Regulamin Ochrony Informacji dla Wykonawcy
Centrum Informatycznych Usług Wspólnych Olsztyna

2 Cel

Celem dokumentu w Centrum Informatycznych Usług Wspólnych Olsztyna jest:

§ 1. Określenie minimalnych środków technicznych i organizacyjnych służących zabezpieczeniu danych.

§ 2. Określenie minimalnych wymagań w zakresie bezpieczeństwa informacji dla podmiotów zewnętrznych.

§ 3. Określenie minimalnych wymagań w zakresie zabezpieczeń systemów teleinformatycznych.

3 Zakres

§ 1. Niniejszy dokument stosują wszystkie podmioty zewnętrzne wykonujące prace na rzecz Centrum Informatycznych Usług Wspólnych Olsztyna (zwanego dalej CIUWO), związane z przetwarzaniem Aktywów informacyjnych Centrum Informatycznych Usług Wspólnych Olsztyna.

§ 2. Niniejszy dokument należy stosować we wszystkich umowach z podmiotami zewnętrznymi, których przedmiot jest związany z ochroną informacji.

§ 3. Stosowanie niniejszego dokumentu określającego minimalne środki techniczne i organizacyjne nie zwalnia podmiotów zewnętrznych ze stosowania środków adekwatnych, tj. dostosowanych do rodzaju przetwarzanych danych i sposobu ich przetwarzania tak, żeby zapewnić bezpieczeństwo przetwarzania stosownie do ryzyka naruszenia praw i wolności osób, których dane dotyczą, a które w konkretnych przypadkach mogą być dalej idące.

4 Terminologia

Pojęcia używane w Regulaminie:

Aktywo i zasób informacyjny - wszelkie informacje w formie papierowej, elektronicznej i innej, przetwarzane (zbierane, utrwalane, przechowywane, opracowywane, zmieniane, udostępniane i usuwane) w sposób tradycyjny lub w systemach informatycznych, będące własnością CIUWO lub wykorzystywane bądź administrowane bądź zarządzane przez CIUWO.

Główny Administrator Bezpieczeństwa Systemów (GABS) – nadzoruje bezpieczeństwo wszystkich systemów teleinformatycznych. Jest odpowiedzialny za dopuszczanie systemów teleinformatycznych do eksploatacji.

System informatyczny, System –zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

System Teleinformatyczny - zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego.

System Zarządzania Bezpieczeństwem Informacji (SZBI)- część całościowego systemu zarządzania, oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji.

5 Postanowienia ogólne

§ 1. Regulamin Ochrony Informacji dla Wykonawcy Centrum Informatycznych Usług Wspólnych Olsztyna (zwany dalej Regulaminem) określa zakres obowiązków i odpowiedzialności podmiotów zewnętrznych w zakresie bezpieczeństwa informacji. Regulamin obejmuje swym zakresem wszystkich użytkowników podmiotów zewnętrznych, mających dostęp do systemów teleinformatycznych Centrum Informatycznych Usług Wspólnych Olsztyna.

§ 2. Podmiot zewnętrzny spełnia wymagania niniejszego Regulaminu przed uzyskaniem dostępu do Systemu Teleinformatycznego CIUWO.

§ 3. Przed rozpoczęciem przetwarzania informacji chronionych, w szczególności danych osobowych przetwarzanych przez CIUWO, podmiot zewnętrzny powinien spełnić następujące warunki:

a. w przypadku przetwarzania Informacji Poufnych - podpisać zobowiązanie do zachowania poufności przetwarzanych danych na wzorze obowiązującym w CIUWO, będącym załącznikiem nr 1 do Regulaminu.

b. w przypadku przetwarzania Informacji Poufnych i Danych - podpisać umowę powierzenia przetwarzania danych osobowych oraz o zachowaniu poufności informacji na wzorze obowiązującym w CIUWO, będącym załącznikiem nr 2 do Regulaminu.

6 Nadawanie, zmiana bądź odebranie uprawnień

§ 1. W przypadku podmiotów zewnętrznych, zakres uprawnień w poszczególnych systemach i aplikacjach ustawia się adekwatnie do przedmiotu umowy i zakresu powierzonych danych osobowych.

§ 2. Lista użytkowników podmiotu zewnętrznego powinna być dostarczona przez osoby ze strony podmiotu zewnętrznego wskazane w umowie jako odpowiedzialne za jej realizację.

§ 3. Po każdej zmianie użytkowników ze strony podmiotu zewnętrznego, jest on zobowiązany do przekazania listy użytkowników ze wskazaniem zmian w ich zakresie uprawnień.

§ 4. Rejestrowanie/wyrejestrowanie użytkowników zewnętrznych Systemu Teleinformatycznego CIUWO oraz nadawanie/zmiana/odebranie uprawnień jest realizowane przez pracowników CIUWO:

a. Podczas rejestracji użytkownika zewnętrznego nadawany jest przez administratora systemu unikalny identyfikator użytkownika oraz ustawiane jest hasło tymczasowe niezbędne do logowania po raz pierwszy do Systemu (zgodne z zasadami opisanymi w niniejszej procedurze) dla użytkownika zewnętrznego Systemu Teleinformatycznego.

b. O nadaniu/zmianie/odebraniu uprawnień właściwych identyfikatorów w odpowiednich systemach i aplikacjach i nadaniu właściwych uprawnień administrator systemu informuje GABS oraz przedstawiciela podmiotu zewnętrznego.

7 Metody i środki uwierzytelniania

Dostęp do poszczególnych części systemu informatycznego jest możliwy wyłącznie poprzez podanie prawidłowego identyfikatora i hasła przyznanych użytkownikowi podczas procesu nadawania uprawnień do Systemu Teleinformatycznego.

Hasła użytkowników

§ 1. Hasła użytkowników do systemów powinny podlegać następującym zasadom:

a. hasło składa się z minimum 8 znaków,

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

c. hasło musi być zmieniane minimum co 30 dni,

d. kolejne hasła muszą być różne,

e. hasła należy przechowywać w sposób gwarantujący ich poufność,

§ 2. Zabrania się udostępniania haseł innym osobom.

§ 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. Zabrania się tworzenia haseł łatwych do odgadnięcia.

§ 5. Logowanie anonimowe do systemu informatycznego jest zabronione dla użytkowników.

§ 6. Uwierzytelnienie następuje wyłącznie po podaniu zgodnego hasła i powiązanego z nim identyfikatora.

§ 7. W przypadku logowania do systemu informatycznego odbywającego się po raz pierwszy, użytkownik ma obowiązek zmiany hasła tymczasowego na właściwe, na znane tylko użytkownikowi.

§ 8. W przypadku systemów, które nie wymuszają automatycznie cyklicznej zmiany hasła oraz nie kontrolują jego znaków, obowiązkiem użytkownika jest zmiana hasła zgodnie z zasadami określonymi w punktach poprzednich.

§ 9. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego bezpieczne przechowywanie.

§ 10. Hasła nie mogą być ujawniane w sposób celowy lub przypadkowy i powinny być znane wyłącznie użytkownikowi.

§ 11. Hasła nie powinny być przechowywane w formie dostępnej dla osób nieupoważnionych:

a. w plikach,

b. na kartkach papieru w miejscach dostępnych dla osób trzecich,

c. w skryptach,

d. w innych zapisach elektronicznych i papierowych, które byłyby dostępne dla osób trzecich.

§ 12. W przypadku podejrzenia ujawnienia haseł osobie nieupoważnionej, hasła muszą zostać natychmiast zmienione przez użytkownika lub Administratora Systemu.

§ 13. Hasło użytkownika sytemu umożliwiające dostęp do Systemu Teleinformatycznego utrzymuje się w tajemnicy również po upływie jego ważności.

§ 14. Zmiany hasła dokonuje użytkownik. W przypadku gdy użytkownik zapomniał hasła, właściwy Administrator Systemu ustawia hasło tymczasowe użytkownikowi z wymuszeniem jego zmiany podczas pierwszego logowania.

§ 15. Hasła przez użytkowników nie powinny być przekazywane przesyłane za pomocą telefonu, faksu, bądź poczty e-mail w formie jawnej.

§ 16. W przypadku grupowego tworzenia kont użytkowników generowane hasła powinny być unikalne.

8 Dostęp zdalny

§ 1. CIUWO prowadzi pisemny wykaz osób i podmiotów zewnętrznych posiadających dostęp zdalny do zasobów Systemu Teleinformatycznego CIUWO.

§ 2. Dostęp zdalny podmiotów zewnętrznych możliwy jest tylko po spełnieniu warunków wymienionych w niniejszym Regulaminie.

§ 3. Dla każdej umowy z podmiotem zewnętrznym Dyrektor CIUWO wyznacza Koordynatora Prac Zdalnych CIUWO (dalej zwany KPZ) zgodnie z wzorem określonym w załączniku nr 4.

§ 4. Podmiot zewnętrzny powierzając prace swoim pracownikom we własnym zakresie udziela im niezbędnych pełnomocnictw.

§ 5. Dostępu udziela się na czas obowiązywania umowy na podstawie pisemnego wniosku przekazanego przez podmiot zewnętrzny do KPZ o podanie potrzebnych identyfikatorów i haseł dostępu.

§ 6. W ramach dostępu zabrania się podmiotowi zewnętrznemu trwale usuwać dane, przeprowadzać jakiekolwiek operacje na dyskach mogące prowadzić do ich uszkodzenia lub utraty danych, w szczególności ich formatowania. Przedstawiciel podmiotu zewnętrznego wykonujący prace, przystępując do czynności, o których wie, że w konsekwencji doprowadzić one mogą do zniszczenia danych, musi poinformować przedstawiciela Zamawiającego i dopiero po jego akceptacji podjąć może te czynności.

§ 7. W przypadku konieczności realizacji prac na środowisku produkcyjnym, podmiot zewnętrzny uzgadnia z KPZ termin prowadzenia prac obarczonych ryzykiem o którym mowa w §8, przed przystąpieniem do prac, przedstawia scenariusz planowanych prac wraz z oceną ryzyka podejmowanych czynności. Podmiot zewnętrzny odpowiada za odstępstwa od przedstawionego scenariusza. Scenariusz powinien obejmować:

a. Czas (moment) podjęcia planowanych prac, przewidywany czas trwania prac.

b. Zakres wykonywanych prac.

c. Informację, czy wymagana jest przerwa w pracy użytkowników.

d. Potencjalne ryzyka podejmowanych czynności.

§ 8. Pracownik lub przedstawiciel podmiotu zewnętrznego wykonujący prace, przystępując do czynności, co do których istnieje wysokie ryzyko utraty danych lub przerwy w działaniu systemu, informuje o ryzyku KPZ.

§ 9. KPZ w przypadku otrzymania informacji o wysokim ryzyku utraty danych ustala możliwość rozpoczęcia prac z bezpośrednim przełożonym, Głównym Administratorem Bezpieczeństwa Systemów, a w przypadku takiej potrzeby - z innymi administratorami, w tym z administratorem systemu sesji zdalnych. Po akceptacji ryzyka przez KPZ w formie dokumentowej, pracownik podmiotu zewnętrznego może rozpocząć realizację czynności objętej wskazanym ryzykiem. W przypadku braku akceptacji ryzyka, strony podejmują działania w celu usunięcia potencjalnych podatności dla ryzyka, a następnie przedstawiciel podmiotu zewnętrznego postępuje zgodnie z §7 i §8 powyżej.

§ 10. Wykonywanie prac polegających na standardowej obsłudze serwisowej, prac nad rozwojem programu będącego w fazie wdrażania nie wymaga każdorazowego ustalenia warunków realizacji czynności, będącej ich częścią. W ramach wykonywania tych czynności obowiązują warunki uzgodnione wcześniej. W szczególności

nie wymagają każdorazowego ustalenia warunków realizacji te czynności, które wynikają z przedmiotu umowy i nie są objęte ryzykami opisanymi w pkt. 6-8. Wykonywanie czynności niestandardowych wymaga każdorazowo określenia warunków.

§ 11. Zabrania się podejmowania czynności zmierzających do penetrowania zasobów sieci CIUWO.

§ 12. Zabrania się dostępu zdalnego z komputerów dostępnych publicznie np. kafejki internetowe, dworce PKP, restauracje, bezprzewodowe sieci miejskie.

§ 13. Dostęp zdalny jest przez CIUWO monitorowany.

§ 14. Monitorowanie odbywa się poprzez:

a. Logowanie ruchu w zakresie wszystkich sesji połączeń.

b. Nadzór nad wykonawcami za pomocą systemu monitorowania zdalnych sesji w zakresie prac wykonywanych zdalnie w sieci Urzędu,

c. Centralny system korelacji logów (SIEM) zbiera informacje ze wszystkich systemów i ocenia stopień zagrożenia sieci LAN.

§ 15. W przypadku realizacji umowy głównej w trybie SaaS, IaaS lub DaaS, zapewnienie realizacji obowiązków określonych w pkt. 8 realizuje podmiot zewnętrzny.

9 Wymagania zabezpieczeń

9.1 Zasady zabezpieczeń zasobów serwerowych i stacji roboczych

§ 1. Do systemu informatycznego 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 zabezpieczeń.

c. Firewall jest uruchomiony w systemie operacyjnym i posiada właściwą konfigurację, odpowiadającą wykonywanym obowiązkom pracowniczym przez użytkowników komputera.

d. Zainstalowane na komputerze oprogramowanie pochodzi z godnych zaufania źródeł.

e. Oprogramowanie jest zainstalowane zgodnie z postanowieniami licencji producenta oprogramowania.

f. Oprogramowanie nie łamie i nie narusza w żadnym stopniu przepisów Ustawy o prawie autorskim i prawach pokrewnych z dnia 4 lutego 1994 r. z późniejszymi zmianami.

§ 2. W przypadku realizacji umowy głównej w trybie SaaS Podmiot zewnętrzny zobowiązuje się dodatkowo do:

a. W zakresie realizacji polityki Antywirusowej - do aktualizacji bazy definicji wirusów i przeprowadzania co najmniej cotygodniowego skanu Antywirusowego wszystkich serwerów na których są zlokalizowane zasoby CIUWO. Skanowanie będzie przeprowadzane w godzinach nocnych/rannych. Ponadto Podmiot zewnętrzny zobowiązuje się do uruchomienia skanowania Antywirusowego na żądanie Zamawiającego w przypadku pozyskania przez niego informacji o zagrożeniu.

b. Celem potwierdzenia wywiązania się z realizacji zadań, przekazania do CIUWO pisemnego raportu 1 (jeden) raz na kwartał, zawierającego:

- planowaną ilość wykonanych kopii zapasowych i rzeczywistą ilość wykonanych kopii zapasowych,

- potwierdzenie przeprowadzenia skanu Antywirusowego wszystkich serwerów, na których są zlokalizowane zasoby Zamawiającego wraz z wynikami skanu.

9.2 Stosowanie zabezpieczeń kryptograficznych

W celu ochrony poufności przesyłanych oraz przechowywanych danych, stosuje się zabezpieczenia kryptograficzne. Miejsca stosowania kryptografii powinny być zgodne z wymaganiami prawnymi oraz regulacjami wewnętrznymi. Zabezpieczenia kryptograficzne należy stosować w szczególności:

§ 1. Na dyskach twardych komputerów przenośnych.

§ 2. Na pendrive'ach.

§ 3. Na nośnikach kopii zapasowych przechowywanych poza Systemem Teleinformatycznym Urzędu.

§ 4. Na urządzeniach typu smartfon oraz tablet w aplikacjach, które przechowują dane objęte ochroną np. dane osobowe.

§ 5. Tunelach VPN.

§ 6. Wiadomościach poczty elektronicznej, w których przesyłane są dane objęte ochroną, w szczególności dane osobowe.

§ 7. Zakres stosowanych rozwiązań kryptograficznych powinien obejmować minimum dane znajdujące się na nośnikach, które objęte są ochroną ze względu na wymagania utrzymania odpowiedniego poziomu poufności.

§ 8. Rozwiązania kryptograficzne powinny wykorzystywać algorytm AES o długości klucza min. 256 bit.

10 Reagowanie na incydenty

§ 1. O ile zawarte między CIUWO a podmiotem zewnętrznym umowy nie przewidują dalej idących zobowiązań, każde naruszenie bezpieczeństwa informacji należy w ciągu 12 godzin od powzięcia informacji o jego wystąpieniu zgłaszać Inspektorowi Ochrony Danych telefonicznie pod numer 89 5273111 wew. 725 lub w formie e-mail za potwierdzeniem odbioru na adres iod@ciuwo.olsztyn.eu z tematem wiadomości „Naruszenie bezpieczeństwa informacji".

§ 2. Inspektor Ochrony Danych w porozumieniu z Dyrektorem CIUWO, jeśli zdarzenie jest ewidentnym naruszeniem bezpieczeństwa, może zdecydować o natychmiastowym odebraniu uprawnień w systemach użytkownikom podmiotu zewnętrznego, przy czym w takiej sytuacji bez zbędnej zwłoki przekazuje on informację o blokadzie dostępu osobie upoważnionej ze strony podmiotu zewnętrznego.

§ 3. Upoważnione osoby z podmiotu zewnętrznego zabezpieczają ślady (np. logi systemowe) naruszenia bezpieczeństwa.

§ 4. W stosownych przypadkach Administrator Danych informuje o wystąpieniu incydentu bezpieczeństwa organ nadzorczy ds. ochrony danych osobowych oraz Podmiot danych.

§ 5. W szczególnych przypadkach Administrator Danych informuje organy ścigania o zaistniałej sytuacji.

§ 6. Sposób zgłaszania incydentów bezpieczeństwa przez Podmioty Zewnętrzne, postępowanie i odpowiedzialność dla naruszeń bezpieczeństwa określa umowa powierzenia przetwarzania danych osobowych oraz o zachowaniu poufności informacji.

11 Postanowienia końcowe

§ 1. Za nadzór nad przestrzeganiem postanowień Regulaminu odpowiada:

a. Ze strony podmiotu zewnętrznego - uprawniony przedstawiciel tego podmiotu.

b. Ze strony CIUWO - Inspektor Ochrony Danych oraz Główny Administrator Bezpieczeństwa Systemów.

§ 2. Naruszając Regulamin, podmiot zewnętrzny może podlegać sankcjom karnym, cywilnym oraz wynikającym z przepisów RODO.

12 Lista dokumentów związanych

§ 1. Wzór zobowiązania do zachowania poufności przetwarzanych danych;

§ 2. Wzór umowy powierzenia przetwarzania danych osobowych oraz o zachowaniu poufności informacji.

13 Załączniki

§ 1. Wzór - wyznaczenie Koordynatora Prac Zdalnych CIUWO.