BURMISTRZ
Gminy i Miasta
DOBCZYCE

ZARZĄDZENIE NR 116/2015
BURMISTRZA GMINY I MIASTA DOBCZYCE

z dnia 21 lipca 2015 r.

W sprawie: zmiany Księgi Zintegrowanego Systemu Zarządzania oraz Polityki Zintegrowanego Systemu Zarzadzania

Na podstawie art. 31 i art. 33 ust. 1 i ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (tj. Dz.U. z 2013 poz. 594 z późn. zm.) **zarządzam, co następuje:**

§ 1. W zarządzeniu nr 11/2015 z dnia 12 lutego 2015 roku wprowadza się następujące zmiany:

1. Wprowadza się nowe wydanie Księgi Zintegrowanego Systemu Zarządzania w brzmieniu określonym w załączniku nr 1 do niniejszego zarządzenia, które zastępuje załącznik nr 1 do zarządzania nr 11/2015 z dnia 12 lutego 2015 r.
2. Wprowadza się nowe wydanie Polityki Zintegrowanego Systemu Zarządzania, która stanowi załącznik nr 2 do niniejszego zarządzenia, zastępując załącznik nr 2 do zarządzania nr 11/2015 z dnia 12 lutego 2015 r.

§ 2. 1. Zobowiązuję Pełnomocnika ds. Zintegrowanego Systemu Zarządzania do udostępnienia pracownikom Księgi ZSZ oraz Polityki ZSZ przez zamieszczenie ich w portalu intranetowym Qsystem.

2. Zobowiązuję wszystkich pracowników Urzędu Gminy i Miasta Dobczyce do zapoznania się z treścią Polityki ZSZ, Księgi ZSZ i do przestrzegania zapisów zawartych w tych dokumentach.

§ 3. Zarządzenie wchodzi w życie z dniem podjęcia.

BURMISTRZ
Gminy i Miasta Dobczyce
Paweł Machnicki

21.07.2015

Załącznik nr 2
do Zarządzenia nr 116/2015
Burmistrza Gminy i Miasta Dobczyce
z dnia 21.07.2015 roku

URZĄD GMINY I MIASTA DOBCZYCE

Polityka
Zintegrowanego Systemu Zarządzania

Misją Urzędu Gminy i Miasta Dobczyce jest rzetelna i etyczna służba publiczna na rzecz Społeczności Lokalnej i Naszych Klientów oraz zrównoważonego rozwoju Gminy Dobczyce.

Urząd Gminy i Miasta Dobczyce przykłada najwyższą wagę do zapewnienia bezpieczeństwa osób i mienia oraz informacji zawartych w systemach informatycznych Urzędu i poza nimi, ponieważ mają one fundamentalne znaczenie dla realizacji misji i celów Urzędu.

Osiąganie celów wynikających z misji odbywa się przez ciągłe doskonalenie skuteczności Zintegrowanego Systemu Zarządzania spełniającego wymagania norm PN-EN ISO 9001:2009, PN-N 18001:2004, PN-EN ISO 27001:2014 oraz wymagania Systemu Przeciwdziałania Zagrożeniom Korupcyjnym.

Dobczyce, 21.07.2015 roku

BURMISTRZ
Gminy i Miasta Dobczyce

Załącznik nr 1
do Zarządzenia nr 116/2015
Burmistrza Gminy i Miasta Dobczyce
z dnia 21.07.2015 roku

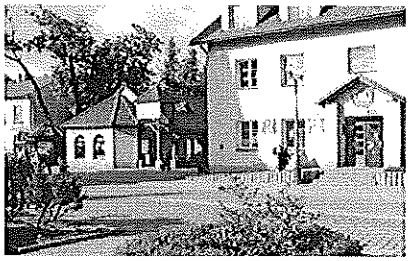
Księga Zintegrowanego Systemu Zarządzania Urzędu Gminy i Miasta Dobczyce

BURMISTRZ
Gminy i Miasta Dobczyce
Paweł Majnicki

Imię i nazwisko		Podpis	Data
Opracowała:	Pełnomocnik Malgorzata Góralik – Piętka		21.07.2015

Spis treści

1. PREZENTACJA URZĘDU GMINY I MIASTA DOBCZYCE



Siedziba Urzędu położona jest w centrum miasta i składa się z trzech połączonych ze sobą budynków. Przeprowadzone remonty dostosowały wnętrze Urzędu do potrzeb Klienta. Trzykondygnacyjny budynek Urzędu nie posiada windy, z tego powodu powstało Biura Obsługi Klienta oraz dostosowano system obsługi Klientów do potrzeb osób niepełnosprawnych i starszych.

Struktura organizacyjna Urzędu dzieli go na Referaty, samodzielne stanowiska pracy oraz doraźnie powoływane zespoły niezbędne do realizacji określonego zadania. Referaty mieszczą się na trzech kondygnacjach.

Biuro Obsługi Klienta (BOK)zlokalizowane jest na parterze zaraz przy wejściu do Urzędu, co znacznie ułatwia sprawną obsługę Klientów. Zadaniem BOK jest udostępnianie wszelkich informacji dotyczących pracy Urzędu oraz sposobu załatwiania spraw w Urzędzie. To tam Klienci uzyskują informację, pobierają formularze i wnioski oraz kierowani są do pracowników merytorycznie odpowiedzialnych za załatwienie konkretnych spraw. Klienci mający problemy z wchodzeniem po schodach oraz osoby niepełnosprawne obsługiwane są w BOK przez schodzący do nich pracowników merytorycznych.

Oficjalne serwisy internetowe umożliwiają klientom pozyskanie informacji o usługach realizowanych przez Urząd, pobranie niezbędnych druków oraz załatwienie spraw przez Internet. W Urzędzie można potwierdzić profil zaufany ePUAP.

Urząd jako jednostka administracji publicznej ma pełną świadomość swojej służebnej roli wobec społeczeństwa i każdego klienta. Specyfika Urzędu powoduje, że świadczone na rzecz klientów usługi są często uwarunkowane przepisami prawnymi i innymi regulacjami. Kierownictwo Urzędu systematycznie wdraża działania doskonalące na rzecz swoich klientów.

W celu sprawniejszej obsługi klientów opracowano Katalog Usług Urzędu zawierający Karty Usług, w których opisane zostały usługi publiczne świadczone na rzecz indywidualnych interesantów wraz z załączonymi do nich wnioskami. Katalog jest dostępny w postaci elektronicznej, dla zainteresowanych klientów wnioski udostępnione są w BOK i na stanowiskach pracy pracowników merytorycznych. Urząd udostępnia również usługi na platformie e-PUAP, z możliwością załatwienia sprawy przez internet.

Podstawy prawne funkcjonowania

- ustawa z dnia 8 marca 1990 r. o samorządzie gminnym,
- ustawa z dnia 21 listopada 2008 r. o pracownikach samorządowych,
- Statut Gminy i Miasta Dobczyce,
- Statut Urzędu Gminy i Miasta Dobczyce,
- Regulamin Organizacyjny Urzędu Gminy i Miasta Dobczyce.

Pełny wykaz aktów prawnych regulujących funkcjonowanie Urzędu znajduje się w systemie informacji prawnej udostępnionym pracownikom Urzędu.

Pracownicy Urzędu w wykonywaniu swoich obowiązków i zadań działają na podstawie prawa i obowiązani są do jego ścisłego przestrzegania.

Polityka ZSZ i Polityka Bezpieczeństwa Informacji i Ochrony Danych Osobowych obowiązuje wszystkich pracowników, dostawców, podwykonawców, audytorów i konsultantów, którzy tworzą, dystrybuują, mają dostęp lub zarządzają informacjami za pomocą systemów informatycznych Urzędu oraz sieci i systemów telekomunikacyjnych, którymi te systemy są połączone.

2. ZAKRES ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA

Struktura Urzędu i realizowane przez Urząd zadania administracyjne zostały objęte Zintegrowanym Systemem Zarządzania zgodnym z normami PN-EN ISO 9001:2009, PN-N 18001:2004 i PN-EN ISO 27001:2014 oraz wymaganiami Systemu Przeciwdziałania Zagrożeniom Korupcyjnym wydanie trzecie, kwiecień 2014.

Zintegrowanym Systemem Zarządzania objęta jest cała struktura organizacyjna Urzędu oraz wszystkie procesy przedstawione na mapie procesów ZSZ.

Projektowanie w Urzędzie dotyczy głównie czynności skierowanych na planowanie długofalowego rozwoju Gminy i Miasta Dobczyce oraz opracowywanie corocznego budżetu Gminy. Projektowanie i rozwój

realizowane są w ramach procesów PZ.1 Zarządzanie Strategią, PZ.3 Zarządzanie finansami oraz PZ.5 Zarządzanie procesami inwestycyjnymi. Dodatkowo aplikacja Qsystem pozwala na projektowanie działań doskonalących. Ze względu na charakter prowadzonych spraw oraz realizowanych procesów Urząd nie prowadzi typowych prac projektowych (w dosłownym rozumieniu). Z tego względu podjęto decyzję o wyłączeniu punktu 7.3 normy PN-EN ISO 9001:2009, który dotyczy projektowania i rozwoju.

Zakres ZSZ w odniesieniu do System Zarządzania Bezpieczeństwem Informacji spełnia wszystkie wymagania normy PN-EN ISO 27001:2014 wymienione w Deklaracji Stosowania będącej załącznikiem nr 1 do Księgi ZSZ.

3. PLANOWANIE ROZWOJU ZSZ ORAZ USTANOWIENIE MISJI I POLITYKI ZSZ

W celu systematycznego rozwoju Gminy i Miasta Dobczyce oraz Urzędu Burmistrz i Kierownictwo Urzędu wraz ze stronami zainteresowanymi opracowali:

1. Strategię Rozwoju Gminy i Miasta Dobczyce określającą priorytety i cele polityki rozwojowej prowadzonej na terenie Gminy. Strategia to jeden z najważniejszych dokumentów, opracowanych w wyniku porozumienia różnych środowisk i jest dowodem silnego poczucia odpowiedzialności społeczności lokalnej za przyszłość Dobczyc. Jest skutecznym narzędziem w procesie rozwoju.
2. Politykę Zintegrowanego Systemu Zarządzania, zawierającą misję. Corocznie cele Polityki ZSZ przekładane są na Plan poprawy ZSZ, działania doskonalące i postępowanie z ryzykami.
3. Politykę Bezpieczeństwa Informacji i Ochrony Danych Osobowych.
4. Wieloletnia Prognozę Finansową.
5. Strategię Rozwiązywania Problemów Społecznych.
6. Program współpracy z organizacjami pozarządowymi.

Dokumenty te podlegają okresowym przeglądom i nowelizacjom.

Polityka ZSZ oraz Polityka Bezpieczeństwa Informacji i Ochrony Danych Osobowych obowiązują wszystkich pracowników, dostawców, podwykonawców, audytorów i konsultantów, którzy tworzą, dystrybuują, mają dostęp lub zarządzają informacjami za pomocą systemów informatycznych Urzędu oraz sieci i systemów telekomunikacyjnych, którymi te systemy są połączone.

Polityka ZSZ oraz Polityka Bezpieczeństwa Informacji i Ochrony Danych Osobowych podlegają przeglądowi w przypadku poważnego naruszenia systemów zabezpieczeń, pojawienia się nowych i istotnych rodzajów ryzyka, zmian regulacji prawnych, którym podlega Urząd lub znaczących zmian infrastruktury technicznej. Ponadto ZSZ przeglądany jest nie rzadziej niż raz w roku, tak by zapewnić jego efektywność i adekwatność niezależnie od zachodzących zmian.

Kierownictwo Urzędu było inicjatorem wdrożenia w Urzędzie Zintegrowanego Systemu Zarządzania zgodnego z normami PN-EN ISO 9001:2009, PN-N 18001:2004 i PN-EN ISO 27001:2014 oraz wymaganiami Systemu Przeciwdziałania Zagrożeniom Korupcyjnym wydanie trzecie kwiecień 2014. Sformułowało też misję Urzędu i Politykę ZSZ oraz Politykę Bezpieczeństwa Informacji i Ochrony Danych Osobowych oraz odpowiedzialne jest za zapewnienie zasobów niezbędnych do ich wdrożenia.

Dokumentacja opracowywana była przy udziale poszczególnych przedstawicieli Kierownictwa Urzędu oraz pracowników merytorycznych. System jest na bieżąco przeglądany zgodnie z przyjętymi zasadami, a dyspozycje oraz działania i projekty doskonalące, działania korygujące i zapobiegawcze oraz decyzje dotyczące postępowania z ryzykiem wynikające z przeglądów są przez Kierownictwo Urzędu przekazywane pracownikom do realizacji.

Role i odpowiedzialność poszczególnych pracowników Urzędu – uczestników procesów ZSZ określone zostały w dokumentacji ZSZ.

4. PODEJŚCIE PROCESOWE DO ZARZĄDZANIA ORAZ DOKUMENTACJA ZSZ

Podstawą skutecznego stosowania ZSZ jest wdrożenie tzw. podejścia procesowego do zarządzania Urzędem, które składa się z następujących etapów:

1. identyfikacja procesów zarządczych i połączenie ich w grupy procesów,
2. wybór procesów objętych zakresem ZSZ,
3. wdrożenie, monitorowanie i ciągłe doskonalenie wybranych procesów.

Wdrożenie ZSZ zostało poprzedzone identyfikacją głównych grup procesów oraz wyborem procesów objętych zakresem ZSZ. Dokumentacja ZSZ, w postaci pełnej listy procesów, dokumentów ZSZ oraz listy właścicieli dokumentów jest dostępna dla wszystkich komórek organizacyjnych Urzędu w programie Qsystem.

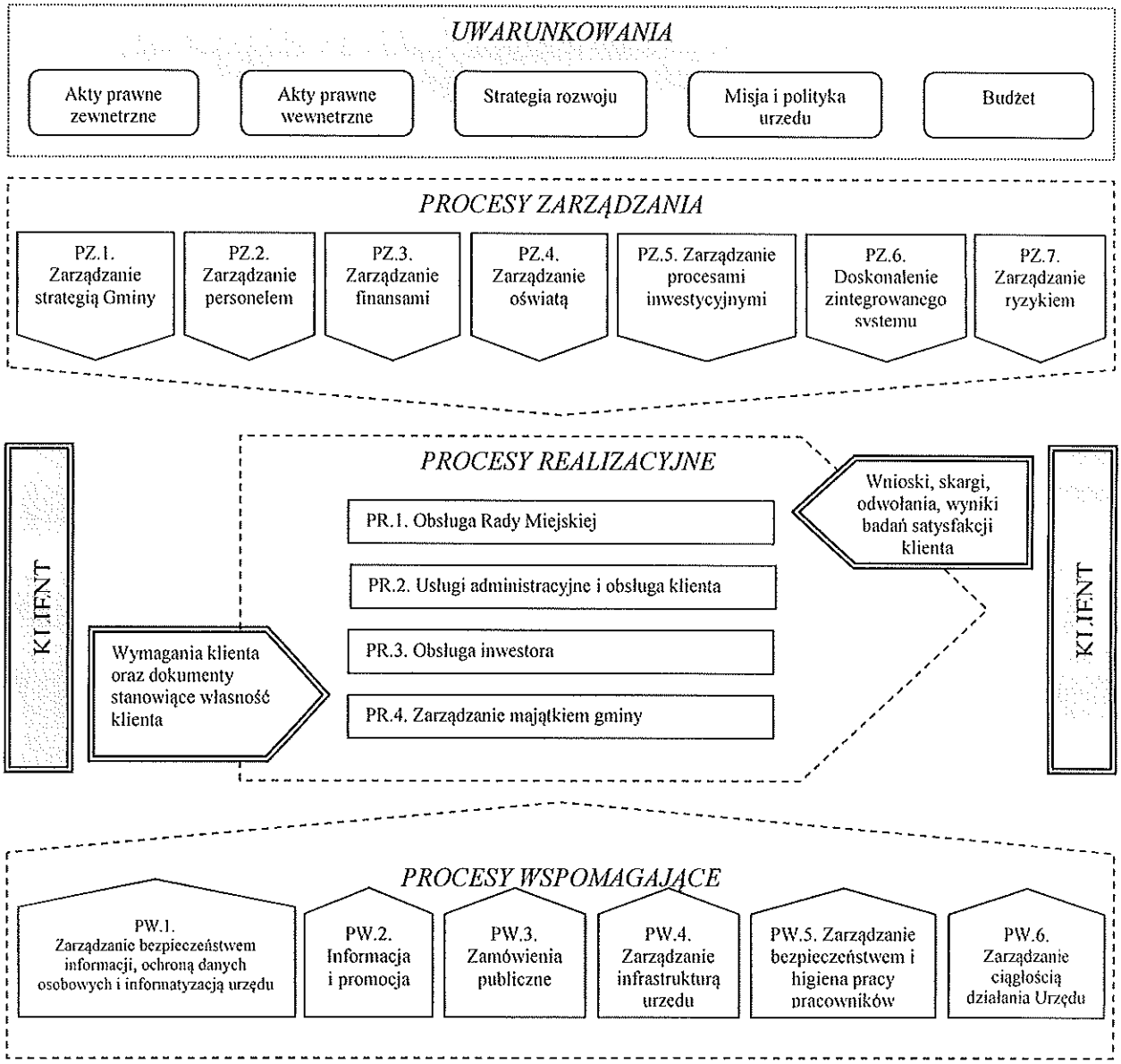
Dokumenty ZSZ są nadzorowane i na bieżąco aktualizowane przez właścicieli dokumentów i procesów zgodnie z PZ.6.1. Zasady nadzoru nad dokumentami, przepisami prawa i zapisami. Dokumenty podlegają archiwizacji na zasadach określonych w Instrukcji kancelaryjnej oraz w Qsystem w postaci elektronicznej.

Przyjęto następujące poziomy procesów:

1. **procesy zarządzania (PZ)** – przy pomocy których kadra zarządzająca wytycza kierunki rozwoju, zabezpiecza zasoby oraz sprawdza funkcjonowanie wdrożonych działań,
2. **procesy realizacyjne (PR)** – w ramach których Urząd dostarcza usługi dla klienta,
3. **procesy wspomagające (PW)** – zapewniające odpowiednie zasoby do sprawnej realizacji działań.

Ponadto Urząd zarządza aktywnie procesami, identyfikuje je, ustala cele i miary oraz określa zakres odpowiedzialności dla każdego właściciela procesu. Zmiany w procesach dokonywane są za zgodą właściciela procesu. Procesy realizacji usług administracyjnych, w ramach których Urząd realizuje swoje zadania realizowane są na podstawie Regulaminu organizacyjnego oraz przepisów prawa wewnętrznego i zewnętrznego.

Procesy ZSZ przedstawiono na mapie procesów:



Ustanowione zostały następujące kluczowe procesy ZSZ:

1. **PZ.1. Zarządzanie strategią** - Celem procesu jest ustalenie zasad realizacji strategii oraz dokonywania oceny stanu realizacji strategii rozwoju Gminy i Miasta Dobczyce, przyjętej uchwałą Rady Miejskiej, w tym zgodności z tą strategią dokumentów planistycznych, polityk i programów przygotowywanych i realizowanych przez Urząd Gminy i Miasta Dobczyce.
2. **PZ.2. Zarządzanie personelem** - Celem procesu jest zapewnienie sprawnego i kompetentnego wykonywania zadań w Urzędzie Gminy i Miasta Dobczyce zgodnie z przepisami prawa i potrzebami klientów, motywowanie pracowników do stałego podnoszenia własnych kwalifikacji i poprawy wykonywanej pracy poprzez szeroki zakres szkoleń oraz pogłębianie wśród pracowników odpowiedzialności za jakość wykonywanej przez nich pracy.
3. **PZ.3. Zarządzanie finansami** - Celem procesu jest ustalenie jednolitego sposobu postępowania, który powinien być przestrzegany przy opracowywaniu, uchwalaniu, realizowaniu i monitorowaniu budżetu gminy w oparciu o budżet zadaniowy. Zakres procesu obejmuje planowanie pracy, systematyczny przegląd, weryfikację, walidację i monitorowanie zmian w planie pracy oraz ocenę wykonania budżetu Gminy i Miasta Dobczyce. Plan pracy opracowywany jest dla zapewnienia planowania zadań oraz odpowiedniego przeznaczania środków finansowych na konkretne zadania.
4. **PZ.4. Zarządzanie oświatą** - Celem procesu jest skuteczna realizacja ustawowych zadań w zakresie oświaty, w taki sposób aby najefektywniej wykorzystać posiadane zasoby i osiągnąć jak najlepsze wyniki nauczania.
5. **PZ.5. Zarządzanie procesami inwestycyjnymi** - Celem procesu jest prowadzenie inwestycji zmierzających do podniesienia jakości życia mieszkańców oraz wpływających na rozwój gminy, zgodnie z obowiązującymi w tym zakresie przepisami prawa, uwzględniając możliwości finansowe gminy.
6. **PZ.6. Doskonalenie zintegrowanego systemu zarządzania** - Celem procesu jest zapewnienie aktualności, dostępności, przeglądu oraz weryfikacji dokumentacji objętej systemem, nadzorowanie niezgodności, prowadzenie przeglądu systemu i wdrażanie działań doskonalących w taki sposób, aby zapewnić bezpieczeństwo informacji oraz świadczenie przez pracowników Urzędu usług najwyższej jakości.
7. **PZ.6 Zarządzanie ryzykiem** - Celem procesu jest prowadzenie analizy ryzyka oraz opracowanie i wdrożenie planu doskonalenia i postępowania z ryzykami.
8. **PR.1. Obsługa Rady Miejskiej** - Celem procesu jest zapewnienie sprawnej i kompleksowej obsługi Rady Miejskiej, Komisji Rady oraz Radnych uwzględniającej wymagania prawne oraz wnioski i uwagi Radnych w taki sposób, aby Radni obsługiwani byli sprawnie, terminowo oraz zgodnie z obowiązującymi przepisami.
9. **PR.2. Usługi administracyjne i obsługa klienta** - Celem procesu jest zapewnienie klientom rzetelnej i zgodnej z obowiązującymi przepisami prawa usługi administracyjnej, osiąganej dzięki doskonaleniu struktur organizacyjnych i technicznych Urzędu oraz pogłębianie wśród pracowników odpowiedzialności za jakość wykonywanej przez nich pracy i kształtowanie przekonania o konieczności realizacji usług wysokiej jakości.
10. **PR.3. Obsługa Inwestora** - Celem procesu jest sprawna i kompleksowa obsługa inwestorów zainteresowanych zlokalizowaniem zakładu na terenie Gminy Dobczyce oraz stworzenie optymalnych warunków dla rozwoju przedsiębiorczości, a także wspieranie działań przedsiębiorców tworzących nowe miejsca pracy.
11. **PR.4. Zarządzanie majątkiem gminy**
    - Celem procesu PR.4.1. Usługi wodociągowe i kanalizacyjne jest zapewnienie odpowiedniej obsługi administracyjnej klientom zwracającym się o świadczenie dla nich usług wodociągowych i kanalizacyjnych oraz realizację nowych przyłączy, administracyjne nadzorowanie usuwania awarii w taki sposób, aby zminimalizować przerwy w dostawach wody oraz zapewnić najwyższą jakość usług świadczonych klientom. W ramach tego procesu prowadzony jest również nadzór nad usługą niezgodną związany z jakością dostarczanej klientom wody. Proces nie obejmuje postępowania pracowników zatrudnionych w brygadach konserwatorsko – remontowych oraz oczyszczalni ścieków.
    - Celem procesu PR.4.2. Zarządzanie drogami jest opisanie administracyjnego postępowania zapewniającego utrzymanie dróg gminnych i wewnętrznych należących do Gminy Dobczyce, mostów i przepustów w należytym stanie technicznym i przejezdności.
    - Celem procesu PR.4.3. Zarządzanie budynkami jest zdefiniowanie administracyjnych działań związanych z zarządzaniem budynkami i obiektami oraz utrzymaniem obiektów komunalnych we właściwym stanie technicznym i osiąganie pożytków z wynajmu lokali użytkowych.
    - Celem procesu PR.4.4. Zarządzanie gruntami jest opisanie administracyjnych postępowań dotyczących zarządzania gruntami, czyli gospodarowanie gminnym zasobem nieruchomości niezabudowanych w taki sposób, aby zapewnić potrzeby społeczności lokalnej, jak i dbałość o stan mienia komunalnego.

12. **PW.1 Zarządzanie bezpieczeństwem informacji, ochroną danych osobowych i informatyzacją Urzędu** - Celem procesu jest prowadzenie działań zapewniających odpowiedni poziom bezpieczeństwa gromadzonych w Urzędzie informacji, realizacja ustawowych wymagań w zakresie ochrony danych osobowych i ochrony baz danych oraz Rozporządzenia w sprawie Krajowych Ram Interoperacyjności, dostarczanie pracownikom Urzędu zasobów w postaci środków technicznych i wiedzy merytorycznej, aby zapewnić bezpieczeństwo danych oraz ciągłość usług realizowanych dla Klientów Urzędu.
13. **PW.2 Informacja i promocja** - Celem procesu jest zapewnienie sprawnej komunikacji między pracownikami, klientami, mediami oraz zagranicznymi partnerami samorządowymi, mającej na celu informowanie zainteresowanych o planach i zadaniach Urzędu oraz jako mechanizm integrujący, budujący wzajemne zaufanie, wzmacniający spójność organizacyjną, wspierający budowanie wizerunku Urzędu, a także usprawniający proces wprowadzania innowacji czy transferu wiedzy. Szybka i pełna informacja jest konieczna do podejmowania adekwatnych decyzji przez pracowników każdego szczebla.
14. **PW.3 Zamówienia publiczne** - Celem procesu jest zgodne z prawem dokonanie wyboru wykonawcy na zasadach określonych w regulaminie zakupów w taki sposób, aby zapewnić przejrzystość wyboru.
15. **PW.4 Zarządzanie infrastrukturą Urzędu** - Celem procesu jest należyte gospodarowanie środkami trwałymi i wyposażeniem Urzędu
16. **PW.5 Zarządzanie bezpieczeństwem i higieną pracy pracowników** - Celem procesu jest rozwijanie świadomości pracowników o bezpieczeństwie i higienie pracy w celu kształtowania zachowań zmniejszających ryzyko wystąpienia zagrożenia dla ludzi.
17. **PW.6 Zarządzanie ciągłością działania Urzędu** - Proces określa szczegółowe zasady utrzymania ciągłości działania Urzędu, a w szczególności przeciwdziałanie przerwom w działalności Urzędu oraz ochrona systemów teleinformatycznych Urzędu przed rozległymi awariami lub katastrofami oraz wznowienie działalności w określonym w zasadach czasie.

5. ZASADY OPISU PROCESÓW ORAZ NADZÓR NAD DOKUMENTAMI I ZAPISAMI ZSZ

5.1. Zasady opisu procesów

Aktualne wersje Księgi ZSZ oraz wszystkich procesów i dokumentów ZSZ są opublikowane i dostępne dla wszystkich pracowników w Qsystem. Za nadzór nad aktualnością dokumentów ZSZ odpowiadają właściciele procesów i dokumentów. Każdy proces ma swojego właściciela, którego obowiązki opisano w punkcie 6.2.

Właściciele procesów są odpowiedzialni za przygotowanie opisów procesów objętych zakresem ZSZ. W tym celu opracowują Karty Procesów lub zasady i regulaminy obowiązujące w procesie. Karta procesu nie jest wymagana w sytuacji opracowania zasad i regulaminów opisujących sposób postępowania w procesie.

Właściciele zasad i regulaminów odpowiadają za przygotowanie opisu procesów w postaci zasad lub regulaminów, w szczególności obejmujących:

1) Przedmiot i zakres procesu,
2) Definicje i obowiązujące skróty,
3) Cel,
4) Odpowiedzialność i kompetencje,
5) Tryb postępowania (opis procesu w formie tekstu, tabeli lub schematu, jeżeli jest to niezbędne),
6) Listę aplikacji informatycznych wspierających realizację procesu,
7) Listę dokumentów powiązanych,
8) Listę formularzy stosowanych w procesie.

Egzemplarze w wersji papierowej regulaminów i zasad znajdują się w sekretariacie Urzędu pod zarządzeniem Burmistrza wprowadzającym dany regulamin lub zasadę oraz u osoby je opracowującej. W sekretariacie Urzędu gromadzone są dokumenty podlegające archiwizacji, a właściciele zasad i regulaminów mają dokumenty do bieżącego wykorzystania. Pozostałe osoby, dla których znajomość zasad i regulaminów jest istotna w realizacji procesów korzystają z wersji elektronicznych zamieszczonych w Qsystem.

Procesy wysokiego ryzyka, w których zdefiniowano zagrożenia wystąpienia działań korupcyjnych wyznaczone są w tabeli analizy ryzyka przygotowywanych zgodnie z PZ.7. Zarządzanie ryzykiem.

5.2. Nadzór nad dokumentami i zapisami

Właściwe funkcjonowanie Urzędu uzależnione jest w głównej mierze od odpowiedniego dostępu do dokumentów i zapisów oraz od właściwego ich nadzorowania. Kierownictwo Urzędu chce mieć pewność, że przyjęty ZSZ gwarantuje, iż we wszystkich miejscach, gdzie jest to konieczne znajdują się aktualne dokumenty. Zasady nadzoru nad dokumentami i zapisami określono w:

- Instrukcji Kancelaryjnej,
- Zasadach nadzoru nad dokumentami, przepisami prawa i zapisami PZ.6.1.,
- Polityce bezpieczeństwa informacji i ochrony danych osobowych,
- Instrukcji obiegu dokumentów finansowo-księgowych.

Zasady nadzoru nad dokumentami, przepisami prawa i zapisami określają sposób opracowywania i nadzoru nad całością dokumentacji zarówno ZSZ, jak i aktów prawnych wykorzystywanych przez pracowników Urzędu. Wszystkie dokumenty ZSZ i dane są po ich przyjęciu lub powstaniu, przeglądane, zatwierdzane i ewidencjonowane, a pracownicy zgodnie z ich obowiązkami, mają stały dostęp do odpowiednich informacji źródłowych.

Dokument i zapis - W ZSZ wykorzystywane są następujące rodzaje dokumentów:

- dostarczające spójnych informacji – zarówno wewnątrz, jak i na zewnątrz o ZSZ (Księga ZSZ),
- ustalające wymagania; takie dokumenty nazywa się przepisami prawnymi, specyfikacjami, zamówieniami lub umowami,
- dostarczające informacji o tym, jak jednakowo wykonywać działania i procesy; takie dokumenty mogą obejmować karty procesów, zasady, regulaminy, instrukcje pracy i rysunki,
- dostarczające obiektywnego dowodu o wykonanych działaniach lub osiągniętych wynikach; takie dokumenty nazywa się zapisami (dokumentacja wytwarzana przez Urząd związana z obsługą klientów i realizowanymi procesami przechowywana w systemie tradycyjnym lub elektronicznym).

6. PROWADZENIE NARAD I PRZEGLĄDÓW ZSZ

Jednym z najważniejszych zadań Kierownictwa Urzędu jest zapewnienie komunikacji wewnętrznej oraz regularne przeprowadzanie systematycznej oceny przydatności, adekwatności, skuteczności i efektywności zasad zarządzania Urzędem, w szczególności w odniesieniu do Polityki ZSZ, celów dotyczących poprawy ZSZ, działań związanych poprawą bezpieczeństwa i higieny pracy oraz zapewnieniem bezpieczeństwa danych i ochrony danych osobowych. Ważną kwestią komunikowaną pracownikom Urzędu jest budowanie wizerunku Urzędu w oparciu o eliminowanie źródeł powstawiania potencjalnych zagrożeń korupcyjnych oraz pełnienie służebnej roli przez Urząd.

W Urzędzie prowadzone są narady kierowników referatów z Kierownictwem Urzędu oraz narady pracownicze.

W Urzędzie wyróżniamy trzy rodzaje przeglądów:

- Roczny przegląd zarządzania,
- Przegląd procesów,
- Narady Kierownictwa Urzędu.

6.1. Roczny przegląd zarządzania

Przeprowadzany jest minimum raz do roku. Celem przeglądu jest zapewnienie stałej przydatności i skuteczności ZSZ w osiąganiu celów oraz weryfikacja i aktualizacja Planu Poprawy ZSZ. Zasady prowadzenia przez Kierownictwo Urzędu przeglądów opisane są w PZ.6.2. Zasady prowadzenia przeglądu zintegrowanego systemu.

Przegląd dokonywany jest na podstawie następujących danych wejściowych:

- dokonanie oceny stopnia realizacji zadań określonych w Planie Poprawy ZSZ oraz Polityce ZSZ i Polityce bezpieczeństwa informacji i ochrony danych osobowych,
- dokonanie oceny możliwości dalszego doskonalenia ZSZ.

Przeglądy zarządzania są wykonywane na podstawie informacji dotyczących:

- wyników audytów jakości,
- stanu realizacji działań i projektów doskonalących,
- informacji zwrotnych od stron zainteresowanych (analizy skarg, wniosków, ankiet, badań satysfakcji),
- informacji związanych z podejmowaniem działań antykorupcyjnych na terenie kraju,
- funkcjonowania procesów i analizy wskaźników procesów,
- realizacji ustaleń podjętych w trakcie poprzednich przeglądów,
- wyników badań benchmarkingowych,
- zdarzenia lub incydentu mającego istotny wpływ na bezpieczeństwo.

Efektem przeglądów zarządzania są decyzje i ustalenie działań związanych z:

- wprowadzeniem zmian służących doskonaleniu skuteczności ZSZ, łącznie z Polityką ZSZ i celami ZSZ;
- opracowaniem Planu poprawy ZSZ,
- uruchomieniem działań i projektów doskonalących i ewentualnie benchmarkingowych,
- uwzględnienie w planie budżetu pozycji niezbędnych dla poprawnego funkcjonowania i rozwoju ZSZ,
- przydzieleniem niezbędnych zasobów.

Z przeglądu opracowywany jest protokół, który zatwierdza Burmistrz. Protokół umieszczany jest przez Pełnomocnika w Qsystem i/lub w intraDok.

6.2. Przeglądy procesów

Przeglądy procesów dokonywane są przez właścicieli procesów w miarę potrzeb. Z przeglądów mogą być sporządzanie zapisy w formie notatki, które umieszczane są w Qsystem, w module Rejestr notatek z przeglądów. Zapisy z ustaleń i przeglądów na poziomie referatu lub procesu dokonywane są przez kierującego referatem lub właściciela procesu, a ustalenia odnotowywane są w kalendarzach Kierowników Referatów oraz pracowników – jako notatki do wykorzystania wewnętrznego.

Podczas przeglądów należy omawiać i odnotowywać w notatce z przeglądu, w zależności od rodzaju przeglądanego procesu, następujące zagadnienia:

1. Ocena stopnia realizacji ustaleń z poprzedniego przeglądu.
2. Ocena stopnia realizacji celów procesów i zadań oraz weryfikacja tych celów, w tym:
   - analiza zebranych wskaźników procesów w Karcie Wyników Organizacji w programie Qsystem,
   - analiza stopnia realizacji celów, trendów i ewentualnych porównań,
   - analiza czy zbierane wskaźniki są odpowiednie dla danego procesu.
3. Ocena propozycji działań i projektów doskonalących, korygujących i zapobiegawczych zgłoszonych w Urzędzie i zakwalifikowanie tematów do opracowania szczegółów działań i ich zarejestrowanie w Qsystem.
4. Przebieg działań i projektów doskonalących, korygujących i zapobiegawczych oraz stopień ich realizacji.
5. Analiza wyników audytów przeprowadzonych w komórce organizacyjnej i stopnia realizacji działań poaudytowych.
6. Analiza informacji na temat skarg i odwołań wnoszonych przez klientów oraz pozyskiwanych od pracowników mających bezpośredni kontakt z klientem.
7. Ocena niezgodności, zdarzeń lub incydentów mających wpływ na bezpieczeństwo danych zidentyfikowanych w referacie lub procesie i określenie kierunków działań niezbędnych do ich eliminacji.
8. Analiza wyników badań satysfakcji klientów i pracowników.
9. Weryfikacja aktualności dokumentów związanych z procesem i działem.

Przeglądy procesów prowadzone są również przez zbieranie i analizowanie wskaźników w oparciu o Kartę Wyników Organizacji. Przeglądy procesów mogą powodować zainicjowanie działań doskonalących związanych z doskonaleniem procesów lub zapobieganiem wystąpieniu negatywnych trendów wskaźników oraz zdarzeń operacyjnych.

7. ZARZĄDZANIE PERSONELEM

W ramach ZSZ szczególną uwagą objęto:

1. określenie niezbędnych kompetencji oraz kwalifikacji pracowników w zależności od zajmowanego stanowiska - kwestie te są regulowane rozporządzeniem Rady Ministrów w sprawie zasad wynagradzania i wymagań kwalifikacyjnych pracowników samorządowych zatrudnionych w urzędach gmin, starostwach powiatowych i urzędach marszałkowskich oraz Regulaminem wynagradzania pracowników Urzędu,
2. zatrudnianie pracowników - regulowane przez PZ.2.5. Regulamin zatrudniania pracowników,
3. nagradzanie, karanie i dyscyplinę pracy – regulowane przez PZ.2.1. Regulamin pracy Urzędu,
4. kwestie wynagradzania pracowników – regulowane przez PZ.2.3. Regulamin wynagradzania pracowników Urzędu,
5. szkolenie pracowników – PZ.2.4. Zasady podnoszenia kwalifikacji,
6. kwestie oceny regulowane przez PZ.2.7. Regulamin oceny okresowej. Oceny pracowników dokonują bezpośredni przełożeni. Głównym celem oceny jest zgromadzenie danych niezbędnych do racjonalnego zarządzania personelem w Urzędzie, którego elementami są między innymi:
   - efektywniejsze wykorzystanie potencjału ludzkiego,
   - właściwe motywowanie pracowników,
   - realizowanie kształcenia i szkolenia pracowników.
7. zarządzanie bezpieczeństwem informacji i danymi osobowymi zgodnie z polityką bezpieczeństwa informacji i ochrony danych osobowych.

Za określenie wymagań dotyczących kwalifikacji i kompetencji pracowników danej komórki organizacyjnej odpowiadają Kierownicy.

Wszyscy pracownicy Urzędu zatrudnieni są zgodnie z wymogami taryfikatora kwalifikacyjnego obowiązującego na danym stanowisku pracy oraz posiadają kompetencje stosownie do wykształcenia, umiejętności i posiadanego doświadczenia zawodowego. Zapisy dotyczące zarządzania personelem przechowywane są w Referacie Organizacyjnym.

8. REAGOWANIE NA WYPADKI PRZY PRACY, SYTUACJE POTENCJALNIE WYPADKOWE ORAZ POWAŻNE AWARIE

Wdrożenie PW.5.3. Zasady reagowania na wypadki przy pracy, sytuacje potencjalnie wypadkowe i poważne awarie świadczy o przygotowaniu Urzędu na możliwość wystąpienia wypadku przy pracy, zdarzenia potencjalnie wypadkowego oraz takiej sytuacji nadzwyczajnej, która mogłaby wpłynąć na niekontrolowany rozwój wydarzeń prowadzący do powstania poważnego zagrożenia dla zdrowia ludzkiego lub środowiska.

Urząd na bieżąco identyfikuje potencjalne sytuacje awaryjne, rejestruje wypadki przy pracy, zdarzenia potencjalnie wypadkowe oraz prowadzi działania zapobiegające ich powstawaniu, aby osiągnąć stan całkowitej gotowości reagowania i łagodzenia ewentualnych skutków, które mogą mieć miejsce w związku z zaistniałym zdarzeniem.

9. ORGANIZOWANIE PRAC I DZIAŁAŃ ZWIĄZANYCH ZE ZNACZĄCYMI ZAGROŻENIAMI

Znaczące zagrożenia, rozumiane jako zagrożenia mogące spowodować poważne i nieodwracalne uszkodzenia zdrowia lub śmierć, występujące w szczególności podczas wykonywania przez pracowników prac szczególnie niebezpiecznych lub w sytuacjach poważnych awarii, nadzorowane są przez ich bezpośrednich przełożonych.

Nadzór nad bezpieczeństwem i higieną pracy pracowników Urzędu sprawuje Specjalista ds. BHP. Ze względu na specyfikę i charakter prowadzonych spraw oraz realizowanych procesów Urząd nie prowadzi prac związanych ze znaczącymi zagrożeniami, a prace te mogą wiązać się jedynie ze zwiększonym zagrożeniem.

Pracownik, który wykonuje prace o podwyższonym ryzyku zobowiązany jest do postępowania zgodnie z następującymi zasadami:

1. Po przybyciu do określonego miejsca jest zobowiązany zgłosić się do osoby zarządzającej (o ile charakter wizyty na to pozwala),
2. Z osobą zarządzającą uzgadnia szczegóły dotyczące przebiegu wizyty,
3. Zapoznaje się we własnym zakresie lub zwraca się do osoby zarządzającej o przekazanie informacji na temat istniejących możliwych zagrożeń w danej jednostce,

4. Stosuje środki ochrony indywidualnej, które są przeznaczone dla pracowników przebywających na określonych stanowiskach,
5. Po terenie jednostki, w której przebywa poruszać się może tylko i wyłącznie z przewodnikiem,
6. Przewodnik oprowadzający po obiektach ma być osobą prowadzącą, natomiast pracownik Urzędu ma iść za przewodnikiem lub co najwyżej na równi z przewodnikiem, natomiast nigdy nie może iść jako pierwszy – z przodu,
7. Zachowuje szczególną ostrożność w czasie całego przebiegu wizyty,
8. W sytuacji, gdyby stał się przyczyną jakiegoś niekorzystnego zdarzenia związanego z bezpieczeństwem i higieną pracy jest zobowiązany niezwłocznie poinformować o zaistniałym fakcie przewodnika.

10. OCHRONA DANYCH, IDENTYFIKACJA AKTYWÓW I ZASOBÓW ORAZ ZARZĄDZANIE RYZYKIEM

W celu zapewnienia jednolitego podejścia do identyfikacji aktywów i analizy ryzyka informacji związanych z działalnością Urzędu opracowano zasady PZ.7. Zarządzanie ryzykiem.

Klasyfikacja oraz analiza zasobów, w tym ryzyk związanych z zasobami obrywa się w oparciu o Zasady zarządzania ryzykiem w Urzędzie PZ.7.1. Właściciele zasobów klasyfikują i poddają analizie ryzyka wszystko to, co ma wartość dla Urzędu i ma wpływ na osiąganie założonych celów i realizację zadań Urzędu. Klasyfikacja zasobu determinuje sposób posługiwania się nim i priorytet jego ochrony. Zasoby chroni się w stopniu proporcjonalnym do znaczenia dla Urzędu oraz zgodnie z obowiązującym prawem. W Urzędzie obowiązuje odmienna klasyfikacja zasobów ze względu na ich charakter: niematerialny (wiedza, doświadczenie, dostępność i świadomość pracowników; dane i informacje niezależnie od ich formy i nośnika) lub materialny (sprzęt i środki służące do przetwarzania informacji, ale także budynki lub ich wydzielone strefy, oprogramowanie, dokumentacja). Zasoby ludzkie Urzędu nie podlegają klasyfikacji. Życie i zdrowie osób jest dobrem najwyższym i ich ochrona w sytuacji zagrożenia jest ważniejsza niż ochrona jakichkolwiek innych zasobów Urzędu.

Klasyfikacja zasobów jest przeprowadzana przez Właścicieli zasobów i właścicieli zasobów teleinformatycznych w porozumieniu z innymi użytkownikami tych zasobów, Pełnomocnikiem Burmistrza ds. Ochrony Informacji Niejawnych oraz zgodnie z wymaganiami prawnymi.

10.1. Klasyfikacja danych i informacji

Informacje ze względu na wartość dla Urzędu są dzielone na następujące kategorie:

1. **informacje publiczne**, które są dostępne bez ograniczeń zarówno pracownikom Urzędu jak i osobom zewnętrznym.
2. **informacje chronione**, których ujawnienie może narazić Urząd na znaczące zagrożenia. Dostęp do danych chronionych jest nadawany imiennie na podstawie zakresu obowiązków wynikającego z zajmowanego stanowiska, oraz z upoważnień. Obejmują one:

a) **dane osobowe** chronione zgodnie z ustawą o ochronie danych osobowych, w tym dane wrażliwe podlegające ochronie na podstawie przepisów szczególnych,

b) **inne dokumenty i informacje,** podlagające ochronie na podstawie przepisów prawnych, lub które Burmistrz i Pełnomocnik ds. ZSZ uznają za szczególnie istotne dla funkcjonowania Urzędu.

3. **informacje niejawne**, chronione zgodnie z ustawą o ochronie informacji niejawnych.

10.2. Klasyfikacja pozostałych zasobów

W Urzędzie obowiązują dwa rodzaje klasyfikacji pozostałych zasobów nie będących informacjami: ze względu na wykorzystywanie do przetwarzania informacji niejawnych i ze względu na wartość oraz znaczenie dla funkcjonowania Urzędu.

Zasoby materialne wykorzystywane do przetwarzania informacji niejawnych są klasyfikowane zgodnie z ustaleniami Ustawy o ochronie informacji niejawnych.

Zasoby materialne nie wykorzystywane do przetwarzania informacji niejawnych są dzielone ze względu na wartość i znaczenie następująco:

- zasoby **materialne zwykłe**, które są łatwo odtwarzalne lub zastępowalne, i od których funkcjonowania nie zależy bezpośrednio funkcjonowanie Urzędu,
- zasoby **materialne wartościowe**, które są drogie lub trudno zastępowalne, ale od których nie zależy bezpośrednio funkcjonowanie Urzędu,

- zasoby **materialne krytyczne**, niezbędne do funkcjonowania Urzędu.

Na potrzeby planów ciągłości funkcjonowania Urzędu zasoby materialne mogą być klasyfikowane według dodatkowych, bardziej szczegółowych zasad.

11. DOSKONALENIE ORAZ MONITOROWANIE I POMIARY PROCESÓW, ZADAŃ I USŁUG

11.1. Analiza i monitorowanie procesów, zadań i usług

Analiza i monitorowanie wyników realizacji zadań i procesów w Urzędzie odbywa się przez:

- systematyczne zbieranie i analizę kluczowych wskaźników procesów, zadań i usług w Karcie Wyników Organizacji,
- przeprowadzane raz w roku badania satysfakcji klientów – obszar ten reguluje PR.2.2. Zasady pomiaru zadowolenia klienta,
- samoocenę stanu kontroli zarządczej,
- analizę zgłoszeń klientów Urzędu w zakresie: skarg, odwołań, zażaleń, wniosków i złej jakości wody pitnej,
- audyty jakości opisane w PZ.6.3. Audyty jakości,
- prowadzenie systematycznych przeglądów procesów i ZSZ zgodnie z PZ.6.2. Zasady prowadzenia przeglądu Zintegrowanego Systemu Zarządzania,
- sprawdzeń przeprowadzanych w trybie ustawy o ochronie danych osobowych.

Wszystkie dokumenty, działania i projekty doskonalące, wynikające z ZSZ oraz notatki, wyniki auditów, wskaźniki zadań i procesów są umieszczane w Qsystem lub w intraDok – zgodnie z decyzją Pełnomocnika.

11.2. Działania doskonalące w tym korygujące i zapobiegawcze oraz postępowanie z ryzykiem

W ZSZ określono zasady identyfikacji działań i projektów doskonalących oraz nadzór nad nimi. Opis postępowania w niniejszym zakresie zamieszczono w PZ.6.4. Zasady nadzorowania działań i projektów doskonalących.

Działania i projekty doskonalące mogą być zainicjowane w wyniku:

1. Zgłoszenia pomysłu pracownika,
2. Wyników auditu,
3. Przeglądu ZSZ,
4. Decyzji Kierownictwa Urzędu,
5. Badania satysfakcji klientów,
6. Samooceny stanu kontroli zarządczej,
7. Skarg, wniosków, zażaleń i odwołań klientów,
8. Wyników analizy porównawczej – benchmarkingu,
9. Analizy wyników kontroli zewnętrznych i wewnętrznych,
10. Analizy ryzyka.

Działania i projekty doskonalące (usprawnienia) są to działania, które może zaproponować każdy pracownik, w celu poprawy efektywności funkcjonowania Urzędu i obsługi klienta. Działania są krótkie, natomiast projekty wymagają zaangażowania większej ilości zasobów i czasu. Projekty podlegają planowaniu i nadzorowi zgodnemu z wymaganiami normy dotyczącymi projektowania i rozwoju oraz PDCA (pętli Deminga).

Działania korygujące to działania podejmowane w celu wyeliminowania przyczyn wykrytej niezgodności, podejmowane po zgłoszeniu niezgodności w Qsystem. Działania zapobiegawcze to działania podejmowane w celu wyeliminowania przyczyn potencjalnej niezgodności lub innej potencjalnej sytuacji niepożądanej. Działania zapobiegawcze wdrażane są po zgłoszeniu niezgodności w Qsystem. Zasadą jest, że każde działanie i projekt doskonalący, działanie korygujące lub zapobiegawcze ma swojego właściciela odpowiedzialnego za realizację i oceniane jest pod względem skuteczności wdrożenia.

Nadzór nad incydentami i awariami obywa się zgodnie z PW.1.3. Zasady zarządzania incydentami związanymi z bezpieczeństwem informacji.

11.3. Analiza ryzyka oraz opracowywania i wdrażania planu doskonalenia i postępowania z ryzykami

Analiza ryzyka dokonywana jest w oparciu o PZ.7.1. Zasady zarządzania ryzykiem w Urzędzie. Opisują one sposób prowadzenia analizy ryzyka oraz opracowanie i wdrożenie działań związanych z minimalizacją ryzyka lub doskonaleniem procesów. Zasady analizy ryzyka obejmują wszystkie czynności związane z identyfikacją procesów, celów i aktywów informacyjnych i materialnych poprzez oszacowanie ryzyk i opracowanie planu doskonalenia i postępowania z ryzykami oraz wdrożenia i oceny jego skuteczności.

11.4. Zbieranie kluczowych wskaźników Systemu Zarządzania – Karta Wyników Organizacji

Wskaźniki dotyczące procesów i zadań gromadzone są w Qsystem w module Karta Wyników Organizacji (KWO), zgodnie z *Instrukcją Qsystem KWO* Właściciele procesów lub zadań odpowiedzialni są za zbieranie i analizę wskaźników procesów i zadań w ramach bieżących przeglądów. Wskaźniki wprowadzane są przez osoby posiadające odpowiednie upoważnienie do edycji KWO. Za przeprowadzenie analizy wskaźników oraz za podjęcie działań doskonalących, korygujących lub zapobiegawczych po analizie odpowiadają osoby wprowadzające wskaźniki. W module KWO Qsystem wskazane są osoby odpowiedzialne za gromadzenie poszczególnych wskaźników. Zbiorcza analiza wskaźników dokonywana jest na przeglądzie ZSZ.

11.5. Prowadzenie analizy porównawczej - benchmarkingu

Decyzję o potrzebie podjęcia badań benchmarkingowych podejmuje Sekretarz lub Burmistrz. Urząd korzysta z dobrych praktyk innych urzędów poprzez analizę baz dobrych praktyk zamieszczonych na różnych stronach internetowych oraz spotkań grupy benchmarkingowej, wymianę doświadczeń i współpracę w organizacjach ponadregionalnych.

Działania i projekty doskonalące powstałe w wyniku benchmarkingu umieszczane są w Qsystem w celu nadzorowania ich realizacji.

12. OPIS SPEŁNIENIA POZOSTAŁYCH WYMAGAŃ

12.1. Identyfikacja i identyfikowalność

Urząd stosuje ustalony system identyfikacji wszystkich wyrobów zgodnie z JRWA. Każda sprawa posiada indywidualny numer – sygnaturę akt, która w połączeniu z systemem oznaczeń referatów pozwala na jednoznaczną identyfikację osób przygotowujących dokumenty dla Klientów.

Obieg dokumentów w Urzędzie jest zorganizowany zgodnie z Instrukcją Kancelaryjną. Sposób identyfikacji i identyfikowalności dokumentów określają obowiązujące w tym zakresie zewnętrzne i wewnętrzne akty prawne:

- Regulamin Organizacyjny Urzędu Gminy i Miasta Dobczyce, w którym przedstawiony jest zakres działania każdej komórki organizacyjnej Urzędu oraz symbol literowy każdej z nich, co umożliwia identyfikację autora sporządzonego dokumentu;
- Instrukcja Kancelaryjna dla organów gmin i związków międzygminnych, która określa zasady i tryb wykonywania czynności kancelaryjnych w Urzędzie, w celu zapewnienia jednolitego sposobu tworzenia, ewidencjonowania i przechowywania dokumentów oraz ochrony przed ich uszkodzeniem, zniszczeniem lub utratą, w tym zobowiązuje pracowników do parafowania sporządzanych przez nich dokumentów przedkładanych do podpisu Burmistrzowi lub osobie przez niego upoważnionej;
- jednolity rzeczowy wykaz akt (JRWA) stanowiący załącznik do Instrukcji Kancelaryjnej.

Akta spraw ostatecznie załatwionych są przekazywane do archiwum Urzędu i przechowywane przez okres ustalony w JRWA. Następnie, w zależności od ich wartości historycznej i praktycznej, są albo przekazywane do Archiwum Państwowego albo za jego zgodą zostają zniszczone.

12.2. Ochrona danych osobowych

Szczególną ochroną Urząd obejmuje dane osobowe klientów. Własność klienta inna niż dane osobowe podlega nadzorowi na podstawie przepisów prawa powszechnie obowiązującego. Własnością klienta są różnego rodzaju dokumenty składane w Urzędzie, w tym także dane osobowe zawarte w tych dokumentach. Urząd posiada zbiory danych osobowych zarejestrowane w GIODO oraz zbiory nierejestrowane (zgodnie z przepisami ustawy

o ochronie danych osobowych). W Urzędzie powołany został Administrator Bezpieczeństwa Informacji, którego zadania określa ustawa o ochronie danych osobowych i rozporządzenia wykonawcze do ustawy.

Dane osobowe chronione są zgodnie z zasadami określonymi w Polityce bezpieczeństwa informacji i ochrony danych osobowych oraz zasadach określonych w procesie PW.1 Zarządzanie bezpieczeństwem informacji, ochroną danych osobowych i informatyzacją urzędu. Dane osobowe zawarte w dokumentach, zbiorach i na nośnikach elektronicznych są wykorzystywane i przechowywane z uwzględnieniem chronionego prawem interesu osoby, której dane te dotyczą. Udostępnianie danych jest możliwe jedynie w przypadkach określonych w ustawie o ochronie danych osobowych. Dostęp do tych danych mają tylko uprawnione osoby. W celu prawidłowego i zgodnego z prawem przetwarzania danych osobowych Urząd powierza wykonywanie tego zadania pracownikom posiadającym w tym zakresie stosowne upoważnienie i zobowiązuje ich do zachowania w tajemnicy wszystkich przetwarzanych danych oraz sposobów ich przetwarzania.

W Urzędzie funkcjonuje system przyjmowania i postępowania z dokumentami dotyczącymi spraw wnoszonych przez klienta. Szczegółowy opis zasad rejestracji, znakowania, przydzielania, załatwiania i przechowywania dokumentów otrzymanych od klientów oraz sposób postępowania z dokumentami regulują przepisy prawne oraz wewnętrzne regulaminy.

W przypadku zagubienia lub zniszczenia dokumentu, klient powiadamiany jest o tym fakcie w formie pisemnej z podaniem przyczyn i propozycji dalszego sposobu załatwienia sprawy.

12.3. Zabezpieczenie wyrobu

Wszystkie dokumenty dostarczone lub tworzone w Urzędzie są zabezpieczone przed zniszczeniem, uszkodzeniem lub utratą. Zasady postępowania z dokumentacją na wszystkich etapach obiegu dokumentów (przyjmowania, tworzenia, gromadzenia, wysyłania, przechowywania) określa Instrukcja Kancelaryjna i Instrukcja archiwalna. Zgodnie z tymi regulacjami Urząd stara się ograniczać czynniki wpływające najbardziej na stan fizyczny przechowywanej dokumentacji i zapewniać coraz lepsze warunki przechowywania akt papierowych pod względem temperatury, wilgotności powietrza, oraz tworząc kopie bezpieczeństwa nośników informatycznych. Dokumenty papierowe są gromadzone w teczkach, segregatorach lub pudłach archiwalnych i przechowywane w miejscach do tego przeznaczonych. Dokumenty elektroniczne przechowywane są zgodnie z zasadami tworzenia i przechowywania kopii zapasowych (PW.1.2. Zasady zarządzania siecią teleinformatyczną, kryptografią i kopiami zapasowymi). Dokumenty bieżące są przechowywane w zamykanych szafach biurowych w komórkach organizacyjnych Urzędu, a akta spraw załatwionych w pomieszczeniach archiwum. Dokumenty zawierające informację niejawną są przechowywane i nadzorowane przez Pełnomocnika ds. informacji niejawnych.

Dokumenty przygotowywane do wysyłki są odpowiednio identyfikowane, przesyłki do klientów są w odpowiedni sposób pakowane, zabezpieczane i wysyłane. Biuro Obsługi Klienta urządzone jest w sposób zabezpieczający dostęp do dokumentów (wniosków i podań klientów) osobom nieuprawnionym.

Pracownicy mają limitowany dostęp do pomieszczeń regulowany przez system jednego klucza. Każdy z pracowników ma dostęp do pokoju, w którym pracuje, Kierownicy mają dostęp do pomieszczeń, w których sami pracują oraz do pomieszczeń zajmowanych przez pracowników podległego im Referatu. Burmistrz, Zastępca Burmistrza i Sekretarz mają dostęp do wszystkich pomieszczeń Urzędu. Zdefiniowane są osoby, które mają dostęp do drzwi wejściowych Urzędu oraz posiadają indywidualne kody dostępu do dezaktywacji alarmu. Dostęp do pomieszczeń regulują zasady PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji. Personel sprzątający ma dostęp do wszystkich pomieszczeń Urzędu, z ograniczeniem dostępu do niektórych pomieszczeń sprzątanych w czasie obecności pracownika.

Wszyscy pracownicy korzystający z komputerów mają chroniony dostęp do zasobów komputera indywidualnym loginem i hasłem. Częstotliwość wymiany hasła uzależniona jest od rodzaju danych gromadzonych i przetwarzanych przez pracownika obsługującego komputer.

13. POTENCJALNE ZAGROŻENIA I ZASADY OCHRONY DANYCH

Zasoby Urzędu, a w szczególności dane i informacje, a także sprzęt niezbędny do przetwarzania i przechowywania tych danych są niezwykle istotne dla ochrony żywotnych interesów Urzędu oraz klientów i wykonawców. W szczególności identyfikuje się niżej podane kategorie zagrożeń, którym mogą podlegać zasoby Urzędu:

- **naruszenie prywatności** (poufności) danych zarówno przez osoby z wewnątrz jak i osoby z zewnątrz Urzędu, a w tym również przez kradzież zasobu,

- **niedostępność systemu** (zasobu) lub znaczna degradacja jego istotnych parametrów funkcjonalnych lub utrata danych (zniszczenie zasobu) na skutek wystąpienia sił wyższych albo nieumyślnego, umyślnego lub przypadkowego działania,
- **naruszenie integralności** danych na skutek nieumyślnego, umyślnego lub przypadkowego działania,
- **niespójne wdrożenie zasad, standardów, procedur** i środków ochrony systemów,
- **niedostępność personelu.**

Zadaniem regulacji zawartych w ZSZ jest zmniejszenie ryzyka płynącego z zagrożeń do akceptowalnego poziomu, to znaczy zminimalizowanie możliwości naruszenia bezpieczeństwa zasobów Urzędu, umożliwienie wczesnego wykrycia takiego naruszenia, zminimalizowanie strat związanych z takim naruszeniem, sprawne usunięcie jego skutków oraz zapewnienie ciągłości pracy Urzędu.

Skuteczna ochrona zasobów Urzędu, a tym samym zapewnienie bezpieczeństwa Urzędu wymaga wspólnego działania i zaangażowania wszystkich pracowników Urzędu. Każda osoba podejmująca pracę w Urzędzie lub uzyskująca dostęp do zasobów informatycznych Urzędu przyjmuje na siebie obowiązek ochrony zasobów Urzędu. Obowiązek ochrony zasobów Urzędu nie znika z chwilą ustania stosunku pracy między pracownikiem a Urzędem.

Za wyjątkiem mienia powszechnie rozumianego w Urzędzie jako mienie ogólnego użytku, pracownicy Urzędu mają prawo używać zasobów Urzędu wyłącznie do celów służbowych, w jasno określonym zakresie, i tylko jeżeli dostęp do tych zasobów został im udzielony albo w ramach obowiązków służbowych (opisu stanowiska pracy), albo w jakikolwiek inny jawny sposób zgodny z prawem i obowiązującymi w Urzędzie procedurami.

W celu zapewnienia bezpieczeństwa Urzędu stosuje się następujące ogólne zasady:

1. **Zasada przywilejów koniecznych:** każdy pracownik posiada prawa dostępu do zasobów Urzędu ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu obowiązków.
2. **Zasada wiedzy koniecznej:** pracownicy posiadają wiedzę o zasobach Urzędu ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych im zadań.
3. **Zasada asekuracji zabezpieczeń:** ochrona zasobów nie może opierać się wyłącznie na jednym mechanizmie zabezpieczenia.
4. **Zasada indywidualnej odpowiedzialności:** Urząd dąży do zapewnienia jednoznacznej odpowiedzialności pracowników za zasoby im powierzone; wszyscy użytkownicy muszą być świadomi swej odpowiedzialności i konsekwencji, które poniosą, jeżeli zaniedbają swoje obowiązki bądź przekażą swoje przywileje innym osobom.

14. NADZOROWANIE WYPOSAŻENIA DO MONITOROWANIA I POMIARÓW

Ze względu na specyfikę i charakter prowadzonych spraw i realizowanych procesów Urząd posiada następujące urządzenia do kontroli i pomiaru: higrometr i termometr w Archiwum Zakładowym, dalmierz laserowy oraz wodomierze i przepływomierze. Wymienione urządzenia pomiarowe są użytkowane zgodnie z odpowiednimi instrukcjami obsługi.

Stosowane przez Urząd w archiwum wyposażenie do monitorowania warunków środowiska (temperatura, wilgotność) podlega nadzorowaniu. Zapewnia to właściwą identyfikację, regularne sprawdzanie i określanie statusu sprawdzeń. Wzorcowanie higrometru i termometru w archiwum zakładowym następuje nie rzadziej niż raz na 5 lat. Za wzorcowanie higrometru i termometru w archiwum odpowiada pracownik Referatu Organizacyjnego. Wzorcowanie odbywa się przez dokonanie oględzin higrometru i termometru oraz pomiarów kontrolnych innym higrometrem i termometrem i porównanie odczytów. Z wzorcowania sporządzanie są notatki służbowe.

Dalmierz laserowy Leica DISTRO D3 o numerze seryjnym 1224431458 to urządzenie służące do pomiaru powierzchni budynków, użytkowane w prowadzonych kontrolach podatkowych przeprowadzanych przez pracowników Urzędu. Wzorcowania dalmierza dokonuje się raz w roku przez Główny Urząd Miar w Warszawie. Dokument wzorcowania przechowywany jest wraz z dalmierzem. Za legalizację Dalmierza odpowiadają pracownicy Referatu Finansowo – Księgowego.

W związku ze specyfiką świadczonych przez Urząd usług dla społeczności lokalnej nadzoruje się legalizację wodomierzy. Wodomierze legalizowane są zgodnie z obowiązującymi przepisami co 5 lat. Za legalizację wodomierzy odpowiadają pracownicy Referatu Gospodarki Komunalnej.

Wymienione urządzenia pomiarowe są oznaczone odpowiednim numerem ewidencyjnym i podlegają konserwacji, użytkowaniu, sprawdzeniu, wzorcowaniu, kalibracji, legalizacji i obsłudze zgodnie z odpowiednimi instrukcjami obsługi tych urządzeń. Za odpowiedni stan techniczny urządzeń pomiarowych i nadzór nad nimi odpowiadają użytkownicy.

15. KONTROLA ZARZĄDCZA

Zgodnie z obowiązującym Regulaminem organizacji kontroli zarządczej w Urzędzie i jednostkach organizacyjnych Gminy Dobczyce oraz zasadami jej koordynacji w Urzędzie sprawowana jest kontrola zarządcza. Kontrola zarządcza w Urzędzie obejmuje audyty jakości, audyt wewnętrzny i kontrolę wewnętrzną. W Urzędzie istnieje system kontroli wewnętrznej i system kontroli finansowej, które umożliwiają prowadzenie monitorowania i analizy niezbędnych dokumentów do zapewnienia jakości usług, zgodności ZSZ i realizacji procesów. Zapisy dotyczące kontroli Urzędu, zarówno wewnętrznych jak i zewnętrznych oraz wniosków i zaleceń z nich wypływających, a także sposobu ich realizacji, są gromadzone i przechowywane.

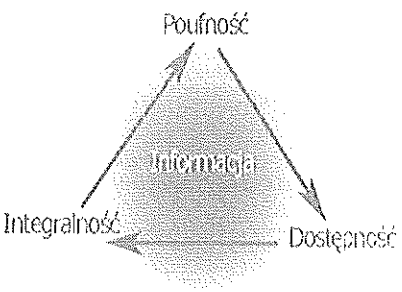
16. STRUKTURA PROCESÓW ZSZ

W załączniku nr 2 przedstawiono strukturę procesów ZSZ. Karty procesów oraz wykazane w strukturze zasady i regulaminy znajdują się w Qsystem.

17. TERMINOLOGIA

- **Akta sprawy** – cała dokumentacja (pisma, dokumenty, notatki, formularze, plany, fotokopie, rysunki, itp.) zawierająca dane lub informacje, które były, są lub mogą być istotne przy rozpatrywaniu danej sprawy.
- **Audyt jakości** – systematyczny, niezależny i udokumentowany proces uzyskiwania dowodu z auditu oraz jego obiektywnej oceny, w celu określenia stopnia spełnienia kryteriów auditu. Niezależne badanie Zintegrowanego Systemu Zarządzania.
- **Benchmarking** – badania porównawcze lub analiza porównawcza.
- **Burmistrz** – Burmistrz Gminy i Miasta Dobczyce.
- **Działania doskonalące** (usprawnienie) – działania, które może zaproponować każdy pracownik w celu poprawy efektywności funkcjonowania organizacji i obsługi klienta.
- **Identyfikacja** – znak sprawy, zespół symboli określających przynależność sprawy do określonej komórki organizacyjnej i określonej grupy spraw.
- **Identyfikowalność** – zdolność do prześledzenia historii, zastosowania lub lokalizacji tego, co jest przedmiotem rozpatrywania.
- **Incydent** - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działania urzędu i zagrażają bezpieczeństwu danych.
- **Infrastruktura** – system urządzeń, wyposażenia i obsługi niezbędny do działania Urzędu.
- **Instrukcja kancelaryjna** – Instrukcja kancelaryjna dla organów gmin i związków międzygminnych określająca zasady i tryb wykonywania czynności kancelaryjnych, ustalona rozporządzeniem Prezesa Rady Ministrów.
- **Jakość** – stopień, w jakim właściwości usługi, procesu lub systemu spełniają wymagania klienta i zainteresowanych stron.
- **Kierownictwo Urzędu** – najwyższe Kierownictwo wraz z Kierownikami Referatów.
- **Kierownicy** – Kierownicy Referatów.
- **Klient** – osoba lub organizacja, która otrzymuje wyrób.
- **Korupcja** – czyn polegający na obiecywaniu, proponowaniu lub wręczaniu przez jakąkolwiek osobę, bezpośrednio lub pośrednio, jakichkolwiek nienależnych korzyści osobie pełniącej funkcję publiczną dla niej samej lub dla jakiejkolwiek innej osoby, w zamian za działanie lub zaniechanie działania w wykonywaniu jej funkcji oraz czyn polegający na żądaniu lub przyjmowaniu przez osobę pełniącą funkcję publiczną bezpośrednio lub pośrednio, jakichkolwiek nienależnych korzyści, dla niej samej lub dla jakiejkolwiek innej osoby lub przyjmowaniu propozycji lub obietnicy takich korzyści, w zamian za działanie lub zaniechanie działania w wykonywaniu jej funkcji.
- **Krajowe Ramy Interoperacyjności** – Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
- **Najwyższe Kierownictwo** – Burmistrz Gminy i Miasta Dobczyce, Zastępca Burmistrza Gminy i Miasta Dobczyce, Skarbnik Gminy i Miasta Dobczyce, Sekretarz Gminy i Miasta Dobczyce.

- **Niezgodność** – niespełnienie wymagania określonego w przepisach prawa, zasadach lub przyjętego zwyczajowo.
- **Pełnomocnik** – przedstawiciel Kierownictwa Urzędu nadzorujący wdrażanie, utrzymanie i doskonalenie Zintegrowanego Systemu Zarządzania w Urzędzie, pełniący również funkcję Administratora Bezpieczeństwa Informacji.
- **Polityka Jakości** – ogół zamierzeń i ukierunkowanie organizacji dotyczące jakości formalnie wyrażone przez najwyższe Kierownictwo.
- **Proces** – zbiór działań wzajemnie powiązanych lub wzajemnie oddziałujących, które przekształcają wejścia w wyjścia.
- **Projekty doskonalące** – projekty, które mają na celu doskonalenie i poprawę działania Urzędu i obsługi klientów. Projekty obejmują działanie w których wymagane jest zaangażowanie większej ilości zasobów i czasu.
- **Przegląd** – działanie podejmowane w celu określenia przydatności, adekwatności i skuteczności przedmiotu rozważań do osiągnięcia ustalonych celów.
- **Przyjęte zwyczajowo** – istnieje zwyczaj lub powszechna praktyka Urzędu, jego klientów i innych stron zainteresowanych, ze rozpatrywana potrzeba lub oczekiwanie jest przyjęte.
- **Sekretarz** – Sekretarz Gminy i Miasta Dobczyce.
- **Strony zainteresowane (interesariusze)** – wszyscy bezpośrednio zainteresowani funkcjonowaniem organizacji, jej działaniami i osiągnięciami.
- **System Przeciwdziałania Zagrożeniom Korupcyjnym (SPZK)** – część systemu zarządzania ukierunkowana na zapewnienie zaufania, że Urząd wdrożył rozwiązania eliminujące lub w znacznym stopniu ograniczające możliwość występowania zjawisk korupcyjnych.
- **Urząd** – Urząd Gminy i Miasta Dobczyce.
- **Wymaganie** – potrzeba lub oczekiwanie, które zostało ustalone, przyjęte zwyczajowo lub jest obowiązkowe.
- **Wyrób lub usługa** – wynik procesu.
- **Zadowolenie klienta** – percepcja klienta dotycząca stopnia, w jakim jego wymagania zostały spełnione.
- **ZSZ** – Zintegrowany System Zarządzania.
- **Strona zainteresowana** – wszyscy bezpośrednio zainteresowani funkcjonowaniem organizacji, jej działaniami i osiągnięciami.
- **Partnerstwo** – relacje robocze pomiędzy dwiema lub więcej stronami, będące źródłem wartości dodanej dla strony
- **Polityka i strategia** – to sposób w jaki organizacja wdraża swoją misję i wizję.
- **Proces** – ciąg działań, który dodaje wartości poprzez wytwarzanie wymaganych rezultatów z szeregu rozmaitych zasobów.
- **Poufność** informacji oznacza, że jest ona dostępna wyłącznie osobom i programom, które zostały upoważnione do korzystania z informacji.
- **Integralność** informacji oznacza, oznacza zapewnienie dokładności i kompletności informacji oraz metod przetwarzania.
- **Dostępność** informacji oznacza zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy gdy jest to potrzebne (możliwość wykorzystania zasobu przez upoważnioną osobę lub program na każde żądanie i w ustalonym czasie)



18. SPIS ZAŁĄCZNIKÓW

1. Deklaracja Stosowania
2. Struktura procesów

Załącznik 1 - Deklaracja stosowania wymagań normy ISO/IEC 27001:2014 w Urzędzie Gminy i Miasta w Dobczycach

Wdrożony Zintegrowany System Zarządzania obejmuje swoim zakresem wszystkie komórki organizacyjne Urzędu

Dobczyce, dnia 21 lipca 2015 roku

Cele stosowania zabezpieczeń i zabezpieczenia

Rozdział	Opis normy/wymaganie	Sposób realizacji
A.5 Polityka bezpieczeństwa informacji		
A.5.1 Kierunki bezpieczeństwa informacji określane przez kierownictwo		
Cel: Zapewnienie przez kierownictwo wytycznych w sparcia dla działań na rzecz bezpieczeństwa informacji, zgodnie z wymaganiami biznesowymi oraz właściwymi normami prawnymi i regulacjami.		
A.5.1.1	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. Dokument ten został zatwierdzony przez kierownictwo i opublikowany w Qsystemie do wiadomości wszystkich pracowników. Zapewniono też przekazanie dokumentu do wiadomości właściwych stron zewnetrznych.
A 5.1.2	Przegląd polityki bezpieczeństwa informacji	Przeglądy ZSZ (w tym przeglądy polityki bezpieczeństwa informacji) odbywają się zgodnie z zasadami opisanymi w rozdziale 6 Księgi Zintegrowanego Systemu Zarządzania
A.6 Organizacja bezpieczeństwa informacji		
A.6.1 Organizacja wewnętrzna		
Cel: Ustanowić strukturę zarządzania w celu zainicjowania oraz nadzorownia wdrażania i eksploatacji bezpieczeństwa informacji w organizacji.		
A.6.1 1	Role i odpowiedzialność za bezpieczeństwo informacji	Najwyższe Kierownictwo Urzędu jest zaangażowane w zapewnienie bezpieczeństwa informacji i ochronę danych osobowych.
A. 6.1.2	Rozdzielenie obowiązków	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. 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	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.6.1.4	Kontakty z grupami zainteresowanych specjalistów	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.6.1.5	Bezpieczeństwo informacji w zarządzaniu projektami	Urząd zarządzając projektem każdorazowo uwzględnia zagadnienia z obszaru bezpieczeństwa informacji np. zawierając umowy ze stronami trzecimi zawiera klauzule zobowiązujące do zapewnienia ochrony danych i poufności
A.6.2 Urządzenia mobilne i telepraca		
Cel: Zapewnić bezpieczeństwo telepracy i stosowania urządzeń mobilnych		
A.6.2.1	Polityka stosowania urządzeń mobilnych	Politykę stosowania urządzeń mobilnych określają procedury PZ. 2.9. Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji oraz PW. 1.1 Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji
A.6.2.2	Telepraca	W systemie teleinformatycznym urzędu nie prowadzi się pracy na odległość.
A.7 Bezpieczeństwo zasobów ludzkich		
A.7.1 Przed zatrudnieniem		
Cel: Zapenić, żeby pracownicy i kontrahenci rozumieli swoja odpowiedzialność i byli odpowiednimi kandydatami do wypełnienia ról, do których są przewidziani.		
A.7.1.1	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.7.1.2	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.7.2 Podczas zatrudnienia.		
Cel: Zapenić, żeby pracownicy i kontrahenci byli świadomi swoich obowiązków dotyczących bezpieczeństwa informacji i wypełniali je.		
A.7.2.1	Odpowiedzialność kierownictwa	Kierownicy komórek organizacyjnych Urzędu odpowiadają za nadzór nad pracownikami, użytkownikami oraz stronami trzecimi w zakresie stosowania zasad wynikających z ZSZ.
A.7.2.2	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.7.2.3	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.7.3 Zakończenie i zmiana zatrudnienia		
Cel: Zabezpieczyć interesy organizacji w trakcie procesu zmiany lub zakończenia zatrudnienia.		

Rozdział	Opis normy/wymaganie	Sposób realizacji
A.7.3.1	Zakończenie zatrudnienia lub zmiana zakresu obowiązków	Odpowiedzialności związane z zakończeniem lub zmianą 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 także PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji.
A.8 Zarządzanie aktywami		
A.8.1 Odpowiedzialność za aktywa		
Cel: Zidentyfikować aktywa organizacji i zdefiniować właściwą odpowiedzialność w dziedzinie ich ochrony.		
A.8.1.1	Inwentaryzacja aktywów	Przeprowadzono inwentaryzację aktywów informacyjnych oraz na jej podstawie, inwentaryzację krytycznych zasobów teleinformatycznych (sprzętowych i programowych) Urzędu zgodnie z PZ.7.1. Nadzór nad ryzykiem. Wyznaczono właścicieli aktywów i krytycznych zasobów teleinformatycznych zidentyfikowanych w Urzędzie.
A.8.1.2	Własność aktywów	Wszystkie istotne aktywa i grupy aktywów mają przydzielonych właścicieli
A. 8.1.3	Akceptowalne użycie aktywów	System zarządzania bezpieczeństwem informacji określa zasady korzystania z grup aktywów i nadzoru nad nimi.
A.8.1.4	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 8.2 Klasyfikacja informacji		
Cel: Zapewnić przypisanie informacjom odpowiedniego poziomu ochrony, zgodnego z ich wagą dla organizacji.		
A 8.2.1	Klasyfikowanie informacji	Klasyfikacja informacji została określona w: - Instrukcji kancelaryjnej, - Przepisach związanych z ochroną infromacji niejawnych, - Księdze ZSZ.
A 8.2.2	Oznaczenie informacji	Zasady oznaczania dokumentów Urzędu określone są w: - Instrukcji kancelaryjnej, - Przepisach związanych z ochroną infromacji niejawnych, - Księdze ZSZ.
A 8.2.3	Postępowanie z aktywami	Zasady postępowania z aktywami określone są w: - Instrukcji kancelaryjnej, - Przepisach związanych z ochroną infromacji niejawnych, - Księdze ZSZ i procedurach systemowych (PW. 1.1,PZ.2.9, PZ.7.1)
A.8.3 Postępowanie z nośnikami		
Cel: Zapobiec nieupranionemu ujawnieniu, modyfikacji, usunięciu lub zniszeniu informacji zapisanych na nośnikach.		
A.8.3.1	Zarządzanie nośnikami wymiennymi	Zasady zarządzania zawiera procedura PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji.
A.8.3.2	Wycofywanie nośników	Zasady wycofywania nośników określane są przez Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacj(PZ.2.9.) oraz PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji.
A.8.3.3	Przekazywanie nośników	Zastosowanie maja zapisy w procedurach Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacj(PZ.2.9.) oraz PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji.
A.9 Kontrola dostępu		
A.9.1 Wymagania biznesowe wobec kontroli dostępu		
Cel: Ograniczyć dostęp do informacji i środków przetwarzania informacji.		
A.9.1.1	Polityka kontroli dostępu	PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji.
A.9.1.2	Dostęp do sieci i usług sieciowych	Określa PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji. PW.1.2. Zasady zadządzania siecią teleinformatyczną, kryptografią i kopiami zapasowymi.
A.9.2 Zarządzanie dostępem użytkowników		
Cel: Zapewnić dostęp upranionym użytkownikom i zapobiec niupranionemu dostepowi do stystemów i usług.		
A.9.2.1	Rejestrowanie i wyrejestrowywanie użytkowników	PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji.
A.9.2.2	Przydzielanie dostępu użytkownikom	PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji.
A.9.2.3	Zarządzanie prawami uprzywilejowanego dostępu	PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji.
A.9.2.4	Zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników	PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji.
A.9.2.5	Przegląd praw dostępu użytkowników	PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji.
A.9.2.6	Odbieranie lub dostosowywanie praw dostępu	PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji.
A.9.3 Odpowiedzialność użytkowników		
Cel: Zapewnić rozliczalność użytkowników w celu ochrony ich informacji uwierzytelniających		
A.9.3.1	Stosowanie poufnych informacji uwierzytelniających	Określają PZ.2.9. Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji oraz PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji.
A.9.4 Kontrola dostępu do systemów i aplikacji		
Cel: Zapobiec nieuprawnionemu dostępowi do systemów i aplikacji.		
A 9.4.1	Ograniczenie dostępu do informacji	PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji.
A 9.4.2	Procedury bezpiecznego logowania	PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji oraz PZ.2.9.Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji
A 9.4.3	System zarządzania hasłami	PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji.
A 9.4.4	Użycie uprzywilejowanych programów narzędziowych	Za nadzór nad programami narzędziowymi odpowiada Pełnomocnik ds. ZSZ oraz Administrator Systemów Informatycznych.
A 9.4.5	Kontrola dostępu do kodów źródłowych programów	PW.1.2. Zasady zadządzania siecią teleinformatyczną, kryptografią i kopiami zapasowymi.
A. 10 Kryptografia		
A.10.1 Zabezpieczenia kryptograficzne		

Rozdział	Opis normy/wymaganie	Sposób realizacji
Cel: Zapewnić właściwe i skuteczne wykorzystanie kryptografii do ochrony poufności, autentyczności i/lub integralności informacji.		
A.10.1.1	Polityka stosowania zabezpieczeń kryptograficznych	PW.1.2. Zasady zadządzania siecią teleinformatyczną, kryptografią i kopiami zapasowymi.
A.10.1.2	Zarządzanie kluczami	PW.1.2. Zasady zadządzania siecią teleinformatyczną, kryptografią i kopiami zapasowymi.
A. 11 Bezpieczeństwo fizyczne i środowiskowe		
A.11.1 Obszary bezpieczne		
Cel: Zapobiec nieuprawnionemu fizycznemu dostępowi, szkodom i zakłóceniom w informacjach i środkach przetwarzania informacji należących do organizacji.		
A.11.1.1	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. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji.
A.11.1.2	Fizyczne zabezpieczenie wejść	Wszystkie fizyczne strefy kontrolowanego dostępu zabezpieczone są kluczem szyfrowym z kontrolowanym dostępem (system jednego klucza).
A.11.1.3	Zabezpieczenia biur, pomieszczeń i obiektów	Określa dokument PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji.
A.11.1.4	Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi	Określa PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji. PW.1.2. Zasady zadządzania siecią teleinformatyczną, kryptografią i kopiami zapasowymi oraz PW. 6.1 Zasady zarządzania ciągłością działania Urzędu
A.11.1.5	Praca w obszarach bezpiecznych	Określono zasady przebywania w strefie chronionej, jak również zasady przyjmowania osób trzecich w strefie chronionej. Określa dokument PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji.
A.11.1.6	Obszary dostaw i załadunku	Obszary publicznie dostępne zostały określone i wyznaczone i sprawowany jest nad nimi nadzór.
A.11.2 Sprzęt		
Cel: Zapobiec utracie, uszkodzeniu, kradzieży lub utracie integralności aktywów oraz zakłóceniom w działaniu organizacji.		
A.11.2.1	Lokalizacja i ochrona sprzętu	Zasady rozmieszczania sprzętu i urządzeń teleinformatycznych określają: PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji. PW.1.2. Zasady zadządzania siecią teleinformatyczną, kryptografią i kopiami zapasowymi.
A.11.2.2	Systemy wspomagające	Wszystkie systemy krytyczne mają potrzymywanie zasilania. Zapewnienie ciągłości działania opisano w procedurze PW. 6.1
A.11.2.3	Bezpieczeństwo okablowania	Okablowanie strukturalne i energetyczne zabezpieczone jest zgodnie z zasadami określonymi w PW.1.2. Zasady zadządzania siecią teleinformatyczną, kryptografią i kopiami zapasowymi.
A.11.2.4	Konserwacja sprzętu	Zasady utrzymania sprzętu określa dokument: PW.1.2. Zasady zadządzania siecią teleinformatyczną, kryptografią i kopiami zapasowymi.
A 11.2.5	Wynoszenie aktywów	Aktywa zabezpieczane są zgodnie z zasadami: PZ.2.9. Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji oraz PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji.
A.11.2.6	Bezpieczeństwo sprzętu i aktywów poza siedzibą	Zasady bezpieczeństwa poza siedzibą określa dokument PZ.2.9. Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji.
A.11.2.7	Bezpieczne zbywanie lub przekazywanie do ponownego użycia sprzętu	Zasady bezpieczenego zbywania sprzętu określają dokumenty PW.4.1. Zasady gospodarowania środkami trwałymi i wyposażeniem urzędu, PW.4.2. Zasady gospodarowania odpadami w urzędzie i PW.1.2. Zasady zarządzania siecią teleinformatyczną, kryptografią i kopiamia zapasowymi.
A.11.2.8	Pozostawianie sprzętu użytkownika bez opieki	PW. 2.9 Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji
A.11.2.9	Polityka czystego biurka i czystego ekranu	PW. 2.9 Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji
A. 12 Bezpieczna eksploatacja		
A.12.1 Procedury eksploatacyjne i odpowiedzialność		
Cel: Zapewnić poprawną i bezpieczną eksploatację środków przetwarzania informacji.		
A.12.1.1	Dokumentowanie procedur eksploatacyjnych	Określono w PW.1.4. Zasady zarządzania rozwojem informatycznym
A.12.1.2	Zarządzanie zmianami	Określono w PW.1.4. Zasady zarządzania rozwojem informatycznym
A.12.1.3	Zarządzanie pojemnością	W przypadku krytycznych zasobów za planowanie pojemności odpowiada Właściciel aktywu.
A.12.1.4	Oddzielanie środowisk rozwojowych, testowych i produkcyjnych	Określono w PW.1.4. Zasady zarządzania rozwojem informatycznym
A.12.2 Ochrona przed szkodliwym oprogramowaniem		
Cel: Zapewnić informacjom i środkom przetwarzania informacji ochronę przed szkodliwym oprogramowaniem.		
A.12.2.1	Zabezpieczenie przed szkodliwym oprogramowniem	PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji.
A.12.3 Kopie zapasowe		
Cel: Chronić przed utratą danych		
A.12.3.1	Zapasowe kopie informacji	PW.1.2. Zasady zadządzania siecią teleinformatyczną, kryptografią i kopiami zapasowymi. PW.6.1. Zasady zarządzania ciagłoscią działania Urzędu
A.12.4 Rejestrowanie zdarzeń i monitorowanie		
Cel: Rejestrować zdarzenia i zbierać materiał dowodowy.		
A.12.4.1	Rejestrowanie zdarzeń	Określa PW.1.3. Zasady zarządzania incydentami związanymi z bezpieczeństwem informacji.
A.12.4.2	Ochrona informacji w dziennikach zdarzeń	Zasady ochrony dzienników określa Administrator Systemów Informatycznych
A.12.4.3	Rejestrowanie działań administratorów i operatorów	Zasady ochrony dzienników określa Administrator Systemów Informatycznych
A.12.4.4	Synchronizacja zegarów	Za synchronizację zegarów odpowiada ASI
A.12.5 Nadzór nad oprogramowanie produkcyjnym		

Rozdział	Opis normy/wymaganie	Sposób realizacji
Cel: Zapewnić integralność systemów produkcyjnych.		
A.12.5.1	Instalacja oprogramowania w systemach produkcyjnych	PW.1.4. Zasady zarządzania rozwojem informatycznym oraz PW. 1.2. Zasady zadządzania siecią teleinformatyczną, kryptografią i kopiami zapasowymi
A.12.6 Zarządzanie podatnościami technicznymi		
Cel: Zapobiec wykorzystywaniu podatności technicznych.		
A.12.6.1	Zarządzanie podatnościami technicznymi	Za nadzór nad podatnościami technicznymi odpowiada Pełnomocnik ds. ZSZ
A.12.6.2	Ograniczenia w instalowaniu oprogramowania	PW. 1.2. Zasady zadządzania siecią teleinformatyczną, kryptografią i kopiami zapasowymi oraz PZ.2.9 Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji
A.12.7 Rozważania dotyczące audytu systemów informacyjnych		
Cel: Zminimalizować wpływ działań audytu na systemy produkcyjne.		
A.12.7.1	Zabezpieczenia audytu systemów informacyjnych	Za zabezpieczenie audytu ZSZ odpowiada Pełnomocnik ds. ZSZ oraz ASI
A. 13 Bezpieczeństwo komunikacji		
A.13.1 Zarządzanie bezpieczeństwem sieci		
Cel: Zapewnić ochronę informacji w sieciach oraz wspomagających je środkach przetwarzania informacji.		
A.13.1.1	Zabezpieczenia sieci	PW.1.2. Zasady zadządzania siecią teleinformatyczną, kryptografią i kopiami zapasowymi.
A.13.1.2	Bezpieczeństwo usług sieciowych	PW.1.2. Zasady zadządzania siecią teleinformatyczną, kryptografią i kopiami zapasowymi.
A.13.1.3	Rozdzielanie sieci	Określa dokument PW.1.3. Zasady zarządzania siecią teleinformatyczną i kryptografią
A.13.2 Przesyłanie informacji		
Cel: Utrzymać bezpieczeństwo informacji przesyłanych wewnątrz organizacji i wymienianych z podmiotami zewnętrznymi.		
A.13.2.1	Polityki i procedury przesyłania informacji	Określają Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacj (PZ.2.9.)
A.13.2.2	Porozumienia dotyczące przesyłania informacji	Określają Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacj (PZ.2.9.)
A.13.2.3	Wiadomości elektroniczne	PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji.
A.13.2.4	Umowy o zachowaniu poufności	Umowy zawierane ze stronami trzecimi (w tym pracownikami) zawierają klauzule zobowiązujace do zapewnienia ochrony danych i poufności.
A. 14 Pozyskiwanie, rozwój i utrzymanie systemów		
A.14.1 Wymagania związane z bezpieczeństwem systemów informacyjnych		
Cel: Zapewnić żeby bezpieczeństwo informacji było nieodłączną częścią systemów informacyjnych w całym cyklu życia. Dotyczy to również wymagań wobec systemów informacyjnych dostarczających usług w sieciach publicznych.		
A.14.1.1	Analiza i specyfikacja wymagań bezpieczeństwa informacji	Określają Zasady zarządzania rozwojem informatycznym (PW.1.4.)
A.14.1.2	Zabezpieczanie usług aplikacyjnych w sieciach publicznych	PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji.
A.14.1.3	Ochrona transakcji usług aplikacyjnych	PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji.
A.14.2 Bezpieczeństwo w procesach rozwoju i wsparcia		
Cel: Zapewnić projektowanie i wdrożenie bezpieczeństwa informacji w rmach cyklu życia systemów informacyjnych.		
A.14.2.1	Polityka bezpieczeństwa prac rozwojowych	Określają Zasady zarządzania rozwojem informatycznym (PW.1.4.)
A.14.2.2	Procedury kontroli zmian w sytemach	Określają Zasady zarządzania rozwojem informatycznym (PW.1.4.)
A.14.2.3	Przegląd techniczny aplikacji po zmianach w platformie produkcyjnej	Określają Zasady zarządzania rozwojem informatycznym (PW.1.4.)
A.14.2.4	Ograniczenia dotyczące zmian w pakietach oprogramowania	Określają Zasady zarządzania rozwojem informatycznym (PW.1.4.)
A.14.2.5	Zasady projektowania bezpiecznych systemów	Określają Zasady zarządzania rozwojem informatycznym (PW.1.4.)
A.14.2.6	Bezpieczne środowisko rozwojowe	Określają Zasady zarządzania rozwojem informatycznym (PW.1.4.)
A.14.2.7	Prace rozwojowe zlecane podmiotom zewnętrznej.	Określają Zasady zarządzania rozwojem informatycznym (PW.1.4.)
A.14.2.8	Testowanie bezpieczeństwa systemów	Określają Zasady zarządzania rozwojem informatycznym (PW.1.4.)
A.14.2.9	Testy akceptacyjne systemów	Określają Zasady zarządzania rozwojem informatycznym (PW.1.4.)
A.14.3 Dane testowe		
Cel: Zapewnić ochronę danych stosowanych do testów.		
A.14.3.1	Ochrona danych testowych	PW.1.2. Zasady zadządzania siecią teleinformatyczną, kryptografią i kopiami zapasowymi.
A. 15 Relacje z dostawcami		
A.15.1 Bezpieczeństwo informacji w relacjach z dostawcami		
Cel: Zapewnić ochrone aktywów organizacji udostępnianych dostawcom.		
A.15.1.1	Polityka bezpieczeństwa informacji w relacjach z dostawcami	PW.1.2. Zasady zadządzania siecią teleinformatyczną, kryptografią i kopiami zapasowymi.PW.1.4. Zasady zarządzania rozwojem informatycznym oraz PZ.2.9. Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji.
A.15.1.2	Uwzględnianie bezpieczeństwa w porozumieniach z dostawcami	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.15.1.3	Łańcuch dostaw technologii informacyjnych i telekomunikacyjnych	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.15.2 Zarządzanie usługami świadczonymi przez dostawców		
Cel: Utrzymać uzgodniony poziom bezpieczeństwa informacji i świadczonych usług zgodnie z umowami z dostawcami.		
A.15.2.1	Monitorowanie i przegląd usług świadczonych przez dostawców	Określono w PW.1.4. Zasady zarządzania rozwojem informatycznym oraz PZ.2.9. Zadania i obowiązki pracowników zwiazane z zapewnieniem bezpieczeństwa informacji.
A.15.2.2	Zarządzanie zmianami w usługach świadczonych przez dostawców	Określono w PW.1.4. Zasady zarządzania rozwojem informatycznym oraz PZ.2.9. Zadania i obowiązki pracowników zwiazane z zapewnieniem bezpieczeństwa informacji.
A. 16 Zarządzania incydentami związanymi z bezpieczeństwem informacji		
A.16.1 Zarządzania incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami		

Rozdział	Opis normy/wymaganie	Sposób realizacji
Cel: Zapewnić spójne i skuteczne podejście do zarządzania incydentami związanymi z bezpieczeństwem informacji, z uwzględnieniem informowania o zdarzeniach i słabościach.		
A.16.1.1	Odpowiedzialność i procedury	Określają Zasady zarządzania incydentami związanymi z bezpieczeństwem informacji (PW.1.3.)
A.16.1.2	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji	Określają zasady zarządzania incydentami związanymi z bezpieczeństwem informacji (PW.1.3.) oraz Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji (PZ.2.9.).
A.16.1.3	Zgłaszanie słabości związanych z bezpieczeństwem informacji	Określają zasady zarządzania incydentami związanymi z bezpieczeństwem informacji (PW.1.3.) oraz Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji (PZ.2.9.).
A.16.1.4	Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji.	Określają zasady zarządzania incydentami związanymi z bezpieczeństwem informacji (PW.1.3.) oraz Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji (PZ.2.9.).
A.16.1.5	Reagowanie na incydenty związane z bezpieczeństwem informacji	Określają zasady zarządzania incydentami związanymi z bezpieczeństwem informacji (PW.1.3.).
A.16.1.6	Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji	Określają zasady zarządzania incydentami związanymi z bezpieczeństwem informacji (PW.1.3.).
A.16.1.7	Gromadzenie materiału dowodowego	Określają zasady zarządzania incydentami związanymi z bezpieczeństwem informacji (PW.1.3.).
A. 17 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania		
A.17.1 Ciągłość bezpieczeństwa informacji		
Cel: Zaleca się uwzględnienie ciągłości bezpieczeństwa informacji w systemach zarzadzania ciągłością działania organizacji.		
A.17.1.1	Planowanie ciągłości bezpieczeństwa informacji	Określają zasady zarządzania siecia teleinformatyczną, kryptografią i kopiami zapasowymi PW.1.2. i Zasady zarządzania ciagłością działania Urzędu PW.6.1.
A.17.1.2	Wdrożenie ciągłości bezpieczeństwa informacji.	Określają zasady zarządzania siecia teleinformatyczną, kryptografią i kopiami zapasowymi PW.1.2. i Zasady zarządzania ciagłością działania Urzędu PW.6.1.
A.17.1.3	Weryfikowanie, przegląd i ocena ciągłości bezpieczeństwa informacji	Określają zasady zarządzania siecia teleinformatyczną, kryptografią i kopiami zapasowymi PW.1.2. i Zasady zarządzania ciagłością działania Urzędu PW.6.1.
A.17.2 Nadmiarowość		
Cel: Zapewnić dostępność środków przetwarzania informacji.		
A.17.2.1	Dostępność środków przetwarzania informacji	Określono w PW.1.4. Zasady zarządzania rozwojem informatycznym
A. 18 Zgodność		
A.18.1 Zgodność z wymaganiami prawnymi i umownymi		
Cel: Unikać naruszenia zobowiązań prawnych, regulacyjnych lub umownych związanych z bezpieczeństwem informacji oraz innych wymagań dotyczących bezpieczeństwa.		
A.18.1.1	Określenie stosownych wymagań prawnych i umownych	Określa PZ.6.1. Zasady nadzoru nad dokumentami, przepisami prawa i zapisami.
A.18.1.2	Prawa własności intelektualnej	Za nadzór nad przestrzeganiem prawa własności intelektualnej odpowiadają Sekretarz oraz Kierownicy komórek organizacyjnych
A.18.1.3	Ochrona zapisów	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.18.1.4	Prywatność i ochrona danych identyfikujących osobę	Ochrona danych osobowych odbywa się w oparciu o ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych i wydanych do niej rozporządzeń wykonawczych. Zasady ochrony danych osobowych określono w - Księdze ZSZ, - Dokumentacji Procesu PW.1.1. Zarządzanie bezpieczeństwem informacji, ochroną danych osobowych i informatyzacja Urzędu.
A.18.1.5	Regulacje dotyczące zabezpieczeń kryptograficznych	Zasady dotyczące zabezpieczeń kryptograficznych określono w zasadach zarządzania siecią teleinformatyczną, kryptografią i kopiami zapasowymi PW.1.2.
A.18.2 Przeglądy bezpieczeństwa informacji		
Cel: Zapewnić zgodne z politykami organizacji i procedurami wdrożenie i stosowanie zasad bezpieczeństwa informacji.		
A.18.2.1	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.18.2.2	Zgodność z politykami bezpieczeństwa i standardami	Regularnie dokonuje się przeglądów ZSZ, w tym Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych. Zasady badania zgodności opisano kompleksowo w Księdze ZSZ w rozdziale 7 - Prowadzenie narad i przeglądów ZSZ.
A.18.2.3	Sprawdzanie zgodności technicznej	Pełnomocnik ds. ZSZ i ASI – każdy w swoim obszarze działania, odpowiedzialni są za nadzorowanie technicznego stanu systemów informatycznych.

BURMISTRZ
Gminy i Miasta Dobczyce
Paweł Machnicki

Sekretarz Gminy
Małgorzata Góralik-Piętka

Struktura procesów Zintegrowanego Systemu Zarządzania

Nr procesu	Nr karty, regulaminu lub zasad	Proces	Regulaminy lub zasady	Właściciel: - procesu - lub grupy procesów - lub dokumentu
KZSZ			Księga Zintegrowanego Systemu Zarządzania	Pełnomocnik ds. ZSZ
PJ			Polityka Zintegrowanego Systemu Zarządzania	Pełnomocnik ds. ZSZ
PBI			Polityka bezpieczeństwa informacji	Administrator Bezpieczeństwa Informacji
Poziom procesów zarządzania				
PZ.1.		**Zarządzanie Strategią Gminy**		Zastępca Burmistrza
PZ.2.	PZ.2	**Zarządzanie personelem**		Burmistrz Gminy i Miasta
	PZ.2.1.		Regulamin pracy	Inspektor ds. kadr i szkoleń
	PZ.2.2.		Zasady badania satysfakcji pracowników	Inspektor ds. kadr i szkoleń
	PZ.2.3.		Regulamin wynagradzania	Inspektor ds. kadr i szkoleń
	PZ.2.4.		Zasady podnoszenia kwalifikacji	Inspektor ds. kadr i szkoleń
	PZ.2.5.		Regulamin zatrudniania pracowników	Inspektor ds. kadr i szkoleń
	PZ.2.6.		Zasady prowadzenia służby przygotowawczej	Inspektor ds. kadr i szkoleń
	PZ.2.7.		Regulamin oceny okresowej	Inspektor ds. kadr i szkoleń
	PZ.2.8.		Przewodnik dla nowozatrudnionych pracowników	Inspektor ds. kadr i szkoleń
	PZ.2.9.		Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji	Administrator Bezpieczeństwa Informacji
PZ.3.	PZ.3.	**Zarządzanie finansami**		Skarbnik Gminy
PZ.4.	PZ.4.	**Zarządzanie Oświatą**		Burmistrz Gminy i Miasta
PZ.5.	PZ.5.	**Zarządzanie procesami inwestycyjnymi**		Burmistrz Gminy i Miasta
PZ.6.	PZ.6.	**Doskonalenie zintegrowanego systemu**		Pełnomocnik ds. ZSZ
	PZ.6.1.		Zasady nadzoru nad dokumentami, przepisami prawa i zapisami	Pełnomocnik ds. ZSZ
	PZ.6.2.		Zasady prowadzenia przeglądu zintegrowanego systemu	Pełnomocnik ds. ZSZ
	PZ.6.3.		Audyty jakości	Pełnomocnik ds. ZSZ
	PZ.6.4.		Zasady nadzorowania działań i projektów doskonalących	Pełnomocnik ds. ZSZ
	PZ.6.5.		Zasady nadzorowania niezgodności	Pełnomocnik ds. ZSZ
PZ.7.	PZ.7.	**Zarządzanie ryzykiem**		Burmistrz Gminy i Miasta
	PZ.7.1.		Zasady zarządzania ryzykiem w Urzędzie	Sekretarz Gminy
	PZ.7.2.		Zasady zarządzania ryzykiem zawodowym	Specjalista ds. BHP

Poziom procesów realizacyjnych - obsługi klienta				
PR.1	PR.1	**Obsługa Rady Miejskiej**		Inspektor ds. Obsługi Rady
	PR.1.1		Zasady obsługi Rady Miejskiej	Inspektor ds. Obsługi Rady
PR.2	PR.2	**Usługi administracyjne i obsługa klienta**		Sekretarz Gminy
	PR.2.1.		Zasady świadczenia usług administracyjnych dla klienta	Sekretarz Gminy
	PR.2.2.		Zasady pomiaru zadowolenia klienta	Inspektor ds. promocji i współpracy międzynarodowej
	PR.2.3.		Kodeks etyczny Urzędnika	Sekretarz Gminy
PR.3.	PR.3.	**Obsługa inwestora**		Burmistrz Gminy i Miasta
	PR.3.1.		Zasady obsługi inwestora	Inspektor ds. przedsiębiorczości i sportu
PR.4.	PR.4.	**Zarządzanie majątkiem gminy**		Burmistrz Gminy i Miasta
	PR.4.1.	Usługi wodociągowe i kanalizacyjne		Kierownik RGK
	PR.4.1.1.		Zasady postępowania w przypadku awarii	Kierownik RGK
	PR.4.1.2.		Zasady postępowania przy realizacji nowych przyłączy	Kierownik RGK
	PR.4.1.3.		Zasady postępowania przy realizacji usługi sprzedaży wody i odbioru ścieków	Kierownik RGK
	PR.4.2.	Zarządzanie drogami		Kierownik RGK
	PR.4.3.	Zarządzanie budynkami i obiektami		Kierownik RGK
	PR.4.4.	Zarządzanie gruntami		Kierownik GPS

Poziom procesów wspomagających				
PW.1.	PW.1.	**Zarządzanie bezpieczeństwem informacji, ochroną danych osobowych i informatyzacją urzędu**		Administrator Bezpieczeństwa Informacji
	PW.1.1.		Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji	Administrator systemów informatycznych
	PW.1.2.		Zasady zarządzania siecią teleinformatyczną, kryptografią i kopiami zapasowymi	Administrator systemów informatycznych
	PW.1.3.		Zasady zarządzania incydentami związanymi z bezpieczeństwem informacji	Administrator systemów informatycznych
	PW.1.4.		Zasady zarządzania rozwojem informatycznym	Administrator systemów informatycznych
PW.2.	PW.2.	**Informacja i promocja**		Zastępca Burmistrza
	PW.2.1.		Zasady międzynarodowej współpracy partnerskiej	Inspektor ds. promocji
	PW.2.2.		Zasady komunikacji i promocji	Inspektor ds. promocji
PW.3.	PW.3.1.	**Zamówienia publiczne**		Inspektor ds. zamówień publicznych
	PW.3.1.		Regulamin zakupów	Inspektor ds. zamówień publicznych
PW.4.	PW.4.	**Zarządzanie infrastrukturą urzędu**		Zastępca Burmistrza
	PW.4.1.		Zasady gospodarowania środkami trwałymi i wyposażeniem urzędu	Główny Księgowy Urzędu
	PW.4.2.		Zasady gospodarowania odpadami w urzędzie	Kierownik RGK
PW.5.	PW.5.	**Zarządzanie bezpieczeństwem i higieną pracy pracowników**		Specjalista ds. BHP
	PW.5.1.		Zasady nadzorowania realizacji usług przez podwykonawców	Specjalista ds. BHP
	PW.5.2.		Zasady monitorowania Bezpieczeństwa i Higieny Pracy	Specjalista ds. BHP
	PW.5.3.		Zasady reagowania na wypadki przy pracy, sytuacje potencjalnie wypadkowe i poważne awarie	Specjalista ds. BHP
	PW.5.4.		Zasady prowadzenia instruktażu stanowiskowego	Specjalista ds. BHP
PW.6.	PW.6.	**Zarządzanie ciągłością działania Urzędu**		Burmistrz Gminy i Miasta
	PW.6.1.		Zasady zarządzania ciągłością działania Urzędu	

BURMISTRZ
Dobczyce
Piotr Machnicki

Sekretarz Gminy
Małgorzata Góralik-Piet