

Wymagania bezpieczeństwa informacji dla kontrahentów i osób zewnętrznych

I. Słownik pojęć

aktywa – wszystko, co ma wartość dla jednostek służb statystyki publicznej i z tego względu wymaga ochrony [na podstawie normy PN-ISO/IEC 27001];

komórka organizacyjna GUS – departament, biuro, wydział, samodzielne stanowisko pracy w Głównym Urzędzie Statystycznym;

jednostka służb statystyki publicznej – jednostki służb statystyki publicznej podległe i podporządkowane Prezesowi GUS (GUS, CBS, CIS, Zakład Wydawnictw Statystycznych, urzędy statystyczne);

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];

Właściciel Aktywu – dyrektor komórki organizacyjnej GUS/dyrektor jssp;

II. Zasady zachowania poufności danych i informacji

1. Kontrahenci i osoby z zewnątrz zobowiązują się do zachowania w poufności wszelkich danych i informacji, niezależnie od sposobu ich pozyskania (zamierzony lub przypadkowy) i bez względu na sposób i formę ich przekazania.
2. Obowiązek, o którym mowa w pkt 1, jeżeli przepisy prawa nie stanowią inaczej, obowiązuje przez okres 10 lat po jej rozwiązaniu, wygaśnięciu lub odstąpieniu od niej, bez względu na przyczynę.
3. Obowiązku zachowania poufności nie stosuje się do danych i informacji:
 - 1) dostępnych publicznie;
 - 2) otrzymanych zgodnie z przepisami prawa powszechnie obowiązującego, od osoby trzeciej bez obowiązku zachowania poufności;
 - 3) które w momencie ich przekazania były już znane kontrahentowi/ osobie z zewnątrz bez obowiązku zachowania poufności;
 - 4) w stosunku do których kontrahent/ osoba z zewnątrz uzyskał(a) pisemną zgodę na ich ujawnienie.
4. W przypadku, gdy ujawnienie wszelkich danych i informacji, co do których kontrahenci i osoby z zewnątrz zobowiązali się zachować w poufności jest wymagane na podstawie przepisów prawa powszechnie obowiązującego, kontrahent/ osoba z zewnątrz poinformuje osobę wskazaną do kontaktu o przyczynach i zakresie ujawnionych Informacji Poufnych. Poinformowanie takie powinno nastąpić w formie pisemnej lub w formie wiadomości wysłanej na adres poczty elektronicznej osoby wskazanej do kontaktu, chyba że takie poinformowanie byłoby sprzeczne z przepisami prawa powszechnie obowiązującego.
5. Kontrahent/ osoba z zewnątrz zobowiązuje się do niewykorzystywania Informacji Poufnych w celach innych niż cel, dla którego zostały mu ujawnione.
6. Kontrahent/ osoba z zewnątrz zobowiązuje się do dołożenia właściwych starań w celu zabezpieczenia Informacji Poufnych przed ich utratą, zniekształceniem oraz dostępem nieupoważnionych osób trzecich.
7. W przypadku utraty lub zniekształcenia Informacji Poufnych lub dostępu nieupoważnionej osoby trzeciej do Informacji Poufnych, Kontrahent/ osoba z zewnątrz bezzwłocznie podejmie odpowiednie do sytuacji działania ochronne oraz poinformuje osobę wskazaną do kontaktu o przyczynach i zakresie ujawnionych Informacji Poufnych. Poinformowanie takie powinno nastąpić w formie pisemnej lub w formie wiadomości wysłanej na adres poczty elektronicznej osoby wskazanej do kontaktu, chyba że takie poinformowanie byłoby sprzeczne z przepisami prawa powszechnie obowiązującego.

III. Bezpieczeństwo fizyczne i środowiskowe

1. Obowiązuje zakaz wnoszenia na teren siedziby GUS jakichkolwiek materiałów niebezpiecznych, których posiadanie i przechowywanie jest zabronione prawem. W przypadku stwierdzenia ich obecności w pomieszczeniach, dyrektor komórki organizacyjnej GUS właściwej ds. administracyjnych lub dyrektor jednostki odpowiedzialny jest za doprowadzenie do ich usunięcia.
2. Wyróżnia się następujące obszary bezpieczne:
 - a) strefa chroniona (strefa administracyjna),
 - b) strefa zabezpieczona (strefa bezpieczeństwa);
3. Wydziela się obszar dostaw i załadunku. Dostęp do pomieszczeń magazynowych jest nadzorowany. Prowadzona jest kontrola ruchu osobowego i materiałowego.
4. Pomieszczenia, w których przetwarzane są informacje wrażliwe dla statystyki publicznej, są wyposażone w zamek mechaniczny lub elektroniczny.

Strefa chroniona (strefa administracyjna):

- 1) na granicach strefy chronionej (strefy administracyjnej) funkcjonuje kontrola dostępu (tripody lub czytniki na drzwiach);
- 2) wejście do strefy chronionej (strefy administracyjnej), kontrahenta/ osoby z zewnątrz wymaga wydania identyfikatora i jego zaewidencjonowania. Ewidencjonowanie wejść do strefy chronionej (strefy administracyjnej) odbywa się poprzez dokonanie przez ochronę/recepcję lub wyznaczonego pracownika wpisu w ewidencji wejść i wyjść do strefy chronionej (strefy administracyjnej) oraz wydanie identyfikatora/karty magnetycznej typu „Gość”;
- 3) za wszelkie naruszenia bezpieczeństwa informacji przez osoby, które uzyskały dostęp do strefy chronionej (strefy administracyjnej) odpowiada dyrektor komórki organizacyjnej GUS/ dyrektor jednostki lub pracownik wnioskujący o przyznanie identyfikatora typu „Gość”;
- 4) osoby, bądź przedstawiciele podmiotów zewnętrznych świadczących usługi, w szczególności kurierzy, zaopatrzeniowcy, serwisanci poruszają się w granicy strefy chronionej (strefy administracyjnej) wyłącznie pod nadzorem wyznaczonego pracownika;
- 5) szczegóły dotyczące wejścia do strefy chronionej GUS określone zostały w zarządzeniu Dyrektora Generalnego GUS w sprawie „Zasad organizacji ruchu osób i pojazdów oraz zabezpieczenia budynku i mienia Głównego Urzędu Statystycznego”.

Strefa zabezpieczona (strefa bezpieczeństwa):

- 1) strefa zabezpieczona (strefa bezpieczeństwa) to wydzielona część strefy chronionej (strefy administracyjnej) wyposażona w dodatkowe, niezależne systemy zabezpieczeń. Rodzaj zabezpieczeń określa Właściciel aktywów przechowywanych w danym pomieszczeniu, stosownie do ich rodzaju i wartości;
- 2) zasoby znajdujące się w strefie zabezpieczonej (strefie bezpieczeństwa) podlegają szczególnej ochronie i są zabezpieczone przed pożarem;
- 3) strefy zabezpieczone (strefy bezpieczeństwa) posiadają zabezpieczenia zapewniające ochronę nośników informacji. Serwerownie wyposażone są w system sygnalizujący wystąpienie pożaru oraz system klimatyzacji. Strefy zabezpieczone (strefy bezpieczeństwa) są chronione systemem sygnalizacji włamania i napadu oraz wyposażone w urządzenia pozwalające na alarmowe powiadomienie obsługi i ochrony. System sygnalizacji napadu i włamania zapewnia skuteczne przekazanie sygnału o realnym zagrożeniu do wskazanych osób, miejsc i urządzeń;
- 4) wstęp do strefy zabezpieczonej (strefy bezpieczeństwa) jest ograniczony tylko do osób, które uzyskały stosowne uprawnienia wydane przez Właściciela aktywów przechowywanych w danym pomieszczeniu. Wejście oraz wyjście ze stref bezpieczeństwa rejestrowane jest przez system kontroli dostępu lub wyznaczonego przez Właściciela aktywów przechowywanych w danym pomieszczeniu pracownika. Wyznaczony pracownik rejestruje tożsamość osób oraz czas ich wejścia i wyjścia;

- 5) dopuszcza się przebywanie kontrahenta i osób z zewnątrz bez uprawnień dostępu do strefy zabezpieczonej (strefy bezpieczeństwa) tylko w wyjątkowych przypadkach, w celu wykonania działań serwisowych i innych określonych w regulacjach wewnętrznych (audyt), za zezwoleniem Właściciela aktywów przechowywanych w danym pomieszczeniu. Przebywanie osób bez uprawnień dostępu do strefy zabezpieczonej (strefy bezpieczeństwa) możliwe jest wyłącznie pod nadzorem pracownika, który posiada uprawnienia dostępu do danej strefy;
- 6) wnoszenie i wnoszenie do i ze strefy zabezpieczonej (strefy bezpieczeństwa) elektronicznych nośników informacji jest uzasadnione (np.: wynikające z procedury dot. kaset backup) lub nadzorowane;
- 7) w strefie zabezpieczonej (strefie bezpieczeństwa) zabronione jest korzystanie z urządzeń fotograficznych, wideo, audio lub innych urządzeń nagrywających, np. kamer w urządzeniach mobilnych w celu rejestracji obrazu lub dźwięku bez pisemnej zgody Właściciela aktywów przechowywanych w danym pomieszczeniu lub wyznaczonego przez niego pracownika.

IV. Dostęp do zasobów teleinformatycznych

1. Dostęp do systemu teleinformatycznego uzyskuje wyłącznie uprawniony kontrahent/osoba z zewnątrz. Dostęp jest indywidualnie zdefiniowany. Kontrahent/osoba z zewnątrz ma dostęp jedynie do zasobów, które są niezbędne.
2. Kontrola dostępu dla kontrahenta/osoby z zewnątrz do systemu teleinformatycznego realizowana jest poprzez mechanizmy uwierzytelniania.
3. Kontrahent/osoba z zewnątrz mogą uzyskać uprawnienia w zakresie korzystania z systemu teleinformatycznego na wniosek Właściciela aktywów. Nie dotyczy to organów umocowanych prawnie.
4. Wniosek o dostęp do sieci statystyki publicznej powinien zawierać informacje o celu podłączenia, przewidywanej liczbie podłączonych stanowisk i użytkowników, metodzie zabezpieczenia przed nieautoryzowanym dostępem.
5. Uprawnienia dla kontrahenta/osoby z zewnątrz nie mogą być przyznane na czas nieokreślony i podlegają aktualizacji co 90 dni.
6. Specyfikacja powinna zawierać w szczególności następujące ustalenia:
 - 1) szyfrowane połączenie powinno być zabezpieczone odpowiednim certyfikatem,
 - 2) zestawione połączenie powinno być jedynie między ściśle określonymi adresami IP podłączanej sieci oraz ściśle określonymi adresami IP sieci wewnętrznej statystyki publicznej oraz dla ściśle określonych portów przypisanych do adresów w sieci teleinformatycznej statystyki publicznej,
 - 3) każdorazowe zestawienie połączenia między podłączaną siecią teleinformatyczną podmiotu zewnętrznego, a siecią teleinformatyczną statystyki publicznej należy autoryzować loginem i hasłem lub certyfikatem lub innym środkiem autoryzacji oraz logowane, z wykluczeniem połączenia typu site2site.
7. Właściciel aktywów zatwierdza uprawnienia użytkowników z innych instytucji do danego systemu będącego w zasobach statystyki publicznej. Użytkownicy z innych instytucji nie mogą posiadać praw administracyjnych.
8. W przypadku zaistnienia potrzeby zrealizowania połączenia wewnętrznej sieci statystyki publicznej z siecią lub systemami zewnętrznymi kontrahenta/osoby z zewnątrz, Centrum Informatyki Statystycznej (CIS) odpowiedzialne jest za przygotowanie bezpiecznego połączenia, z uwzględnieniem stosownych reguł w firewallu (oraz innych systemach służących do zabezpieczenia komunikacji), szyfrowania połączenia np. za pośrednictwem usługi VPN, minimalnego niezbędnego zakresu uprawnień przyznanych na z góry zdefiniowany czas oraz zastosowania innych, niezbędnych środków ochrony.

9. W przypadku połączenia wewnętrznej sieci statystyki publicznej z systemami zewnętrznymi ruch odbywa się w jedną, tj. pracownicy jssp będą łączyć się z siecią kontrahenta, zaś kontrahent nie będzie miał dostępu do zasobów sieciowych statystyki publicznej.
10. Połączenie zostanie w pełni zaszyfrowane, a cały ruch będzie przesyłany przez bezpieczny tunel VPN.
11. Połączenie z zewnętrzną siecią może być przyznane jedynie dla wąskiej, wcześniej zdefiniowanej grupy użytkowników oraz przyznane na czas nie dłuższy niż okres realizacji umowy.

V. Ochrona przed szkodliwym oprogramowaniem i kodem mobilnym

1. Wszystkie elektroniczne nośniki informacji dostarczone z zewnątrz do sieci statystyki publicznej są dopuszczone do używania po wcześniejszym sprawdzeniu ich programem antywirusowym na komputerze odizolowanym od sieci statystyki publicznej.
2. Wszystkie pliki przed wysłaniem pocztą elektroniczną lub przekazaniem stronom trzecim (kontrahentowi/osobie zewnętrznej) są testowane oprogramowaniem antywirusowym.

VI. Naruszenia bezpieczeństwa informacji oraz wnioski dotyczące bezpieczeństwa informacji

1. Zasady bezpieczeństwa informacji obowiązują wszystkich kontrahentów/osoby z zewnątrz, które otrzymują dostęp do zasobów informacyjnych statystyki publicznej.
2. Odpowiedzialność za bezpieczeństwo informacji statystyki publicznej obejmuje działania, które miały miejsce w siedzibie GUS oraz wszelkie sytuacje, w których informacje związane z działalnością są przetwarzane poza jej siedzibą.
3. Kontrahent/osoba z zewnątrz mają obowiązek zgłaszania każdego zdarzenia, które narusza lub może naruszać wymagania bezpieczeństwa informacji osobie (pracownikowi statystyki publicznej) wskazanej do kontaktu natychmiast po jego wykryciu – osoba wskazana do kontaktu zgłasza zdarzenie związane z bezpieczeństwem informacji przez dedykowaną stronę www (<https://serwisdesk>), e-mailem: SD@stat.gov.pl bądź, w godzinach pracy urzędu, telefonicznie (22 608 3689).