

Polityka Bezpieczeństwa Informacji Statystyki Publicznej - wyciąg

I. Definicje i skróty

Słownik pojęć i wykaz skrótów stanowi załącznik nr 2 do zarządzenia wewnętrznego Prezesa GUS w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji w statystyce publicznej i odnosi się do całego SZBI w jssp.

II. Cel PBI

Zapewnienie zaangażowania pracowników jssp w utrzymanie bezpieczeństwa systemów informacyjnych, określenie kierunków rozwoju zarządzania bezpieczeństwem tych systemów, przy jednoczesnym spełnieniu wymogów obowiązującego prawa oraz zagwarantowaniu sprawnego funkcjonowania GUS i innych jssp.

III. Sformułowanie strategii bezpieczeństwa informacji

1. Bezpieczeństwo informacji to stan określony przez przyjęty zbiór norm, zasad, rozwiązań oraz środków i metod ochrony informacji.
2. Bezpieczeństwo informacji jest zapewnione, jeżeli ryzyko naruszenia poufności, integralności lub dostępności chronionych aktywów statystyki publicznej nie przekracza akceptowalnych progów przy zachowaniu zasad sformułowanych w niniejszej PBI.
3. Żadna procedura ani regulacja wewnętrzna obowiązująca w statystyce publicznej nie może naruszać zasad określonych w niniejszej PBI oraz w innych regulacjach z niej wynikających.

IV. Misja statystyki publicznej

Misją statystyki publicznej jest dostarczanie wiarygodnych, rzetelnych, niezależnych oraz wysokiej jakości informacji statystycznych na temat stanu i zmian zachodzących w społeczeństwie, gospodarce i środowisku naturalnym, odpowiadających na potrzeby użytkowników krajowych i międzynarodowych.

(...)

VII. Podstawowe zasady zarządzania bezpieczeństwem informacji

1. W celu zapewnienia bezpieczeństwa informacji statystyki publicznej stosuje się następujące podstawowe zasady:
 - 1) **zasada przywilejów koniecznych** – każdy pracownik posiada prawa dostępu do informacji statystyki publicznej ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu obowiązków;
 - 2) **zasada wiedzy koniecznej** – pracownicy posiadają wiedzę o informacjach statystyki publicznej ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych im zadań;
 - 3) **zasada asekuracji zabezpieczeń** – ochrona informacji statystyki publicznej nie może opierać się wyłącznie na jednym mechanizmie zabezpieczenia;
 - 4) **zasada rozliczalności** – statystyka publiczna dąży do zapewnienia jednoznacznej odpowiedzialności pracowników za powierzone im informacje. Wszyscy pracownicy muszą być świadomi swej odpowiedzialności oraz konsekwencji wynikających z naruszenia bezpieczeństwa informacji;
 - 5) **zasada czystego biurka i ekranu** – obejmuje:

- a) nośniki informacji, jeśli nie są aktualnie wykorzystywane, należy przechowywać w miejscach uniemożliwiających dostęp do nich osobom nieuprawnionym,
 - b) w pomieszczeniach, w których mogą przebywać osoby trzecie, monitory należy ustawić tak, aby uniemożliwić tym osobom wgląd do przetwarzanych informacji lub jeśli nie jest to możliwe, w czasie przebywania osoby trzeciej, zablokować komputer albo wyłączyć monitor,
 - c) po zakończeniu pracy należy wylogować się z systemu;
- 6) **zasada „przyrzeczenia o zachowaniu tajemnicy statystycznej”** – pracownicy jssp, rachmistrze spisowi, ankieeterzy statystyczni oraz inne osoby wykonujące czynności w imieniu i na rzecz statystyki publicznej, mający bezpośredni dostęp do danych jednostkowych, są obowiązani do bezwzględnej przestrzegania tajemnicy statystycznej i mogą być dopuszczeni do wykonywania tych czynności po złożeniu Prezesowi GUS i dyrektorowi jssp pisemnego przyrzeczenia;
- 7) **zasada „3R”** – dostęp do wynikowych informacji statystycznych, w szczególności podstawowych wielkości i wskaźników, jest równoprawny, równorzędny i równoczesny.

VIII. Organizacja bezpieczeństwa informacji w statystyce publicznej

1. Potencjalne zagrożenia:
 - 1) informacje jssp, w szczególności informacje, a także sprzęt niezbędny do ich przechowywania i przetwarzania, są istotne dla realizacji zadań statystyki publicznej;
 - 2) identyfikuje się następujące kategorie zagrożeń, którym mogą podlegać informacje jssp:
 - a) naruszenie poufności danych przez pracowników, kontrahentów lub jednostki zewnętrzne współpracujące z GUS i innymi jssp,
 - b) naruszenie integralności danych na skutek awarii systemu teleinformatycznego, umyślnego, nieumyślnego lub przypadkowego działania,
 - c) niedostępność zasobu lub znaczna degradacja jego istotnych parametrów funkcjonalnych lub utrata danych (zniszczenie zasobu) na skutek awarii systemu teleinformatycznego, wystąpienia siły wyższej albo umyślnego, nieumyślnego lub przypadkowego działania,
 - d) stosowanie niespójnych zasad (standardów lub procedur) i środków ochrony systemów teleinformatycznych;
 - 3) zadaniem regulacji zawartych w PBI jest zmniejszenie ryzyka wynikającego z zagrożeń do akceptowalnego poziomu, czyli zminimalizowanie możliwości naruszenia bezpieczeństwa informacji jssp, umożliwienie wczesnego wykrycia takiego naruszenia, zminimalizowanie strat związanych z takim naruszeniem oraz sprawne usunięcie jego skutków.
2. Cel zapewnienia bezpieczeństwa informacji w jssp:
 - 1) bezpieczeństwo informacji w jssp jest zapewnione, jeżeli ryzyko naruszenia poufności, integralności lub dostępności chronionych informacji nie przekracza akceptowalnych parametrów przy zachowaniu zasad sformułowanych w niniejszym dokumencie i dokumentacji SZBI;
 - 2) szacowania ryzyka w bezpieczeństwie informacji dokonuje się w trakcie procesu identyfikacji, analizy i oceny ryzyka poprzez określenie poziomu istotności aktywu, prawdopodobieństwa wystąpienia zagrożenia, wpływu zagrożenia dla poufności, integralności i dostępności informacji oraz poziomu zastosowanych zabezpieczeń;
 - 3) szacowanie ryzyka w bezpieczeństwie informacji odbywa się zgodnie z metodologią określoną w Polityce Zarządzania Ryzykiem.
3. Wymagania dotyczące stron zainteresowanych:
 - 1) PBI oraz inne dokumenty SZBI obowiązują wszystkich pracowników oraz kontrahentów mających dostęp do informacji jssp;
 - 2) o zmianach wymagań jssp wynikających z obowiązujących przepisów prawa istotnych dla bezpieczeństwa informacji, zainteresowane strony są powiadamiane przez dyrektora jssp;
 - 3) Wykaz stron zainteresowanych wraz z ich wymaganiami przygotowywany jest zgodnie ze wzorem stanowiącym załącznik nr 1;

- 4) za koordynację prac związanych z wypełnieniem i aktualizacją Wykazu stron zainteresowanych odpowiada komórka organizacyjna GUS właściwa ds. bezpieczeństwa informacji;
 - 5) aktualizacja Wykazu stron zainteresowanych (zewnętrznych i wewnętrznych) skutkuje utworzeniem kolejnej jego wersji;
 - 6) aktualny Wykaz stron zainteresowanych (zewnętrznych i wewnętrznych) oraz wersje archiwalne tego wykazu są dostępne w Intranecie (<http://intranet/GUS/ST/DokumentySZBI>).
4. Role i obowiązki związane z zapewnieniem bezpieczeństwa informacji:
- 1) Prezes GUS – zapewnia utrzymanie ustanowionego w statystyce publicznej SZBI oraz zatwierdza polityki w tym zakresie;
 - 2) Pełnomocnik ds. SZBI:
 - a) zatwierdza dokumenty SZBI w statystyce publicznej, inne niż wymienione w pkt 1 i 3,
 - b) zapewnia zgodność SZBI z wymaganiami normy PN-ISO/IEC 27001. W tym celu przeprowadza audyty bezpieczeństwa informacji w jssp, mające na celu ocenę zgodności stosowanych rozwiązań SZBI z wymaganiami normy PN-ISO/IEC 27001,
 - c) koordynuje i monitoruje realizację zadań wynikających z SZBI oraz nadzoruje funkcjonowanie SZBI statystyki publicznej, w tym prowadzi rejestr ryzyk związanych z bezpieczeństwem informacji i zatwierdza plany postępowania z ryzykiem,
 - d) przedstawia Prezesowi GUS wyniki przeglądów SZBI, o których mowa w części XXIV w jssp,
 - e) przeprowadza w zakresie merytorycznym szkolenia z zakresu bezpieczeństwa informacji;
 - 3) dyrektor jssp:
 - a) zatwierdza dokumenty SZBI obowiązujące wyłącznie w danej jednostce;
 - b) odpowiada za zapewnienie środków finansowych na utrzymanie i rozwój infrastruktury teleinformatycznej w podległej mu jednostce;
 - 4) KIT – odpowiada za koordynację i realizację prac w zakresie budowy, wdrażania i utrzymania systemów teleinformatycznych statystyki publicznej wraz z udzielaniem wsparcia użytkownikom w czasie eksploatacji systemów). Wyznacza administratorów systemów i WAS (ewentualnie ich zastępców) dla danego systemu teleinformatycznego;
 - 5) dyrektor komórki organizacyjnej GUS właściwej ds. administracyjnych – odpowiada za prowadzenie ewidencji wydanych urządzeń do składania podpisu kwalifikowanego bądź niekwalifikowanego oraz za spełnienie wymagań środowiskowych dla urządzeń i instalacji elektroenergetycznych w GUS. Za powyższe działania w pozostałych jssp odpowiada dyrektor tej jednostki;
 - 6) PBF – odpowiada za bezpieczeństwo fizyczne w danej jednostce;
 - 7) Dyrektor komórki organizacyjnej GUS właściwej ds. kadrowych – organizuje szkolenia z zakresu bezpieczeństwa informacji;
 - 8) POIN – zapewnia ochronę informacji niejawnych w danej jednostce;
 - 9) AS – administruje systemami teleinformatycznymi i sieciami teleinformatycznymi z zachowaniem poufności, integralności i dostępności, wykrywa i analizuje działania w systemie teleinformatycznym niezgodne z wymaganiami SZBI oraz usuwa we współpracy z właściwym PBC ewentualne skutki będące wynikiem takich działań;
 - 10) PBC – odpowiada za przestrzeganie wymagań zawartych w dokumentach SZBI w zakresie dotyczącym bezpieczeństwa infrastruktury teleinformatycznej w danej jednostce;
 - 11) Pełnomocnik ds. zarządzania incydentami bezpieczeństwa informacji – odpowiada za prawidłową obsługę i zarządzanie incydentami bezpieczeństwa informacji w jssp, prowadzi rejestr incydentów, dokonuje jego przeglądu i sporządza dla pełnomocnika ds. SZBI roczny raport z obsługi incydentów bezpieczeństwa informacji w jssp;
 - 12) IOD – odpowiada za monitorowanie zgodności z obowiązującymi przepisami prawa działań związanych z ochroną danych osobowych w danej jednostce;
 - 13) Właściciel aktywu – odpowiada za nadzór nad eksploatacją, rozwojem, utrzymaniem, korzystaniem, bezpieczeństwem i dostępem do aktywu powierzony mu na mocy regulaminów wewnętrznych obowiązujących w danej jednostce;
 - 14) Właściciel ryzyka – odpowiada za monitorowanie i systematyczną ocenę przypisanych ryzyk oraz za efektywność działań ograniczających te ryzyka;

- 15) bezpośredni przełożony – odpowiada za stosowanie wymagań zawartych w dokumentacji bezpieczeństwa informacji przez swoich podwładnych;
 - 16) pracownik lub użytkownik ma obowiązek:
 - a) zapoznawania się z dokumentami SZBI,
 - b) przestrzegania wymagań SZBI,
 - c) dołożenia wszelkich starań, aby chronić powierzone mu i używane przez niego zasoby jssp,
 - d) zgłaszania na Serwis Desk GUS oraz jssp – do właściwego lokalnego PBC każdego zauważonego przypadku naruszenia bezpieczeństwa informacji zgodnie z „Procedurą dotyczącą zarządzania zdarzeniami związanymi z bezpieczeństwem informacji przetwarzanych w statystyce publicznej”.
- (...)

XI. Urządzenia mobilne i telepraca

1. Zasady przyznawania uprawnień pozwalających na zdalny dostęp określa odrębna procedura wchodząca w skład dokumentacji bezpieczeństwa informacji.
2. W przypadku komputerów będących w domenie statystyki publicznej bądź podłączanych do sieci teleinformatycznej statystyki publicznej zabronione jest, za wyjątkiem dostępu zdalnego, korzystanie z łączy internetowych innych niż dostarczane przez statystykę publiczną.
3. Przemieszczanie informacji wrażliwych dla pracodawcy na elektronicznych nośnikach (w tym urządzeniach przenośnych i nośnikach informacji) poza siedzibę jssp, wymaga stosowania środków ochrony (technicznych i organizacyjnych) zabezpieczających je w najlepszy dostępny sposób przed nieuprawnionym dostępem i ujawnieniem.
4. Pracownik wykonuje pracę na odległość wykorzystując sprzęt teleinformatyczny stanowiący jego własność bądź będący własnością jssp.
5. Dostęp do konfiguracji BIOS komputera musi być zabezpieczony hasłem.
6. Jeżeli urządzenie mobilne nie jest użytkowane, musi być przechowywane w bezpiecznym miejscu w pomieszczeniu, w którym pracownik zwyczajowo wykonuje pracę w jssp.
7. W przypadku utraty sprzętu teleinformatycznego osoba odpowiedzialna za ten sprzęt niezwłocznie powiadamia o tym fakcie swojego bezpośredniego przełożonego, oraz przesyła zgłoszenie na Serwis Desk/do właściwego lokalnego PBC zgodnie z *Procedurą dotyczącą zarządzania zdarzeniami związanymi z bezpieczeństwem informacji przetwarzanych w statystyce publicznej*.
8. W przypadku kradzieży sprzętu teleinformatycznego poza siedzibą jssp, osoba odpowiedzialna za ten sprzęt ma również obowiązek niezwłocznego zgłoszenia tego faktu Policji. W zgłoszeniu pracownik, poza danymi ogólnymi, podaje okoliczności utraty sprzętu teleinformatycznego oraz opis charakteru utraconych danych wraz z podaniem ich znaczenia dla jssp. W szczególności w zgłoszeniu należy określić, czy utracone dane zawierały informacje wrażliwe dla statystyki publicznej.
9. Pracownika użytkującego własny sprzęt teleinformatyczny do pracy na odległość zobowiązuje się do stosowania poniższych zasad:
 - 1) sprzęt teleinformatyczny musi być technicznie sprawny, musi posiadać wyłącznie legalne oprogramowanie, tj. system operacyjny oraz inne aplikacje niezbędne do realizacji zadań służbowych są użytkowane z poszanowaniem praw autorskich;
 - 2) oprogramowanie zainstalowane na sprzęcie teleinformatycznym musi zapewniać bezproblemowe współdziałanie z usługami i serwisami udostępnionymi przez jssp do realizacji obowiązków służbowych;
 - 3) sprzęt teleinformatyczny musi mieć zainstalowane oprogramowanie antywirusowe z włączoną aktualizacją bazy wirusów;
 - 4) sprzęt teleinformatyczny musi być skonfigurowany w sposób umożliwiający automatyczne instalowanie poprawek bezpieczeństwa do systemu operacyjnego i używanych aplikacji.

XII. Bezpieczeństwo zasobów ludzkich

1. Nabór pracowników – zatrudnienie, staże, praktyki i wolontariaty oraz zawieranie umów cywilnoprawnych z pracownikami odbywa się zgodnie z procedurami wynikającymi z obowiązujących przepisów prawa.
2. Bezpieczeństwo podczas zatrudnienia oraz zawierania umów cywilnoprawnych:
 - 1) zasady wynikające z SZBI obowiązują wszystkich pracowników jeżeli będą posiadali dostęp do zasobów informacyjnych jssp;
 - 2) osoby, o których mowa w pkt. 1 mają obowiązek przestrzegania zasad bezpieczeństwa informacji obowiązujących w jssp;
 - 3) dyrektor jssp przygotowujący projekt umowy zlecenia lub umowy o dzieło z osobą fizyczną, która w ramach wykonywania umowy będzie posiadała dostęp do zasobów informacyjnych jednostki, ma obowiązek wprowadzić do niej klauzulę dotyczącą obowiązku przestrzegania zasad bezpieczeństwa informacji. *Wymagania bezpieczeństwa informacji dla kontrahentów i osób zewnętrznych* są załączane do umowy;
 - 4) każdy pracownik w pierwszym dniu pracy ma obowiązek:
 - a) zapoznać się z zapisami PBI obowiązującej w statystyce publicznej,
 - b) potwierdzić zapoznanie się z PBI własnoręcznym podpisem;
 - 5) oświadczenie o zapoznaniu się z zapisami PBI pracownik komórki organizacyjnej GUS właściwej ds. kadrowych albo osoba odpowiedzialna za prowadzenie spraw kadrowych w jednostce załącza do dokumentacji pracownika;
 - 6) uprawnienia do pracy w systemie teleinformatycznym są nadawane po zapoznaniu się z zapisami PBI obowiązującymi w statystyce publicznej oraz odbyciu szkolenia z bezpieczeństwa informacji;
 - 7) każda osoba podejmująca pracę, staż, praktykę, wolontariat w jssp lub uzyskująca dostęp do jej zasobów informacyjnych, przyjmuje na siebie obowiązek ochrony tych zasobów;
 - 8) obowiązek ochrony zasobów jssp, w przypadku współpracy z kontrahentami określany jest w ramach umów zawartych z tymi podmiotami (*Wymagania bezpieczeństwa informacji dla kontrahentów i osób zewnętrznych*);
 - 9) pracownicy mogą być (w zależności od pełnionej funkcji i zakresu obowiązków) związani umowami o zachowaniu poufności, a obowiązek jej zachowania może istnieć również po zakończeniu świadczenia pracy;
 - 10) pracownik, który naruszył zasady bezpieczeństwa informacji podlega odpowiedzialności dyscyplinarnej i porządkowej zgodnie z obowiązującymi przepisami prawa;
 - 11) naruszenie zasad bezpieczeństwa informacji przez praktykanta może skutkować natychmiastowym przerwaniem praktyki i rozwiązaniem umowy na zasadach każdorazowo określonych w umowie. W takim przypadku praktyka nie jest zaliczana;
 - 12) naruszenie zasad bezpieczeństwa informacji przez stażystę może skutkować natychmiastowym przerwaniem stażu i powiadomieniem instytucji kierującej na staż;
 - 13) w przypadku umowy cywilnoprawnej, na podstawie której osoba fizyczna wykonuje pracę na rzecz jssp, w umowie musi być zawarta klauzula, że naruszenie zasad bezpieczeństwa informacji przez taką osobę może skutkować natychmiastowym jej rozwiązaniem oraz stanowi podstawę do żądania pokrycia powstałej szkody lub zapłaty kary umownej;
 - 14) naruszenie zasad bezpieczeństwa informacji przez wolontariusza może skutkować natychmiastowym rozwiązaniem współpracy;
 - 15) informacje przetwarzane przy użyciu sprzętu teleinformatycznego jssp nie mogą być uznawane za prywatne. Powyższą zasadę stosuje się odpowiednio do informacji przetwarzanych na sprzęcie teleinformatycznym będącym własnością pracownika, który wykonuje pracę w formie telepracy na rzecz statystyki publicznej;
 - 16) na pracowniku spoczywa obowiązek poinformowania o wymogu, o którym mowa w pkt 15 swoich korespondentów w momencie przekazywania im służbowych adresów pocztowych lub numerów telefonicznych pracowników, o ile nie wynika to z już stosowanych rozwiązań technicznych i organizacyjnych;

- 17) pracownicy zobowiązani są do zachowania poufności w odniesieniu do informacji powierzonych im do przechowywania lub przesłania, z wyjątkiem sytuacji, gdy jest to niezbędne do przywrócenia ciągłości działania, a zaistniała sytuacja została objęta odpowiednią procedurą, której uruchomienie zostało zaakceptowane przez Pełnomocnika ds. SZBI;
- 18) odpowiedzialność za bezpieczeństwo informacji statystyki publicznej obejmuje nie tylko siedzibę jssp, ale także wszelkie miejsca, w których informacje związane z działalnością jssp są przetwarzane poza jej siedzibą. Obejmuje to w szczególności zdalny dostęp do sieci teleinformatycznej statystyki publicznej;
- 19) Prezes GUS, dyrektorzy komórek organizacyjnych GUS oraz dyrektorzy jednostek są odpowiedzialni za promowanie świadomości bezpieczeństwa informacji wśród pracowników;
- 20) z inicjatywy komórki organizacyjnej GUS właściwej ds. bezpieczeństwa informacji, za pomocą poczty elektronicznej, ulotek lub publikacji w Intranecie (<http://intranet/GUS/ST/Incydenty/bezpieczestwa/Forms/AllItems.aspx>) przekazywane są wiadomości o potencjalnych zagrożeniach oraz o metodach zapobiegania tym zagrożeniom.

3. Szkolenia:

- 1) szkolenia pracowników w zakresie bezpieczeństwa informacji mają na celu uzyskanie przez nich optymalnego poziomu wiedzy i umiejętności, które pozwolą właściwie korzystać z systemów teleinformatycznych służących do przetwarzania informacji w jssp;
- 2) program zwiększania świadomości pracowników w zakresie bezpieczeństwa informacji obejmuje:
 - a) szkolenia cykliczne w formie e-learning przy wykorzystaniu elektronicznej platformy szkoleniowej – każda osoba zatrudniona na podstawie umowy o pracę odbywa szkolenie co najmniej raz na cztery lata lub częściej w przypadku znaczącej, w opinii Pełnomocnika ds. SZBI, zmiany w przepisach dotyczących bezpieczeństwa informacji. Szkolenie cykliczne, dostępne na platformie szkoleniowej, kończy się testem sprawdzającym. Osoby nowo zatrudnione kierowane są na pierwsze dostępne szkolenie cykliczne w przeciągu 12 miesięcy od daty zatrudnienia,
 - b) szkolenie z zakresu bezpieczeństwa informacji przed uzyskaniem dostępu do zasobów informacyjnych statystyki publicznej,
 - c) szkolenia w ramach służby przygotowawczej w służbie cywilnej,
 - d) udostępnianie dokumentów SZBI do zapoznania się pracownikom,
 - e) publikowanie informacji związanych z bezpieczeństwem informacji – pracownicy mają stały dostęp do aktualnych przepisów oraz są informowani (w postaci elektronicznej) o ich zmianach przez komórkę organizacyjną GUS właściwą ds. bezpieczeństwa informacji,
 - f) poinformowanie, gdzie w Intranecie (<http://intranet/GUS/ST/DokumentySZBI>) znajduje się dokumentacja bezpieczeństwa informacji (polityki, regulaminy, zasady, wytyczne, wymagania, metodyki, procedury i instrukcje oraz projekty tych dokumentów);
- 3) szkolenia mogą być przeprowadzane w formie samokształcenia w oparciu o dostarczone uczestnikom materiały szkoleniowe. Uczestnicy mają możliwość konsultacji z osobą odpowiedzialną za merytoryczną stronę szkolenia;
- 4) komórka organizacyjna GUS właściwa ds. kadrowych przekazuje informację o szkoleniach cyklicznych dyrektorom komórek organizacyjnych GUS/dyrektorom jednostek oraz pracownikom na stanowiskach samodzielnych, podległych bezpośrednio Prezesowi GUS;
- 5) wnioski wynikające z naruszenia bezpieczeństwa informacji lub niewłaściwego funkcjonowania systemu teleinformatycznego są wykorzystywane podczas szkoleń pracowników w celu zapobiegania wystąpieniu podobnych incydentów;
- 6) w przypadku zmiany zasad bezpieczeństwa informacji, ciągłości działania lub ochrony danych osobowych, Pełnomocnik ds. SZBI aktualizuje materiały szkoleniowe oraz publikowane informacje. Przeprowadzane są także dodatkowe szkolenia (w formie e-learning). Wymóg dodatkowego szkolenia dotyczy wszystkich pracowników;
- 7) za merytoryczne przygotowanie i przeprowadzenie szkolenia w jssp odpowiada Pełnomocnik ds. SZBI. Za organizację szkoleń cyklicznych w formie e-learning przy wykorzystaniu elektronicznej platformy szkoleniowej odpowiada dyrektor komórki organizacyjnej GUS właściwej ds. kadrowych. Za organizację szkoleń w ramach służby przygotowawczej w służbie cywilnej odpowiada dyrektor komórki organizacyjnej GUS właściwej ds. kadrowych/dyrektor jednostki;

4. Zakończenie i zmiana zatrudnienia oraz zakończenie umowy cywilnoprawnej:
 - 1) pracownicy po ustaniu zatrudnienia lub innej formy współpracy lub po zmianie zakresu obowiązków są zobowiązani do zachowania w tajemnicy wszelkich informacji uzyskanych w trakcie wykonywania obowiązków służbowych, których ujawnienie mogłoby narazić na szkodę prawnie chroniony interes pracodawcy, a także sposobów zabezpieczenia informacji w jssp;
 - 2) pracownik komórki organizacyjnej GUS właściwej ds. kadrowych/pracownik ds. kadrowych w jednostce na bieżąco powiadamiają CIS za pomocą systemu Serwis Desk (gmach GUS)/pracownika komórki organizacyjnej właściwej ds. informatyki, o rozwiązaniu umowy z pracownikiem lub o jego przeniesieniu (do innej komórki organizacyjnej/jednostki), a także o wcześniejszym niż planowano zakończeniu stażu, praktyki, wolontariatu. W przypadku osoby fizycznej świadczącej pracę na podstawie umowy cywilnoprawnej powiadomienie, o którym mowa w zdaniu pierwszym przekazuje dyrektor komórki organizacyjnej GUS, która koordynuje daną umowę/dyrektor jednostki;
 - 3) administrator systemu w jssp niezwłocznie, po otrzymaniu takiej informacji usuwa, modyfikuje, lub blokuje uprawnienia do zasobów informacyjnych. Zbiory danych zgromadzone przez pracownika, z którym rozwiązano umowę są własnością jssp i mogą być usuwane lub zachowywane w zależności od decyzji jego przełożonego;
 - 4) pracownik komórki organizacyjnej GUS właściwej ds. kadrowych/dyrektor komórki organizacyjnej GUS, która koordynuje daną umowę na bieżąco powiadamia dyrektora komórki organizacyjnej GUS właściwej ds. administracyjnych oraz PBF w GUS o ustaniu zatrudnienia lub innej formy współpracy z osobami określonymi w pkt 1 lub o ich przeniesieniu;
 - 5) czynności opisane w pkt 1-4 i 6, w pozostałych jednostkach wykonują właściwi pracownicy tych jednostek;
 - 6) po otrzymaniu informacji, o której mowa w pkt 4 przez PBF w GUS/wyznaczonego pracownika jednostki, prawa dostępu do stref chronionych (administracyjnych/bezpieczeństwa) są niezwłocznie przez nich usuwane lub odpowiednio modyfikowane.
- (...)

XIV. Kontrola dostępu do systemu teleinformatycznego

1. Dostęp do zasobów systemów teleinformatycznych:
 - 1) kontrolę dostępu do systemu teleinformatycznego realizuje się poprzez mechanizmy uwierzytelniania użytkowników;
 - 1) dostęp do systemu teleinformatycznego mogą uzyskać wyłącznie uprawnieni użytkownicy i musi być on indywidualnie zdefiniowany dla każdego użytkownika. Użytkownik może mieć dostęp jedynie do zasobów, które są mu niezbędne do wykonywania obowiązków służbowych;
 - 2) identyfikacja użytkownika w systemie teleinformatycznym odbywa się na podstawie identyfikatora skojarzonego z hasłem. Z identyfikatorem związane są również prawa dostępu określające uprawnienia użytkownika;
 - 3) blokowany jest dostęp do systemu teleinformatycznego dla użytkownika, który trzykrotnie pod rząd podał błędne hasło. Odblokowania dokonuje administrator systemu, który nie może w tym celu tworzyć automatów (skryptów) programowych odblokowujących dostęp np. po określonym czasie;
 - 4) stosowane są konta indywidualne, zapewniające zachowanie rozliczalności;
 - 5) użytkownik sam ustala hasło, którym się posługuje (nie dotyczy pierwszego rejestrowania się w systemie teleinformatycznym, gdy hasło nadaje administrator systemu);
 - 6) system teleinformatyczny wymusza wybór hasła odpowiedniej jakości, zgodnie z wymaganiami zawartymi w części XIV ust. 4 (Zakres odpowiedzialności użytkowników i hasła dostępu);
 - 7) tożsamość każdego użytkownika systemu teleinformatycznego musi być jednoznacznie określona (identyfikacja) i musi być sprawdzona przed rozpoczęciem pracy w systemie teleinformatycznym (uwierzytelnienie);
 - 8) o ile pozwala na to oprogramowanie, na ekranie powitalnym użytkownika przy każdym logowaniu muszą być zawarte następujące informacje:

- a) pouczenie użytkownika o tym, że kontynuując pracę w systemie teleinformatycznym potwierdza uprawnienia do korzystania z zasobów teleinformatycznych,
 - b) stwierdzenie, że użytkownika zna i akceptuje zasady dotyczące bezpieczeństwa systemu teleinformatycznego;
- 9) wszystkie systemy teleinformatyczne powinny posiadać uaktywnioną opcję wygaszacza ekranu w przypadku braku aktywności użytkownika w systemie. Czas uaktywnienia wygaszacza ekranu nie może być dłuższy niż 10 minut. Odblokowanie wygaszacza ekranu wymaga podania hasła. Podobnie, wszystkie sesje dostępu do zasobów informacyjnych (a w szczególności do komend systemu operacyjnego) są zawieszane (lub zrywane) po 10 minutach bezczynności;
 - 10) w systemie teleinformatycznym nie mogą być aktywne ogólnodostępne profile domyślne „Gość”;
 - 11) użytkownik wykonuje pracę na komputerze z uprawnieniami lokalnego użytkownika;
 - 12) ograniczanie dostępu do zasobów teleinformatycznych, realizuje się z uwzględnieniem następujących uwarunkowań:
 - a) dostęp do sieci teleinformatycznej mogą mieć tylko urządzenia sieciowe, które uzyskały akceptację administratora systemu; jeśli to możliwe, mechanizmy kontroli umożliwiają wykrycie obecności nieautoryzowanych urządzeń,
 - a) logiczny dostęp do sieci mają tylko zarejestrowani użytkownicy jednoznacznie zidentyfikowani,
 - b) dostęp do komend systemu operacyjnego – tylko użytkownicy, których zakres obowiązków wymaga dostępu do systemu operacyjnego, mogą być uprawnieni do logowania się bezpośrednio na serwerach sieciowych,
 - c) dostęp do aplikacji i baz danych statystyki publicznej wymaga uprzedniej identyfikacji i uwierzytelnienia użytkownika; przyznane użytkownikowi uprawnienia do korzystania z poszczególnych aplikacji i baz danych powinny być ograniczone wyłącznie do zakresu jego obowiązków służbowych;
 - 13) nadanie lub zmiana uprawnień użytkownika następuje na pisemny wniosek (w postaci papierowej lub elektronicznej) złożony przez bezpośredniego przełożonego w systemie Serwis Desk (gmach GUS)/do pracownika komórki organizacyjnej właściwej ds. informatyki w jednostce. Złożone wnioski muszą być rejestrowane oraz przechowywane co najmniej przez cykl życia systemu teleinformatycznego;
 - 14) nazwa profilu użytkownika musi być unikatowa i nie powinna zmieniać się przez cały okres jego pracy w jssp, chyba że wynika to ze zmiany nazwiska użytkownika;
 - 15) osoby niebędące pracownikami mogą uzyskać uprawnienia w zakresie korzystania z systemu teleinformatycznego na wniosek Właściciela aktywu. Nie dotyczy to organów umocowanych prawnie;
 - 16) uprawnienia użytkowników niebędących pracownikami nie mogą być przyznane na czas nieokreślony i muszą podlegać aktualizacji co 90 dni;
 - 17) uprawnienia administratora systemu są przyznawane, na wniosek Właściciela aktywu, wyłącznie osobom odpowiedzialnym za administrowanie systemami;
 - 18) liczba użytkowników posiadających uprawnienia administratora danego systemu teleinformatycznego powinna być ograniczona do niezbędnego minimum, jednak nie może to być mniej niż 2 osoby;
 - 19) osoby mające dostęp do systemu teleinformatycznego a niebędące pracownikami muszą podpisać zobowiązanie, że będą przestrzegać zasad opisanych w *Wymaganiach bezpieczeństwa informacji dla kontrahentów i osób zewnętrznych*;
 - 20) warunki korzystania z połączenia wewnętrznej sieci statystyki publicznej z systemami zewnętrznymi regulują podpisane umowy, szczegółowo precyzujące warunki techniczne i funkcjonalne połączenia. Umowa musi zawierać klauzulę dotyczącą przestrzegania zasad bezpieczeństwa systemów informacyjnych statystyki publicznej;
 - 21) konto użytkownika musi być zablokowane po 30 dniach kalendarzowych nieaktywności;
 - 22) w przypadku nieobecności pracownika (urlop bezpłatny, macierzyński, wychowawczy lub inne nieobecności dłuższe niż 30 dni) jego bezpośredni przełożony zobowiązany jest powiadomić:
 - a) komórkę organizacyjną GUS właściwą ds. kadrowych/pracownika ds. kadrowych w jednostce,

- b) CIS za pomocą systemu Serwis Desk (gmach GUS)/pracownika komórki organizacyjnej właściwej ds. informatyki w jednostce oraz
 - c) PBF w GUS/pracownika wyznaczonego przez dyrektora jednostki – najpóźniej pierwszego dnia planowanej nieobecności pracownika. Jeżeli nieobecność pracownika jest nieplanowana (kolejne zwolnienie lekarskie, z którego wynika, że łączna nieobecności pracownika będzie dłuższe niż 30 dni) – pierwszego dnia w którym przełożony pozyskał taką informację;
- 23) uprawnienia użytkownika powinny być zablokowane w przypadku nieprawidłowego funkcjonowania podsystemów kontroli dostępu. Decyzje o dalszych działaniach podejmuje Właściciel aktywu;
 - 24) uprawnienia nadane użytkownikowi muszą być okresowo weryfikowane przez administratora systemu nie rzadziej niż co 12 miesięcy. Właściciele aktywów są zobowiązani niezwłocznie informować za pomocą systemu Serwis Desk (gmach GUS)/innego podobnego systemu teleinformatycznego jednostki administratorów systemów odpowiedzialnych za poszczególne konta o zmianach w zakresie obowiązków podległych pracownikom skutkujących koniecznością zmiany ich uprawnień;
 - 25) uprawnienia posiadane przez użytkownika nie mogą być rozszerzane, o ile nie istnieje umotywowana potrzeba związana ze zmianą warunków wykonywania pracy lub zakresu obowiązków użytkownika;
 - 26) systemy teleinformatyczne przetwarzające informacje sklasyfikowane jako wrażliwe dla statystyki publicznej muszą być skonfigurowane w taki sposób, aby umożliwić dostęp do tych zasobów wyłącznie tym użytkownikom, którzy mają do tego prawo;
 - 27) systemy teleinformatyczne przetwarzające informacje sklasyfikowane jako wrażliwe dla statystyki publicznej są wyposażone w narzędzia pozwalające na monitorowanie i rejestrowanie działań użytkowników;
 - 28) w miarę możliwości technicznych uprawnienia w systemach aplikacyjnych muszą uniemożliwiać jednoczesne wprowadzanie i autoryzowanie tej samej transakcji przez jednego użytkownika;
 - 29) użytkownikom zakazuje się podłączania do sieci teleinformatycznej statystyki publicznej własnych urządzeń. Powyższa regulacja nie dotyczy sytuacji opisanej w części XI (Urządzenia mobilne i telepraca);
 - 30) użytkownik jest odpowiedzialny za ochronę istotnych danych przetwarzanych w systemach teleinformatycznych, w trakcie wykonywania obowiązków służbowych. Takie dane należy zapisywać na dyskach sieciowych, które podlegają procedurze codziennego tworzenia kopii bezpieczeństwa. Zapisanie pliku na komputerze użytkownika nie gwarantuje ochrony danych;
 - 31) użytkownik jest zobowiązany do systematycznego usuwania z dysków sieciowych zasobów, które utraciły swoją istotność.
2. Przydzielanie dostępu użytkownikom:
- 1) w procesie nadawania uprawnień obowiązują następujące zasady:
 - a) reguła niezbędnego dostępu – ograniczenia praw do niezbędnych przy wykonaniu powierzonych użytkownikowi zadań i obowiązków,
 - b) reguła indywidualnego konta – zabezpieczonego procedurą uwierzytelnienia (identyfikacji i autoryzacji), umożliwiającego rozliczalność działań użytkownika;
 - 2) z przyczyn techniczno-organizacyjnych możliwe jest zastosowanie loginu grupowego lub niezabezpieczonego konta, jednak każdy taki przypadek musi być udokumentowany i odnotowany jako odstępstwo od realizacji postanowień niniejszego dokumentu;
 - 3) dostęp do zasobów oraz uprawnienia do korzystania z nich nadawane są jedynie w zakresie wiedzy koniecznej, tj. niezbędnym do wykonywania aktualnie powierzonych użytkownikowi zadań i obowiązków, na wniosek przełożonego pracownika;
 - 4) uprawnienia administratora systemu są nadawane przez WAS;
 - 5) w przypadku konieczności nadania uprawnień pracownikom stron trzecich, wskazane osoby mogą otrzymać uprawnienia na wniosek dyrektora komórki organizacyjnej GUS, która koordynuje umowę/dyrektora jednostki;
 - 6) w przypadku systemu teleinformatycznego administrator systemu tworzy konto, nadaje użytkownikowi uprawnienia i potwierdza fakt nadania wpisem na wniosku (data, podpis). W celach

audytowych, złożone wnioski muszą być rejestrowane oraz przechowywane (w postaci papierowej lub elektronicznej) co najmniej przez cykl życia systemu teleinformatycznego;

- 7) tworząc użytkownikowi hasło w systemie teleinformatycznym, administrator systemu tworzy dla niego hasło tymczasowe, które przekazuje osobiście albo za pomocą bezpiecznego kanału komunikacji. Niedopuszczalne jest stosowanie systemów teleinformatycznych, które nie dają możliwości ustawienia hasła startowego;
 - 8) użytkownik zobowiązany jest do zmiany hasła przy pierwszym logowaniu. Zasada ta nie obejmuje systemów opartych na mechanizmie logowania jednokrotnego (ang. single-sign-on, SSO) i integracji z kontem w Active Directory. W przypadku integracji mechanizmu logowania z domeną, administrator systemu informuje użytkownika o nadaniu uprawnień i możliwości rozpoczęcia pracy w systemie;
 - 9) w przypadku nadawania uprawnień do zasobów innych niż systemy domenowe, administrator systemu jest zobowiązany do zapoznania użytkownika z zasadami korzystania z zasobu, zakresem odpowiedzialności za korzystanie z zasobu oraz uzyskania w formie pisemnej dowodu potwierdzającego zrozumienie niniejszych zasad i fakt przekazania zasobu do użytkownika;
 - 10) KIT w porozumieniu z Pełnomocnikiem ds. SZBI może dopuścić do stosowania mechanizm nadawania pakietu podstawowych uprawnień do systemu teleinformatycznego automatycznie po przyjęciu nowozatrudnionej osoby bez konieczności wypełniania wniosku o nadanie uprawnień (np. konto domenowe, poczta elektroniczna, Intranet);
 - 11) w systemach teleinformatycznych, w których do zarządzania uprawnieniami zdefiniowano procedurę nadawania uprawnień, należy postępować zgodnie ze zdefiniowaną procedurą.
3. Odbieranie praw dostępowych:
- 1) dyrektor komórki organizacyjnej GUS/dyrektor jednostki zobowiązany jest poinformować administratora systemu o konieczności odebrania/modyfikacji/zablokowania uprawnień do zasobów informacyjnych w związku ze zmianą powierzonych użytkownikowi zadań i obowiązków;
 - 2) informacja, o której mowa w punkcie wyżej, przekazywana jest przez system Serwis Desk (gmach GUS)/pracownika komórki organizacyjnej właściwej ds. informatyki w jednostce, a jeżeli nie jest to możliwe na wniosku (w postaci papierowej lub elektronicznej) o nadanie/odebranie uprawnień;
 - 3) w przypadku zaprzestania przez użytkownika świadczenia pracy lub zakończenia obowiązującej umowy, niezależnie od zawartości wniosku, każdy administrator systemu musi zweryfikować, czy były pracownik nie posiada nadanych uprawnień w systemie teleinformatycznym przez niego nadzorowanym;
 - 4) po otrzymaniu wniosku administrator systemu odbiera dostęp do zasobu i archiwizuje wniosek. W celach audytowych, złożone wnioski muszą być rejestrowane oraz przechowywane (w postaci papierowej lub elektronicznej) co najmniej przez cykl życia systemu teleinformatycznego;
 - 5) w każdym przypadku odebrania uprawnień użytkownikowi, jeżeli jest to technicznie możliwe, jego konto (nazwa użytkownika) musi zostać zablokowane;
 - 6) w przypadku odebrania uprawnień do zasobów informacyjnych, wynikającego z zakończenia zatrudnienia lub innej formy współpracy, pracownik komórki organizacyjnej GUS właściwej ds. kadrowych/pracownik ds. kadrowych w jednostce/dyrektor komórki organizacyjnej GUS lub jednostki, która koordynuje daną umowę na bieżąco powiadamiają CIS za pomocą systemu Serwis Desk/pracownika komórki organizacyjnej właściwej ds. informatyki w jednostce, o konieczności odebrania uprawnień najpóźniej z dniem ustania stosunku pracy lub innej formy współpracy, chyba że osoba kończąca zatrudnienie/inną formę współpracy nie świadczy pracy przed ustaniem umowy. W takim przypadku, uprawnienia muszą być odebrane w dniu ustania obowiązku świadczenia pracy;
 - 7) w przypadku zmiany zatrudnienia lub innej formy współpracy (np. komórki organizacyjnej, stanowiska) wszystkie uprawnienia do systemów teleinformatycznych powinny zostać nadane użytkownikowi na wniosek aktualnego przełożonego;
 - 8) zasada ta nie obejmuje podstawowych uprawnień, jak np. dostęp do konta domenowego, poczty elektronicznej, dostęp do pomieszczeń, pod warunkiem, że zakres dostępu nie uległ zmianie.
4. Zakres odpowiedzialności użytkowników i hasła dostępu:

- 1) systemy teleinformatyczne muszą wymuszać wprowadzenie minimalnej długości hasła, okresu maksymalnej ważności hasła (nie dłuższej niż 30 dni) oraz uniemożliwiają powtórne (5 ostatnich haseł) wykorzystanie tego samego hasła;
- 2) oprogramowanie nie może wyświetlać hasła jawnym tekstem na monitorze komputera;
- 3) oprogramowanie nie może przechowywać ani zapisywać hasła w postaci jawnego tekstu. Algorytm kodowania haseł powinien być jednostronny;
- 4) hasła dla użytkowników muszą mieć długość minimum osiem znaków oraz składać się z:
 - a) dużych i małych liter,
 - b) cyfr,
 - c) znaków specjalnych;
- 5) użytkownicy nie mogą używać haseł opartych na ciągu znaków ulegających zmianie w zależności od daty lub innego przewidywalnego czynnika;
- 6) użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego przechowywanie. Zabronione jest zapisywanie haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób. W szczególności zabronione jest umieszczanie haseł w treści skryptów systemowych i programów;
- 7) hasła nie mogą być wpisywane w obecności osób trzecich, które mogłyby zauważyć treść wpisywanego hasła;
- 8) jeśli istnieje podejrzenie, że hasło zostało ujawnione, należy je natychmiast zmienić i powiadomić administratora systemu;
- 9) użytkownik ponosi pełną odpowiedzialność za użycie zasobów teleinformatycznych jssp przy wykorzystaniu jego hasła do momentu powiadomienia administratora systemu o ujawnieniu hasła. Jeżeli dojdzie do incydentu bezpieczeństwa informacji z wykorzystaniem loginu i hasła użytkownika, to może on ponieść odpowiedzialność, jeżeli dopuścił do ujawnienia swojego hasła;
- 10) w przypadku, gdy użytkownik musi posiadać dostęp do wielu systemów lub aplikacji, co stwarza konieczność przypisania mu wielu profili użytkownika, może on posługiwać się tym samym hasłem we wszystkich swoich profilach. Wyjątkiem są profile administracyjne, które powinny być zabezpieczone innym hasłem;
- 11) użytkownik korzystający z zewnętrznych usług internetowych zabezpieczanych hasłem (np. serwisu bankowego) nie powinien używać w celu dostępu do nich takiego samego hasła, jak w przypadku dostępu do systemu teleinformatycznego jssp;
- 12) używane w jssp systemy teleinformatyczne wyposażone są w mechanizm kontroli dostępu do systemu;
- 13) systemy teleinformatyczne używane przez wielu użytkowników powinny korzystać z unikatowych identyfikatorów użytkowników i haseł przyporządkowanych poszczególnym pracownikom, a także z mechanizmu ograniczającego przywileje użytkowników;
- 14) przed przekazaniem do użytkownika systemu teleinformatycznego konieczna jest zmiana wszystkich haseł domyślnych ustawionych przez dostawcę lub ich zablokowanie;
- 15) jeśli oprogramowanie zapewnia takie możliwości, należy wymusić automatyczną zmianę hasła tymczasowego podczas pierwszego logowania do systemu. Jeśli oprogramowanie na to nie pozwala, należy sporządzić odpowiednie instrukcje obowiązujące pracowników;
- 16) oprogramowanie stosowane w jssp musi uniemożliwiać użytkownikom wybór łatwych do odgadnięcia haseł;
- 17) w przypadku naruszenia bezpieczeństwa systemu teleinformatycznego lub w przypadku podejrzenia takiego naruszenia, administrator systemu musi zablokować dostęp do systemu teleinformatycznego i podjąć działania opisane w *Procedurze zarządzania zdarzeniami związanymi z bezpieczeństwem informacji przetwarzanych w statystyce publicznej*;
- 18) hasła dostępu do profili z uprawnieniami administratora systemu muszą mieć długość minimum czternastu znaków:
 - a) spełniać warunki wymienionych w pkt 4,
 - b) być przechowywane w bezpiecznym miejscu, w sposób zapewniający utrzymanie ich w tajemnicy,
 - c) aktualizowane przy każdej ich zmianie,

- d) niszczone jeżeli są nieaktualne;
 - 19) udostępnienie osobom, innym niż ich właściciele, hasła dostępu do profilu z uprawnieniami administratora stanowi naruszenie bezpieczeństwa informacji;
 - 20) w przypadku konieczności udzielenia osobom trzecim dostępu do profilu uprzywilejowanego, hasło dostępu powinno być przed udzieleniem takiego dostępu zmienione na tymczasowe, a po wykorzystaniu zmienione na nowe;
 - 21) w jssp można korzystać także z innych metod uwierzytelniania, w szczególności z wykorzystaniem podpisu niekwalifikowanego, którym możliwe jest logowanie do systemu teleinformatycznego w sieci teleinformatycznej statystyki publicznej, haseł jednorazowych;
 - 22) urządzenie do podpisu kwalifikowanego bądź niekwalifikowanego jest automatycznie blokowane po przekroczeniu ustalonej, maksymalnej liczby błędnych wpisów kodu PIN;
 - 23) komórka organizacyjna GUS właściwa ds. administracyjnych zobowiązana jest do prowadzenia dokładnej ewidencji wydanych urządzeń do podpisu kwalifikowanego bądź niekwalifikowanego. W przypadku zakończenia świadczenia pracy urządzenie do podpisu kwalifikowanego bądź niekwalifikowanego należy zwrócić do komórki organizacyjnej GUS właściwej ds. administracyjnych;
 - 24) w przypadku utraty urządzenia do składania podpisu kwalifikowanego bądź niekwalifikowanego należy niezwłocznie powiadomić komórkę organizacyjną GUS właściwą ds. administracyjnych;
 - 25) pracownik, któremu zostało wydane urządzenie do składania podpisu kwalifikowanego bądź niekwalifikowanego, ma obowiązek zapoznania się i przestrzegania zasad postępowania z kluczami do podpisu elektronicznego, ujętych w odpowiednich dokumentach SZBI.
5. Kontrola dostępu do aplikacji:
- 1) kontrola dostępu do aplikacji musi być określona w dokumentacji aplikacji;
 - 2) oprogramowania użytkowe (aplikacje), eksploatowane w systemie teleinformatycznym posiadają:
 - a) mechanizmy autoryzacji i sprawdzania wprowadzanych danych pod względem ich kompletności (dane są oceniane w trakcie procesu ich wprowadzania),
 - b) mechanizmy kontroli przetwarzanych danych, zapobiegające nieautoryzowanemu usunięciu lub modyfikacji danych;
 - 3) mechanizmy kontroli dotyczące specyficznych systemów teleinformatycznych mogą zawierać dodatkowe wymagania, inne niż wskazane w pkt 2 i są uregulowane w dokumentach SZBI ich dotyczących;
 - 4) wszystkie raporty generowane przez kluczowe systemy teleinformatyczne są rejestrowane, z uwzględnieniem identyfikatora użytkownika zlecającego dany raport, oraz oznaczone datą i godziną jego wygenerowania.
6. Monitorowanie dostępu do systemu:
- 1) kluczowe systemy teleinformatyczne są monitorowane w celu wykrywania w nich nieuprawnionych działań;
 - 2) zdarzenia w systemie teleinformatycznym są zapisywane i archiwizowane. Zapisy te zawierają:
 - a) identyfikatory użytkowników,
 - b) daty i czasy zarejestrowania i wyrejestrowania w systemie,
 - c) identyfikator komputera użytkownika lub terminala (nazwę komputera w systemie),
 - d) zapisy udanych i nieudanych prób dostępu do systemu;
 - 3) monitorowane są fakty użycia urządzeń przetwarzania informacji, zapewniając weryfikację i rozliczanie użytkowników wykonujących procesy, do których zostali uprawnieni;
 - 4) logi systemowe są zabezpieczone przed manipulacją i nieuprawnionymi zmianami oraz systematycznie przeglądane przez administratora systemu pod kątem właściwego wykorzystywania systemu teleinformatycznego i zarządzania nim.
7. Monitorowanie i analiza przypadków naruszenia bezpieczeństwa:
- 1) każdy system teleinformatyczny musi być wyposażony w mechanizmy umożliwiające administratorowi systemu weryfikację stanu zabezpieczeń systemu. Mechanizmy te powinny co najmniej umożliwiać rejestrację prób uzyskania dostępu do systemu;

- 2) wszystkie systemy teleinformatyczne muszą być objęte mechanizmami wykrywającymi automatycznie próby instalacji nieautoryzowanego oprogramowania;
 - 3) w systemie teleinformatycznym muszą być logowane istotne zdarzenia dotyczące działań użytkowników i funkcjonowania urządzeń;
 - 4) wszystkie systemy aplikacyjne statystyki publicznej, które przetwarzają informacje sklasyfikowane jako wrażliwe dla statystyki publicznej, muszą rejestrować w dzienniku informacje na temat każdego przypadku ich przetwarzania. Jeżeli jest to możliwe, dzienniki należy gromadzić na jednym wydzielonym komputerze, administrowanym przez innego administratora;
 - 5) wszystkie logi systemowe muszą być regularnie przeglądane przez administratorów odpowiednich systemów lub aplikacji;
 - 6) w celu ograniczenia nadużyć, zwiększenia odpowiedzialności użytkowników i umożliwienia zarządzania systemami musi być zapewniona możliwość rekonstrukcji istotnych działań użytkowników na podstawie dzienników i innych zarejestrowanych materiałów;
 - 7) zegary systemów teleinformatycznych muszą być zsynchronizowane, by ułatwić analizę zdarzeń zachodzących równocześnie w kilku systemach.
8. Każdy pracownik który stwierdził niewłaściwe funkcjonowanie systemu teleinformatycznego ma obowiązek zgłosić ten fakt na Serwis Desk (gmach GUS)/w pozostałych jednostkach – do właściwego lokalnego PBC zgodnie z *Procedurą dotyczącą zarządzania zdarzeniami związanymi z bezpieczeństwem informacji przetwarzanych w statystyce publicznej*.

(...)

XVIII. Bezpieczna eksploatacja

1. Procedury eksploatacyjne oraz zakresy odpowiedzialności:
 - 1) w celu zapewnienia prawidłowej i bezpiecznej eksploatacji kluczowego oprogramowania użytkowego wprowadza się, realizuje i dokumentuje procedury eksploatacyjne, które muszą być zgodne z cyklem życia tego oprogramowania. W przypadku nowych systemów teleinformatycznych procedury eksploatacyjne obejmują prace projektowe, testowanie, obsługę i ich rozwój;
 - 2) dokumentacja systemów teleinformatycznych wprowadzanych do eksploatacji musi zawierać instrukcje ich bezpiecznej eksploatacji oraz dokładny opis zastosowanych w ich konstrukcji mechanizmów zabezpieczających, zarządzanych i nadzorowanych przez wyznaczoną grupę użytkowników;
 - 3) dokumentacja systemu teleinformatycznego musi być chroniona przed nieuprawnionym dostępem;
 - 4) procedury eksploatacyjne są opracowywane przez KIT oraz, w przypadku systemu administrowania podpisem elektronicznym, dyrektora komórki organizacyjnej GUS właściwej ds. finansów;
 - 5) za zorganizowanie pracy, zapewnienie bezpieczeństwa oraz prawidłową eksploatację systemu teleinformatycznego i sprzętu komputerowego, przydzielonego do poszczególnych komórek organizacyjnych GUS/jednostek, odpowiedzialni są Właściciele aktywów;
 - 6) za bezpieczeństwo i dostęp do terminala lub komputera oraz za jego prawidłową eksploatację odpowiedzialny jest użytkownik danego terminala lub komputera;
 - 7) tak dalece, jak jest to możliwe i praktyczne, należy wymagać podziału uprawnień, tak, aby żaden użytkownik nie mógł uzyskać dostępu, modyfikować lub korzystać z aktywów bez autoryzacji drugiego użytkownika tych aktywów lub wykrycia takiego przypadku dostępu i modyfikacji (monitorowanie działań, ślady audytowe lub nadzór);
 - 8) uprawnienia użytkownika w systemie teleinformatycznym określa dyrektor komórki organizacyjnej GUS/dyrektor jednostki w porozumieniu i za zgodą Właścicieli aktywów, do których podległy pracownik otrzymuje dostęp;
 - 9) wnioski mające na celu podniesienie poziomu bezpieczeństwa informacji należy zgłaszać do Pełnomocnika ds. SZBI zgodnie z *Procedurą zgłaszania wniosków*, który przeprowadza analizę wniosku, a w razie potrzeby podejmuje konsultacje z właściwymi komórkami organizacyjnymi GUS/innymi jednostkami. Wdrażanie rozwiązań służących podnoszeniu poziomu bezpieczeństwa,

- które wymagają kompleksowych zmian lub poniesienia dodatkowych nakładów finansowych, muszą zostać zaakceptowane przez Prezesa GUS;
- 10) wnioski dotyczące funkcjonowania systemu teleinformatycznego należy zgłaszać do CIS zgodnie z *Procedurą zgłaszania wniosków*. Zmiany w systemach teleinformatycznych wynikające z wniosków wymagają uzgodnienia z komórką organizacyjną GUS właściwą ds. bezpieczeństwa informacji;
 - 11) prace rozwojowe (programistyczne, testowe, itp.) nie mogą być prowadzone w środowisku produkcyjnym.
2. Zarządzanie zmianą:
 - 1) przed każdą dokonywaną zmianą w systemie teleinformatycznym/aplikacji należy przeanalizować, czy ma ona wpływ na treść istniejącej dokumentacji bezpieczeństwa informacji, w razie potrzeby należy dokonać aktualizacji dokumentacji;
 - 2) należy poinformować wszystkich odbiorców systemu lub aplikacji, w których dokonano zmian funkcjonalnych, zmieniających sposób użytkowania systemu lub aplikacji;
 - 3) przed przeprowadzeniem zmiany należy opracować procedurę wyjścia ze zmiany, opisującą sposób przywrócenia systemu do stanu sprzed zmiany;
 - 4) w przypadku niepomyślnie przeprowadzonej zmiany bądź poprawki aplikacji, administrator systemu przeprowadza procedurę wyjścia ze zmiany;
 - 5) w przypadku niepowodzenia operacji wycofania się ze zmiany uruchamiany jest proces zarządzania incydentami bezpieczeństwa informacji;
 - 6) wdrożenie i testowanie zmiany do momentu zatwierdzenia wdrożenia, może odbywać się wyłącznie w wydzielonym środowisku gwarantującym separację systemu, w którym wdrażane są zmiany (wyjątek stanowi brak możliwości technicznych lub licencyjnych dla stworzenia wydzielonego środowiska testowego);
 - 7) przeprowadzanie zmian w systemach teleinformatycznych należy wykonać przy spełnieniu następujących minimalnych wymagań:
 - a) planowanie modyfikacji stosownie do potrzeb powinno obejmować uzgodnienie parametrów modyfikacji (np. czasu, zakresu zmiany) z osobami zainteresowanymi (np. Właścicielem aktywu, administratorami systemów, aplikacji, baz danych, osobami odpowiedzialnymi za bezpieczeństwo.) oraz analizę wpływu na systemy powiązane,
 - b) przed dokonaniem modyfikacji należy wykonać kopię zapasową środowiska systemu – oprogramowania, konfiguracji i danych – celem umożliwienia, w przypadku wystąpienia problemów, powrotu do pierwotnego stanu systemu;
 - 8) nie jest wymagane spełnienie wszystkich powyższych punktów w przypadku zmian wprowadzanych do systemów teleinformatycznych w celu usunięcia awarii;
 - 9) każda informacja o wdrożeniu zmiany w systemie teleinformatycznym wpisywana jest do dziennika administracyjnego tego systemu.
 3. Nadzór nad zmianami w systemach IT dokonywanymi przez podmioty zewnętrzne:
 - 1) o zamiarze wprowadzenia zmian w systemach teleinformatycznych powinni zostać poinformowani, w udokumentowany sposób, z odpowiednim wyprzedzeniem: administrator systemu, KIT, właściwy PBC i IOD w jssp oraz Właściciel aktywu;
 - 2) za nadzorowanie zmian dokonywanych w systemie teleinformatycznym przez podmiot zewnętrzny po stronie jssp odpowiedzialny jest wyznaczony administrator systemu;
 - 3) zmiany inicjowane i dokonywane przez podmiot zewnętrzny podlegają takim samym regułom ich wprowadzania, jak pozostałe zmiany;
 - 4) postępowanie opisane w niniejszym punkcie może ulec zmianie w przypadku, gdy umowa pomiędzy podmiotem zewnętrznym a jssp posiada odrębne zapisy odnoszące się do dokonywanych zmian w systemach teleinformatycznych;
 - 5) szczegółowa procedura wprowadzania zmian określona zostanie w odrębnym dokumencie SZBI.
 4. Planowanie i odbiór systemów teleinformatycznych:
 - 1) CIS jest odpowiedzialne za monitorowanie i regulację wykorzystania zasobów oraz przewidywanie przyszłej pojemności systemów teleinformatycznych, aby zapewnić ich właściwą wydajność.

Zarządzanie pojemnością systemu teleinformatycznego opisuje właściwa *instrukcja do systemu teleinformatycznego*;

- 2) przed opracowaniem, nabyciem lub istotną modyfikacją systemu teleinformatycznego muszą zostać wyraźnie sprecyzowane przez przyszłego Właściciela aktywu w porozumieniu z komórką organizacyjną GUS właściwą ds. bezpieczeństwa informacji i CIS wymagania w zakresie jego bezpieczeństwa. We współpracy z dostawcami lub innymi komórkami organizacyjnymi GUS/innymi jednostkami zajmującymi się opracowywaniem funkcjonalności projektowanego systemu musi zostać przeprowadzona przez przyszłego Właściciela aktywu analiza możliwych dostępnych rozwiązań w celu zapewnienia równowagi między bezpieczeństwem informacji a innymi celami (łatwość używania, prostota działania, możliwość instalacji kolejnych wersji, odpowiedni koszt);
- 3) każda zmiana polegająca na dodaniu, wymianie lub odłączeniu jakiegokolwiek elementu systemu teleinformatycznego wymaga zgody KIT oraz Pełnomocnika ds. SZBI;
- 4) CIS ustala standardy konfiguracyjne sprzętu komputerowego i oprogramowania. Standardy te podlegają zatwierdzeniu przez Pełnomocnika ds. SZBI w formie Wymagań i stanowią podstawę ustalania wymagań wobec dostawców sprzętu i oprogramowania. Wszelkie zamówienia przekraczające te standardy muszą być zatwierdzone łącznie przez KIT i Pełnomocnika ds. SZBI;
- 5) kupowane, budowane lub modyfikowane systemy teleinformatyczne muszą spełniać wymogi zawarte w niniejszym dokumencie;
- 6) wybór dostawcy jest regulowany osobnymi przepisami;
- 7) specyfikacja zamówienia, w zakresie wymogów sprzętowych, musi być zatwierdzona łącznie przez KIT i Pełnomocnika ds. SZBI przed rozpoczęciem programowania lub przed nabyciem oprogramowania;
- 8) kwestie własności oprogramowania i związanych z nim praw autorskich są określane w umowach zawieranych przez jssp. Jeśli jest to możliwe, jssp powinna być właścicielem praw autorskich zarówno kodu źródłowego, jak i kodu wynikowego;
- 9) zapewnienie odpowiedniej pomocy technicznej musi być określane w umowach. Pomoc techniczna musi zapewniać efektywne rozwiązywanie problemów związanych z danym systemem teleinformatycznym lub aplikacją w czasie określonym w umowie;
- 10) nowe systemy teleinformatyczne muszą być poddane testom zgodnie z właściwą procedurą;
- 11) decyzja o przeniesieniu nowego lub zmodyfikowanego systemu teleinformatycznego ze środowiska testowego do środowiska produkcyjnego jest podejmowana przez przyszłego Właściciela aktywu i zatwierdzana przez kierownika projektu/innego upoważnionego przez Prezesa GUS pracownika;
- 12) przed przekazaniem do użytkowania oprogramowania opracowanego na rzecz statystyki publicznej, 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;
- 13) w przypadku podjęcia decyzji o przechowywaniu kodu źródłowego pisanego na zamówienie statystyki publicznej 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 statystyce publicznej, jak na przykład upadłość lub likwidacja dostawcy oprogramowania lub niewywiązywanie się przez niego z postanowień umowy dotyczących aktualizacji oprogramowania;
- 14) transakcje używane dla celów kontrolnych, testowych, szkoleniowych lub innych celów nieprodukcyjnych, muszą być odseparowane od transakcji używanych w środowisku produkcyjnym;
- 15) za każdym razem, kiedy działanie oprogramowania opracowanego w statystyce publicznej nie zakończy się w oczekiwany sposób, użytkownik powinien w widoczny sposób zostać poinformowany o fakcie wystąpienia błędu;

- 16) osoba opracowująca oprogramowanie przeznaczone do wykorzystania w bieżącej działalności statystyki publicznej, przed oddaniem go do eksploatacji sporządza jego dokumentację techniczną i użytkową. Dokumentacja powinna być przygotowana w sposób umożliwiający zrozumienie działania tego oprogramowania przez osoby niemające doświadczenia w jego użytkowaniu;
 - 17) narzędzia i programy służące do testowania mogą być używane wyłącznie przez upoważnionych pracowników dla celów testowych i rozwojowych;
 - 18) środowisko produkcyjne powinno być odseparowane od środowiska testowego i programistycznego. Jeśli nie jest to możliwe, musi być zapewnione pełne rozdzielanie zasobów sprzętowych i dyskowych lub zagwarantowana minimalna dostępność zasobów niezbędnych do funkcjonowania środowiska produkcyjnego;
 - 19) poziom uprawnień do modyfikacji danych i systemu osób pracujących w środowiskach produkcyjnym, testowym i programistycznym musi być zróżnicowany;
 - 20) najszersze uprawnienia mogą posiadać osoby pracujące w środowisku programistycznym. Uprawnienia w środowiskach testowym i produkcyjnym muszą być ściśle ograniczone;
 - 21) pracownicy zajmujący się opracowywaniem oprogramowania wykorzystywanego do prowadzenia działalności operacyjnej nie mogą mieć dostępu do informacji użytkowanych w środowisku produkcyjnym, z wyjątkiem informacji niezbędnych do prawidłowego opracowania oprogramowania oraz z wyjątkiem sytuacji awaryjnych w zakresie do tego niezbędnym. Dostępem do kont awaryjnych zarządza administrator systemu;
 - 22) testowanie akceptacyjne nowych lub zmodyfikowanych aplikacji nie może być przeprowadzane przez osoby zajmujące się opracowywaniem programów;
 - 23) wszystkie opracowywane aplikacje muszą być ulokowane na przeznaczonych do tego celu serwerach, nie na stacjach roboczych;
 - 24) dostawcy powinni być zaangażowani w formalne testy wspólnie z użytkownikami systemów teleinformatycznych w jssp.
5. Testowanie i montaż sprzętu:
- 1) nowe elementy infrastruktury teleinformatycznej są testowane zgodnie z wymaganiami określonymi w niniejszym dokumencie;
 - 2) CIS/inna wdrażająca jednostka musi być poinformowana w postaci elektronicznej przez Właściciela aktywu o planowanej instalacji sprzętu komputerowego z wyprzedzeniem umożliwiającym sprawdzenie możliwości technicznych podłączenia do istniejącej sieci teleinformatycznej;
 - 3) sprzęt komputerowy musi być odpowiednio przetestowany przez CIS/inną wdrażającą jednostkę przed przeniesieniem do środowiska produkcyjnego.
6. (...)
7. Zapasowe kopie informacji:
- 1) dla wszystkich istotnych danych muszą być tworzone kopie zapasowe, dzięki czemu w przypadku uszkodzenia systemu teleinformatycznego możliwe jest odtworzenie danych i kontynuowanie działalności. Kopie zapasowe stanowią gwarancję, że mogące wystąpić problemy związane z systemem teleinformatycznym, nie będą miały wpływu na działalność operacyjną statystyki publicznej i jej partnerów. Zasady wykonywania kopii zapasowych są określone w procedurze dotyczącej wykonywania kopii zapasowych;
 - 2) procedury dotyczące wykonywania kopii zapasowej uwzględniają potrzeby statystyki publicznej oraz aktualny stan przepisów prawa;
 - 3) jeśli kopia bezpieczeństwa obejmuje całą przestrzeń dyskową serwera, częstotliwość wykonywania kopii zapasowej tego serwera ma być równa częstotliwości wykonywania kopii zapasowej najbardziej krytycznej aplikacji znajdującej się na tym serwerze;
 - 4) kopie zapasowe muszą być wykonywane przed każdą aktualizacją systemu teleinformatycznego lub czynnością serwisową w dwóch przypadkach: jeśli standardowo kopie są wykonywane rzadziej niż codziennie lub jeśli kopie standardowe wykonywane są przyrostowo;

- 5) właściciele informacji zobowiązani są w postaci elektronicznej do przekazywania do CIS/komórki organizacyjnej właściwej ds. informatyki jednostki spisu zbiorów danych przechowywanych w systemach komputerowych, z których należy wykonać kopie zapasowe;
 - 6) administrator systemu przeprowadza okresowe testy odtwarzania danych nie rzadziej niż raz na 6 miesięcy. Procedura odzyskiwania danych produkcyjnych może być przeprowadzana wyłącznie na systemach testowych, w środowisku testowym;
 - 7) raporty z testów przechowywane są w CIS. Jeżeli jednostka ma własny system teleinformatyczny raporty przechowywane są w tej jednostce;
 - 8) jeśli system teleinformatyczny służący do tworzenia kopii zapasowych nie posiada funkcji kontroli poprawności zapisu, testy odtwarzania danych należy przeprowadzać co trzy miesiące;
 - 9) odtworzenie pliku wiąże się z odtworzeniem jego lokalizacji w systemie plików;
 - 10) plik odtwarzany nie może być przekazany użytkownikowi w żaden inny sposób;
 - 11) dla kluczowych systemów produkcyjnych musi być opracowana procedura tworzenia kopii zapasowych;
 - 12) procedura odtwarzania danych musi zawierać wytyczne, zapewniające zachowanie integralności danych odtwarzanych i danych już istniejących;
 - 13) nośniki zawierające kopie zapasowe powinny być przechowywane, co najmniej do czasu utworzenia czwartej kopii, tzn. zawsze powinny być dostępne, co najmniej trzy ostatnie kopie;
 - 14) nośniki zawierające kopie zapasowe (z wyłączeniem kopii wykonywanych przez automatyczną bibliotekę taśmową) muszą być wyposażone w etykiety, na których mają znajdować się aktualne informacje o źródle kopii zapasowej oraz czasie jej wykonania. Wymóg oznaczania etykietą kopii zapasowych nie dotyczy zbiorów danych, których kopie są wykonywane na urządzenia sieciowe lub dyski zewnętrzne;
 - 15) nośniki informacji przeznaczone do wykonywania kopii danych powinny być wymienione nie później niż w momencie osiągnięcia 80% zużycia określonego w odniesieniu do czasu przechowywania danych lub ilości dokonanych zapisów zagwarantowanych przez producenta nośnika;
 - 16) kopie zapasowe muszą być przechowywane poza pomieszczeniami, w których zostały utworzone, w pomieszczeniach na tyle oddalonych, aby lokalny pożar czy zalanie wodą nie zniszczył jednocześnie nośników w obu pomieszczeniach. Pomieszczenia te powinny zabezpieczać przed zniszczeniem w skutek pożaru, zalania, jak również przed kradzieżą i nieuprawnionym dostępem.
8. Dzienniki administratora systemu teleinformatycznego:
- 1) każdy system teleinformatyczny musi posiadać dziennik administratora, prowadzony przez administratora właściwego dla danego systemu;
 - 2) dzienniki administratora systemu teleinformatycznego muszą być prowadzone w formie elektronicznej;
 - 3) zapisy dzienników, aby nie stracić wartości dowodowej, muszą być zabezpieczone przed modyfikacją;
 - 4) dziennik administratora musi zawierać:
 - a) czas zajścia zdarzenia w systemie teleinformatycznym (sukcesu lub niepowodzenia),
 - b) informację na temat zdarzenia w systemie teleinformatycznym (np. użyte pliki) lub niepowodzenia (np. wystąpił błąd i podjęto działania korygujące),
 - c) informację jakiego konta użyto i który z administratorów lub operatorów brał udział w tym użyciu,
 - d) informację o zastosowanych metodach rozwiązania problemu;
 - 5) działania serwisowe w systemie teleinformatycznym osób niebędących uprawnionymi pracownikami (np. modyfikacja konfiguracji, czynności serwisowe), muszą być dokonywane w obecności administratora systemu i zostać przez niego zatwierdzone oraz muszą być odnotowane w dzienniku administratora;
 - 6) administrator systemu cyklicznie (co 3 miesiące) bądź na polecenie KIT/Pełnomocnika ds. SZBI, przygotowuje na podstawie dzienników raporty dotyczące funkcjonowania systemu;
 - 7) przegląd dzienników wykonuje upoważniony przez KIT/dyrektora jednostki pracownik;

- 8) przegląd polega na sprawdzeniu poprawności i kompletności wpisów w dzienniku systemowym ze stanem faktycznym;
 - 9) przegląd musi zostać udokumentowany w formie pisemnej (postać papierowa/elektroniczna).
9. Logi systemowe:
- 1) logi systemowe powinny być zabezpieczone przed modyfikacją;
 - 2) administratorzy systemów zobowiązani są do regularnego przeglądania logów systemowych w poszukiwaniu niestandardowych zapisów świadczących o próbach nieautoryzowanych działań w sieci teleinformatycznej statystyki publicznej. Wszystkie powyższe przypadki niezwłocznie należy zgłosić na Serwis Desk/do właściwego lokalnego PBC zgodnie z *Procedurą dotyczącą zarządzania zdarzeniami związanymi z bezpieczeństwem informacji przetwarzanych w statystyce publicznej*;
 - 3) dostęp do informacji zawartych w logach mogą mieć tylko:
 - a) upoważnieni pracownicy kontroli/audytu,
 - b) pracownicy odpowiedzialni za bezpieczeństwo systemów,
 - c) pracownicy administrujący systemami,
 - d) PBC w GUS,
 - e) upoważnieni audytorzy zewnętrzni w zakresie realizowanego audytu;
 - 4) CIS w okresach półrocznych sporządza w formie pisemnej dla komórki organizacyjnej GUS właściwej ds. bezpieczeństwa informacji raporty o wykrytych nieprawidłowościach w systemach teleinformatycznych;
 - 5) raporty są wykorzystywane przy sporządzaniu rocznych raportów z obsługi incydentów bezpieczeństwa informacji dla Pełnomocnika ds. SZBI.
- (...)

XX. Rozwój i utrzymanie systemów teleinformatycznych – wymagania bezpieczeństwa

1. Aplikacje przetwarzające dane statystyki publicznej muszą identyfikować użytkowników uzyskujących dostęp do danych za pośrednictwem identyfikatora skojarzonego z hasłem. Z identyfikatorem muszą być powiązane prawa dostępu określające uprawnienia użytkownika w ramach aplikacji.
2. Zalecane jest, aby ograniczenia w dostępie do aplikacji były powiązane z dostępem do odpowiednich zasobów (zbiorów danych) z poziomu systemu operacyjnego lub bazy danych. Zalecane jest, aby do identyfikacji i uwierzytelnienia użytkowników aplikacje wykorzystywały mechanizmy oferowane przez system operacyjny i bazę danych.
3. W przypadku, jeżeli ochrona dostępu do aplikacji opiera się tylko na rozwiązaniach oferowanych przez aplikację, architektura systemów operacyjnych i sieci teleinformatycznej uniemożliwia użytkownikom dostęp do zasobów z pominięciem aplikacji (bezpośrednio z poziomu systemu operacyjnego lub bazy danych).
4. W przypadku, jeżeli ochrona dostępu do aplikacji opiera się na systemie haseł wykorzystywanych tylko na potrzeby aplikacji, hasła te nie mogą być zapisywane w zbiorach baz danych w formie jawnej lub przy zastosowaniu zabezpieczeń umożliwiających odtworzenie hasła na podstawie zawartości bazy danych.
5. Przed wprowadzeniem lub modyfikacją danych aplikacja musi dokonać identyfikacji użytkownika wprowadzającego dane. W przypadku masowego przetwarzania danych za pośrednictwem interfejsu, funkcji wbudowanej w aplikację lub polecenia wsadowego, aplikacja musi zidentyfikować użytkownika zlecającego wykonanie operacji masowego przetwarzania oraz identyfikator jednoznacznie identyfikujący polecenie wsadowe lub plik źródłowy z danymi dla interfejsu.
6. Zalecane jest, aby zawartość informacyjna zbiorów danych aplikacji (model danych) dla każdego rekordu danych umożliwiała zidentyfikowanie użytkownika, który jako ostatni dokonał wprowadzenia lub modyfikacji danych. Jeżeli dla określonych zbiorów danych (np. parametrów konfiguracyjnych aplikacji) nie jest możliwe zarejestrowanie osoby dokonującej zmiany, zalecane jest, aby konfiguracja praw dostępu uniemożliwiała wprowadzanie i modyfikację danych.

7. Dla wybranych zbiorów danych (aplikacja powinna umożliwiać taką opcję) odtworzenie historii (dziennika) zmian dokonanych w danych wraz z podaniem identyfikatora użytkownika dokonującego zmiany, terminu dokonania operacji oraz (w miarę możliwości) modyfikowanych wartości. Dla każdej aplikacji, w ramach opracowywania wymagań funkcjonalnych, Właściciel aktywów określa, dla których zbiorów danych funkcja tworzenia dziennika ma być aktywna.
8. Mechanizmy ochrony praw dostępu w aplikacjach musi ograniczać dostęp do danych zgodnie z uprawnieniami nadanymi użytkownikom.
9. Aplikacje przeznaczone do udostępnienia treści w Internecie przed ich opublikowaniem powinny zostać przetestowane przez pracowników CIS pod kątem bezpieczeństwa (testy penetracyjne). Testy bezpieczeństwa powinny być również przeprowadzane po każdej większej aktualizacji aplikacji.
10. W uzupełnieniu do powyższych wymogów Właściciel aktywów lub dyrektor CIS w porozumieniu z Pełnomocnikiem ds. SZBI może zdefiniować dodatkowe wymogi wobec bezpieczeństwa aplikacji, o ile wynikają one z uzasadnionych wymagań funkcjonalnych.
11. W uzupełnieniu do opisanych powyżej zabezpieczeń technicznych Właściciel aktywów koordynuje przygotowanie i zatwierdza do wykorzystania instrukcje zapewniające prawidłową eksploatację aplikacji, w tym adekwatne procedury kontroli poprawności pracy aplikacji i nanoszenia ewentualnych korekt do danych.

XXI. Relacje z dostawcami

1. Zasady bezpieczeństwa informacji obowiązują wszystkich kontrahentów, którzy w trakcie realizacji umowy otrzymują dostęp do zasobów informacyjnych statystyki publicznej.
2. Przy opracowywaniu projektów SIWZ, projektów umów, negocjacji umów z kontrahentem, dyrektor jssp w porozumieniu z Pełnomocnikiem ds. SZBI identyfikuje wymagania bezpieczeństwa w odniesieniu do systemów informacyjnych jssp. W odniesieniu do kontrahenta oraz nabywanych produktów lub usług, należy wziąć pod uwagę:
 - 1) zasady kontroli dostępu do systemów teleinformatycznych, w tym:
 - a) dozwolone metody dostępu oraz kontroli,
 - b) autoryzację praw dostępu i przywilejów dla użytkownika,
 - c) prowadzenie listy osób uprawnionych do korzystania z udostępnianych usług wraz z ich prawami i przywilejami w odniesieniu do każdej z nich,
 - d) przyznawanie, zmiana i odbieranie praw dostępu lub przerywanie połączeń między systemami,
 - e) przyjęcie zasady, że dostęp jest zabroniony, jeśli nie został jawnie przyznany,
 - 2) poziom ochrony zasobów, w tym:
 - a) poufność, integralność, dostępność oraz inne właściwości zasobów, istotne dla danej umowy,
 - b) ograniczenie kopiowania i ujawniania informacji,
 - c) korzystanie z zapisów o zachowaniu poufności,
 - d) wymagane zabezpieczenia i mechanizmy ochrony fizycznej,
 - e) ochronę przed złośliwym oprogramowaniem,
 - f) zapewnianie zwrotu lub niszczenia zasobów w chwili zakończenia umowy lub w innym uzgodnionym w umowie czasie,
 - g) aktualną listę zasobów,
 - 3) powiadamianie, raportowanie i śledzenie zdarzeń związanych z naruszeniem bezpieczeństwa informacji lub ciągłości działania,
 - 4) prawo do monitorowania i blokowania działań związanych z zasobami informacyjnymi jssp,
 - 5) nadzór realizacji umowy,
 - 6) oczekiwany oraz nieakceptowany poziom usług,
 - 7) wymagania dla ciągłości usług, w tym pomiaru ich dostępności i niezawodności,
 - 8) weryfikowalne kryteria wydajności, sposób ich monitorowania i raportowania,
 - 9) strukturę i zakres raportowania oraz formy raportów,

- 10) zarządzanie zmianami oraz wymagania dotyczące instalowania i utrzymywania oprogramowania/sprzętu,
 - 11) prawo do przeprowadzenia audytów określonych w umowie, ustalenie zakresu audytów, ewentualnego zlecenia tych czynności stronie trzeciej,
 - 12) zabezpieczenia, jakie kontrahent ma wdrożyć u siebie lub u poddostawców, jeśli tacy występują,
 - 13) odpowiedzialność wynikającą z przepisów prawa oraz odpowiedzialność finansową,
 - 14) prawo do własności intelektualnej i praw autorskich,
 - 15) szkolenie pracowników lub kontrahenta,
 - 16) warunki renegocjacji lub zakończenia umowy, w tym:
 - a) wdrożenie i utrzymywanie BCP na wypadek rozwiązania umowy przed ustalonym terminem,
 - b) renegocjację umowy ze względu na zmianę wymagań bezpieczeństwa informacji w jssp;
3. W przypadku, gdy kontrahent w trakcie wykonywania umowy ma lub może mieć dostęp do zasobów informacyjnych jssp, w umowach z kontrahentami wprowadzana jest klauzula dotycząca obowiązku przestrzegania bezpieczeństwa informacji. Klauzula ta powinna zawierać: zobowiązanie kontrahenta do przestrzegania *Wymagań bezpieczeństwa informacji dla kontrahentów i osób zewnętrznych*, ochrony udostępnionych zasobów informacyjnych poprzez ograniczenie ich kopiowania i udostępniania oraz do ich zwrotu lub zniszczenia w momencie zakończenia umowy:
- 1) do umów, o których mowa w ust 2, dołączane będą w formie załącznika Wymagania bezpieczeństwa informacji dla kontrahentów i osób zewnętrznych. Umowy te muszą zawierać zapis, że w przypadku zmian Wymagania bezpieczeństwa informacji dla kontrahentów i osób zewnętrznych, zamawiający (jssp) zobowiązuje się do niezwłocznego, pisemnego powiadomienia wykonawcy o nowych wymaganiach i przekazania ich aktualnej wersji;
 - 2) naruszenie bezpieczeństwa informacji przez kontrahenta stanowi podstawę do odstąpienia przez jssp od umowy i żądania pokrycia ewentualnej szkody lub zapłaty kary umownej;
 - 3) kontrahenci mający dostęp do zasobów informacyjnych na podstawie odrębnych przepisów/upoważnień, przed przyznaniem dostępu do zasobów informacyjnych otrzymują do zapoznania się Wymagania bezpieczeństwa informacji dla kontrahentów i osób zewnętrznych;
 - 4) odpowiedzialność za bezpieczeństwo informacji statystyki publicznej obejmuje działania, które miały miejsce w siedzibie jssp oraz wszelkie sytuacje, w których informacje związane z działalnością jssp są przetwarzane poza jej siedzibą. Obejmuje to w szczególności zdalny dostęp do sieci teleinformatycznej statystyki publicznej.

XXII. Zarządzanie incydentami

1. Dokumentem regulującym proces zgłaszania oraz obsługi zdarzeń związanych z bezpieczeństwem informacji jest *Procedura zarządzania zdarzeniami związanymi z bezpieczeństwem informacji przetwarzanych w statystyce publicznej*.
2. Pojęcia oraz role związane z obsługą zdarzeń, noszących znamiona incydentu bezpieczeństwa informacji, zostały szczegółowo ujęte w procedurze, o której mowa w ust 1.
3. Zapisy procedury obowiązują wszystkich pracowników oraz pracowników reprezentujących podmiot zewnętrzny, mających dostęp do systemów teleinformatycznych.
4. Na potrzeby obsługi naruszenia ochrony danych osobowych opracowano Procedurę oceny i notyfikacji naruszeń ochrony danych osobowych wraz z Instrukcją dla pracowników/współpracowników w zakresie rozpoznawania naruszeń ochrony danych osobowych.

XXIII. Zgodność

1. Zgodność z wymaganiami prawa:
 - 1) wszystkie działania związane z przetwarzaniem informacji w jssp muszą być zgodne z wymaganiami przepisów prawa krajowego, Unii Europejskiej, prawa międzynarodowego;
 - 2) wykaz aktów prawnych i innych regulacji związanych z funkcjonowaniem SZBI statystyki publicznej sporządza komórka organizacyjna GUS właściwa ds. bezpieczeństwa informacji na formularzu stanowiącym załącznik nr 4;

- 3) wykaz jest aktualizowany na bieżąco, a zmiana wykazu skutkuje utworzeniem kolejnej jego wersji;
 - 4) aktualny wykaz oraz wersje archiwalne są dostępne w Intranecie (http://intranet/GUS/ST/dokumenty_SZBI).
2. Prawo do własności intelektualnej:
- 1) w przypadku tworzenia dóbr intelektualnych na zlecenie jssp, w umowie z wykonawcą musi być zawarty zapis o przekazaniu praw autorskich do dzieła na rzecz zamawiającego (jssp);
 - 2) użytkowanie własności intelektualnej w jssp może być dokonywane zgodnie z zawartymi zapisami w umowach i licencjach. Naruszanie prawa własności intelektualnej jest zagrożone sankcjami dyscyplinarnymi oraz wynikającym z przepisów prawa krajowego, Unii Europejskiej, prawa międzynarodowego;
 - 3) własność intelektualna wykorzystywana przez jssp dotyczy w szczególności oprogramowania i jego aktualizacji – wykupionych licencji i aktualizacji. Wszystkie programy wykorzystywane przez jssp muszą posiadać ważne licencje;
 - 4) powielanie, przekształcanie do innego formatu lub wyodrębnianie z nagrań komercyjnych (filmów, nagrań dźwiękowych itd.), kopiowanie całości lub części książek, artykułów, raportów lub innych dokumentów, może odbywać się tylko z zachowaniem zgodności z prawem autorskim;
 - 5) nadzór oraz administrowanie oprogramowaniem sprawowane są wyłącznie przez pracowników CIS. KIT odpowiada za prawidłowe zarządzanie licencjami dotyczącymi centralnych zakupów i ich przechowywanie, administrowanie aktualizacjami oraz zarządzanie uprawnieniami do oprogramowania używanego w jssp;
 - 6) CIS przechowuje dokumentację licencyjną, kopie umów, nośniki z oprogramowaniem dotyczące centralnych zakupów dla statystyki publicznej. Każda z jednostek przechowuje u siebie dokumentację licencyjną oraz kopie nośników oprogramowania komputerowego zakupionego we własnym zakresie, po uprzednim zgłoszeniu tego faktu do CIS;
- (...)

XXV. Ochrona danych osobowych w jssp

1. Zgodnie z przepisami RODO, ADO wyznacza osobę odpowiedzialną za obszar ochrony danych osobowych w jssp, powierzając jej funkcję IOD i zapewnia adekwatne środki oraz zasoby niezbędne do wykonywania powierzonych jej zadań.
2. Szczegółowy zestaw praw, reguł, zasad i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i przetwarzania danych osobowych w statystyce publicznej jest opisany w dokumentach SZBI regulujących ochronę danych osobowych w statystyce publicznej.

XXVI. Uwarunkowania prawne

1. PBI została sformułowana w wyniku realizacji wymagań określonych w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
2. PBI została opracowana zgodnie z wymaganiami normy ISO/IEC 27001 i jest zgodna z obowiązującymi przepisami prawa.