Załącznik nr 1

numer sprawy: CIS-WAZ.2720.59.2018

Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest usługa pt. „Przeprowadzenie inwentaryzacji zasobów informacyjnych wybranych procesów, określenie schematu klasyfikacji oraz wdrożenie wybranych polityk tematycznych, wytycznych i procedur bezpieczeństwa IT”.

I. Spis treści

II. Terminy i definicje

CIS – Centrum Informatyki Statystycznej

GUS – Główny Urząd Statystyczny

MF – Ministerstwo Finansów

Mikrodane – poufne dane statystyczne o handlu wewnętrznym przekazywane przez MF z systemu INTARSTAT

OBM – Operacyjna Baza Mikrodanych – wydzielone w Organizacji środowisko do przetwarzania i składowania mikrodanych

Organizacja – GUS i CIS

System wymiany - systemu do wymiany poufnych danych statystycznych

III. Tło akcji

W 2015 r. Eurostat i wybrane państwa członkowskie przeprowadziły w ramach projektu SIMSTAT próbną wymianę mikrodanych z handlu wewnętrznego pochodzących z systemu INTRASTAT (dane zbierane oraz kontrolowane dla celów statystyki handlu zagranicznego przez Ministerstwo Finansów, dalej jako „MF").

Celem projektu SIMSTAT było przetestowanie zdolności państw członkowskich do wymiany mikrodanych statystycznych na próbnych danych. Wymiana danych między hubem Eurostatu a GUS była przeprowadzona przez komponent SIMSTAT przy użyciu bramki CCN w Ministerstwie Finansów. Wymiana danych w projekcie SIMSTAT została zakończona sukcesem. Wymiana danych miała charakter próbny i nie jest obecnie prowadzona.

Eurostat, w ramach realizowanej obecnie Wizji ESS 2020, planuje rozpocząć od 2020 r. wymianę mikrodanych dot. handlu wewnętrznego pomiędzy państwami członkowskimi. W tym celu realizowany jest projekt ESDEN (*European statistical data exchange network*). Dane dot. wywozu towarów z Polski będą wysyłane przez GUS wraz z ID partnera zagranicznego (*towar od partnera X <polskiego> do partnera Y z kraju członkowskiego w ujęciu miesięcznym*). Dane będą wysyłane poprzez centralny punkt (hub utworzony w Eurostat) do innych państw członkowskich. Dane innych państw będą przysyłane do GUS przez hub centralny.

Dane przeznaczone do wymiany mają różny poziom zabezpieczeń zależnie od regulacji krajowych państw członkowskich. ESSC (Komitet Sterujący ESS) w maju 2016 r. przyjął dokument „Wspólne ramy bezpieczeństwa IT ESS" (*IT Common Security Framework* lub *IT Security Framework*) określający jednolity standard zabezpieczeń dla wszystkich państw członkowskich. Dokument został przygotowany na podstawie rodziny norm ISO/IEC 27000 wraz z powiązanymi normami (w szczególności ISO/IEC 27000, 27001 i 27002). Dokument zawiera ponad 90 wymagań dotyczących bezpieczeństwa informacji. Zakres

dokumentu pokrywa przede wszystkim obszar systemów teleinformatycznych i organizacyjny, w mniejszym stopniu procesów kadrowych i bezpieczeństwa fizycznego.

Wymiana mikrodanych z handlu wewnętrznego została wpisana do aktualnie procedowanego dokumentu FRIBS (Framework Regulation Integrating Business Statistics) jako obowiązkowa od 2021 r. Eurostat planuje umożliwić fizyczną wymianę danych po weryfikacji czy dane państwo spełnia wymagania bezpieczeństwa określone w IT Security Framework. W związku z powyższym Eurostat zaplanował certyfikację państw członkowskich oraz Eurostatu przez zewnętrznego audytora. GUS / CIS został zgłoszony do procesu certyfikacyjnego na 2019 r.

Zakres certyfikacji określają dwa dokumenty:

- „Wspólne ramy bezpieczeństwa IT ESS" w zakresie wskazania obszarów certyfikacji, dowodów koniecznych do wykazania spełnienia wymagań oraz koniecznych przeglądów bezpieczeństwa.
- Dokument „Mitigation of risks related to the exchange of identifiable micro-data" stanowiący uzupełnienie powyższego dokumentu o wskazanie wymagań, które mają zastosowanie do całej organizacji (obszar organizacji) lub jedynie obszaru wykorzystania mikrodanych z handlu wewnętrznego (obszar MDE, ang. Micro Data Exchange) (Kolumna „Docelowy zakres wdrożenia" w Tabeli nr 1).

IV. Cel zamówienia

Celem realizacji zamówienia jest podniesienie bezpieczeństwa IT w obszarze wymiany poufnych danych statystycznych zgodnie z wymaganiami Wspólnych Ram Bezpieczeństwa IT Europejskiego System Statystycznego.

Cel zostanie osiągnięty przez napisanie i wdrożenie dokumentacji bezpieczeństwa wspierających Politykę bezpieczeństwa informacji dla obszaru wymiany mikrodanych statystycznych wymienianych obowiązkowo między Eurostatem a Rzeczpospolitą Polską lub między Państwami członkowskimi.

Rezultatem zamówienia będzie powstała i wdrożona dokumentacja bezpieczeństwa w organizacji.

Polityki, standardy i wytyczne będą utrzymywane w pracy operacyjnej organizacji przez uprawnionych pracowników organizacji. Zostaną poddawane przeglądom, będą monitorowane i rozwijane wg metody zaproponowanej przez Eurostat w ESS Core IT Security Framework, tj.: Planuj– Wykonuj – Sprawdzaj – Działaj.

V. Opis danych i procesów

W systemie zakłada się realizację trzech procesów z wykorzystaniem wdrożonej / wdrażanej infrastruktury:

- PROCES 1 - przyjęcie zbioru z mikrodanymi z MF poprzez wdrożoną w Organizacji sieć krajową Testa krajowa / gov.net lub przyjęcie danych na nośniku zewnętrznym w przypadku niemożności użycia wydzielonej sieci, a następnie walidacja wstępna (z możliwością podglądu zbiorów) oraz

przekazanie zbioru do wydzielonego środowiska OBM (z wykorzystaniem nośnika usb / płyty, w przyszłości przez odwołanie bezpośrednie):

- Zbiór z danymi pochodzącymi z systemu INTRASTAT z Ministerstwa Finansów jest przesyłany raz w miesiącu
- Zbiór ma stałą strukturę.

- PROCES 2 - po zaakceptowaniu zbioru przez właściciela biznesowego w systemie OBM przesłanie zbioru przez System (z użyciem komponentów EDAMIS4) do huba Eurostatu.
- PROCES 3 - Zbiór danych z mikrodanymi pochodzącymi z Państw Członkowskich przyjmowany będzie przez sieć Testa europejską, następnie bez walidacji merytorycznej (walidacja wykonywana będzie w hubie Eurostatu) dane będą przekazywane do wydzielonego środowiska OBM, w którym dokonywane będzie przetwarzanie zbioru zgodnie z aktualnymi potrzebami.
  - Zbiory z danymi pochodzącymi z innych Państwa członkowskich będą importowane z HUBu Eurostatu raz w miesiącu w podziale na Państwa, tj. przewidywana liczba zbiorów wynosi 26.
  - Zbiór ma stałą strukturę.

VI. Zgodność z dokumentacją bezpieczeństwa w Organizacji

Przedmiot zamówienia wynika z wymagań dokumentu „Wspólne ramy bezpieczeństwa IT ESS" i dokumentów powiązanych. Szczegółowy zakres wymagań został przedstawiony w następnych rozdziałach. Celem wdrożenia dokumentacji jest dostosowanie Organizacji do wymogów wymiany mikrodanych i przygotowanie jej do planowanej certyfikacji. Zakres certyfikacji określają:

- Dokument „Wspólne ramy bezpieczeństwa IT ESS" (ang. IT Common Security Framework lub IT Security Framework), zaakceptowany przez European Statistical System Committee, w zakresie wskazania obszarów certyfikacji, dowodów koniecznych do wykazania spełnienia wymagań oraz koniecznych przeglądów bezpieczeństwa.
- Dokument „Mitigation of risks related to the exchange of identifiable micro-data" zaakceptowany przez Vision Impelementation Group, stanowiący uzupełnienie powyższego dokumentu o wskazanie kontrolek bezpieczeństwa, które:
  - Mają kluczowe znaczenie w procesie certyfikacji (podział „major / minor")
  - Mają zastosowanie do całej organizacji lub jedynie obszaru wykorzystania mikrodanych obrotu towarami z handlu zagranicznego.

Dokumenty określone w pkt. 1 zostały opracowane na podstawie rodziny norm ISO27000:2015. Wymagania i struktura dokumentów jest zgodna z przedstawionymi w ww. normach.

Dokumentacja bezpieczeństwa dotychczas wdrożona w Organizacji mająca zastosowanie do procesu wymiany mikrodanych:

1. Polityka Bezpieczeństwa Informacji Statystyki Publicznej zawierająca ogólne cele i podział ról bezpieczeństwa w Organizacji.

2. Procedura zarządzania zdarzeniami związanymi z bezpieczeństwem informacji przetwarzanych w statystyce publicznej
3. Zasady przeprowadzania analizy ryzyka w zakresie utraty atrybutów bezpieczeństwa informacji w statystyce publicznej
4. Polityka bezpieczeństwa teleinformatycznego zawierająca:
    a. Zasady bezpieczeństwa zasobów statystyki publicznej
    b. Polityka przesyłania informacji i wiadomości elektronicznych
    c. Wytyczne dot. Zabezpieczenia przed nieautoryzowanym przesyłaniem informacji
    d. Polityka poufnych informacji uwierzytelniających
    e. Wytyczne dotyczące zarządzania poufnymi informacjami uwierzytelniającymi użytkowników
    f. Polityka zabezpieczenia kryptograficznego
    g. Standardy zabezpieczeń kryptograficznych
    h. Polityka zarządzania kluczami kryptograficznymi
    i. Wytyczne dot. Wykrywania szkodliwego oprogramowania
    j. Wytyczne dot. Zapobiegania rozprzestrzenianiu szkodliwego oprogramowania
    k. Wytyczne dot. Odzyskiwania zainfekowanego oprogramowania
    l. Standardy zarządzania ryzykiem w zakresie podatności oprogramowania
    m. Polityka ponownego użycia zasobów
    n. Polityka ochrony zapisów
    o. Polityka akceptowalnego wykorzystania aktywów
    p. Polityka kontroli dostępu do aktywów
    q. Wytyczne dotyczące wykorzystania urządzeń prywatnych do celów służbowych
    r. Wytyczne dotyczące zwrotu aktywów
    s. Wytyczne dotyczące zarządzania nośnikami wymiennymi
    t. Wytyczne dotyczące przekazywania nośników
    u. Wytyczne dotyczące rejestrowania i wyrejestrowania użytkowników
    v. Wytyczne dotyczące przydzielania dostępu użytkownikom
    w. Wytyczne dotyczące przeglądu praw dostępu użytkowników
    x. Wytyczne dotyczące odbierania lub dostosowywania praw dostępu
    y. Standardy zarządzania zmianą
    z. Standardy zarządzania incydentami
    aa. Standard oceny zdarzeń związanych z bezpieczeństwem informacji
    bb. Standardy reagowania na incydenty związane z bezpieczeństwem informacji
    cc. Wytyczne dot. Zgłaszania podatności (słabości) związanych z bezpieczeństwem informacji
    dd. Wytyczne dotyczące wyciągania wniosków związanych z bezpieczeństwem informacji
    ee. Polityka gromadzenia materiału dowodowego
5. Zasady przyjęcia zbiorów danych administracyjnych oraz form i trybów ich przepływu w procesie przetwarzania.

6. Polityka bezpieczeństwa teleinformatycznego przetwarzania mikrodanych wymienianych pomiędzy Państwami członkowskimi Unii Europejskiej zawierająca:
    a. Zdefiniowane role i odpowiedzialność
    b. Polityka postępowania z nośnikami
    c. Polityka przekazywania nośników
    d. Polityka bezpieczeństwa prac rozwojowych
    e. Wytyczne dot. bezpieczeństwa prac rozwojowych
    f. Standard bezpieczeństwa prac rozwojowych
    g. Polityka zmian w pakietach oprogramowania
    h. Wytyczne dotyczące kontroli nad instalowanym oprogramowaniem
    i. Wytyczne dot. dostępu do środowisk rozwojowych, testowych i produkcyjnych
    j. Standard zabezpieczenia informacji
    k. Wytyczne dot. zabezpieczenia informacji w oprogramowaniu
    l. Wytyczne dotyczące rejestrowania zdarzeń
    m. Wytyczne dot. ochrony transakcji
    n. Wytyczne dotyczące zabezpieczenia biur, pomieszczeń i obiektów
    o. Standard kontroli dostępu do sieci i usług sieciowych
    p. Standard zarzadzania pojemnością
7. Dokumentacja bezpieczeństwa OBM:
    a. Polityka bezpieczeństwa systemu Operacyjnej Bazy Mikrodanych.
    b. Analiza ryzyka systemu Operacyjnej Bazy Mikrodanych.
    c. Instrukcja zarządzania informatycznym systemem Operacyjnej Bazy Mikrodanych.
    d. Polityka bezpieczeństwa danych osobowych systemu Operacyjnej Bazy Mikrodanych.
    e. Szczegółowy wykaz odpowiedzialności dotyczący systemu Operacyjnej Bazy Mikrodanych.

VII. Opis środowiska MDE:

System wymiany

Projektowany system wymiany będzie punktem odbierania i wysyłania zbiorów. Dane docelowo trafią do wdrożonego systemu OBM. Wymiana danych nastąpi poprzez dostarczony przez Eurostat system Edamis4 przy użyciu wydzielonej sieci gov.net / TESTA. Docelowo łącze powinno przesyłać dane na wydzieloną stację roboczą. Dane powinny być przekazywane do systemów produkcyjnych (OBM) przy pomocy zewnętrznych nośników danych (płyta lub inne) lub w przyszłości odwołania bezpośredniego.

OBM

Wdrożony w Organizacji system OBM jest bazą, w której m.in. prowadzone są prace na zbiorach danych z zewnętrznych systemów informacyjnych. Dane z zewnętrznych systemów informacyjnych są przekształcane w dane statystyczne, jak również przetwarzane w zakresie wyliczania dodatkowych

zmiennych, wyodrębniania podzbiorów i łączenia zbiorów. Wdrożony System Operacyjnej Bazy Mikrodanych obejmuje infrastrukturę sprzętowo-systemowo-narzędziową (sprzęt komputerowy, oprogramowanie systemowe, oprogramowanie narzędziowe) oraz oprogramowanie aplikacyjne (programy komputerowe będące efektem prac programistycznych Wykonawcy systemu). Baza wykorzystuje narzędzia bazodanowe MS SQL i analityczne SAS oraz R.

Użytkownicy

W obszarze wymiany poufnych danych statystycznych definiuje się dwa rodzaje uprawnień użytkowników:

- Konto podstawowe – wykorzystywane do pracy z danymi oraz wysyłania i odbierania danych przekazywanych z sieci Testa;
- Konto administracyjne – służące tylko do administrowania stacjami roboczymi oraz serwerami i innymi urządzeniami w celu uzyskania zgodności z wymaganiami zdefiniowanymi dla sieci Testa oraz zdefiniowanymi przez Eurostat.

Następujące role mogą być łączone oraz mogą być realizowane w oparciu o konta użytkownika uprzywilejowanego (konto administracyjne):

- Administrator OBM;
- Administrator systemu do wymiany poufnych danych statystycznych.

Następujące role mogą być łączone oraz muszą być realizowane w oparciu o konta podstawowe (konto bez uprawnień administracyjnych):

- Użytkownika odbierającego dane;
- Użytkownika wysyłającego dane;
- Użytkownik posiadający dostęp do danych.

Zasady administrowania obydwoma grupami użytkowników (z uprawnieniami administracyjnymi i bez tych uprawnień) muszą być zgodne z przyjętymi w Organizacji zasadami, zgodnymi z wymaganiami normy ISO 27001.

Szacowana liczba użytkowników:

- Administrator systemu do wymiany poufnych danych statystycznych –3 osoby
- Użytkownik odbierający dane – 5 osób;
- Użytkownik wysyłający dane – 5 osób;
- Użytkownik posiadający dostęp do danych – 4 osoby.

VIII. Wymagania formalne dla dokumentów

Wykonawca będzie zobowiązany do wykonania Przedmiotu zamówienia z należytą starannością, zgodnie z zasadami wiedzy technicznej, obowiązującymi przepisami prawa polskiego i europejskiego oraz w taki

sposób, aby zastosowane rozwiązania pozwoliły na zminimalizowanie kosztów inwestycyjnych, wydatków rzeczowych, w tym eksploatacyjnych.

Dokumentacja zostanie przygotowane z uwzględnieniem następujących wymagań:

1. Będzie opracowaniem kompletnym i wyczerpującym z punktu widzenia celu, któremu ma służyć,
2. Zostanie przygotowany w języku polskim, w formie papierowej (format A-4, średnia ilość znaków na stronie – 1 900) oraz formie elektronicznej w formacie plików do edycji. Forma graficzna publikacji, czcionki, formatowanie strony, wygląd ew. ilustracji, itp. zostanie ustalona po podpisaniu umowy,
3. Lista dokumentów i materiałów źródłowych, które posłużyły Wykonawcy do opracowania dokumentacji zostanie przygotowana w wersji elektronicznej.
4. Wykonawca zobowiązuje się do przekazywania Zamawiającemu wszelkich informacji mających wpływ na realizację Przedmiotu zamówienia oraz do niezwłocznego udzielania odpowiedzi i wyjaśnień na zgłaszane przez Zamawiającego uwagi dotyczące jego realizacji w formie pisemnej.
5. Wykonawca dostarczy Zamawiającemu ostateczną i zaakceptowaną przez Zamawiającego wersję dokumentów, w wersji papierowej w 2 egzemplarzach oraz w wersji elektronicznej na nośniku optycznym CD lub DVD. Dokumenty zostaną dostarczone do siedziby Zamawiającego.
6. Wykonawca na każdym etapie realizacji Przedmiotu zamówienia będzie ściśle współpracował z przedstawicielami Zamawiającego, ponadto w miarę bieżących potrzeb, odbywać się będą spotkania robocze Zamawiającego z Wykonawcą.
7. Dokumentacja powinna być przygotowana jedynie na potrzeby realizacji niniejszego zamówienia.
8. Na potrzeby opracowania przedmiotu zamówienia zamawiający udostępni po podpisaniu umowy posiadane materiały i dokumenty, które mogą być pomocne przy realizacji zamówienia.

IX. Harmonogram

Wykonawca będzie zobowiązany do wykonania Przedmiotu zamówienia w poniższych terminach i w następujący sposób:

1. W terminie do 2 dni roboczych od dnia zawarcia umowy weźmie udział w spotkaniu organizacyjnym z Zamawiającym w siedzibie Centrum Informatyki Statystycznej w Warszawie. Celem spotkania będzie omówienie i uzgodnienie harmonogramu prac.
2. Wykonawca dostarczy wymagane dokumenty na nie mniej niż 2 dni robocze przez końcową datą odbioru. Szczegółowy harmonogram dostarczania dokumentów zostanie uzgodniony z wykonawcą po podpisaniu umowy.
3. Wykonawca zobowiązuje się do wprowadzenia uwag lub poprawek zamawiającego w dokumentach przed datą odbioru przedmiotu zamówienia.

X. Odbiór Przedmiotu Zamówienia

Dokumentacja opracowana w ramach realizacji Przedmiotu Zamówienia weryfikowana będzie według następujących kryteriów:

1. zawartość merytoryczna – treść dokumentu powinna zawierać informacje istotne, niosące treść adekwatną do zakresu dokumentu;
2. zakres – treść dokumentu winna obejmować uzgodniony zakres prac, wszystkie kwestie mieszczące się w uzgodnionym zakresie muszą zostać zawarte w dokumencie;
3. klarowność – dokument winien być tak napisany, by czytelnik był w stanie zrozumieć jego treść bez potrzeby zasięgania wyjaśnień u autora, szczególnie istotna jest struktura oraz czytelność raportów i specyfikacji, w określonych przypadkach dokument winien zawierać słowniczek używanych terminów lub inne materiały pomocnicze;
4. precyzja – specyfikacje, opisy czy uwagi zawarte w dokumencie winny być poprawne, jednoznaczne i kompletne.

XI. Zadania Wykonawcy

1. Wykonawca opracuje i przedstawi Zamawiającemu następujące dokumenty będące uzupełnieniem dokumentów określonych w rozdziale VI pkt 4 i 6:

Tabela 1 – Lista dokumentów do opracowania

L.p.	**Nazwa dokumentu**	**Docelowy zakres wdrożenia**
1	Schemat klasyfikacji informacji	Generalny
2	Wytyczne do znakowania informacji	MDE
3	Procedura znakowania informacji	MDE
4	Procedura postępowania z aktywami	Generalny
5	Procedura utrzymywania klasyfikacji informacji	Generalny
6	Procedura klasyfikacji informacji dla zasobu MDE	MDE
7	Polityka zarządzania strefami zabezpieczonymi	MDE
8	Polityka relacji z dostawcami	MDE
9	Polityka kopi zapasowych	MDE
10	Polityka ciągłości działania	MDE
11	Procedura eksploatacyjna	MDE

12	Inwentaryzacja zasobów informacyjnych	MDE

2. Docelowy zakres wdrożenia dokumentu oznacza dla:
   - MDE – dokument dotyczy wyłącznie procesów 1, 2 i 3 określonych w rozdziale V.
   - Generalny – dokument dotyczy całej Organizacji.
3. Każdy z ww. dokumentów:
   - musi być opracowany na podstawie rodziny norm ISO 27000.
   - musi być zgodny z aktualnie wdrożonymi dokumentami w organizacji lub proponować ich zmianę. W przypadku uznania, po analizie przeprowadzonej w ramach zamówienia, dotychczas wdrożonych i wykorzystywanych polityk, standardów, wytycznych lub innych dokumentów za wystraczające do realizacji celów niniejszego zamówienia, Zamawiający po weryfikacji uzna je za spełniające cel niniejszego zamówienia.
4. Szczegółowe wymagania dla ww. dokumentów znajdują się w poniższych rozdziałach.

XII. Schemat klasyfikacji informacji

1. Zadaniem Wykonawcy jest opracowanie schematu klasyfikacji informacji.
2. Celem schematu klasyfikacji informacji jest zdefiniowanie właściwego poziomu atrybutów dla informacji.
3. Wymagania dla schematu klasyfikacji informacji:
   a. Schemat klasyfikacji informacji zostanie opracowany na podstawie grup informacji aktualnie wyodrębnionych w Polityce Bezpieczeństwa Informacji, tj. na podstawie wkładu dostarczonego przez Zamawiającego, oraz obowiązujących wymagań prawnych. Schemat nie będzie uwzględniał informacji tajnych i zastrzeżonych. Aktualnie istnieje 6 grup informacji i 4 podgrupy.
   b. Zaproponowany schemat klasyfikacji informacji będzie zawierał wydzielone grupy informacji z uwzględnieniem jako przykładu informacji z procesów określonych w rozdziale V (MDE).
   c. Każda z informacji zostanie przypisana do jednej z trzech grup: jawna, do użytku wewnętrznego i poufna.
   d. Schemat będzie umożliwiał przypisanie informacjom lub ich typom atrybutów obowiązujących w statystyce publicznej , tj. poufność (C), integralność (I), dostępność (A) i rozliczalność (R). Definicje atrybutów zapewnia Zamawiający. Dla każdego z atrybutów będzie określony poziom oddziaływania (parametr) w trzystopniowej skali (ograniczony, średni, krytyczny).
   e. Z poziomem parametrów powinny być powiązane docelowe metody zabezpieczenia informacji.
   f. Poziom parametrów będzie określał właściciel informacji, który będzie mógł zmienić proponowaną dla typu informacji wartość parametrów.
   g. Do informacji będzie przypisane określone ryzyko wg zaproponowanego podziału przez Zamawiającego.
   h. Do informacji będzie przypisany właściciel informacji.
4. Schemat powinien zostać dostarczony w postaci tabeli w pliku w formacie xlsx.

XIII. Wytyczne do znakowania informacji

1. Dokument dedykowany wyłącznie procesom MDE.
2. Wytyczne do znakowania informacji będą opisowym wprowadzeniem do procedury znakowania informacji.
3. Muszą zawierać zapisy określające gdzie i jak będą przypisywane znaczniki do informacji z procesów określonych w rozdziale V z uwzględnieniem jak traktowane są aktywa w zależności od rodzaju nośnika.

XIV. Procedura znakowania informacji

1. Dokument dedykowany wyłącznie procesom MDE.
2. Procedura będzie dotyczyć elektronicznej postaci informacji. W systemie OBM informacje są znakowane w postaci protokołów zbioru oraz ustalane są metadane zbioru. Dla informacji w postaci papierowej istnieją wewnętrzne regulacje w JRWA.
3. Oznaczenie powinno odwoływać się do miejsca informacji w schemacie klasyfikacji informacji.
4. Procedura powinna określać dopuszczalne przypadki, w których etykiety ze względów technicznych lub kosztowych można pominąć.
5. Znaczniki muszą być łatwo rozpoznawalne przez pracowników.

XV. Procedura postępowania z aktywami

1. Procedura postępowania z aktywami powinna być zgodna ze schematem klasyfikacji informacji.
2. Procedura musi być zgodna z istniejącym w organizacji zarządzeniem dot. pozyskiwania, przetwarzania, składowania i przekazywania informacji.
3. W szczególności procedura musi określać wymagania dot.:
    a. Ograniczeń dostępu dla każdego poziomu klasyfikacji.
    b. Uprawnionych odbiorców aktywów.
    c. Ochrony kopii informacji na poziomie zgodnym z ochroną oryginalnych informacji.
    d. Przechowywania aktywów teleinformatycznych zgodnie z wytycznymi producenta.
    e. Oznakowania egzemplarzy nośników.
    f. Zawierania porozumień z innymi organizacjami dot. klasyfikacji informacji.

XVI. Procedura utrzymywania klasyfikacji informacji

1. Procedura utrzymywania klasyfikacji informacji powinna być zgodna ze schematem klasyfikacji informacji.
2. W szczególności procedura musi określać wymagania dot.:
    a. Sposobu określenia podatności informacji na nieautoryzowaną zmianę lub ujawnienie.
    b. Określenia potencjalnego poziomu oddziaływania dla nieautoryzowanej zmiany lub ujawnienia informacji wynikającej z parametrów atrybutów informacji.

c. Potencjalnych procesów biznesowych, które powinny zostać zintegrowane ze schematem klasyfikacji informacji.
d. Metodykę przeglądu i weryfikacji schematu klasyfikacji informacji.

XVII. Procedura klasyfikacji informacji dla zasobu MDE

1. Dokument dedykowany wyłącznie procesom MDE.
2. Procedura utrzymywania klasyfikacji informacji powinna być zgodna ze schematem klasyfikacji informacji i procedurą utrzymywania klasyfikacji informacji.
3. W szczególności procedura musi określać wymagania dot. procesów MDE.:
   a. Proponowane techniczne i organizacyjne zabezpieczenia dla zachowania bezpieczeństwa informacji w procesach MDE.
   b. Mierniki dla zabezpieczeń określonych w pkt a.

XVIII. Polityka zarządzania strefami zabezpieczonymi

1. Dokument dedykowany wyłącznie procesom MDE.
2. Zamawiający posiada wydzielone strefy ograniczonego dostępu w budynku GUS, w których zlokalizowane są kluczowe urządzenia infrastruktury teleinformatycznej przeznaczone do przetwarzania informacji z MDE.
3. W szczególności polityka musi określać wymagania dot.:
   a. Określenie czynności / procesów MDE które powinny odbywać się w strefach zabezpieczonych oraz wyjątków od powyższego.
   b. Usytuowania urządzeń przetwarzających dane MDE w strefach zabezpieczonych.
   c. Określenia parametrów fizycznego bezpieczeństwa ww. urządzeń (ochrona fizyczna, fizyczne bezpieczeństwo urządzeń od zdarzeń nieprzewidzianych).
   d. Dostępu do stref zabezpieczonych.

XIX. Polityka relacji z dostawcami

1. Dokument dedykowany wyłącznie procesom MDE.
2. Celem wdrożenia polityki jest określenie zasad dostępu do informacji MDE przez strony trzecie.
3. W szczególności polityka musi określać wymagania dot.:
   a. Identyfikowania typów dostawców (usługodawcy IT, outsourcing, porozumienia o przekazywaniu danych).
   b. Procesu zarządzania relacjami z dostawcami.
   c. Minimalnych wymagań bezpieczeństwa dla danego rodzaju informacji.
   d. Zabezpieczeń wdrożonych w celu zapewnienia integralności informacji.
   e. Zapisów umownych zabezpieczających przed nieautoryzowaną zmianą lub utratą informacji przez dostawcę.

XX. Polityka kopi zapasowych

1. Dokument dedykowany wyłącznie procesom MDE.
2. Polityka musi być zgodna z polityką ciągłości działania.
3. W szczególności polityka musi określać wymagania dot.:
    a. Regularnego wykonywania i testowania kopii zapasowych danych MDE.
    b. Retencji i ochrony danych MDE.
    c. Sposobów szyfrowania kopii zapasowych.
    d. Warunków technicznych wykonywania kopii zapasowych.
    e. Zasad harmonogramizowania wykonywania kopii zapasowych.
    f. Zasad tworzenia spisu kopii zapasowych.
    g. Zasad odtwarzania z kopii zapasowych.
    h. Zasad przechowywania kopii zapasowych.

XXI. Polityka ciągłości działania

1. Dokument dedykowany wyłącznie procesom MDE.
2. Polityka musi być zgodna z polityką kopii zapasowych.
3. W szczególności polityka musi określać wymagania dot.:
    a. Ról i organizacji pracy w procesie odpowiedzi na zdarzenia zagrażające lub przerywające ciągłość działania.
    b. Określenia odpowiedzialności pracowników odpowiedzialnych za zarządzanie incydentem i utrzymanie bezpieczeństwa informacji.
    c. Wprowadzenia zabezpieczeń powiązanych z planem działań na wypadek utraty ciągłości działania.
    d. Zasad zmian w niniejszej polityce w powiązaniu z analizą ryzyka.
    e. Zasad dotyczących weryfikowania, przeglądu i oceny bezpieczeństwa informacji.
4. Polityka musi zawierać plan działań na wypadek utraty ciągłości działania, w którym zostaną uwzględnione standardowe odpowiedzi i działania naprawcze wobec zdarzeń zagrażających lub przerywających ciągłość działania.

XXII. Procedura eksploatacyjna MDE

1. Dokument dedykowany wyłącznie procesom MDE.
2. W szczególności procedura musi określać wymagania dot.:
    a. Dokumentowania procedur eksploatacyjnych MDE.
    b. Ról i odpowiedzialności w zakresie procedur eksploatacyjnych.
    c. Instalacji i konfiguracji oprogramowania, w tym wykonywania kopii zapasowych.
    d. Przetwarzania i postępowania z informacją.
    e. Instrukcji obsługi błędów lub wyjątków.
    f. Kontaktów umożliwiających uzyskanie wsparcie technicznego i eskalację.
    g. Procedur ponownego uruchamiania i odtwarzania systemu na wypadek awarii.
    h. Zarządzania śladem audytowym oraz systemowymi dziennikami zdarzeń.

i. Procesów monitorowania.

XXIII. Inwentaryzacja zasobów informacyjnych.

1. Zadaniem wykonawcy będzie zidentyfikowanie informacji i innych aktywów związanych z informacjami i środkami przetwarzania w procesach MDE oraz przygotowanie na tej podstawie spisu aktywów.
2. Do przeprowadzenia inwentaryzacji MDE Zamawiający udostępni informacje z wdrożonych systemów:
   a. CMDB w ramach systemu SerwisDesk – baza, w której znajdują się informacje o zasobach sprzętowych i oprogramowaniu.
   b. SCCM – system do zbierania on-line informacji o sprzęcie i oprogramowaniu oraz jego konfiguracji (osobny dla serwerów i stacji roboczych).
   c. UpTimeDC – system do inwentaryzacji sprzętu w serwerowniach.
3. Wymagania dot. spis aktywów:
   a. Do każdego ze zidentyfikowanych aktywów musi istnieć możliwość przypisania właściciela i identyfikacji informacji wg klasyfikacji ze schematu klasyfikacji informacji.
   b. Spis w zakresie rzeczowym będzie uwzględniał informacje o aktywach udostępnione przez Zamawiającego z ww. systemów. Wykonawca dokona oględzin istniejących aktywów w celu weryfikacji stanu faktycznego ze stanem przedstawionym przez Zamawiającego.
   c. Spis w rozdziale V będzie uwzględniał informacje określone w rozdziale V.
   d. Wykonawca po zapoznaniu się z CMDB wskaże repozytorium do przechowywania i utrzymywania spisu informacji i aktywów MDE. Jeżeli spis będzie utrzymywany poza CMDB, Wykonawca zaproponuje metodę utrzymywania spisu zgodną z normą ISO 27002.
   e. Wykonawca opracuje procedurę utrzymania spisu określającą podstawę wpisu informacji do spisu oraz zasady ich przetwarzania, składowania, przekazywania, usuwania i niszczenia.