Załącznik nr 3 do umowy

Wymagania bezpieczeństwa informacji
dla kontrahentów i osób zewnętrznych

I. Wstęp

1. Wymagania bezpieczeństwa informacji dla kontrahentów i osób zewnętrznych (Wymagania) stanowią element Systemu Zarządzania Bezpieczeństwem Informacji w statystyce publicznej[1].
2. Wymagania stanowią zbiór zasad obowiązujących:
   a) kontrahentów realizujących dostawy lub świadczących usługi na rzecz jednostek służb statystyki publicznej (jssp);
   b) osoby spoza jssp, które uzyskują dostęp do zasobów informacyjnych na podstawie odrębnych przepisów prawa lub umów cywilno-prawnych.

II. Słownik pojęć

Główny Użytkownik – wyznaczony dla danego systemu przez Prezesa Głównego Urzędu Statystycznego kierownik jednostki służb statystyki publicznej lub inna wskazana osoba odpowiedzialna za zainicjowanie powstania systemu, ustalenie jego założeń i funkcjonalności oraz utrzymanie systemu i określanie kierunków jego rozwoju;

Jssp (jednostka organizacyjna służb statystyki publicznej) – Główny Urząd Statystyczny lub inna jednostka organizacyjna statystyki publicznej, utworzona na podstawie przepisów ustawy o statystyce publicznej [na podstawie ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej];

Incydent związany z bezpieczeństwem informacji (incydent bezpieczeństwa informacji) – pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji [na podstawie normy PN ISO/IEC 27000];

Pełnomocnik ds. SZBI – dyrektor komórki organizacyjnej GUS właściwej ds. bezpieczeństwa informacji [definicja własna];

System teleinformatyczny (TI) – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne [na podstawie art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne];

III. Bezpieczeństwo fizyczne i środowiskowe

1. W jssp wyróżnia się następujące obszary bezpieczne:
   a) Strefa chroniona (strefa administracyjna).
   b) Strefa zabezpieczona (strefa bezpieczeństwa).
2. Strefa chroniona (strefa administracyjna) to powierzchnia będąca w użytkowaniu jssp.
3. Na granicach strefy chronionej (administracyjnej) funkcjonuje kontrola dostępu (m.in. tripody i czytniki na drzwiach).
4. Dostęp do pomieszczeń magazynowych jest nadzorowany, prowadzona jest kontrola ruchu osobowego i materiałowego.
5. Osoby przebywające w strefie administracyjnej zobowiązane są do noszenia identyfikatorów w widocznym miejscu.
6. Strefa zabezpieczona (bezpieczeństwa) to wydzielona część strefy chronionej (administracyjnej), tj. pomieszczenia, w których znajdują się newralgiczne urządzenia systemów teleinformatycznych (serwerownie) oraz prowadzące do nich korytarze wyposażona w dodatkowe, niezależne systemy zabezpieczeń i kontroli dostępu.
7. Wstęp do strefy zabezpieczonej (bezpieczeństwa) jest ograniczony tylko do osób, które uzyskały stosowne uprawnienia. Wejście oraz wyjście ze stref bezpieczeństwa jest rejestrowane. Rejestruje się tożsamość osób oraz czas ich wejścia i wyjścia.
8. Wnoszenie i wynoszenie do i ze stref zabezpieczonych (bezpieczeństwa) elektronicznych nośników informacji jest nadzorowane.

---

[1] Zarządzenie nr 27 Prezesa Głównego Urzędu Statystycznego z dnia 22.12.2015 r. w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji w statystyce publicznej, zmienione zarządzeniem wewnętrznym nr 19 Prezesa Głównego Urzędu Statystycznego z dnia 12.06.2019 r.

9. W strefach zabezpieczonych (bezpieczeństwa) zabronione jest korzystanie z urządzeń fotograficznych, wideo, audio lub innych urządzeń nagrywających, np. kamer w urządzeniach przenośnych, w celu rejestracji obrazu lub dźwięku bez upoważnienia Głównego Użytkownika, do którego należy dane pomieszczenie.
10. Dopuszcza się przebywanie osób bez uprawnień dostępu do stref zabezpieczonych (bezpieczeństwa) tylko w wyjątkowych przypadkach, w określonym celu, za zezwoleniem Głównego Użytkownika. Przebywanie osób bez uprawnień dostępu do stref zabezpieczonych (bezpieczeństwa) możliwe jest wyłącznie pod nadzorem osoby posiadającej uprawnienia dostępu do danej strefy.
11. Pobyt osoby, która nie posiada uprawnień do przebywania w strefie zabezpieczonej (bezpieczeństwa), musi zostać odnotowany w stosownym rejestrze (tożsamość osoby, czas wejścia i wyjścia).
12. Ciągi komunikacyjne obiektów są zaopatrzone w tabliczki informujące o kierunku ewakuacji i w miarę potrzeby wyposażone w oświetlenie awaryjne. Zgodnie z przepisami prawa opracowane są instrukcje przeciwpożarowe.

IV. Dostęp do zasobów systemów teleinformatycznych

1. Dostęp do systemu teleinformatycznego mogą uzyskać wyłącznie uprawnieni użytkownicy.
2. Osoby niebędące pracownikami jssp nie mogą uzyskać profilu użytkownika ani uprawnień w zakresie korzystania z systemów teleinformatycznych bez uprzedniej, pisemnej zgody Głównego Użytkownika. Nie dotyczy to organów umocowanych prawnie.
3. Uprawnienia użytkowników niebędących pracownikami jssp mogą być przyznane tylko na czas określony (do 90 dni) z możliwością przedłużenia.
4. Warunki korzystania z połączenia wewnętrznej sieci jssp z zewnętrznymi sieciami regulują podpisane umowy, szczegółowo precyzujące warunki techniczne i funkcjonalne połączenia.
5. Zobowiązanie do przestrzegania niniejszych Wymagań, ochrony udostępnionych zasobów informacyjnych poprzez ograniczenie ich kopiowania i udostępniania oraz do ich zwrotu lub zniszczenia w momencie zakończenia umowy zawierają klauzule dotyczące obowiązku przestrzegania zasad bezpieczeństwa informacji.
6. Osoby wykonujące pracę na rzecz jssp posiadają dostęp tylko do zasobów, które są im niezbędne do realizacji prac – dostęp do innych zasobów jest zabroniony.

V. Ochrona danych osobowych

1. Kontrahent zobowiązuje się przetwarzać powierzone dane osobowe zgodnie z umową, rozporządzeniem RODO[2] oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
2. Kontrahent oświadcza, że stosuje środki bezpieczeństwa spełniające wymogi RODO.
3. Osoby przetwarzające dane osobowe, muszą uzyskać stosowne upoważnienie do przetwarzania danych osobowych we wskazanym zakresie.
4. Z kontrahentem oraz osobami spoza jssp, dopuszczonymi do przetwarzania danych osobowych na podstawie umów cywilno-prawnych zawiera się umowę powierzenia przetwarzania danych osobowych.
5. Umowy powierzenia zawierają szczegółowe uregulowania w zakresie przetwarzania powierzonych danych osobowych i ich ochrony.

VI. Dostęp do zasobów jssp z sieci innych instytucji

1. Jssp może umożliwić dostęp do sieci teleinformatycznej osobom i podmiotom uprawnionym na mocy przepisów prawa.
2. Wniosek o dostęp do sieci jssp powinien zawierać informacje o celu podłączenia, przewidywanej liczbie podłączonych stanowisk i użytkowników, metodzie zabezpieczenia przed nieautoryzowanym dostępem.
3. Przed wydaniem decyzji o zgodzie na podłączenie do sieci jssp zasięga się opinii Pełnomocnika ds. SZBI.
4. Specyfikacja techniczna połączenia musi być załącznikiem do porozumienia lub umowy zawartej pomiędzy jssp i instytucjami. Specyfikacja powinna zawierać w szczególności następujące ustalenia:
   a) połączenie powinno być szyfrowane oraz zabezpieczone odpowiednim certyfikatem;
   b) połączenie powinno być zestawiane jedynie między ściśle określonymi adresami IP podłączanej sieci oraz ściśle określonymi adresami IP sieci wewnętrznej jssp oraz dla ściśle określonych portów przypisanych do adresów w sieci jssp;
   c) każdorazowe zestawienie połączenia między podłączaną siecią a siecią jssp powinno być autoryzowane hasłem lub certyfikatem oraz podlegać rejestrowaniu (logowaniu);
   d) zasoby udostępniane użytkownikom z innych instytucji obejmują wyłącznie dostęp do aplikacji - nie są udostępniane takie zasoby jak serwery plików lub poczta elektroniczna.

---

[2] 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).

5. Użytkownicy z innych instytucji nie mogą posiadać praw administracyjnych.

VII. Ochrona przed szkodliwym oprogramowaniem i kodem mobilnym

1. Wszystkie elektroniczne nośniki informacji dostarczone z zewnątrz jssp nie mogą być użyte bez wcześniejszego sprawdzenia programem antywirusowym.
2. Wszystkie pliki przed wysłaniem lub przekazaniem stronom trzecim (osobom niebędącym pracownikami jssp) są testowane oprogramowaniem antywirusowym.

VIII. Odbiór systemu

1. Przed przekazaniem do użytkowania oprogramowania opracowanego na rzecz jssp, osoby je opracowujące muszą usunąć wszystkie specjalne ścieżki dostępu tak, aby dostęp był możliwy jedynie z zastosowaniem zasad bezpieczeństwa informacji. Oznacza to, że muszą być usunięte wszystkie nieudokumentowane funkcje pozwalające ominąć system zabezpieczeń. Muszą zostać również usunięte wszystkie uprawnienia systemowe ustanowione dla potrzeb prowadzenia prac nad oprogramowaniem, lecz zbędne w środowisku produkcyjnym.
2. W przypadku podjęcia decyzji o przechowywaniu kodu źródłowego pisanego na zamówienie jssp poza siedzibą jssp, konieczne jest również zawarcie umów depozytowych dotyczących takiego kodu źródłowego z podmiotami niezależnymi od dostawcy oprogramowania. Umowy te powinny określać niezależny podmiot, któremu twórca oprogramowania dostarczy kod źródłowy i wszystkie jego aktualizacje. Powinny też określać sytuacje, w których kod źródłowy zostanie udostępniony jssp, jak na przykład upadłość lub likwidacja dostawcy oprogramowania lub niewywiązywanie się przez niego z postanowień umowy dotyczących aktualizacji oprogramowania.

IX. Naruszenia bezpieczeństwa informacji oraz wnioski dotyczące bezpieczeństwa informacji

1. Odpowiedzialność za bezpieczeństwo informacji jssp obejmuje wszelkie sytuacje, w których informacje związane z działalnością jssp są przetwarzane, także poza jej siedzibą. Obejmuje to w szczególności zdalny dostęp do sieci teleinformatycznej jssp.
2. Pracownicy reprezentujący podmiot zewnętrzny mają obowiązek zgłaszania wszelkich zdarzeń, które naruszają lub mogą naruszyć przepisy prawa oraz polityki, procedury i instrukcje Urzędu dotyczące bezpieczeństwa informacji.
3. Każdy incydent związany z bezpieczeństwem informacji w jssp powinien być zgłoszony niezwłocznie.
4. Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji odbywa się przez dedykowaną stronę www (http://serwisdesk), e-mailem serwisdesk@stat.gov.pl bądź, w godzinach pracy urzędu, telefonicznie (22 608 3689).
5. Wnioski mające na celu podniesienie poziomu bezpieczeństwa informacji można zgłaszać z wykorzystaniem dostępnych metod komunikacji, o których mowa w ust. 4).
6. Naruszenie zasad bezpieczeństwa informacji przez praktykanta może skutkować natychmiastowym przerwaniem praktyki i rozwiązaniem umowy. W takim przypadku praktyka nie jest zaliczana.
7. Naruszenie zasad bezpieczeństwa informacji przez stażystę może skutkować natychmiastowym przerwaniem stażu i powiadomieniem instytucji kierującej na staż.
8. Naruszenie zasad bezpieczeństwa informacji przez wolontariusza może skutkować natychmiastowym przerwaniem świadczenia usług wolontariatu.
9. Naruszenie zasad bezpieczeństwa informacji przez osobę fizyczną, zatrudnioną na podstawie umowy innej niż umowa o pracę, może skutkować natychmiastowym rozwiązaniem umowy i stanowi podstawę do żądania pokrycia powstałej szkody lub zapłaty kary umownej wynikającej z zawartej umowy.
10. Naruszenie bezpieczeństwa informacji przez kontrahenta stanowi podstawę do odstąpienia przez jssp od umowy i żądania pokrycia ewentualnej szkody lub zapłaty kary umownej, wynikającej z zawartej umowy.