Załącznik 1 - Deklaracja stosowania w Urzędzie Gminy i Miasta w Dobczycach

Wdrożony Zintegrowany System Zarządzania obejmuje swoim zakresem wszystkie komórki organizacyjne Urzędu

Dobczyce, dnia 15 listopada 2013 roku

Rozdział	Opis normy/wymaganie	Sposób realizacji
A.5 Polityka bezpieczeństwa		
A.5.1 Polityka bezpieczeństwa informacji		
A.5.1.1	Dokument polityki bezpieczeństwa informacji	Zdefiniowano „Politykę Bezpieczeństwa Informacji i Ochrony Danych Osobowych w Urzędzie Gminy i Miasta Dobczyce", określającą cele bezpieczeństwa informacji, podstawy funkcjonowania Systemu Bezpieczeństwa Informacji, a także wyrażającą zaangażowanie w jej realizowanie najwyższego kierownictwa Urzędu
A 5.1.2	Przegląd informacji polityki bezpieczeństwa	Przeglądy ZSZ odbywają się zgodnie z zasadamiw opisanymi w rozdziale 7 Księgi Zintegrowanego Systemu Zarządzania
A.6 Organizacja bezpieczeństwa informacji		
A.6.1 Wewnętrzna organizacja		
A.6.1 1	Zaangażowanie kierownictwa w bezpieczeństwo informacji	Najwyższe Kierownictwo Urzędu jest zaangażowane w zapewnienie bezpieczeństwa informacji i ochronę danych osobowych.
A.6 1.2	Koordynacja bezpieczeństwa informacji	Rolę koordynatora bezpieczeństwa informacji pełni Administrator Bezpieczeństwa Informacji wraz z Administratorem Sieci Informatycznej. Za operacyjne utrzymanie i doskonalenie ZSZ odpowiada Pełnomocnik ds. ZSZ
A.6.1.3	Przypisywanie obowiązków związanych z bezpieczeństwem informacji	W Księdze ZSZ oraz dokumentacji procesu PW.1 określono obowiązki i odpowiedzialności związane z bezpieczeństwem informacji dla wybranych stanowisk. Opracowano klasyfikację i przeprowadzono inwentaryzację aktywów informacyjnych. Każdy aktyw informacyjny ma przypisanych właścicieli aktywów.
A.6.1.4	Proces autoryzacji środków przetwarzania informacji	Wprowadzenie do funkcjonowania nowych systemów informatycznych następuje po ich przetestowaniu i weryfikacji zgodności z wymaganiami stawianymi przez przepisy prawne, dokumentację procesu PW.1 Zarządzanie bezpieczeństwem informacji, ochroną danych osobowych oraz informatyzacją Urzędu.
A 6.1.5	Umowy o poufności	Umowy zawierane ze stronami trzecimi (w tym pracownikami) zawierają klauzule zobowiązujace do zapewnienia ochrony danych i poufności.
A.6.1.6	Kontakty z organami władzy	Urząd utrzymuje kontakty z organami ścigania (Policją i organami egzekwującymi przestrzeganie przepisów prawa w dziedzinie bezpieczeństwa informacji: Agencją Bezpieczeństwa Wewnętrznego, Biurem Generalnego Inspektora Ochrony Danych Osobowych). Zgodnie z zawartymi umowami utrzymywana jest współpraca z dostawcami usług telekomunikacyjnych i informatycznych.
A.6.1.7	Kontakty z grupami zainteresowanymi zapewnieniem bezpieczeństwa	Urząd utrzymuje kontakty z instytucjami zaangażowanymi w ochronę bezpieczeństwa. Należą do nich: 1 Nadzór bankowy, 2 GIODO, 3 Specjalistyczna prasa i eksperci, 4 Firmy doradcze specjalizujące się w ochronie danych.
A.6.1.8	Niezależny przegląd bezpieczeństwa informacji	Prowadzone są systematyczne kontrole oraz audyty. Na podstawie odrębnie zawartych przez Urząd umów odbywają się niezależne audyty wynikające z ustawy o finansach publicznych oraz certyfikacji wdrożonego systemu bezpieczenstwa Informacji zgodnego z normą PN-EN ISO 27001.
A.6.2 Osoby trzecie.		
A 6.2.1	Określenie ryzyk związanych ze stronami zewnętrznymi	Obowiązują zasady przyjmowania osób trzecich w sposób zapewniajacy ochronę danych (podwyższone blaty, wydzielone miejsca dla Klientów). W zakresie ochrony fizycznej Urząd współpracuje z zewnętrzną firmą ochroniarską. Dostęp wszelkich podmiotów oraz osób trzecich jest kontrolowany.Budynek Urzędu zabezpieczony jest alarmem antywłamaniowym. Dostęp do pomieszczeń w systemie klucza szyfrowanego.
A6.2.2	Bezpieczeństwo podczas kontaktów z klientami	Urząd ma wydzielone strefy dla przyjmowania klientów. Klienci zawsze przebywają w pokojach z pracownikami Urzędu.
A 6.2.3	Bezpieczeństwo w umowach ze stroną trzecią	Wdrożono zasady w sprawie ochrony danych osobowych i ochrony tajemnicy przedsiębiorstwa w Urzędzie. Określono zasady umieszczania klauzul poufności oraz innych zasad związanych z bezpieczeństwem informacji w umowach zawieranych z podmiotami zewnętrznymi.
A.7 Zarządzanie aktywami		
A7.1 Odpowiedzialność za aktywa		

Rozdział	Opis normy/wymaganie	Sposób realizacji
A.7.1.1	Inwentaryzacja aktywów	Przeprowadzono inwentaryzację aktywów informacyjnych oraz na jej podstawie, inwentaryzację krytycznych zasobów teleinformatycznych (sprzętowych i programowych) Urzędu zgodnie z PZ.6.6. Nadzór nad ryzykiem. Wyznaczono właścicieli aktywów i krytycznych zasobów teleinformatycznych zidentyfikowanych w Urzędzie.
A.7.1.2	Własność aktywów	Wszystkie istotne aktywa i grupy aktywów mają przydzielonych właścicieli
A. 7.1.3	Akceptowalne użycie aktywów	System zarządzania bezpieczeństwem informacji określa zasady korzystania z grup aktywów i nadzoru nad nimi.
A 7.2 Klasyfikacja informacji		
A7.2.1	Wytyczne do klasyfikacji	W Księdze ZSZ oraz procesie PZ.6 Doskonalenie ZSZ i PW.1 Zarządzanie bezpieczeństwem informacji, ochroną danych osobowych i informatyzacją Urzędu opracowano szczegółowe wytyczne do klasyfikacji aktywów.
A7.2.2	Oznaczanie i postępowanie z informacjami.	Zasady oznaczania dokumentów Urzędu określone są w: - Instrukcji kancelaryjnej, - Przepisach związanych z ochroną infromacji niejawnych, - Księdze ZSZ.
A.8 Bezpieczeństwo osobowe.		
A.8.1 Przed zatrudnieniem		
A.8.1.1	Role i zakresy odpowiedzialności	Księga ZSZ oraz regulaminy i zasady systemu określają szczegółowe zakresy odpowiedzialności za informacje.
A.8.1.2	Postępowanie sprawdzające	Podczas naboru na wolne stanowiska urzędnicze weryfikowane są: tożsamość, wykształcenie i referencje kandydata. W przypadku stanowisk ważnych z punktu widzenia bezpieczeństwa referencje weryfikowane są telefonicznie.
A.8.1.3.	Zasady i warunki zatrudnienia	Kierownicy komórek organizacyjnych Urzędu odpowiadają za podpisanie przez podległych im pracownikow właściwych obowiązujących oświadczeń o zachowaniu poufności. Oświadczenia przechowywane są w teczkach akt personalnych pracowników. Kierownicy odpowiadają również za przygotowanie wniosku o dostęp do informacji i zasobów Urzędu zgodnie z zakresem obowiązków pracownika.
A.8.2 Podczas zatrudnienia.		
A.8.2.1	Odpowiedzialność kierownictwa	Kierownicy komórek organizacyjnych Urzędu odpowiadają za nadzór nad pracownikami, użytkownikami oraz stronami trzecimi w zakresie stosowania zasad wynikających z ZSZ.
A.8.2.2	Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji	Przeprowadzane są szkolenia dla kadry kierowniczej z zakresu ZSZ. Osoby, które uzyskują dostęp do danych osobowych i informacji chronionych przechodzą odpowiednie szkolenia.
A.8.2.3	Postępowanie dyscyplinarne	Wobec pracowników łamiących obowiązujące zasady i regulaminy ZSZ, a w szczególności bezpieczeństwa informacji oraz bezpieczeństwa teleinformatycznego, w Urzędzie stosuje się procedury postępowania dyscyplinującego zgodne z kodeksem pracy.
A.8.3 Zakończenie lub zmiana zatrudnienia		
A.8.3.1	Odpowiedzialność związana *z* zakończeniem zatrudnienia	Odpowiedzialności związane z zakończeniem zatrudnienia określają regulaminy i zasady określone w PZ.2 Zarządzanie personelem, a w szczególności: PZ.2.1 Regulamin pracy oraz PZ.2.9. Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji.
A.8.3.2	Zwrot aktywów	Odpowiedzialności związane z zakończeniem zatrudnienia określają PZ.2 Zarządzanie personelem, a w szczególności: PZ.2.1 Regulamin pracy oraz PZ.2.9. Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji.
A.8.3.3	Odebranie praw dostępu	Odpowiedzialności związane z zakończeniem zatrudnienia określają PZ.2 Zarzadzanie personelem, a w szczególności: PZ.2.1 Regulamin pracy oraz PZ.2.9. Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji, a także PW.1.2. Zasady zarządzania dostępem do informacji.
A.9 Bezpieczeństwo fizyczne i środowiskowe		
A.9. Obszary bezpieczne		
A.9.1.1	Fizyczna granica obszaru bezpiecznego	Na terenie Urzędu wyodrębnione są fizyczne strefy kontrolowanego dostępu do obiektów, a w ramach tych stref obszary bezpieczne o ograniczonym dostępie, w których odbywa się wytwarzanie, przetwarzanie, przechowywanie lub przesyłanie informacji krytycznych. Dostęp ten określa PW.1.1. Zasady dostępu do pomieszczeń, pracy w obszarach chronionych i zabezpieczenia kluczowego wyposażenia teleinformatycznego.
A.9.1.2	Fizyczne zabezpieczenie wejścia	Wszystkie fizyczne strefy kontrolowanego dostępu zabezpieczone są kluczem szyfrowym z kontrolowanym dostępem (system jednego klucza).

Rozdział	Opis normy/wymaganie	Sposób realizacji
A.9.1.3	Zabezpieczenia biur, pomieszczeń i urządzeń	Określa dokument PW.1.1. Zasady dostępu do pomieszczeń, pracy w obszarach chronionych i zabezpieczenia kluczowego wyposażenia teleinformatycznego.
A.9.1.4	Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi	Określa PW.1.1. Zasady dostępu do pomieszczeń, pracy w obszarach chronionych i zabezpieczenia kluczowego wyposażenia teleinformatycznego.
A.9.1.5	Praca w obszarach bezpiecznych	Określono zasady przebywania w strefie chronionej, jak również zasady przyjmowania osób trzecich w strefie chronionej. Określa dokument PW.1.1. Zasady dostępu do pomieszczeń, pracy w obszarach chronionych i zabezpieczenia kluczowego wyposażenia teleinformatycznego.
A.9.1.6	Obszary publicznie dostępne, dostaw i załadunku	Obszary publicznie dostępne zostały określone i wyznaczone.
A.9.2 Zabezpieczenie sprzętu		
A.9.2.1	Lokalizacja sprzętu i jego ochrona	Zasady rozmieszczania sprzętu i urządzeń teleinformatycznych określają: PW.1.1. Zasady dostępu do pomieszczeń, pracy w obszarach chronionych i zabezpieczenia kluczowego wyposażenia teleinformatycznego. PW.1.2. Zasady zarzadzania dostępem do informacji.
A.9.2.2	Systemu wposmagające	Wszystkie systemy krytyczne mają potrzymywanie zasilania.
A.9.2.3	Bezpieczeństwo okablowania	Okablowanie strukturalne i energetyczne zabezpieczone jest zgodnie z zasadami określonymi w PW.1.3. Zasady zarządzania siecią teleinformatyczną i kryptografią.
A.9.2.4	Utrzymanie sprzętu	Zasady utrzymania sprzętu określa dokument: PW.1.3. Zasady zarządzania siecią teleinformatyczną i kryptografią.
A.9.2.5	Bezpieczeństwo sprzętu poza siedzibą	Zasady bezpieczeństwa sprzętu poza siedzibą określa dokument PZ.2.9. Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji.
A.9.2.6	Bezpieczne zbywanie lub przekazanie do ponownego użycia sprzętu	Zasady bezpieczenego zbywania sprzętu określają dokumenty PW.4.1.1. Zasady gospodarowania środkami trwałymi i wyposażeniem urzędu, PW.5.1. Zasady gospodarowania odpadami w urzędzie i PW.1.3. Zasady zarządzania siecią teleinformatyczną i kryptografią.
A.9.2.7	Wynoszenie mienia	Sprzęt przenośny jest zabezpieczony zgodnie z zasadami: PZ.2.9. Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji oraz PW.1.1. Zasady dostępu do pomieszczeń, pracy w obszarach chronionych i zabezpieczenia kluczowego wyposażenia teleinformatycznego.
A.10 Zarządzanie komunikacją i stosowaniem.		
A.10.1 Procedury stosowania i zakresy odpowiedzialności		
A.10.1.1	Dokumentowanie procedur eksploatacyjnych	Określono w PW.1.7. Zasady zarządzania rozwojem informatycznym
A.10.1.2	Zarządzanie zmianami	Określono w PW.1.7. Zasady zarządzania rozwojem informatycznym
A.10.1.3	Rozdzielanie obowiązków	Zasadą jest, że funkcje ABI oraz ASI pełnią rożne osoby. Uwzględniono to w strukturze organizacyjnej i zakresach obowiązków
A.10.1.4	Oddzielanie urządzeń rozowjowych, testowych i eksplatacyjnych	Określono w PW.1.7. Zasady zarządzania rozwojem informatycznym
A.10.2 Zarządzanie dostawami wykonywanymi przez osoby trzecie		
A.10.2.1	Dostarczanie usług	Określono w PW.1.7. Zasady zarządzania rozwojem informatycznym oraz PZ.2.9. Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji.
A.10.2.2	Monitorowanie i przegląd usług świadczonych przez strony trzecie	Określono w PW.1.7. Zasady zarządzania rozwojem informatycznym oraz PZ.2.9. Zadania i obowiązki pracowników zwiazane z zapewnieniem bezpieczeństwa informacji.
A. 10.2.3	Zarządzanie zmianami w usługach świadczonych przez strony trzecie	Określono w PW.1.7. Zasady zarządzania rozwojem informatycznym oraz PZ.2.9. Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji.
A.10.3 Planowanie i akceptacja systemu		
A.10.3.1	Zarządzanie pojemnością	W przypadku krytycznych zasobów za planowanie pojemności odpowiada Właściciel aktywu.
A.10.3.2	Akceptacja systemu	Określa dokument PW.1.7 Zasady zarządzania rozwojem informatycznym
A.10.4 Ochrona przed kodem złośliwym i kodem mobilnym		
A.10.4.1	Zabezpieczenia przed kodem szkodliwym	Określają zasady zarządzania siecią teleinformatyczną i kryptografią (PW.1.3.)
A.10.4.2	Zabezpieczenia przed kodem mobilnym	Określają zasady zarządzania siecią teleinformatyczną i kryptografią (PW.1.3.)
A.10.5 Archiwizacja		

Rozdział	Opis normy/wymaganie	Sposób realizacji
A.10.5.1	Zapasowe kopie informacji	Określają zasady zarządzania kopiami zapasowymi i ciągłością działania (PW.1.5.)
A.10.6 Zarządzanie bezpieczeństwem sieciowym		
A.10.6.1	Zabezpieczenie sieci	Określa dokument PW.1.3. Zasady zarządzania siecią teleinformatyczną i kryptografią
A.10.6.2	Bezpieczeństwo usług sieciowych	Określa dokument PW.1.3. Zasady zarządzania siecią teleinformatyczną i kryptografią
A.10.7 Postępowanie z nośnikami		
A.10.7.1	Zarządzanie wymiennymi nośnikami komputerowymi	Określają Zasady zarządzania dostępem do informacji (PW.1.2.)
A.10.7.2	Niszczenie nośników	Określane przez Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacj(PZ.2.9.) oraz Zasady zarządzania dostępem do informacji (PW.1.2.)
A.10.7.3	Procedury postępowania z informacjami	Określają zasady zarządzania dostępem do informacji (PW.1.2.)
A.10.7.4	Bezpieczeństwo dokumentacji systemowej	Określają Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji (PZ.2.9.)
A.10.8 Wymiana informacji		
A.10.8.1	Polityka i procedury wymiany informacji	Określają Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacj(PZ.2.9.)
A.10.8.2	Umowy dotyczące wymiany informacji	Określają Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacj(PZ.2.9.)
A.10.8.3	Transportowanie nośników fizycznych	Określają Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacj(PZ.2.9.)
A.10.8.4	Wiadomości elektroniczne	Określają zasady korzystania z internetu i poczty elektornicznej (PW.1.4.)
A.10.8.5	Biznesowe systemy informacyjne	Określają zasady korzystania z internetu i poczty elektornicznej (PW.1.4.)
A.10.9 Elektroniczne usługi handlowe		
A.10.9.1	Handel elektroniczny	Urząd nie prowadzi handlu elektronicznego.
A.10.9.2	Transakcje online	Urząd nie prowadzi handlu elektronicznego.
A.10.9.3	Informacje dostępne publicznie	Zasady udostępniania informacji publicznych reguluje ustawa o dostępie do informacji publicznej. Za utrzymanie strony internetowej odpowiada Biuro Promocji.
A.10.10 Monitoring		
A.10.10.1	Dziennik Audytu	Pełnomocnik ds. ZSZ nadzoruje dzienniki audytu niezbędne do monitorowania systemów
A.10.10.2	Monitorowanie użycia systemu	Za monitorowanie użycia systemów teleinformatycznych odpowiada ASI zgodnie z Zasadami zarządzania siecią teleinformatyczną i kryptografią (PW.1.3.)
A.10.10.3	Ochrona informacji zawartych w dziennikach	Zasady ochrony dzienników określa Administrator Systemów Informatycznych
A.10.10.4	Dzienniki administratora i operatora	Zasady ochrony dzienników określa Administrator Systemów Informatycznych
A.10.10.5	Rejestrowanie błędów	Określa PW.1.6. Zasady zarządzania incydentami związanymi z bezpieczeństwem informacji.
A.10.10.6	Synchronizacja zegarów	Za synchronizację zegarów odpowiada ASI
A.11 Kontrola dostępu		
A.11.1 Wymaganie biznesowe związane z dostępem do systemu		
A.11.1.1	Polityka kontroli dostępu	Określają Zasady zarządzania dostępem do informacji (PW.1.2.)
A.11.2 Zarządzanie dostępem użytkowników		
A.11.2.1	Rejestracja użytkowników	Określają Zasady zarządzania dostępem do informacji (PW.1.2.)
A.11.2.2	Zarządzanie przywilejami	Określają Zasady zarządzania dostępem do informacji (PW.1.2.)
A.11.2.3	Zarządzanie hasłami użytkowników	Określają Zasady zarządzania dostępem do informacji (PW.1.2.)
A.11.2.4	Przegląd praw dostępu użytkowników	Określają Zasady zarządzania dostępem do informacji (PW.1.2.)
A.11.3 Zakres odpowiedzialności użytkowników		
A.11.3.1	Użycie haseł	Określają PZ.2.9. Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji oraz PW.1.2 Zasady zarządzania dostępem do informacji
A.11.3.2	Pozostawienie sprzętu użytkownika bez opieki	Określa PZ.2.9. Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji
A.11.3.3	Polityka czystego biurka i czystego ekranu	Określa PZ.2.9. Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji
A.11.4 Kontrola dostępu do sieci		
A.11.4.1	Polityka korzystania z usług sieciowych	Określa dokument PW.1.3. Zasady zarządzania siecią teleinformatyczną i kryptografią
A.11.4.2	Uwierzytelnienie użytkowników przy połączeniach zewnętrznych	Określa dokument PW.1.4. Zasady korzystania z internetu i poczty elektronicznej
A.11.4.3	Identyfikacja sprzętu w sieci	Określa dokument PW.1.3. Zasady zarządzania siecią teleinformatyczną i kryptografią
A.11.4.4	Ochrona zdalnych portów diagnostycznych	W sieci teleinformatycznej urzędu nie wykorzystuje się zdalnych portów diagnostycznych

Rozdział	Opis normy/wymaganie	Sposób realizacji
A.11.4.5	Rozdzielanie sieci	Określa dokument PW.1.3. Zasady zarządzania siecią teleinformatyczną i kryptografią
A.11.4.6.	Kontrola połączeń sieciowych	Określa dokument PW.1.3. Zasady zarządzania siecią teleinformatyczną i kryptografią
A.11.4.7	Kontrola dróg połączeń w sieciach	Określa dokument PW.1.3. Zasady zarządzania siecią teleinformatyczną i kryptografią
A.11.5 Kontrola dostępu do systemów operacyjnych		
A.11.5.1	Bezpieczne procedury rejestracji	Określa PW.1.2. Zasady zarządzania dostępem do informacji.
A.11.5.2	Identyfikacja i potwierdzenie tożsamości klienta.	Określa PW.1.2. Zasady zarządzania dostępem do informacji.
A.11.5.3	System zarządzania hasłami	Określa PW.1.2. Zasady zarządzania dostępem do informacji.
A.11.5.4	Użycie systemowych programów narzędziowych	Za nadzór nad programami narzędziowymi odpowiada Pełnomocnik ds. ZSZ oraz Administrator Systemów Informatycznych.
A.11.5.5	Upłynięcie czasu sesji	Określa PW.1.2. Zasady zarządzania dostępem do informacji.
A.11.5.6	Ograniczenie czasu trwania połączenia	Określa PW.1.2. Zasady zarządzania dostępem do informacji.
A.11.6 Kontrola dostępu do aplikacji i informacji.		
A.11.6.1	Ograniczenie dostępu do informacji	Określają: PW.1.1. Zasady dostępu do pomieszczeń, pracy w obszarach chronionych i zabezpieczenia kluczowego sprzętu teleinformatycznego PW.1.2. Zasady zarządzania dostępem do informacji.
A.11.6.2	Izolowanie systemów wrażliwych	Określają: PW.1.1. Zasady dostępu do pomieszczeń, pracy w obszarach chronionych i zabezpieczenia kluczowego sprzętu teleinformatycznego PW.1.2. Zasady zarządzania dostępem do informacji.
A.11.7 Komputery przenośne i praca na odległość		
A.11.7.1	Przetwarzanie i komunikacja mobilna	Określa dokument: Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji (PZ.2.9.)
A.11.7.2	Praca na odległość	W systemie teleinformatycznym urzędu nie prowadzi się pracy na odległość.
A.12 Uzyskiwanie, rozwój i utrzymanie systemów informacyjnych.		
A.12.1 Wymagania bezpieczeństwa względem systemów informacyjnych.		
A.12.1.1	Analiza i opis wymagań bezpieczeństwa	Określają Zasady zarządzania rozwojem informatycznym (PW.1.7.)
A.12.2 Bezpieczeństwo systemów aplikacji		
A.12.2.1	Potwierdzenie ważności danych wejściowych	Za spójność, integralność i dostępność oraz walidacje systemów odpowiadają Administrator Systemów Informatycznych, Właściciel Aktywu Informacyjnego, Właściciel Aplikacji i Pełnomocnik ds. ZSZ.
A.12.2.2	Kontrola przetwarzania wewnętrznego	Za spójność, integralność i dostępność oraz walidacje systemów odpowiadają Administrator Systemów Informatycznych, Właściciel Aktywu Informacyjnego, Właściciel Aplikacji i Pełnomocnik ds. ZSZ.
A.12.2.3	Integralność wiadomości	Za spójność, integralność i dostępność systemów odpowiadają Administrator Systemów Informatycznych, Właściciel Aktywu Informacyjnego, Właściciel Aplikacji i Pełnomocnik ds. ZSZ.
A.12.2.4	Potwierdzenie poprawności danych wyjściowych	Za spójność, integralność i dostępność oraz walidacje systemów odpowiadają Administrator Systemów Informatycznych, Właściciel Aktywu Informacyjnego, Właściciel Aplikacji i Pełnomocnik ds. ZSZ oraz użytkownicy.
A.12.3 Zabezpieczenia kryptograficzne.		
A.12.3.1	Polityka korzystania z zabezpieczeń kryptograficznych	Określają zasady zarządzania siecią teleinformatyczną i kryptografią (PW.1.3.).
A.12.3.2	Zarządzanie kluczami	Określają zasady zarządzania siecią teleinformatyczną i kryptografią (PW.1.3.).
A.12.4 Bezpieczeństwo plików systemowych		
A.12.4.1	Zabezpieczenie eksploatowanego oprogramowania	Określają zasady zarządzania siecią teleinformatyczną i kryptografią (PW.1.3.).
A.12.4.2	Ochrona systemowych danych testowych	Określają zasady zarządzania siecią teleinformatyczną i kryptografią (PW.1.3.).
A.12.4.3	Kontrola dostępu do kodów źródłowych programów	Określają zasady zarządzania siecią teleinformatyczną i kryptografią (PW.1.3.).
A.12.5 Bezpieczeństwo w procesach rozwojowych i obsługi informatycznej		
A.12.5.1	Procedury kontroli zmian	Określają Zasady zarządzania rozwojem informatycznym (PW.1.7.)
A.12.5.2	Techniczny przeląd aplikacji po zmianach w systemie operacyjnym	Określają Zasady zarządzania rozwojem informatycznym (PW.1.7.)
A.12.5.3	Ograniczenia dotyczące zmian w pakietach oprogramowania	Określają Zasady zarządzania rozwojem informatycznym (PW.1.7.)
A.12.5.4	Przeciek informacji	Określają Zasady zarządzania incydentami związanymi z bezpieczeństwem informacji (PW.1.6.)
A.12.5.5	Prace rozwojowe nad oprogramowaniem powierzone firmie zewnętrznej.	Określają Zasady zarządzania rozwojem informatycznym (PW.1.7.)
A.12.6 Zarządzanie podatnościami technicznymi		
A.12.6.1	Nadzór nad podatnościami technicznymi	Za nadzór nad podatnościami technicznymi odpowiada Pełnomocnik ds. ZSZ
A.13 Zarządzanie wydarzeniami związanymi z bezpieczeństwem informacji		

Rozdział	Opis normy/wymaganie	Sposób realizacji
A.13.1 Raportowanie wydarzeń związanych z bezpieczeństwem informacji i słabych punktów		
A.13.1.1	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji	Określają zasady zarządzania incydentami związanymi z bezpieczeństwem informacji (PW.1.6.) oraz Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji (PZ.2.9.).
A. 13.1.2	Zgłaszanie słabości systemu bezpieczeństwem	Określają zasady zarządzania incydentami związanymi z bezpieczeństwem informacji (PW.1.6.) oraz Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji (PZ.2.9.).
A.13.2 Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami		
A.13.2.1	Zakres odpowiedzialności i procedury	Określają zasady zarządzania incydentami związanymi z bezpieczeństwem informacji (PW.1.6.).
A.13.2.2	Nauka z incydentów związanych z bezpieczeństwem informacji	Określają zasady zarządzania incydentami związanymi z bezpieczeństwem informacji (PW.1.6.).
A.13.2.3	Gromadzenie dowodów	Określają zasady zarządzania incydentami związanymi z bezpieczeństwem informacji (PW.1.6.).
A.14 Zarządzanie ciągłością działania.		
A.14.1 Aspekty zarządzania ciągłością działania		
A.14.1.1	Wprowadzenie bezpieczeństwa informacji do procesu zarządzania ciągłością działania	Określają zasady zarządzania kopiami zapasowymi i ciągłością działania PW.1.5.
A.14.1.2	Ciągłość działania i szacowanie ryzyka	Określają zasady zarządzania kopiami zapasowymi i ciągłością działania PW.1.5.
A.14.1.3	Opracowanie i wdrażenie planów ciągłości działania uwzględniających bezpieczeństwo informacji	Określają zasady zarządzania kopiami zapasowymi i ciągłością działania PW.1.5.
A.14.1.4	Struktura planowania ciągłości działania	Określają zasady zarządzania kopiami zapasowymi i ciągłością działania PW.1.5.
A.14.1.5	Testowanie, utrzymywanie i ponowna ocena planów ciągłości działania	Określają zasady zarządzania kopiami zapasowymi i ciągłością działania PW.1.5.
A.15 Zgodność.		
A.15.1 Zgodność z przepisami prawa		
A.15.1.1	Określenie odpowiednich przepisów prawa	Określa PW.6.1. Zasady nadzoru nad dokumentami, przepisami prawa i zapisami.
A.15.1.2	Prawo do własności intelektualnej (IPR)	Za nadzór nad przestrzeganiem prawa własności intelektualnej odpowiadają Sekretarz oraz Kierownicy komórek organizacyjnych
A.15.1.3	Zabezpieczenie zapisów organizacji	Dokumentacja, procedury i zapisy są nadzorowane zgodnie z: - Instrukcją kancelaryjną, - Zasadami ochrony informacji niejawnych, - Zasadami ochrony danych osobowych, - Zasadami nadzoru nad dokumentami, przepisamia prawa i zapisami (PZ.6.1.). Zgodnie z klasyfikacją informacji stosuje się odpowiedni sposób zabezpieczenia poszczególnych grup informacji chronionych.
A.15.1.4	Ochrona danych osobowych i prywatność informacji dotyczących osób fizycznych	Ochrona danych osobowych odbywa się w oparciu o ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002 r. Nr 101, poz. 926 – tekst jednolity z późniejszymi zmianami) i wydanych do niej rozporządzeń wykonawczych. Zasady ochrony danych osobowych określono w - Księdze ZSZ, - Dokumentacji Procesu PW.1.1. Zarządzanie bezpieczeństwem informacji, ochrona danych osobowych i informatyzacja Urzędu.
A.15.1.5	Zapobieganie nadużywaniu urządzeń przetwarzających informacje	W celu zapobiegania nadużywaniu krytycznych zasobów teleinformatycznych służących do przetwarzania informacji, w Urzędzie stosowane są m.in. następujące zabezpieczenia: a) wdrożono proces monitorowania działań w sieci i systemach teleinformatycznych, w tym zintegrowany system wykrywania oprogramowania szkodliwego, intruzów i przeciwdziałania włamaniom z sieci publicznej i od wewnątrz sieci korporacyjnej, b) są utrzymywane i przeglądane na bieżąco oraz archiwizowane rejestry działań w sieci i systemach teleinformatycznych, c) zdefiniowano i wdrożono właściwe procedury autoryzacji, d) wdrożono zasady dostępu osób i podmiotów trzecich do zasobów informacyjnych, w tym teleinformatycznych Urzędu, e) wdrożono zabezpieczenia fizyczne dostępu do zasobów, zasady wynoszenia mienia poza teren Urzędu i użycia komputerów przenośnych, f) funkcjonuje system reagowania na incydenty bezpieczeństwa oraz zarządzania ciągłością działania.
A.15.1.6	Regulacje dotyczące zabezpieczeń kryptograficznych	Zasady dotyczące zabezpieczeń kryptograficznych określono w PW.1.3. Zasady zarządzania siecią teleinformatyczną i kryptografią.
A.15.2 Zgodność z politykami i standardami bezpieczeństwa i zgodność techniczna.		

Rozdział	Opis normy/wymaganie	Sposób realizacji
A.15.2.1	Zgodność z politykami i standardami bezpieczeństwa	Regularnie dokonuje się przeglądów ZSZ, w tym Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych. Zasady badania zgodności opisano kompleksowo w Księdze ZSZ w rodziale 7 - Prowadzenie narad i przeglądów ZSZ.
A.15.2.2	Sprawdzanie zgodności technicznej	Pełnomocnik ds. ZSZ i ASI – każdy w swoim obszarze działania, odpowiedzialni są za nadzorowanie technicznego stanu systemów informatycznych.
A.15.3 Rozważania dotyczące audytu systemu		
A.15.3.1	Zabezpieczenie audytu systemu	Za zabezpieczenie audytu ZSZ odpowiada Pełnomocnik ds. ZSZ oraz ASI
A.15.3.2	Ochrona narzędzi audytu systemów informacyjnych	Narzędzia służące do przeprowadzania audytów systemów i sieci teleinformatycznych Urzędu muszą: a) pochodzić z zaufanych źródeł dystrybucji, b) być sprawdzane przed każdym użyciem pod kątem zawartości kodów szkodliwych i integralności, c) być przechowywane w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym, bądź modyfikację ich kodu.