

Zasady bezpieczeństwa informacji w relacjach z dostawcami

1. Celem dokumentu jest określenie minimalnych wymagań w zakresie:
 - a) bezpieczeństwa informacji dla dostawców mających dostęp na mocy zawartych umów do informacji Urzędu Miasta Gorzowa Wielkopolskiego;
 - b) zabezpieczeń systemów informatycznych dostawcy.
 2. Niniejszy dokument stosuje dostawca zgodnie z zawartą umową z Urzędem Miasta Gorzowa Wielkopolskiego.
 3. Za nadzór nad przestrzeganiem niniejszego dokumentu odpowiedzialni są:
 - a) pracownik Urzędu Miasta Gorzowa Wielkopolskiego odpowiedzialny za koordynację współpracy z dostawcą;
 - b) dostawca, który został zobowiązany do jego przestrzegania w ramach zawartych umów.
 4. Zasady bezpieczeństwa informacji w relacjach z dostawcami, zwane dalej Zasadami bezpieczeństwa, określają zakres obowiązków i odpowiedzialności dostawców w zakresie bezpieczeństwa informacji Urzędu Miasta Gorzowa Wielkopolskiego.
 5. Zasady bezpieczeństwa obejmują swym zakresem wszystkie podmioty, będące dostawcami produktów lub usług, mające dostęp do informacji Urzędu Miasta Gorzowa Wielkopolskiego.
 6. Zasady bezpieczeństwa są syntezą wymagań zawartych w dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji Urzędu Miasta Gorzowa Wielkopolskiego.
 7. Pracownik Urzędu Miasta Gorzowa Wielkopolskiego odpowiedzialny za sporządzenie umowy/porozumienia z dostawcą, jest każdorazowo zobligowany do uwzględnienia niniejszych Zasad bezpieczeństwa.
 8. Dostawca będzie udostępniać wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w Zasadach bezpieczeństwa i przepisach prawa powszechnie obowiązującego oraz umożliwi audytorowi ds. Systemu Zarządzania Bezpieczeństwem Informacji lub upoważnionemu przez Prezydenta Miasta Gorzowa Wielkopolskiego przeprowadzenie audytów Systemu Zarządzania Bezpieczeństwem Informacji i inspekcji w tym zakresie. W przypadku stwierdzenia nieprawidłowości podczas audytu Systemu Zarządzania Bezpieczeństwem Informacji lub inspekcji, ich uzasadnione koszty ponosi dostawca.
 9. Dostawca spełnia wymagania Zasad bezpieczeństwa przed uzyskaniem dostępu do informacji Urzędu Miasta Gorzowa Wielkopolskiego, co potwierdzają przedstawiciele dostawcy realizujący zadania na rzecz Urzędu Miasta Gorzowa Wielkopolskiego. Wykonawca poświadcza spełnienie tych warunków podpisując zlecenie realizacji prac na rzecz Urzędu Miasta Gorzowa Wielkopolskiego.
 10. Przed rozpoczęciem przetwarzania informacji, w szczególności danych osobowych, dostawca powinien spełnić następujące warunki:
 - a) podpisać zobowiązanie do zachowania poufności przetwarzanych informacji na wzorze obowiązującym w Urzędzie Miasta Gorzowa Wielkopolskiego,
 - b) jeżeli realizacja umowy związana jest z przetwarzaniem danych osobowych:
 - w stosownym przypadku podpisać umowę powierzenia przetwarzania danych osobowych,
 - w stosownym przypadku wydać upoważnienia osobom przetwarzającym powierzone przez Administratora Danych Osobowych dane osobowe.
- ### **1. Zasady ogólne dotyczące przetwarzania informacji**
1. Zasady postępowania dla dokumentów papierowych i danych elektronicznych zawierających informacje Urzędu Miasta Gorzowa Wielkopolskiego:
 - a) dokumenty papierowe, wydruki komputerowe:
 - wydruki zabezpiecza się przed dostępem osób nieupoważnionych,
 - wszelkie wydruki zawierające dane osobowe muszą być przechowywane w miejscu niedostępnym dla osób nieupoważnionych,
 - w przypadku, gdy do pomieszczeń po godzinach pracy mają dostęp osoby nieupoważnione, dokumenty zawierające informacje zabezpiecza się na ten czas w szafach zamykanych na klucz, dotyczy to również kopii dokumentów,
 - wydruki zawierające informacje po upływie czasu ich wykorzystania przez dostawcę zgodnie z umową należy niszczyć przy pomocy niszczarki o skuteczności niszczenia min. P4 lub przechowywać

w pojemnikach przeznaczonych do bezpiecznego niszczenia dokumentacji dostarczanych przez upoważniony podmiot,

- po zakończeniu każdego dnia pracy osoby mające dostęp do informacji stosują zasadę „czystego biurka” w odniesieniu do dokumentów i innych nośników zawierających informacje.

b) informacje w formie elektronicznej – przechowywanie:

- 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,

- dokumenty i dane mogą być przesyłane wyłącznie za pośrednictwem kanałów szyfrowanych, w szczególności VPN, za pomocą algorytmu AES,

- dane osobowe szczególnie (zgodne z art. 9 RODO) mogą być przesyłane pocztą elektroniczną wyłącznie w formie zaszyfrowanej za pomocą algorytmu AES, natomiast hasło do odszyfrowania należy przesłać innym kanałem komunikacji np.: poprzez SMS,

- w sytuacji, kiedy konieczna jest wymiana informacji zawierających dane szczególnie (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 e-mail lub SMS.

c) zasady postępowania w przypadku korzystania z zewnętrznych nośników elektronicznych (pendrive, zewnętrzne dyski magnetyczne, aparaty fotograficzne, dyktafony, kamery i inne) zawierających informacje:

- zewnętrzne nośniki elektroniczne zawierające informacje Urzędu Miasta Gorzowa Wielkopolskiego zabezpiecza się przed dostępem osób nieupoważnionych np. poprzez zabezpieczenie w szafie zamykanej na klucz; za bezpieczne przechowywanie tych nośników odpowiedzialni są pracownicy dostawcy,

- przenoszenie informacji na zewnętrznym nośniku elektronicznym poza siedzibę Urzędu Miasta Gorzowa Wielkopolskiego lub dostawcy może odbywać się tylko zgodnie z zapisami niniejszych zasad bezpieczeństwa; informacje znajdujące się na takich nośnikach muszą być zaszyfrowane algorytmem AES, 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,

- nośniki zewnętrzne z informacjami chronionymi Urzędu Miasta Gorzowa Wielkopolskiego należy przechowywać w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym,

- informacje Urzędu Miasta Gorzowa Wielkopolskiego w postaci elektronicznej należy usuwać z nośnika niezwłocznie po ustaniu ich przydatności, w sposób uniemożliwiający ich ponowne odzyskanie,

- 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.

2. Zasady haseł użytkowników aplikacji i systemów informatycznych wykorzystywanych do przetwarzania informacji:

a) hasła muszą podlegać następującym zasadom:

- składać się z minimum 8 znaków,

- spełniać warunek złożoności polegający na występowaniu w nim: wielkiej i małej litery, oraz cyfry lub znaku specjalnego (np. !@#),

- być zmieniane minimum co 30 dni,

- muszą być różne,

- należy je przechowywać w sposób gwarantujący ich poufność.

b) zabrania się udostępniania haseł osobom nieupoważnionym,

c) zabrania się tworzenia haseł na podstawie:

- cech i numerów osobistych (np. dat urodzenia, imion itp.),

- sekwencji klawiszy klawiatury (np. qwerty, 12qwaszx),

- identyfikatora użytkownika.

d) zabrania się tworzenia haseł łatwych do odgadnięcia,

e) przypadku logowania do systemu informatycznego odbywającego się po raz pierwszy, pracownik dostawcy ma obowiązek zmiany hasła tymczasowego na właściwe, na znane tylko pracownikowi dostawcy,

- f) w przypadku systemów informatycznych, które nie wymuszają cyklicznej zmiany hasła oraz nie kontrolują jego złożoności, obowiązkiem pracownika dostawcy jest samodzielna cykliczna zmiana hasła zgodnie z zasadami określonymi powyżej,
- g) pracownik dostawcy ponosi pełną odpowiedzialność za utworzenie hasła i jego bezpieczne przechowywanie,
- h) hasła tworzone przez pracownika dostawcy nie mogą być ujawniane w sposób celowy lub przypadkowy i mogą być znane wyłącznie pracownikowi dostawcy,
- i) hasła nie mogą być przechowywane w formie dostępnej dla osób nieupoważnionych:
 - w plikach,
 - na kartkach w miejscach dostępnych dla osób trzecich,
 - w skryptach,
 - w innych zapisach elektronicznych i papierowych, które byłyby dostępne dla osób trzecich.
- j) w przypadku podejrzenia ujawnienia hasła osobie nieupoważnionej, pracownik dostawcy niezwłocznie zmienia hasło i zgłasza incydent wyznaczonemu pracownikowi Urzędu Miasta Gorzowa Wielkopolskiego,
- k) pracownik dostawcy utrzymuje hasło w tajemnicy również po upływie jego ważności,
- l) zabrania się przekazywania hasła za pomocą telefonu, przesyłania z pomocą faksu i poczty e-mail w formie jawnej (niezaszyfrowanej).

3. Zasady zabezpieczeń komputerów zawierających informacje:

Do systemu informatycznego Urzędu Miasta Gorzowa Wielkopolskiego 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 Urzędu Miasta Gorzowa Wielkopolskiego.

4. Zasady zabezpieczania komputerów przenośnych zawierających informacje.

- a) użytkownik komputera przenośnego, zawierającego informacje Urzędu Miasta Gorzowa Wielkopolskiego, zobowiązany jest:
 - stosować ochronę kryptograficzną wobec danych przetwarzanych na komputerze przenośnym,
 - zabezpieczyć dostęp do komputera na poziomie systemu operacyjnego stosując identyfikator i hasło,
 - nie zezwalać na używanie komputera osobom nieupoważnionym,
 - zachować szczególną ostrożność przy podłączaniu komputera przenośnego do sieci publicznych poza budynkami i pomieszczeniami Urzędu Miasta Gorzowa Wielkopolskiego lub dostawcy.
- b) komputer przenośny nie może być pozostawiany w miejscu narażającym go na kradzież (np. w otwartym pomieszczeniu, w samochodzie),
- c) powyższe zasady stosuje się odpowiednio do tabletów oraz smartfonów.

5. Usługi zarządzane zewnętrznymi (w tym w chmurze):

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. Aplikacje internetowe:

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

7. Ochrona sieci:

a) wymagane jest stosowanie jednej z metod ochrony sieci:

- 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,
- 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.

b) urządzenia sieciowe (przełączniki, routery, firewall lub równoważne):

- w przypadku wszystkich firewall sieciowych (lub równoważnych urządzeń sieciowych) dostawca musi:
 - zmienić domyślne hasło administracyjne na alternatywne, które jest trudne do odgadnięcia — lub całkowicie wyłączyć zdalny dostęp administracyjny,
 - 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: dostęp tylko poprzez VPN lub drugi składnik uwierzytelniania np. kod jednorazowy lub lista dozwolonych adresów IP, która ogranicza dostęp do niewielkiego zakresu zaufanych adresów.
- domyślne blokować niewierzytelne połączenia przychodzące,
- zapewnić, że przychodzące reguły firewall są zatwierdzone i udokumentowane przez upoważnioną osobę.

2. Postanowienia końcowe

W przypadku naruszenia przez dostawcę postanowień Zasad bezpieczeństwa, Administrator Danych Osobowych jest uprawniony do nałożenia kar umownych wynikających z podpisanej umowy.