
    e. stosować ochronę kryptograficzną wobec danych przetwarzanych na komputerze przenośnym;
    f. zabezpieczyć dostęp do komputera na poziomie systemu operacyjnego stosując identyfikator i hasło;
    g. nie zezwalać na używanie komputera osobom nieupoważnionym;
    h. zachować szczególną ostrożność przy podłączaniu komputera przenośnego do sieci publicznych poza budynkami i pomieszczeniami NID 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 w przypadku przetwarzania danych NID.

6.4 Usługi zarządzane zewnętrznie (w tym cloud)

W przypadku korzystania z usług zarządzanych zewnętrznie, 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.

6.5 Ochrona sieci

6.5.1 Wymagane jest stosowanie jednej z metod ochrony sieci dostawcy:

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 zapora oparta na hoście; działa to w taki sam sposób, jak firewall brzegowy, ale chroni tylko jedno urządzenie, na którym jest skonfigurowany.

7 Zgłaszanie incydentu bezpieczeństwa informacji

1. Każdy incydent bezpieczeństwa informacji NID wymaga odpowiedniej reakcji, w tym w szczególności poinformowania o wystąpieniu naruszenia NID. Obowiązek w tym zakresie spoczywa **na dostawcach,** którzy uzyskali dostęp na mocy zawartej umowy do informacji chronionych NID.

2. Dostawca jest zobligowany do posiadania opracowanego dokumentu Polityki Bezpieczeństwa Informacji i/lub Polityki Bezpieczeństwa Danych Osobowych wraz z zasadami obsługi incydentów bezpieczeństwa informacji oraz naruszeń ochrony danych osobowych, o których mowa w art. 4 ust 12 RODO.

3. W przypadku powierzenia przez NID dostawcy do przetwarzania danych osobowych, NID mając na uwadze potrzebę zachowania gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych przez dostawcę będącym także podmiotem przetwarzającym w świetle RODO zastrzega sobie prawo audytu dostawcy w celu weryfikacji wiarygodność w obszarze ochrony danych osobowych.

4. W przypadku naruszenia bezpieczeństwa informacji chronionych NID, dostawca postępuje zgodnie z zapisami umowy zawartej pomiędzy NID i tym dostawcą.

5. Naruszeniem bezpieczeństwa informacji może być w szczególności:

   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. Kradzież lub zagubienie dokumentów lub nośników z informacjami podlegającymi ochronie;

   f. Wyciek informacji chronionych, w tym w szczególności danych osobowych;

   g. Utrata danych;

   h. Nieuprawnione uszkodzenie lub zniszczenie danych.

8 Postanowienia końcowe

W przypadku naruszenia przez dostawcę postanowień Zasad bezpieczeństwa, NID jest uprawniony do rozwiązania umowy z dostawcą i/lub nałożenia kar umownych wynikających z podpisanej umowy.