ZARZĄDZENIE NR 126/2015
BURMISTRZA GMINY I MIASTA DOBCZYCE

z dnia 30 lipca 2015 r.

w sprawie: wprowadzenia zmienionych wersji:
Zasad zarządzania siecią teleinformatyczną, kryptografią i kopiami zapasowymi,
Procedury: Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji,
Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych

Na podstawie art. 30 ust.1, 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 187/2014 z dnia 1 grudnia 2014 roku wprowadza się następujące zmiany:

1. Wprowadza się nowe wydanie procedury **Zasady zarządzania siecią teleinformatyczną, kryptografią i kopiami zapasowymi** PW.1.2 w brzmieniu określonym w załączniku nr 1 do niniejszego zarządzenia, a która zastępuje załącznik nr 8 do zarządzania nr 187/2014 z 1.12.2014r.
2. 1) Wprowadza się nowe wydanie procedury **Zadania i obowiązki pracowników związane z zapewnieniem bezpieczeństwa informacji,** stanowiące załącznik nr 2 do niniejszego zarządzenia, które wchodzą w strukturę procesów zintegrowanego systemu zarządzania pod numerem PZ.2.9, a która zastępuje załącznik nr 11 do zarządzania nr 187/2014 z 1.12.2014r.
3. Wprowadza się nowe wydanie **Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych**, w brzmieniu określonym w załącznik nr 3 do niniejszego zarządzenia, która zastępuje, załącznik nr 12 do zarządzania nr 187/2014 z 1.12.2014r.

§ 2. 1. Zobowiązuję Pełnomocnika ds. Zintegrowanego Systemu Zarządzania do udostępnienia pracownikom zasad, o których mowa w §1 oraz polityki, o której mowa w §2 przez zamieszczenie ich w portalu intranetowym Qsystem.

2. Zobowiązuję wszystkich pracowników Urzędu Gminy i Miasta Dobczyce do zapoznania się z treścią dokumentów, o których mowa w §1 i do ich przestrzegania.

§ 3. Zarządzenie wchodzi w życie z dniem podjęcia.

BURMISTRZ
Gminy i Miasta Dobczyce
Paweł Machnicki

Załącznik nr [illegible]
do Zarządzenia nr [illegible]
Burmistrza Gminy i Miasta Dobczyce
z dnia 30 lipca 2015 roku

POLITYKA BEZPIECZEŃSTWA INFORMACJI I OCHRONY DANYCH OSOBOWYCH

1. Urząd Gminy i Miasta Dobczyce dba o bezpieczeństwo informacji, podejmując działania zmierzające do zapewniania, że informacje przetwarzanie w Urzędzie są dokładne i kompletne, dostępne na żądanie wyłącznie osobom do tego upoważnionym.
2. Niniejszym dokumentem Burmistrz ustanawia dokumentację opisującą sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę danym przetwarzanym w Urzędzie. Dokumentacja ta wchodzi w Strukturę Procesów Zintegrowanego Systemu Zarzadzania i jest zgodna z normą PN–EN ISO 27001:2014.
3. Przetwarzanie danych osobowych i informacji odbywa się w budynku Urzędu zlokalizowanym w Dobczycach, Rynek 26.
4. Dokumentacja Zintegrowanego Systemu Zarządzania wskazuje:
   a) wykaz zbiorów danych osobowych wraz ze wskazaniem aplikacji zastosowanych do ich przetwarzania,
   b) warunki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych,
   c) opis struktury zbiorów danych ze wskazaniem zawartości pól informacyjnych i powiazania pomiędzy zbiorami, a także sposób przepływu danych pomiędzy systemami.
5. Urząd Gminy i Miasta Dobczyce wspiera procesy zmierzające do zapewnienia bezpieczeństwa danych przez rozwój, wdrażanie, uaktualnianie dokumentacji Zintegrowanego Systemu Zarzadzania obejmującej odpowiednie zasady i procedury obowiązujące wszystkich pracowników i użytkowników informacji.
6. Podstawą działania w tym zakresie jest spełnianie wymogów: ustawy z dnia 29 sierpnia 1997 o ochronie danych osobowych, ustawy z dnia 17 lutego 2005 o informatyzacji działalności podmiotów realizujących zadania publiczne oraz normy PN–EN ISO 27001:2014.
7. Celem polityki jest:
   - spełnienie wymagań prawnych oraz normy PN–EN ISO 27001:2014,
   - zwiększenie świadomości i zaangażowanie pracowników Urzędu w ochronę informacji,
   - zapewnienie bezpieczeństwa usług oferowanych przez Urząd,
   - zmniejszenie ryzyka utraty informacji.
8. Cele te osiągane będą przez:
   - monitorowanie zmian w przepisach prawa,
   - realizację szkoleń dla pracowników Urzędu,
   - identyfikację, opracowanie, wdrożenie i nadzorowanie realizacji procedur, zasad i instrukcji niezbędnych do zapewnienia bezpieczeństwa informacji i ochrony danych osobowych,
   - zarządzanie ryzykiem oraz wdrażanie niezbędnych zabezpieczeń,
   - zarządzanie ciągłością działania i ustanowienie procedur awaryjnych.
9. Struktura Zintegrowanego Systemu Zarzadzania oraz zakres uprawnień i odpowiedzialności określone zostały w Księdze Zintegrowanego Systemu Zarzadzania.
10. Wszyscy pracownicy Urzędu są zobowiązani do przestrzegania zasad Zintegrowanego Systemu Zarządzania.
11. Deklaruje się spełnienie wszystkich wymagań prawnych w zakresie ochrony informacji i ciągłe doskonalenie Zintegrowanego Systemu Zarządzania. Zestawienie zabezpieczeń obowiązujących w Urzędzie opisane zostało w Deklaracji Stosowania.

Dobczyce, 30 lipca 2015 roku

BURMISTRZ
Gminy i Miasta Dobczyce
Paweł Machnicki

Zasady zarządzania siecią teleinformatyczną, kryptografią i kopiami zapasowymi

SPIS TREŚCI

SPIS TREŚCI

1 PRZEDMIOT 2
2 DEFINICJE I OBOWIĄZUJĄCE SKRÓTY 2
3 ZASADY ZARZĄDZANIA BEZPIECZEŃSTWEM TELEINFORMATYCZNYM 2
3.1 Organizacja zasobów sieciowych 2
3.2 Wymagania dotyczące bezpieczeństwa okablowania i zarządzania dostępem do sieci LAN. 2
3.3 Wymagania dotyczące zabezpieczania przed awariami 3
3.4 Wymagania odnośnie obowiązkowego tworzenia kopii zapasowej wyników bieżącej pracy. 3
3.5 Standardy stacji roboczej oraz wymagania okresowego przeglądu stacji 3
3.6 Wymagania dotyczące ochrony przed oprogramowaniem szkodliwym 4
3.7 Zasady przekazywania sprzętu do ponownego użycia 4
3.8 Zasady monitorowania systemów teleinformatycznych 4
3.9 Zasady zapewnienia legalności oprogramowania 4
3.10 Zasady prowadzenia zbiorów danych osobowych 5
4 ZASADY KORZYSTANIA Z ZABEZPIECZEŃ KRYPTOGRAFICZNYCH 5
5 ZASADY ZARZĄDZANIA KOPIAMI BEZPIECZEŃSTWA 5
5.1 Wykonywanie kopii zapasowych 5
5.2 Archiwizowanie kopii zapasowych 6
5.3 Odtwarzanie kopii zapasowych 6
6 DOKUMENTY ZWIĄZANE 6
7 APLIKACJE INFORMATYCZNE 7
8 ZAPISY 7
9 ZAŁĄCZNIKI I FORMULARZE 7

	Imię i nazwisko	Data	Podpis
Opracował:	Michał Ładyga - ASI	30.07.2015	
Właściciel procesu:	Administrator Bezpieczeństwa Informacji		

30.07.2015 BURMISTRZ Gminy i Miasta Dobczyce Paweł Machnicki

1 PRZEDMIOT

Przedmiotem niniejszego dokumentu są zasady zarządzania siecią teleinformatyczną i kryptografią.

2 DEFINICJE I OBOWIĄZUJĄCE SKRÓTY

- **Burmistrz** – Burmistrz Gminy i Miasta Dobczyce;
- **Urząd** – Urząd Gminy i Miasta Dobczyce;
- **ZSZ** – Zintegrowany System Zarządzania;
- **ABI** – Administrator Bezpieczeństwa Informacji;
- **ASI** – Administrator Systemów Informatycznych;
- **Dane wrażliwe** – dane, o których mowa w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych;
- **GIODO** – Generalny Inspektor Ochrony Danych Osobowych;

3 ZASADY ZARZĄDZANIA BEZPIECZEŃSTWEM TELEINFORMATYCZNYM

3.1 Organizacja zasobów sieciowych

1. Sieć Urzędu złożona jest z zasobów teleinformatycznych połączonych ze sobą w sieć lokalną LAN, administrowaną przez pracowników Zespołu ds. obsługi informatycznej.
2. Wszystkie urządzenia przyłączane do sieci LAN muszą spełniać wymagania dotyczące dostępu do sieci, określone w punkcie 3.2.
3. Dopuszcza się dodatkowy podział części sieci LAN na odrębne zbiory zasobów sieciowych w postaci wirtualnych sieci lokalnych (VLAN).
4. Dopuszczalne jest tworzenie dedykowanych lokalnych sieci komputerowych przeznaczonych do przetwarzania informacji niejawnych o ile są one logicznie oddzielone od sieci ogólnego przeznaczenia.
5. Połączenie wewnętrznej sieci Urzędu z Internetem jest realizowane za pośrednictwem dedykowanych urządzeń (UTM, router brzegowy) zapewniających ochronę zasobów komputerowych znajdujących się w sieci Urzędu. Nadzór nad prawidłowym funkcjonowaniem tych urządzeń sprawuje ASI.
6. Kopie konfiguracji urządzeń sieciowych przechowywane są przez ASI na specjalnie do tego celu przeznaczonych serwerach i trwałych nośnikach danych.
7. Jeśli pozwala na to oprogramowanie urządzeń sieciowych, dostęp administracyjny do urządzeń możliwy jest poprzez indywidualne profile chronione hasłami.
8. W sytuacjach wyjątkowych dopuszcza się zdalny dostęp do sieci komputerowej Urzędu dla ASI w celu usunięcia usterek, z zachowaniem wszelkich środków bezpieczeństwa.
9. Zakazane jest wykorzystywanie przez pracowników jakichkolwiek urządzeń do samodzielnego uzyskiwania dostępu do Internetu lub innych sieci zewnętrznych z komputerów podłączonych równocześnie do sieci Urzędu. Użytkownikom zakazuje się również podłączania do sieci komputerowej Urzędu własnych urządzeń.

3.2 Wymagania dotyczące bezpieczeństwa okablowania i zarządzania dostępem do sieci LAN

1. Sieć LAN zabezpieczona jest przed dostępem osób trzecich.
2. Przełączniki sieciowe zamknięte są na klucz w specjalnych szafach w taki sposób, aby możliwa była ich wizualna kontrola.
3. Przełączniki sieciowe są regularnie monitorowane – wizualnie lub zdalnie. Za poprawne działanie odpowiedzialny jest ASI, który prowadzi odpowiednie zapisy z monitorowania w postaci logów urządzenia.
4. Gniazdka sieciowe w poszczególnych pomieszczeniach są aktywne tylko wtedy, gdy są wykorzystywane przez daną stację roboczą lub inne urządzenie sieciowe. Urządzenia podłączone do sieci Urzędu są jednoznacznie identyfikowane i tylko w takim przypadku przypisany jest dostęp do sieci Urzędu.
5. Za poprawne podłączenie urządzeń do sieci LAN oraz właściwą adresacje urządzeń odpowiedzialny jest ASI.

6. Opracowana jest dokumentacja techniczna zawierająca opis i wizualizacje okablowania strukturalnego i elementów aktywnych sieci teleinformatycznej.

3.3 Wymagania dotyczące zabezpieczania przed awariami

1. Wszystkie stacje robocze, serwery, drukarki, przełączniki sieciowe i inny sprzęt informatyczny będący na wyposażeniu Urzędu jest regularnie sprawdzany i konserwowany w celu zapewnienia pełnej dostępności i integralności.
2. Konserwacja zewnętrzna sprzętu obejmuje utrzymanie urządzeń w należytej czystości poprzez wykonywanie takich czynności jak: czyszczenie elementów zewnętrznych (klawiatur, myszy, monitorów itp.).
3. Za utrzymanie urządzeń w należytej czystości odpowiedzialni są użytkownicy.
4. Konserwacja wewnętrzna sprzętu obejmuje usuwanie gromadzącego się wewnątrz stacji roboczych i innych urządzeń kurzu, mogącego spowodować przegrzanie lub niewłaściwą pracę podzespołów, a także akustyczną i wizualną kontrolę podzespołów pod kątem poprawności działania. Za regularną konserwację odpowiedzialny jest Zespół ds. obsługi informatycznej.
5. Sprzęt informatyczny będący na wyposażeniu Urzędu chroniony jest przed potencjalnymi zakłóceniami w sieci zasilającej.
6. Serwery posiadają dedykowane źródło zasilania awaryjnego w postaci UPS-ów. Ich czas działania w przypadku awarii zasilania powinien wystarczyć na nieprzerwaną pracę przynajmniej na czas niezbędny do prawidłowego wyłączenia sprzętu.
7. Stacje robocze podłączane są tylko do gniazdek typu DATA, które podłączone są do wydzielonej sieci elektrycznej. Urządzenia peryferyjne typu drukarki, skanery itp. powinny posiadać zabezpieczenie w postaci listwy przepięciowej.
8. Za kontrolę poprawnego podłączenia sprzętu odpowiedzialni są użytkownicy. Wszelkie nieprawidłowości powinny być natychmiastowo zgłaszane do ASI.

3.4 Wymagania odnośnie obowiązkowego tworzenia kopii zapasowej wyników bieżącej pracy

1. W celu ochrony przed utratą informacji, stosowane jest dedykowane oprogramowanie do automatycznego tworzenia kopii zapasowych ze stacji roboczej do wydzielonego zasobu sieciowego.
2. W przypadku stosowania oprogramowania wymienionego w punkcie 1, użytkownik odpowiada za określenie i wskazanie ASI zakresu danych służbowych podlegających automatycznej kopii zapasowej.
3. Wszelkie kopie zapasowe znajdujące się na serwerach, są archiwizowane i przechowywane w bezpiecznej lokalizacji zapasowej.

3.5 Standardy stacji roboczej oraz wymagania okresowego przeglądu stacji

1. Każda stacja robocza, która ma zostać włączona do sieci informatycznej Urzędu jest przygotowana pod kątem wymagań dla danego stanowiska pracy określonych we wniosku o przyznanie uprawnień do zasobów teleinformatycznych, stanowiącym załącznik F/01 do procedury PW.1.1. Oprócz powyższych wymagań dla każdej stacji roboczej powinno się stosować następujące standardy:
    a. Podzespoły stacji roboczej dobierane są w sposób spełniający wymagania stawiane przez wykorzystywane oprogramowanie.
    b. System operacyjny stacji roboczych skonfigurowany jest w sposób uniemożliwiający użytkownikowi modyfikację kluczowych parametrów systemu, instalację oraz usuwanie dodatkowego sprzętu i oprogramowania.
    c. Dostęp administracyjny do systemu operacyjnego każdej stacji roboczej posiada ASI.
    d. Każda stacja robocza zabezpieczona jest przed oprogramowaniem szkodliwym.
2. ASI dokonuje okresowego przeglądu funkcjonujących w sieci Urzędu stacji roboczych, który obejmuje: czyszczenie komputera, analizę przestrzeni dyskowej pod względem występowania zbędnych plików, analizę podzespołów pod kątem występowania błędów oraz analizę poprawności działania urządzeń peryferyjnych. Z przeglądów tych prowadzi odpowiednie zapisy.
3. Każdy użytkownik stacji roboczej zobowiązany jest do natychmiastowego zgłaszania ASI wszelkich zauważonych uszkodzeń stacji roboczej.

3.6 Wymagania dotyczące ochrony przed oprogramowaniem szkodliwym

1. Każda stacja robocza podłączona do sieci informatycznej Urzędu posiada oprogramowanie chroniące przed oprogramowaniem szkodliwym (tj. wirusy, robaki internetowe, programy szpiegowskie i wyłudzające poufne informacje osobiste). Oprogramowanie musi być aktywne przez cały czas działania stacji roboczej.
2. Wszystkie stacje robocze oraz serwery mają opracowane jednolite zasady konfiguracji oraz regularnego uaktualniania programów antywirusowych.
3. Proces aktualizacji bazy danych oprogramowania antywirusowego przebiega automatycznie bez interwencji użytkownika.
4. Każda stacja robocza poddawana jest regularnym testom przez program antywirusowy na obecność oprogramowania szkodliwego. Pełne skanowanie systemu przeprowadzane jest nie rzadziej niż co 14 dni. Skanowanie obszarów krytycznych systemu operacyjnego wykonywane jest przy każdym uruchomieniu systemu.
5. Wskazane jest aby w miarę możliwości technicznych stosować narzędzia administracyjne umożliwiające centralny nadzór nad konfiguracją oprogramowania antywirusowego zainstalowanego na stacjach roboczych. Ponadto narzędzia takie powinny umożliwiać monitorowanie stanu ochrony i raportów dotyczących bezpieczeństwa każdego komputera.
6. Każdy użytkownik komputera zobowiązany jest do przestrzegania podstawowych zasad ochrony wymienionych w punkcie 6.2 procedury PZ.2.9.

3.7 Zasady przekazywania sprzętu do ponownego użycia

1. W przypadku przekazywania sprzętu komputerowego do ponownego użycia, należy zadbać o trwałe usunięcie z nośników danych wszystkich informacji chronionych, przetwarzanych na przekazywanym sprzęcie. W sytuacji, gdy nośnik zawiera dane poufne, należy go wycofać z przekazywanego sprzętu.
2. Jeśli zachodzi konieczność użyczenia lub awaryjnego wykorzystania w innej lokalizacji sprzętu teleinformatycznego, należy uprzednio stworzyć kopię zapasową konfiguracji urządzenia, a następnie przywrócić sprzęt do ustawień fabrycznych.
3. Za wszystkie czynności związane z przygotowywaniem do przekazania nośników informacji i urządzeń teleinformatycznych odpowiada ASI.

3.8 Zasady monitorowania systemów teleinformatycznych

1. ASI zobowiązany jest do regularnego monitorowania poprawności działania systemów teleinformatycznych Urzędu.
2. Monitoring obejmuje wszystkie punkty istotne ze względu na zapewnienie ciągłości funkcjonowania systemów.
3. W miarę możliwości technicznych urządzenia sieciowe posiadają funkcje alarmowe, umożliwiające automatyczne powiadamianie ASI o wystąpieniu sytuacji wyjątkowych.

3.9 Zasady zapewnienia legalności oprogramowania

1. Na każdym serwerze i każdej stacji roboczej będącej na wyposażeniu Urzędu znajduje się tylko takie oprogramowanie, którego pochodzenie jest legalne i zainstalowane jest ono zgodnie z zapisami obowiązującymi w przypisanej do niego licencji. O rodzaju zainstalowanego oprogramowania i jego wersji decyduje ASI w momencie przygotowania sprzętu i oddania go do użytku.
2. Zabrania się dokonywania modyfikacji, usuwania i instalowania oprogramowania bez wiedzy i zgody ASI.
3. Jeżeli na danej stacji roboczej zachodzi potrzeba dodania lub modyfikacji programu niezbędnego do poprawnego wykonywania obowiązków służbowych, użytkownik zobowiązany jest poinformować o tym fakcie ASI, który sprawdza możliwość jego zainstalowania lub aktualizacji pod kątem zapisów w licencji i dokonuje modyfikacji.
4. Zabrania się użytkowania na stacjach roboczych Urzędu oprogramowania nie instalowanego bezpośrednio na komputerze (portable) a uruchamianego np. z pamięci przenośnej. Użytkownik ponosi pełną odpowiedzialność, w przypadku jeżeli efekty wykorzystania takiego oprogramowania (np. powstałe dokumenty) wskazywać będą, że zostały one stworzone przy użyciu nielegalnego oprogramowania.
5. ASI prowadzi wykaz posiadanych przez Urząd licencji wraz z wykazem sprzętów, do których są one przypisane.

6. W przypadku wykrycia oprogramowania znajdującego się na stacji roboczej niezgodnie z powyższymi regułami, ASI niezwłocznie usuwa to oprogramowanie wraz z plikami utworzonymi przy jego pomocy.

3.10 Zasady prowadzenia zbiorów danych osobowych

1. Wszystkie zbiory danych osobowych podlegają zgłoszeniu do rejestru prowadzonego przez ABI.
2. ABI decyduje o konieczności zgłoszenia zbioru danych do rejestracji GIODO, uwzględniając rodzaj przetwarzanych w zbiorze danych i obowiązujące w tym zakresie przepisy prawne.
3. W Urzędzie prowadzi się jawny rejestr zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania, na formularzu F/01 do PW.1.2.
4. Zgłoszenie nowego lub wykreślenia zbioru danych osobowych wymaga aktualizacji rejestru. Za aktualizację rejestru odpowiada ABI.
5. Za zgłoszenie zbioru danych do rejestracji oraz aktualizacji lub wykreślenia zbioru danych odpowiada Kierownik Referatu i osoby zatrudnione na samodzielnych stanowiskach, w których prowadzony jest zbiór.
6. Pracownicy merytoryczni w porozumieniu z Kierownikami Referatów, przed rozpoczęciem przetwarzania danych osobowych w zbiorze zgłaszają zbiór do rejestracji ABI, na formularzu F/03 do PW.1.2.
7. Kierownicy referatów zobowiązani są zgłaszać ABI każdą zmianę informacji dotyczącą przetwarzanych przez podległych im pracowników zbiorów danych osobowych w terminie 20 dni od dnia dokonania zmiany w zbiorze, z zastrzeżeniem pkt. 7, na formularzu F/03 do PW.1.2.
8. Jeśli zmiana informacji dotycząca przetwarzanych zbiorów danych osobowych dotyczy rozszerzenia zakresu przetwarzanych danych o dane wrażliwe Kierownicy Referatów zobowiązani są do jej zgłoszenia przed dokonaniem zmiany w zbiorze.

4 ZASADY KORZYSTANIA Z ZABEZPIECZEŃ KRYPTOGRAFICZNYCH

1. Zabezpieczenia kryptograficzne stosuję się w Urzędzie w celu uwierzytelniania dokumentów i osób podczas komunikacji z klientem.
2. Dostęp do zabezpieczeń kryptograficznych posiadają wybrane osoby. Wyznaczane są one przez Burmistrza na podstawie zakresu obowiązków lub pełnionej funkcji.
3. Każda z osób mających dostęp do zabezpieczeń kryptograficznych posiada przypisany imiennie klucz, którym posługuje się w zakresie wykonywanych obowiązków.
4. Osoby korzystające z zabezpieczeń zobowiązane są do szczególnej uwagi w zakresie przechowywania kart dostępu, kodów PIN i innych zabezpieczeń tak, aby nie dostały się one do osób nieuprawnionych oraz do nie udostępniania informacji o zabezpieczeniach.
5. Wykaz osób posiadających dostęp do zabezpieczeń prowadzi ASI.
6. W przypadku korzystania ze znajdujących się na ewidencji wymiennych elektronicznych nośników informacji poza Urzędem stosuje się funkcje szyfrujące dla zawartych na nich informacji.
7. Wymagane jest także, aby stosować funkcje szyfrujące dla połączeń realizowanych na potrzeby zdalnej pomocy technicznej, świadczonej przez zewnętrznych dostawców.

5 ZASADY ZARZĄDZANIA KOPIAMI BEZPIECZEŃSTWA

5.1 Wykonywanie kopii zapasowych

1. Dane i funkcje systemów teleinformatycznych sklasyfikowane są jako krytyczne, jeśli niedostępność tych systemów uniemożliwi funkcjonowanie Urzędu (np. dany proces nie może być wykonywany bez użycia komputerów), a skutki tej niedostępności będą negatywne dla Urzędu. Kopie bezpieczeństwa informacji znajdujących się w systemach sklasyfikowanych jako krytyczne powinny być wykonywane codziennie. Za klasyfikację danych i systemów odpowiada ASI, w porozumieniu z ABI i Kierownikami Referatów.
2. Dane i funkcje systemów teleinformatycznych powinny być sklasyfikowane jako zwykłe, jeśli niedostępność tych systemów nie będzie mieć negatywnego wpływu na funkcjonowanie Urzędu. Kopie bezpieczeństwa informacji znajdujących się w systemach sklasyfikowanych jako zwykłe powinny być wykonywane przynajmniej raz w tygodniu.
3. Procedury dotyczące wykonywania kopii bezpieczeństwa uwzględniają zarówno potrzeby Urzędu, jak i aktualny stan przepisów prawa.
4. Jeśli kopia bezpieczeństwa obejmuje cały serwer, częstotliwość wykonywania kopii bezpieczeństwa

tego serwera jest równa częstotliwości wykonywania kopii bezpieczeństwa najbardziej krytycznej aplikacji znajdującej się na tym serwerze.

5. Kopie bezpieczeństwa serwerów wykonywane są przed każdą aktualizacją systemu lub czynnością serwisową jeśli standardowa częstotliwość wykonywania kopii jest większa niż jeden dzień lub jeśli kopie standardowe wykonywane są przyrostowo.
6. Pliki zawierające kopie zapasowe danych z systemów krytycznych przechowywane są co najmniej do czasu utworzenia czwartej kopii, tzn. zawsze powinny być dostępne co najmniej trzy ostatnie kopie.
7. Pliki zawierające kopie zapasowe danych z systemów sklasyfikowanych jako zwykłe przechowywane są co najmniej do czasu utworzenia drugiej kopii, tzn. zawsze powinna być dostępna co najmniej jedna kopia.
8. Pliki zawierające kopie zapasowe opatrzone są nazwą wskazującą źródło kopii zapasowej oraz czas jej wykonania, w miarę możliwości technicznych kopie zapasowe danych zgromadzonych na serwerach i stacjach roboczych wykonywane są w sposób automatyczny.
9. Wskazane jest, aby kopie zapasowe wykonywane były poza godzinami pracy Urzędu. W uzasadnionych przypadkach kopie zapasowe mogą być wykonywane w godzinach pracy Urzędu, w sposób niezakłócający pracy innych systemów teleinformatycznych.
10. Wszystkie operacje związane z wykonywaniem kopii zapasowych i archiwizacji danych z systemów krytycznych rejestrowane są przez system wykonujący kopie zapasowe.

5.2 Archiwizowanie kopii zapasowych

1. Kopie bezpieczeństwa danych zawartych w systemach krytycznych archiwizowane są przynajmniej raz w tygodniu i przechowywane w bezpiecznej lokalizacji poza siedzibą Urzędu.
2. Dopuszcza się przechowywanie archiwum kopii bezpieczeństwa danych z systemów krytycznych w zdalnej lokalizacji dostępnej poprzez Internet. Pliki zgromadzone w zdalnej lokalizacji są szyfrowane, a dostęp do zdalnego zasobu odbywa się z wykorzystaniem bezpiecznego połączenia internetowego.
3. Kopie bezpieczeństwa danych zawartych w systemach sklasyfikowanych jako zwykłe archiwizowane są przynajmniej raz w miesiącu i przechowywane w bezpiecznej lokalizacji poza siedzibą Urzędu. Dopuszcza się, aby archiwa danych z systemów „zwykłych" były przechowywane w szafie pancernej zlokalizowanej w siedzibie Urzędu.
4. Kopie zapasowe danych chronionych muszą być archiwizowane zgodnie z procedurami obejmującymi przechowywanie informacji chronionych na trwałych nośnikach danych.
5. Do celów archiwizacyjnych nie należy wykorzystywać mediów, które nie stanowią wiarygodnego sposobu przechowywania informacji.

5.3 Odtwarzanie kopii zapasowych

1. Odtwarzanie danych zawartych w kopiach zapasowych i archiwach przeprowadzane jest zgodnie z instrukcjami odtworzeniowymi, opracowanymi i przechowywanymi przez ASI.
2. ASI przeprowadza okresowe testy odtwarzania danych. Procedura odtwarzania danych produkcyjnych przeprowadzana jest w środowisku testowym. Z prowadzonych testów ASI prowadzi odpowiednie zapisy. może być mniejsza niż raz na trzy miesiące.
3. Dla systemów sklasyfikowanych jako zwykłe testowa procedura odtwarzania danych nie może być wykonywana rzadziej niż raz na 6 miesięcy.
4. ASI prowadzi dziennik testowego odtwarzania danych, w którym znajduje się data odtwarzania, nazwa odtwarzanych danych i wynik operacji. Dziennik ten, stanowiący załącznik F/02 i może być prowadzony w postaci elektronicznej.
5. Odtworzenie pliku wiąże się z odtworzeniem jego lokalizacji w systemie plików. Plik odtwarzany nie powinien być przekazany użytkownikowi w żaden inny sposób.
6. Poza procesem testowania kopii bezpieczeństwa dane mogą być odzyskiwane tylko i wyłącznie przez osoby upoważnione przez ABI.

6 DOKUMENTY ZWIĄZANE

- Zgłoszenia zbiorów danych do GIODO.

7 APLIKACJE INFORMATYCZNE

Qsystem

8 ZAPISY

Brak

9 ZAŁĄCZNIKI I FORMULARZE

Lp.	Nazwa	Lokalizacja, nazwa pliku
1	Wykaz zbiorów danych osobowych F/01	Qsystem
2	Rejestr odtwarzania kopii bezpieczeństwa F/02	Qsystem
3	Zgłoszenie zbioru danych do rejestracji F/03	Qsystem

Formularz F/01 do PW.1.2

L.p.	Nazwa zbioru danych	Oznaczenie Administratora Danych, adres siedziby, numer REGON	Oznaczenie podmiotu, któremu powierzono przetwarzanie danych na podstawie umowy lub porozumienia i adres jego siedziby	Podstawa upoważenia prowadzenia danych	Podstawa prawna ochrony danych i informacji	Data wpisu zbioru do rejestru	Data ostatniej aktualizacji informacji	Data wykreślenia zbioru z rejestru
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								

Historia zmian w dokumencie:

Data	Rodzaj zmiany (nowy wpis, aktualizacja, wykreślenie)	Zakres zmiany

Rejestr odtwarzania kopii bezpieczeństwa

Formularz F/03 do PW.1.2

Nazwa systemu	Nazwa zadania	Klasyfikacja systemu (krytyczne/zwykłe)	Data odtwarzania	Status	Uwagi

ZGŁOSZENIE ZBIORU DANYCH DO REJESTRACJI

☐ zgłoszenie zbioru na podstawie art. 36a ust. 2 pkt. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),

☐ zgłoszenie zbioru na podstawie art. 40 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),

☐ zgłoszenie zbioru, w którym będą przetwarzane dane określone w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,

☐ zgłoszenie zmian w zarejestrowanym zbiorze danych.

Część A. Wniosek

Wnoszę o wpisanie zbioru danych osobowych o nazwie:

Zbiór danych osobowych przetwarzany jest:
☐ W programie komputerowym o nazwie:
☐ w postaci tradycyjnej (wyłącznie papierowej).

Część B. Charakterystyka

Dane zgłaszającego

1. Powierzenie przetwarzania danych osobowych:

☐ administrator danych powierzył w drodze umowy zawartej na piśmie przetwarzanie danych innemu podmiotowi (art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych),
☐ administrator danych przewiduje powierzenie przetwarzania danych innemu podmiotowi.

W przypadku powierzenia przetwarzania danych innemu podmiotowi podaj nazwę i adres siedziby lub nazwisko, imię i adres miejsca zamieszkania podmiotu, któremu powierzono przetwarzanie danych osobowych:

2. Podstawa prawna upoważniająca do prowadzenia zbioru danych:

☐ zgoda osoby, której dane dotyczą, na przetwarzanie danych jej dotyczących,

☐ przetwarzanie jest niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa:
- ☐Ustawa z dnia 7 września 1991 r. o systemie oświaty (Dz. U. z 2004 r. Nr 256, poz. 2572 z późn. zm.)
- ☐Ustawa z dnia 19 lutego 2004 r. o systemie informacji oświatowej (Dz. U. Nr 49, poz. 463 z późn. zm.)
- ☐Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2001 r. Nr 142, poz. 1591 z późn. zm.)
- ☐Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2000 r. Nr 98, poz. 1071 z późn. zm.)
- ☐Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2006 r. Nr 97, poz. 673 z późn. zm.)
- ☐Ustawa z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (Dz. U. z 2006 r. Nr 139, poz. 993 z późn. zm.)
- ☐Ustawa z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepe3nosprawnych (Dz. U. z 2010 r. Nr 214 poz. 1407 z późn. zm.)
- ☐Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (Dz. U. z 2007 r. Nr 70, poz. 473 z późn. zm.)

☐Ustawa z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2005 r. Nr 229, poz. 1954 z późn. zm.)
☐Ustawa z dnia 17 maja 1989 r. Prawo geodezyjne i kartograficzne (Dz. U. z 2010 r. Nr 193, poz. 1287 z późn. zm.)
☐Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. Nr 112, poz. 1198 z późn. zm.)
☐Ustawa z dnia 12 marca 2004 r. o pomocy społecznej (Dz. U. z 2009 r. Nr 175, poz. 1362 z późn. zm.)
☐Ustawa z dnia 28 listopada 2003 r. o świadczeniach rodzinnych (Dz. U. z 2006 r. Nr 139, poz. 992 z późn. zm.)
☐Ustawa z dnia 21 czerwca 2001 r. o dodatkach mieszkaniowych (Dz. U. Nr 71, poz. 734 z późn. zm.)
☐Ustawa z dnia 7 września 2007 r. o pomocy osobom uprawnionym do alimentów (Dz. U. z 2009 r. Nr 1, poz. 7 z późn. zm.)
☐Inne, jakie?

☐ przetwarzanie jest konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,

☐ przetwarzanie jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego – w przypadku odpowiedzi twierdzącej , należy opisać te zadania:

☐ przetwarzanie jest niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Część C. Cel przetwarzania danych, opis kategorii osób, których dane dotyczą, oraz zakres przetwarzanych danych

3. Cel przetwarzania danych w zbiorze: *proszę dokładnie opisać cel, dla którego administrator przetwarza dane w zbiorze, np. realizacja zadań ustawowych-prowadzenie ewidencji ludności:*

4. Opis kategorii osób, których dane dotyczą, *np. osoby fizyczne, osoby prawne, klienci, darczyńcy, wnioskodawcy, itp*:

5. Zakres przetwarzanych w zbiorze danych o osobach:

☐ nazwiska i imiona,
☐ imiona rodziców,
☐ data urodzenia,
☐ miejsce urodzenia,
☐ adres zamieszkania lub pobytu,
☐ numer ewidencyjny PESEL,
☐ Numer Identyfikacji Podatkowej,
☐ miejsce pracy
☐ zawód,
☐ wykształcenie,
☐ seria i numer dowodu osobistego,
☐ numer telefonu

6. Inne dane osobowe, oprócz wymienionych w pkt 5, przetwarzane w zbiorze – należy podać jakie: np. *stan cywilny, nazwisko rodowe, itp.*

7. Dane przetwarzane w zbiorze, na podstawie art. 27 ust. 1 ustawy:
a) ujawniają bezpośrednio lub w kontekście:

☐ pochodzenie rasowe,
☐ pochodzenie etniczne,
☐ poglądy polityczne,
☐ przekonania religijne,
☐ przekonania filozoficzne,
☐ przynależność wyznaniową,
☐ przynależność partyjną,
☐ przynależność związkową,
☐ stan zdrowia,
☐ kod genetyczny
☐ nałogi,
☐ życie seksualne,

b) dotyczą:

☐ skazań,
☐ mandatów karnych,
☐ orzeczeń o ukaraniu,
☐ innych orzeczeń wydanych w postępowaniu sądowym

lub administracyjnym

Jeśli nie zakreślono żadnej odpowiedzi, należy przejść od razu do pkt 9.

8. Podstawa prawna przetwarzania danych wskazanych w pkt 7:

☐ osoby, których dane dotyczą, będą wyrażać na to zgodę na piśmie,

☐ przepis szczególny innej ustawy zezwala na przetwarzanie bez zgody osoby, której dane dotyczą, jej danych osobowych – w przypadku odpowiedzi twierdzącej, należy podać odniesienie do przepisu tej ustawy:

☐Ustawa z dnia 7 września 1991 r. o systemie oświaty (Dz. U. z 2004 r. Nr 256, poz. 2572 z późn. zm.)
☐Ustawa z dnia 19 lutego 2004 r. o systemie informacji oświatowej (Dz. U. Nr 49, poz. 463 z późn. zm.)
☐Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2001 r. Nr 142, poz. 1591 z późn. zm.)
☐Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2000 r. Nr 98, poz. 1071 z późn. zm.)
☐Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2006 r. Nr 97, poz. 673 z późn. zm.)
☐Ustawa z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (Dz. U. z 2006 r. Nr 139, poz. 993 z późn. zm.)
☐Ustawa z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepe3nosprawnych (Dz. U. z 2010 r. Nr 214 poz. 1407 z późn. zm.)
☐Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (Dz. U. z 2007 r. Nr 70, poz. 473 z późn. zm.)
☐Ustawa z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2005 r. Nr 229, poz. 1954 z późn. zm.)
☐Ustawa z dnia 17 maja 1989 r. Prawo geodezyjne i kartograficzne (Dz. U. z 2010 r. Nr 193, poz. 1287 z późn. zm.)
☐Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. Nr 112, poz. 1198 z późn. zm.)
☐Ustawa z dnia 12 marca 2004 r. o pomocy społecznej (Dz. U. z 2009 r. Nr 175, poz. 1362 z późn. zm.)
☐Ustawa z dnia 28 listopada 2003 r. o świadczeniach rodzinnych (Dz. U. z 2006 r. Nr 139, poz. 992 z późn. zm.)
☐Ustawa z dnia 21 czerwca 2001 r. o dodatkach mieszkaniowych (Dz. U. Nr 71, poz. 734 z późn. zm.)
☐Ustawa z dnia 7 września 2007 r. o pomocy osobom uprawnionym do alimentów (Dz. U. z 2009 r. Nr 1, poz. 7 z późn. zm.)
☐Inne, jakie?

☐ przetwarzanie danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora,

☐ przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem,

☐ przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie,

☐ przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych,

☐ przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą,

☐ przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

Część D. Sposób zbierania oraz udostępniania danych

9. Dane do zbioru będą zbierane:

☐ od osób, których dotyczą,
☐ z innych źródeł niż osoba, której dane dotyczą.

10. Dane ze zbioru będą udostępniane:

☐ podmiotom innym, niż upoważnione na podstawie przepisów prawa.

11. Odbiorcy lub kategorie odbiorców, którym dane mogą być przekazywane – należy podać nazwę i adres siedziby lub nazwisko, imię i adres miejsca zamieszkania odbiorcy danych:

12. Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego – należy podać nazwę państwa:

Część E. – WYPEŁNIA ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI
Opis środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36-39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

13. Zbiór danych osobowych jest prowadzony:

a) ☐ centralnie,
☐ w architekturze rozproszonej,

b) ☐ wyłącznie w postaci papierowej,
☐ z użyciem systemu informatycznego,

c) ☐ z użyciem co najmniej jednego urządzenia systemu informatycznego służącego do przetwarzania danych osobowych połączonego z siecią publiczną (np. Internetem),
☐ bez użycia żadnego z urządzeń systemu informatycznego służącego do przetwarzania danych osobowych połączonego z siecią publiczną (np. Internetem).

14. Zostały spełnione wymogi określone w art. 36-39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych: [1]

a) ☐ został wyznaczony administrator bezpieczeństwa informacji nadzorujący przestrzeganie zasad ochrony przetwarzanych danych osobowych,
☐ administrator danych sam wykonuje czynności administratora bezpieczeństwa informacji,

b) ☐ do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych

c) ☐ prowadzona jest ewidencja osób upoważnionych do przetwarzania danych,

d)☐ została opracowana i wdrożona polityka bezpieczeństwa,

e)☐ została opracowana i wdrożona instrukcja zarządzania systemem informatycznym,

f) ☐ inne środki, oprócz wymienionych w ppkt a - e, zastosowane w celu zabezpieczenia danych:

Środki ochrony fizycznej danych:
☐ Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi).
☐ Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności ogniowej >= 30 min.
☐ Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie - drzwi klasy C.
☐ Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej.
☐ Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy.
☐ Dostęp do pomieszczeń, w których przetwarzany jest zbiory danych osobowych objęte są systemem kontroli dostępu.
☐ Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych.
☐ Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony.
☐ Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych przez cała dobę jest nadzorowany przez służbę ochrony.
☐ Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej niemetalowej szafie.
☐ Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej metalowej szafie.
☐ Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętym sejfie lub kasie pancernej.

---

[1] Administrator danych prowadzący zbiór w systemie tradycyjnym (papierowym) zobowiązany jest do zastosowania środków określonych w pkt 14 ppkt a-d, a w przypadku prowadzenia zbioru w systemie informatycznym, ponadto środka określonego w pkt 14 ppkt e.

☐ Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej niemetalowej szafie.
☐ Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej metalowej szafie.
☐ Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętym sejfie lub kasie pancernej.
☐ Zbiory danych osobowych przetwarzane są w kancelarii tajnej, prowadzonej zgodnie z wymogami określonymi w odrębnych przepisach.
☐ Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.
☐ Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentow.

Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:
☐ Zbiór danych osobowych przetwarzany jest przy użyciu komputera przenośnego.
☐ Komputer służący do przetwarzania danych osobowych nie jest połączony z lokalną siecią komputerową.
☐ Zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
☐ Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej/ komputerze przenośnym zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS.
☐ Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
☐ Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem karty procesorowej oraz kodu PIN lub tokena.
☐ Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem technologii biometrycznej.
☐ Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.
☐ Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł.
☐ Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.
☐ Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.
☐ Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
☐ Zastosowano procedurę oddzwonienia (callback) przy transmisji realizowanej za pośrednictwem modemu.
☐ Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamieci dyskowej.
☐ Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
☐ Użyto system Firewall do ochrony dostępu do sieci komputerowej.
☐ Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej.

Środki ochrony w ramach narzędzi programowych i baz danych:
☐ Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.
☐ Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.
☐ Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
☐ Dostęp do zbioru danych osobowych wymaga uwierzytelnienia przy użyciu karty procesorowej oraz kodu PIN lub tokena.
☐ Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem technologii biometrycznej.
☐ Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
☐ Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.
☐ Zastosowano kryptograficzne środki ochrony danych osobowych.
☐ Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
☐ Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

Środki organizacyjne:

☐ Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.

☐ Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.

☐ Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy.

☐ Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.

☐ Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

Inne, jakie?

Część F.

Informacja o sposobie wypełnienia warunków technicznych i organizacyjnych, o których mowa w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024)

15. Zastosowano środki bezpieczeństwa na poziomie[2]:

☐ podstawowym,
☐ podwyższonym,
☐ wysokim,

[2] Należy wskazać odpowiedni poziom bezpieczeństwa określony w § 6 ww. rozporządzenia (UWAGA! Dotyczy wyłącznie administratorów przetwarzających dane w systemie informatycznym);
– jeżeli wnioskodawca przetwarza dane wymienione w pkt 7 zgłoszenia, należy zastosować środki bezpieczeństwa przynajmniej na poziomie podwyższonym;
– w przypadku, gdy przynajmniej jedno urządzenie systemu informatycznego służącego do przetwarzania danych osobowych połączone jest z siecią publiczną, należy zastosować środki bezpieczeństwa na poziomie wysokim;
– w pozostałych przypadkach wystarczające jest zastosowanie środków bezpieczeństwa na poziomie podstawowym.

ZADANIA I OBOWIĄZKI PRACOWNIKÓW ZWIĄZANE Z ZAPEWNIENIEM BEZPIECZEŃSTWA INFORMACJI

1 Przedmiot i zakres regulaminu 2
2 Definicje i obowiązujące skróty 2
3 Polityka personalna w zakresie zarządzania bezpieczeństwem informacji i ochrony danych osobowych 2
3.1 Tryb postępowania związany z nadawaniem uprawnień nowo zatrudnionym pracownikom 3
3.2 Zasady obowiązujące Wykonawców, stażystów i osoby trzecie 3
3.3 Postępowanie dyscyplinujące 3
3.4 Zmiany miejsca pracy oraz ustanie stosunku pracy 4
3.5 Zasady obowiązujące Administratorów Systemów Informatycznych 4
4 Kształtowanie świadomości znaczenia bezpieczeństwa informacji 4
5 Zasady postępowania użytkownika zasobów teleinformatycznych 4
5.1 Szczegółowe zasady postępowania użytkownika zasobów teleinformatycznych 5
5.2 Przetwarzanie informacji na stanowisku pracy 7
5.3 Ochrona przed oprogramowaniem szkodliwym 7
5.4 Postępowanie z elektronicznymi nośnikami informacji 7
5.5 Nadzór nad dokumentami drukowanymi 8
5.6 Wykorzystywanie zasobów teleinformatycznych poza siedzibą Urzędu 8
5.7 Przetwarzanie danych osobowych 9
5.8 Rejestr incydentów i problemów związanych z bezpieczeństwem 9
6 Dokumenty związane 9
7 Aplikacje informatyczne 10
8 Załączniki i formularze 10

	Imię i nazwisko	Data	Podpis
Opracował:	Małgorzata Góralik-Piętka	30.07.2015	
Właściciel procesu:	Administrator Bezpieczeństwa Informacji		

30.07.2015 Burmistrz Gminy i Miasta Dobczyce Paweł Machnicki

1 Przedmiot i zakres regulaminu

Przedmiotem regulaminu jest określenie zasad, które muszą zostać spełnione przez pracowników Urzędu w celu wdrożenia i utrzymania systemu zarządzania bezpieczeństwem informacji oraz ochrony danych osobowych.

Zasady te muszą być przestrzegane, by zapewnić odpowiednie przygotowanie pracowników przed ich upoważnieniem do przetwarzania danych oraz umożliwieniem im dostępu do danych, a także odebranie uprawnień w przypadku rozwiązania stosunku pracy lub zmiany zakresu zadań i upoważnień. Ponadto regulamin ten zapewnia odpowiedni poziom świadomości i odpowiedzialności z zakresu bezpieczeństwa.

2 Definicje i obowiązujące skróty

- **Burmistrz** – Burmistrz Gminy i Miasta Dobczyce;
- **Urząd** – Urząd Gminy i Miasta Dobczyce.
- **ZSZ – ZSZ** – Zintegrowany System Zarządzania;
- **ABI** – Administrator Bezpieczeństwa Informacji;
- **Właściciel systemu teleinformatycznego** – Kierownik referatu merytorycznego lub pracownik na samodzielnym stanowisku, którzy w ramach realizowanych w referatach lub na stanowiskach pracy zadań merytorycznych są głównym użytkownikiem systemu teleinformatycznego;
- **Właściciel aktywu** – Kierownik referatu oraz osoby na samodzielnych stanowiskach pracy odpowiedzialne za realizację zadań Urzędu, m.in. w procesach ZSZ;
- **Polityka bezpieczeństwa** – polityka bezpieczeństwa informacji i ochrony danych osobowych;

3 Polityka personalna w zakresie zarządzania bezpieczeństwem informacji i ochrony danych osobowych

Polityka personalna obowiązuje wszystkich pracowników Urzędu, osoby zatrudnione tymczasowo oraz dostawców i ich pracowników. Wszyscy pracownicy Urzędu oraz osoby związane bezpośrednio z funkcjonowaniem Urzędu odpowiedzialni są za bezpieczeństwo informacji oraz aktywa informacyjne Urzędu.

Wszyscy pracownicy Urzędu, osoby związane umowami, dostawcy oraz osoby posiadające dostęp do pomieszczeń Urzędu muszą przestrzegać standardów określonych w polityce bezpieczeństwa Urzędu. W ich zakresie obowiązków znajduje się zapis o odpowiedzialności za bezpieczeństwo informacji oraz danych osobowych.
Wszyscy użytkownicy powinni zapoznać się z wymaganiami ZSZ, a w szczególności zasadami bezpieczeństwa danych i ochrony danych osobowych. Pracownicy muszą zobowiązać się na piśmie do przestrzegania zasad obowiązujących w zakresie bezpieczeństwa danych osobowych. Wszelkie pytania dotyczące bezpieczeństwa danych kierowane powinny być do ABI.

Przed uzyskaniem dostępu do pomieszczeń oraz informacji Urzędu wszyscy pracownicy muszą podpisać wymagane przepisami prawa oświadczenia i przyrzeczenia o zachowaniu tajemnic ustawowo chronionych. Podpisane oświadczenia wpinane są do akt osobowych pracowników.
Przed uzyskaniem dostępu do strefy przetwarzania danych osobowych oraz do samych danych osobowych wszyscy pracownicy Urzędu muszą podpisać oświadczenie pracownika dotyczące ochrony danych osobowych oraz uzyskać upoważnienie do przetwarzania danych osobowych.

3.1 Tryb postępowania związany z nadawaniem uprawnień nowo zatrudnionym pracownikom

Tryb postępowania związany z nadawaniem uprawnień dostępu do urzędu i do danych osobowych określone są w Procesach PZ.2 Zarządzanie personelem oraz PW.1. Zarzadzanie bezpieczeństwem informacji, ochroną danych osobowych i informatyzacją urzędu.

3.2 Zasady obowiązujące Wykonawców, stażystów i osoby trzecie

W umowach z Wykonawcami, w przypadkach gdy mają oni dostęp do danych Urzędu powinny znaleźć się zapisy dotyczące ochrony danych. Dopuszczalne jest podpisanie odrębnej umowy dotyczącej ochrony i przetwarzania danych z dostawcą. Istotne postanowienia umowy dotyczące ochrony informacji i przetwarzania danych osobowych zawiera załącznik Z/01. Sformułowane w załączniku istotne postanowienia umowy mogą być włączone do umowy zasadniczej, przy realizacji której zachodzi konieczność przetwarzania danych. W przypadku powierzenia przetwarzania danych odrębną umową istotne postanowienia umowy dotyczące ochrony informacji i przetwarzania danych osobowych należy rozszerzyć o odpowiednie zapisy i odpowiednio zmodyfikować. Natomiast w umowie zasadniczej należy wprowadzić zapisy dodatkowe dotyczące rozwiązania lub odstąpienia od umowy zasadniczej w przypadku kiedy Wykonawca utraci uprawnienie do przetwarzania danych.

Na umowach, w których zawarte są zapisy dotyczące ochrony i przetwarzania danych osobowych powinna znajdować się parafka ABI. W umowach tych można wymienić z imienia i nazwiska oraz funkcji osoby, które będą upoważnione do dostępu do zasobów Urzędu. Imienne upoważnienia do przetwarzania danych wydawane są przez Administratora Danych lub przez ABI (jeśli posiada pisemne upoważnienie) lub przez Wykonawcę, zgodnie z zapisami umowy. Pracownicy Urzędu merytorycznie odpowiedzialni za realizację umowy zobowiązani są do poinformowania Wykonawcy o zakresie jego odpowiedzialności za bezpieczeństwo informacji Urzędu.

Stażyści i praktykanci zobowiązani są do podpisania wymaganych przepisami prawa oświadczenia i przyrzeczenia o zachowaniu tajemnic ustawowo chronionych. Oświadczenie to oraz upoważnienie do przetwarzania danych jest aktualizowane po zmianie zakresu danych, do których stażyści i praktykanci uzyskują dostęp. Dostęp tych osób do informacji niejawnych jest regulowany przez procedury ochrony informacji niejawnych.

3.3 Postępowanie dyscyplinujące

Naruszenie postanowień Polityki bezpieczeństwa i ochrony danych osobowych oraz regulacji niniejszego regulaminu może stanowić podstawę do podjęcia działań dyscyplinujących wobec zatrudnionych w Urzędzie pracowników.

Każdy użytkownik przed otrzymaniem dostępu do sieci informatycznej Urzędu musi podpisać oświadczenie mówiące, że jest świadomy tego, że wszelkie operacje w sieci komputerowej Urzędu mogą być monitorowane oraz wyraża zgodę na to monitorowanie.
Informacje przechowywane lub przekazywane przy użyciu sprzętu teleinformatycznego Urzędu nie mogą być uznawane za prywatne.

Odpowiedzialność za bezpieczeństwo informacji Urzędu obejmuje nie tylko siedzibę Urzędu, ale także wszelkie sytuacje, w których informacje związane z działalnością Urzędu przetwarzane są poza jej siedzibą, w szczególności zdalny dostęp do sieci komputerowej Urzędu oraz dane przetwarzane na urządzeniach przenośnych.

Naruszanie przez użytkownika obowiązujących zasad bezpieczeństwa teleinformatycznego wynikających z niniejszego dokumentu grozi poniesieniem przez niego konsekwencji poczynając od odpowiedzialności porządkowej, a na rozwiązaniu umowy o pracę kończąc. Naruszenie

obowiązujących zasad w zakresie ochrony danych osobowych skutkować może odpowiedzialnością karną.

3.4 Zmiany miejsca pracy oraz ustanie stosunku pracy

Inspektor ds. Kadr i szkoleń w porozumieniu z Kierownikiem referatu niezwłocznie powiadamiają Pełnomocnika ds. ZSZ o odejściu pracownika lub jego przeniesieniu do innego referatu lub powierzeniu pracownikowi innych zadań.

Kierownik referatu wypełnia odpowiedni formularz zmiany uprawnień lub formularz wniosku o zablokowanie konta, zgodnie z PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji, a następnie kieruje go do ABI.

Niezwłocznie po otrzymaniu i akceptacji wniosku dotyczącego odejścia pracownika lub jego przeniesienia do innego referatu lub zadań ABI zleca ASI odpowiednie zmodyfikowanie praw dostępu tego pracownika oraz Inspektorowi ds. kadr i szkoleń zmianę upoważnień. Zbiory danych pracownika odchodzącego mogą być usuwane lub zachowywane w zależności od decyzji Właściciela aktywu. Wszystkie przedmioty wydane pracownikowi takie jak komputer przenośny, klucze, karta podpisu elektronicznego, pieczątki, oprogramowanie, dane, dokumenty i instrukcje muszą być zwrócone:

1. Komputer, oprogramowanie, karta podpisu elektronicznego, dane na dyskach przekazywane są do ASI.
2. Dokumenty i instrukcje, klucze przekazywane są Kierownikowi referatu,
3. Pieczątki przekazywane są Asystentowi Burmistrza.

Powyższe czynności muszą zostać potwierdzone na karcie obiegowej pracownika. Tryb postępowania zarządzania zmianami w prawach dostępu do systemów zawarty jest w dokumentacji procesu PW.1 Zarządzanie bezpieczeństwem informacji, ochroną danych osobowych i informatyzacją urzędu.

3.5 Zasady obowiązujące Administratorów Systemów Informatycznych

Administratorzy Systemów Informatycznych nie będą zapoznawać się z treścią informacji przekazywanych w systemach teleinformatycznych z wyjątkiem sytuacji, gdy jest to niezbędne do przeprowadzenia prac konserwacyjnych, usunięcia awarii systemowych lub gdy zachodzi sytuacja nadzwyczajna, objęta procedurą postępowania w sytuacjach awaryjnych a na uruchomienie procedury wyraził zgodę Burmistrz.

4 Kształtowanie świadomości znaczenia bezpieczeństwa informacji

Administrator Danych, Pełnomocnik ds. ZSZ, ABI oraz Kierownicy referatów (Właściciele aktywu) są odpowiedzialni za promowanie świadomości bezpieczeństwa informacji wśród wszystkich pracowników Urzędu. Zwiększanie świadomości użytkowników w zakresie bezpieczeństwa informacji obejmować powinno również regularne szkolenia związane z bezpieczeństwem i dostępem do danych.
Administrator Systemów Informatycznych w porozumieniu z Pełnomocnikiem ds. ZSZ publikuje komunikaty dotyczące bieżących kwestii z zakresu bezpieczeństwa informacji, za pomocą Qsystem oraz z wykorzystaniem poczty elektronicznej.

5 Zasady postępowania użytkownika zasobów teleinformatycznych

Użytkownik zasobów teleinformatycznych zobowiązany jest do przestrzegania następujących reguł:

1. Przestrzegać politykę bezpieczeństwa informacji,
2. Dbać o bezpieczeństwo powierzonych mu aktywów niezbędnych do realizacji jego zadań, w tym aktywów teleinformatycznych,
3. Przetwarzać informacje w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym,
4. Korzystać z informacji przeznaczonych wyłącznie dla niego,

5. Korzystać z haseł zgodnie z zasadami w ZSZ,
6. Zgłaszać wszelkie nieprawidłowości w funkcjonowaniu sprzętu teleinformatycznego Administratorowi Systemów Informatycznych,
7. Nie ingerować w ustawienia sprzętu i oprogramowania systemów teleinformatycznych, zastrzeżone dla Administratora Systemów Informatycznych,
8. Nie udostępniać sprzętu teleinformatycznego osobom nieupoważnionym.
9. Nie przechowywać i nie przetwarzać żadnych plików mających charakter prywatny, niezwiązanych z wykonywaną pracą oraz naruszających przepisy ustawy o prawie autorskim i prawach pokrewnych.

5.1 Szczegółowe zasady postępowania użytkownika zasobów teleinformatycznych

Do obowiązków użytkownika zasobów (urządzeń, systemów, sieci i usług) teleinformatycznych Urzędu należy:

1. Zabezpieczanie eksploatowanego przez użytkownika sprzętu komputerowego, udostępnianych przy jego pomocy informacji oraz wymiennych elektronicznych nośników informacji (dyskietek, taśm, płyt CD-ROM, nośników USB itp.) przed dostępem osób nieuprawnionych.
2. Zapobieganie nieuprawnionemu dostępowi do zasobów teleinformatycznych Urzędu poprzez stosowanie się do poniższych zasad:
   a) W każdej sytuacji, kiedy pracownik opuszcza aktualne stanowisko pracy, na którym pozostaje włączony komputer, zobowiązany jest do zastosowania blokady dostępu do informacji prezentowanych na ekranie;
   b) Niezależnie od postanowień punktu a, tam gdzie to jest możliwe, należy stosować ochronę stanowiska roboczego poprzez zastosowanie funkcji wygaszacza ekranu aktywującego się automatycznie (po 10 minutach bezczynności dla komputerów stacjonarnych, po 5 minutach dla komputerów przenośnych) oraz chronionego hasłem użytkownika;
   c) Użytkownik nadzoruje realizowane na stanowisku prace serwisowe związane z powierzonym zasobem teleinformatycznym, wykonywane przez pracowników Urzędu oraz podmiotów trzecich (np. serwisantów);
   d) W uzasadnionych przypadkach użytkownik występuje do przełożonego o umożliwienie dostępu do zasobów teleinformatycznych (do których na co dzień nie ma uprawnień) w sytuacjach rzeczywiście uzasadnionych potrzebami wynikającymi z realizacji zadań służbowych oraz niezwłocznie informuje go o konieczności wycofania dostępu do tych zasobów;
   e) Użytkownik nie może udostępniać lokalnych zasobów (dysków, drukarek) innym użytkownikom sieci Urzędu. Wymiana informacji powinna odbywać się przy wykorzystaniu współdzielonych udziałów sieciowych zlokalizowanych na udostępnionych w tym celu serwerach plików.
3. Zapobieganie nieautoryzowanemu dostępowi fizycznemu osób do krytycznych zasobów teleinformatycznych i ich wykorzystaniu, jest realizowane poprzez stosowanie się do poniższych zasad:
   a) Pracownicy zobowiązani są do zamykania na klucz pomieszczeń biurowych oraz obszarów bezpiecznych o ograniczonym dostępie lub stosowania innych dopuszczonych i wdrożonych w Urzędzie zabezpieczeń tego typu obszarów, w których znajdują się krytyczne zasoby teleinformatyczne, zarówno w czasie chwilowej nieobecności wszystkich pracowników w danym pomieszczeniu czy obszarze bezpiecznym w trakcie pracy, jak i po jej zakończeniu. Klucze do powyższych pomieszczeń nie mogą być pozostawiane w czasie pracy w zamku drzwi. Zgubienie klucza należy natychmiast zgłosić do pracownika obsługującego system klucza.
   b) Osoby trzecie mogą przebywać w pomieszczeniu lub obszarze bezpiecznym o ograniczonym dostępie, w którym usytuowane są krytyczne zasoby teleinformatyczne, tylko w obecności i pod nadzorem pracownika upoważnionego do świadczenia w nim pracy.

4. Zgłaszanie przez pracowników wszelkich stwierdzonych zdarzeń, mogących prowadzić do incydentów bezpieczeństwa teleinformatycznego za pośrednictwem Qsystem lub w inny możliwy sposób Zespołowi ds. obsługi informatycznej. Należy zgłaszać również wszelkie incydenty związane z nieuprawnionym ujawnieniem, zniszczeniem lub modyfikacją informacji w dowolnej formie (np. papierowej, elektronicznej) związanej z ich przetwarzaniem przy wykorzystaniu zasobów teleinformatycznych. Po stwierdzeniu naruszenia bezpieczeństwa, jeżeli istnieje taka możliwość, należy podjąć akcję prewencyjną mającą na celu zapobieganie dalszemu rozszerzaniu się skutków zdarzenia. Zgłaszać należy wszystko, co jest lub może stanowić zagrożenie dla bezpieczeństwa informacji. Przykładowymi zdarzeniami mogącymi skutkować naruszeniem bezpieczeństwa teleinformatycznego lub incydentem bezpieczeństwa informacji mogą być:
    a) Stwierdzenie nie realizowania zadań i obowiązków pracowników związanych z zapewnieniem bezpieczeństwa informacji,
    b) Ujawnienie (w tym kradzież) informacji chronionych w Urzędzie ze względu na atrybut poufności,
    c) Utrata integralności lub długotrwała niedostępność informacji zawartych w zasobach teleinformatycznych,
    d) Znalezienie niezabezpieczonego nośnika informacji oznaczonego lub zaewidencjonowanego w sposób obowiązujący w Urzędzie,
    e) Podejrzenie zaistnienia próby lub stwierdzenie włamania do zasobu teleinformatycznego,
    f) Podejrzenie zaistnienia próby nieuprawnionego wejścia lub stwierdzenie przebywania osoby nieuprawnionej w pomieszczeniu lub obszarze bezpiecznym o ograniczonym dostępie, w którym eksploatowany jest zasób teleinformatyczny,
    g) Kradzież przydzielonego urządzenia służącego do przetwarzania informacji lub służącego do autoryzacji użytkownika, w tym zwłaszcza urządzenia przenośnego,
    h) Podejrzenie naruszenia ustawy o prawie autorskim i prawach pokrewnych, ustawy o ochronie informacji niejawnych, ustawy o ochronie danych osobowych, ustawy o publicznym obrocie papierami wartościowymi.
5. Używanie przez pracowników Urzędu oprogramowania pochodzącego z legalnych źródeł i zgodnie z warunkami udzielonej Urzędowi licencji, dopuszczonego do użytkowania na podstawie obowiązujących w Urzędzie standardów, w oparciu o obowiązującą ustawę o prawie autorskim i prawach pokrewnych.
6. Zakaz samowolnego instalowania oprogramowania i dokonywania nieautoryzowanych zmian w ustawieniach systemu operacyjnego użytkowanego komputera oraz dokonywania zmian w ustawieniach sprzętu teleinformatycznego.
7. Stosowanie się do poniższych zasad w zakresie ochrony i używania haseł do udostępnionych zasobów teleinformatycznych:
    a. Zakaz ujawniania przez użytkownika jakichkolwiek aktualnych lub nie aktualnych haseł. Administrator Systemów Informatycznych, w porozumieniu z użytkownikiem nadają osobiste hasło dostępu do zasobów teleinformatycznych i odpowiadają za utrzymanie go w tajemnicy.
    b. Zabrania się zapisywania haseł i ich przechowywania w sposób jawny, nie gwarantujący ich poufności, w tym również w postaci elektronicznej.
    c. Jeśli użytkownik stwierdzi lub podejrzewa, że jego hasło straciło swoją poufność zobowiązany jest do wystąpienia do Administratora Systemów Informatycznych o jego natychmiastową zmianę oraz poinformowania o fakcie naruszenia poufności hasła zgodnie z określonymi zasadami zgłaszania zdarzeń mogących prowadzić do incydentów bezpieczeństwa informacji.
    d. Zmiana hasła dostępu do zasobów teleinformatycznych następuje nie rzadziej niż co 30 dni.
    e. Hasła do zasobów teleinformatycznych muszą składać się przynajmniej z 8 znaków i być konstruowane z wykorzystaniem co najmniej 3 spośród 4 grup znaków (małe litery, duże litery, cyfry, znaki specjalne). Jeżeli dostęp do systemu teleinformatycznego

jest autoryzowane kodem PIN, składającym się z samych cyfr, musi on liczyć przynajmniej 4 znaki. W przypadku opracowania odrębnej polityki haseł dla krytycznego zasobu teleinformatycznego, należy przestrzegać zasad w niej określonych, a sformułowane wyżej reguły konstrukcji haseł nie obowiązują.

f. Hasła dostępu do zasobów teleinformatycznych zmieniane są przynajmniej raz na rok, poza przypadkami wskazanymi w punkcie 6.7.c. oraz każdorazowo na wniosek użytkownika. W przypadku opracowania odrębnej polityki haseł dla krytycznego zasobu teleinformatycznego, należy przestrzegać zasad dla niego określonych, zaś określona wyżej reguła częstotliwości zamiany haseł nie obowiązuje.
g. Zabrania się używania jako haseł lub ich części: słów pochodzących z dowolnego słownika wyrazów w dowolnym języku naturalnym (np. polskim, angielskim itd.), akronimów, dat urodzin, imienin oraz imion własnych (w tym swoich, osób bliskich, znajomych), ciągów kolejnych cyfr (np. 1234), nazw ulubionych zespołów, filmów, imion bohaterów itp. - z uwagi na łatwość ich odgadnięcia przy wykorzystaniu automatycznie działającego oprogramowania do łamania haseł.
h. Zobowiązuje się użytkowników do starannego i bezpiecznego prowadzenia procesu logowania do systemu teleinformatycznego, polegającego na uniemożliwieniu podejrzenia hasła przez osobę trzecią w trakcie tego procesu. Następujące po sobie bezkrytyczne próby błędnego wprowadzenia przez użytkownika hasła traktowane są przez chronione zasoby teleinformatyczne jako próba włamania, skutkiem czego następuje czasowa lub całkowita blokada dostępu do konta użytkownika. W każdym z powyższych przypadków użytkownik zobowiązany jest do zgłoszenia takiego faktu do Administratora Systemów Informatycznych.
i. Użytkownik powinien zostać poinformowany przez bezpośredniego przełożonego o tym, że może być pociągnięty do odpowiedzialności za nieprzestrzeganie obowiązujących zasad zarządzania hasłami, prowadzące w skutkach do użycia tych systemów, przez osobę nieuprawnioną.

5.2 Przetwarzanie informacji na stanowisku pracy

Wytwarzanie, przetwarzanie i przechowywanie na stanowiskach pracy informacji chronionych ze względu na atrybut poufności może odbywać się po spełnieniu odpowiednich zasad i wymagań bezpieczeństwa.

5.3 Ochrona przed oprogramowaniem szkodliwym

Przestrzeganie podstawowych zasad ochrony przed oprogramowaniem szkodliwym jest obowiązkiem użytkownika komputera, co polega na:

a. Konsekwentnym unikaniu posługiwania się danymi pochodzącymi z niepewnych źródeł, zwłaszcza spoza sieci wewnętrznej Urzędu.
b. Każdorazowym zwróceniu się o pomoc do Administratora Systemów Informatycznych, przy wystąpieniu jakichkolwiek wątpliwości co do zawartości wymiennego nośnika elektronicznego.
c. Natychmiastowym wyłączeniu użytkowanego komputera, a następnie zgłoszeniu do Administratora Systemów Informatycznych podejrzenia wystąpienia ataku przez szkodliwe oprogramowanie.

5.4 Postępowanie z elektronicznymi nośnikami informacji

Zabrania się używania wszelkich elektronicznych nośników informacji nie będących własnością Urzędu, w tym nośników stanowiących prywatną własność pracowników.
Wszystkie wykorzystywane służbowe wymienne nośniki elektroniczne (dyskietki, płyty CD i DVD, pamięci Flash itp.) zawierające jakiekolwiek dane muszą być opisane.

Wszystkie używane wymienne nośniki elektroniczne zawierające jakiekolwiek informacje służbowe muszą być chronione przed ich utratą. Ponadto należy stosować właściwe zasady zawarte

w wewnętrznych aktach organizacyjnych Urzędu dotyczących postępowania z informacją chronioną. Wymienne elektroniczne nośniki informacji należy szczególnie zabezpieczać w trakcie ich transportu poza obszarem chronionym przez Urząd, w tym poprzez obowiązkowe stosowanie funkcji szyfrujących dla zawartych na nich informacji.
Należy dbać o to, aby informacje służbowe nie podlegały nieuzasadnionej dystrybucji. Należy usuwać z nośników elektronicznych informacje nieistotne, nieaktualne oraz takie, których dalsze przechowywanie nie jest już w żaden sposób uzasadnione. W przypadku, gdy informacji nie da się bezpiecznie usunąć z nośnika w sposób elektroniczny (np. w przypadku płyt CD jednokrotnego zapisu), nośnik taki należy zniszczyć fizycznie.

Każdy zbędny, uszkodzony lub przeznaczony do likwidacji elektroniczny nośnik informacji zawierający informacje chronione ze względu na atrybut poufności musi być do czasu jego bezpiecznego zniszczenia przechowywany w sposób szczegółowo określony dla danej grupy informacji chronionych. Bezwarunkowo zabrania się wyrzucania takich elektronicznych nośników informacji do standardowych koszy na śmieci lub niszczenia ich na własną rękę. Wymienne elektroniczne nośniki informacji podlegają właściwej ochronie do czasu ich ostatecznego zniszczenia zgodnie z podanymi wyżej zasadami lub obowiązującymi procedurami.

Szczegółowe zasady niszczenia zbędnych, uszkodzonych lub przeznaczonych do likwidacji elektronicznych nośników informacji zawierających informacje chronione w Urzędzie ze względu na atrybut poufności lub ich ponownego wykorzystania, określono we właściwych, wewnętrznych aktach organizacyjnych dotyczących grup informacji chronionych lub w dokumentacji ZSZ.
Dla pozostałych informacji służbowych przechowywanych na wymiennych elektronicznych nośnikach informacji, a także w stosunku do uszkodzonych wymiennych elektronicznych nośników informacji ich niszczenie przeprowadza bezpośredni użytkownik w sposób nieodwracalny. Wymienne elektroniczne nośniki informacji wielokrotnego zapisu należy przekazać do Administratora Systemów Informatycznych w celu bezpiecznego usunięcia informacji zawartych na tych nośnikach.

5.5 Nadzór nad dokumentami drukowanymi

Drukowanie przez pracowników dokumentów zawierających informacje chronione ze względu na atrybut poufności na urządzeniach drukujących rozmieszczonych poza pomieszczeniami zamykanymi zabezpieczone jest poprzez indywidualny kod PIN wprowadzany przez użytkownika przy urządzeniu w chwili uruchomienia procesu wydruku dokumentu. Jeżeli drukarka usytuowana poza pomieszczeniem zamykanym nie zapewnia takiego zabezpieczenia, drukowanie na niej informacji chronionych jest zabronione.
Pracownicy urzędu zobowiązani są do przestrzegania w stosunku do wszystkich drukowanych dokumentów zawierających informacje służbowe zasady, że dokumenty te należy zabrać z drukarki niezwłocznie po ich wydrukowaniu.

5.6 Wykorzystywanie zasobów teleinformatycznych poza siedzibą Urzędu

1. Zabrania się pracownikom wynoszenia poza siedzibę Urzędu sprzętu teleinformatycznego, ewidencjonowanych elektronicznych nośników informacji bez zgody bezpośredniego przełożonego pracownika.
2. Wszelkie użycie krytycznych zasobów teleinformatycznych poza siedzibą Urzędu, niezależnie od prawa własności do tych zasobów, wymaga wcześniej zatwierdzenia ich użycia przez właściciela danego zasobu w porozumieniu z ABI.
3. Zabrania się przesyłania za pośrednictwem sieci teleinformatycznej Urzędu informacji nie mających związku z wykonywanymi obowiązkami służbowymi.
4. Należy chronić zasoby teleinformatyczne wykorzystywane poza siedzibą Urzędu przed fizycznym uszkodzeniem przez zachowanie odpowiednich środków ostrożności w trakcie ich użytkowania (bezpieczne środowisko pracy i zasada „czystego biurka") i transportu.

5. Sprzęt i urządzenia teleinformatyczne znajdujące się poza siedzibą Urzędu nie mogą pozostawać bez nadzoru w miejscach publicznych.
6. W przypadku kradzieży lub zgubienia sprzętu teleinformatycznego należy niezwłocznie powiadomić ABI, który podejmuje decyzję o konieczności powiadomienia policji oraz zgłoszeniu zdarzenia mogącego prowadzić do incydentu bezpieczeństwa informacji zgodnie z zasadami określonymi w PW.1.3.

5.7 Przetwarzanie danych osobowych

Zgodnie z obowiązującymi w Urzędzie zasadami, pracownicy uzyskują dostęp do danych osobowych po otrzymaniu pisemnego upoważnienia do przetwarzania danych osobowych.
Przetwarzanie wszelkich zbiorów danych osobowych podlegających w Urzędzie ochronie na mocy ustawy o ochronie danych osobowych oraz innych przepisów prawnych, odbywa się zgodnie z obowiązującymi w tym zakresie zasadami zawartymi w dokumentacji ZSZ oraz Polityce Bezpieczeństwa Informacji I Ochrony Danych Osobowych.

Każdy pracownik tworząc zbiór danych osobowych, zobowiązany jest w porozumieniu z ABI oraz Administratorem Systemów Informatycznych zgłosić zbiór danych osobowych do rejestracji, przed rozpoczęciem przetwarzania zawartych w nim danych osobowych. Sposób dokonywania zgłoszeń do rejestracji, aktualizacji oraz wykreślenia zbiorów danych osobowych opisany jest w pkt. 3.10 Zasad zarządzania siecią teleinformatyczną, kryptografią i kopiami zapasowymi PW.1.2.

Pracownicy odpowiedzialni za opracowywanie i merytoryczny nadzór nad realizacją umów, w zakresie których istnieć będzie konieczność zapewnienia drugiej stronie dostępu do infrastruktury sieciowej Urzędu, pozostałych zasobów teleinformatycznych Urzędu lub przetwarzanych w nich informacji i danych (w tym danych osobowych), zobowiązani są do umieszczania w umowach zawartych z tymi podmiotami zapisów dotyczących ochrony danych, zgodnie z opisem zawartym w pkt. 3.2. regulaminu. Zakres dostępu do zasobów teleinformatycznych powinien być w każdym z takich przypadków ograniczany do niezbędnego minimum, a sposób realizacji dostępu uzgodniony wcześniej z Zespołem ds. obsługi informatycznej oraz ABI.

5.8 Rejestr incydentów i problemów związanych z bezpieczeństwem

Pełnomocnik ds. ZSZ nadzoruje prowadzenie przez Zespół ds. obsługi informatycznej rejestru incydentów związanych z bezpieczeństwem teleinformatycznym.
Każdy zasób teleinformatyczny stanowiący własność Gminy Dobczyce, znajdujący się lub eksploatowany na jej terenie może zostać poddany monitorowaniu bezpieczeństwa przez upoważnionych do tego pracowników Urzędu, a w szczególności pracowników zespołu ds. obsługi informatycznej oraz audytorów wewnętrznych i audytorów jakości.

W Urzędzie obowiązuje zasada identyfikowalności zmian dokonanych w systemach teleinformatycznych na podstawie przydzielonych pracownikowi danych identyfikacyjnych. Wszelkie działania i operacje, jakie są wykonywane przez pracownika po poprawnym zalogowaniu się z wykorzystaniem przydzielonego mu identyfikatora i używanego hasła osobistego do dowolnego zasobu teleinformatycznego udostępnionego mu lokalnie na tym komputerze bądź w sieci teleinformatycznej Urzędu, rejestrowane są przez odpowiednie programy monitorujące poszczególne zasoby teleinformatyczne, niezależnie od tego czy użytkownikiem aktualnie pracującym przy komputerze jest sam pracownik, czy też inna osoba mająca chwilowy dostęp do niewłaściwie zabezpieczonej przez niego sesji.

6 Dokumenty związane

PW.1.1. Kontrola dostępu do Urzędu, danych osobowych, informacji i aplikacji
PW.1.2. Zasady zarządzania siecią teleinformatyczną, kryptografią i kopiami zapasowymi
PW.1.3. Zasady zarządzania incydentami związanymi z bezpieczeństwem informacji

PW.1.4. Zasady zarządzania rozwojem informatycznym
PZ.7.1. Zasady zarządzania ryzykiem w Urzędzie

7 Aplikacje informatyczne

Qsystem

8 Załączniki i formularze

Lp.	Nazwa	Lokalizacja, nazwa pliku
1.	Wzór oświadczenia o zachowaniu tajemnic ustawowo chronionych - Formularz F/01	Qsystem
2.	Wzór upoważnienia do przetwarzania danych osobowych - Formularz F/02	Qsystem
3.	Karta obiegowa urzędnika – Formularz F/03	Qsystem
4	Wzór istotnych postanowień umowy dotyczących ochrony informacji i przetwarzania danych osobowych - Załącznik Z/01	Qsystem

....
(imię i nazwisko) (data)

.....
(adres zamieszkania)

.....

O Ś W I A D C Z E N I E

Ja, niżej podpisany(a) niniejszym oświadczam, że:

1. Znane mi są zasady obowiązujące w Zintegrowanym Systemie Zarządzania i określone w dokumentacji ochrony danych osobowych obowiązujących w Urzędzie Gminy i Miasta Dobczyce i niniejszym zobowiązuję się do ich stosowania i przestrzegania.
2. Oświadczam, iż znana jest mi treść przepisów art. 39 ust. 2 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych - o obowiązku zachowania tajemnicy danych osobowych, do których mam dostęp w czasie i po ustaniu zatrudnienia oraz jestem świadomy/a odpowiedzialności karnej, za zawiniony brak ochrony tych danych przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, jak również nielegalnym ich ujawnieniem lub pozyskaniem.
3. Zobowiązuję się do ochrony i nie ujawniania jakichkolwiek haseł oraz kodów zabezpieczających powierzonych mi celem korzystania z informacji przetwarzanych w zasobach teleinformatycznych, których administratorem jest Burmistrz Gminy i Miasta Dobczyce, a także do nie ujawniania osobom nieuprawnionym zabezpieczeń organizacyjnych i technicznych stosowanych dla zapewnienia ochrony informacji i zasobów teleinformatycznych służących do ich przetwarzania, przez cały czas mojego zatrudnienia oraz po jego ustaniu.
4. Zobowiązuję się do zachowania tajemnicy ustawowo chronionej zgodnie z ustawą z dnia 21 listopada 2008 roku o pracownikach samorządowych.
5. Zgodnie z art. 294 § 2, w związku z art. 293 Ustawy z dnia 29 sierpnia 1997r Ordynacja podatkowa: *Przyrzekam, że będę przestrzegal/a tajemnicy skarbowej. Oświadczam, że są mi znane przepisy o odpowiedzialności karnej za ujawnienie tajemnicy skarbowej.*
6. Jestem świadomy(a) odpowiedzialności i konsekwencji za naruszenie powyższych zobowiązań na podstawie art. 266 §1 ustawy z dnia 06 czerwca 1997 r. Kodeks Karny oraz art. 52 w związku z art. 100 § 2 pkt. 4 ustawy z dnia 26 kwietnia 1974 Kodeks Pracy.
7. Jestem świadomy(a) odpowiedzialności za próby lub dokonanie nieuprawnionego podsłuchu komputerowego, nieuprawnionego dostępu do zasobów teleinformatycznych, zapisów na elektronicznych nośnikach informacji Urzędu lub nieuprawnionego niszczenia, uszkadzania, usuwania, zmieniania danych w nich przetwarzanych bądź gromadzonych albo utrudniania dostępu do tych danych, czy też innego zakłócania pracy systemu lub sieci teleinformatycznej, na podstawie art. 267 §1, 2 i 3, art. 268 §2 i art. 165 §1 pkt 4 ustawy z dnia 06 czerwca 1997 r. Kodeks Karny.
8. Jestem świadomy(a) tego, że wszelkie operacje w sieci komputerowej Urzędu mogą być monitorowane i wyrażam zgodę na monitorowanie sieci komputerowej oraz przydzielonego mi do pracy stanowiska komputerowego.

....
(miejscowość i data) (czytelny podpis)

Dobczyce, dnia .....

RO.077._____

Upoważnienie imienne

do przetwarzania danych osobowych

Na podstawie art. 37 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych *(podać aktualny publikator ustawy)* upoważniam Panią / Pana:

.....
(imię i nazwisko osoby upoważnionej)

zatrudnioną (ego) w

Urzędzie Gminy i Miasta Dobczyce
Referat .....
(nazwa jednostki i komórki organizacyjnej)

na stanowisku: .....

do przetwarzania od dnia ..... roku danych osobowych zawartych w dokumentacji papierowej oraz elektronicznej związanej z wykonywanymi czynnościami w ramach zakresu obowiązków, a w szczególności związanych z:

a) .....

b) .....

c) .....

i nadaję identyfikator: ..... do przetwarzania danych osobowych w systemach teleinformatycznych:

L.p.	Nazwa zbioru danych osobowych	Program przetwarzający zbiór danych osobowych

Upoważnienie wygasa z chwilą cofnięcia upoważnienia, przeniesienia na inne stanowisko pracy albo rozwiązania stosunku pracy.

Traci ważność upoważnienie z dnia .....
znak sprawy

.....

(podpis administratora danych)

KARTA OBIEGOWA

Imię i nazwisko pracownika: .....

Zdaję:

1). Sprzęt komputerowy wraz oprogramowaniem[1] .....
(data i podpis odbierającego)

2). Karta podpisu elektronicznego[1] .....
(data i podpis odbierającego)

3). Dokumenty i instrukcje (w tym teczki spraw)[2] .....
(data i podpis odbierającego)

4). Pokój oraz klucz od pokoju[2] nr ....
(data i podpis odbierającego)

5). Służbowy telefon komórkowy[1] .....
(data i podpis odbierającego)

6). Pieczątki[3] .....
(data i podpis odbierającego)

7). Kasa Zapomog. – Pożyczkowa[4] .....
(data i podpis członka Komisji)

8). Fundusz Socjalny[5] .....
(data i podpis członka Komisji)

.....
(data i podpis pracownika)

[1] zwrot do Zespołu ds. obsługi informatycznej
[2] zwrot do kierownika referatu
[3] zwrot do Asystenta Burmistrza (sekretariat)
[4] podpis Członka Komisji Kasy Zapomogo-Pożyczkowej przy Urzędzie Gminy i Miasta Dobczyce
[5] podpis Członka Komisji Socjalnej w Urzędzie Gminy i Miasta Dobczyce

Postanowienia dotyczące ochrony danych osobowych:

1. Zamawiający stosownie do art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2014, poz. 1182 ze zm.), zwanej dalej Ustawą, powierza Wykonawcy przetwarzanie danych osobowych, w imieniu i na rzecz Zamawiającego, na warunkach opisanych w niniejszym paragrafie.
2. Zamawiający oświadcza, że jest Administratorem Danych w rozumieniu Ustawy w odniesieniu do powierzonych Wykonawcy danych osobowych.
3. Dane osobowe mogą być przetwarzane przez Wykonawcę wyłącznie w celu realizacji umowy. Wykonawca nie decyduje o celach przetwarzania danych.
4. Przy przetwarzaniu danych osobowych Wykonawca przestrzega zasad wskazanych w niniejszym paragrafie, w Ustawie, w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz.1024), zwane dalej Rozporządzeniem.
5. Wykonawca przed rozpoczęciem przetwarzania danych osobowych podejmie środki zabezpieczające zbiory danych, o których mowa w art. 36-39 Ustawy oraz Rozporządzeniu.
6. Do przetwarzania danych osobowych mogą być dopuszczeniu jedynie pracownicy Wykonawcy posiadający imienne upoważnienia do przetwarzania danych osobowych.
7. Imienne upoważnienia, o których mowa w pkt. 6 są ważne do chwili odwołania. Upoważnienie wygasa z chwilą ustania zatrudnienia upoważnionego pracownika oraz w przypadku zakończenia realizacji umowy.
8. Zamawiający umocowuje Wykonawcę do wydawania i odwoływania pracownikom imiennych upoważnień do przetwarzania danych osobowych. Upoważnienia przechowuje Wykonawca w swojej siedzibie.
9. Wykonawca prowadzi ewidencję pracowników upoważnionych do przetwarzania danych osobowych w związku z wykonywaniem umowy.
10. Wykonawca jest zobowiązany do podjęcia wszelkich kroków służących zachowaniu przez pracowników mających dostęp do powierzonych danych osobowych, danych w poufności.
11. Wykonawca niezwłocznie informuje Zamawiającego o:
    a) Wszelkich przypadkach naruszenia tajemnicy danych osobowych lub o ich niewłaściwym użyciu;
    b) Wszelkich czynnościach z własnym udziałem w sprawach dotyczących ochrony danych osobowych przeprowadzonych w szczególności przed Generalnym Inspektorem Ochrony Danych Osobowych, urzędami państwowymi, policją lub przed sądem.
12. Wykonawca zobowiązuje się do udzielania Zamawiającemu, na każde jego żądanie, informacji na temat przetwarzania danych osobowych, o których mowa w niniejszym paragrafie, a w szczególności niezwłocznego przekazywania informacji o każdym przypadku naruszenia przez niego i jego pracowników obowiązków dotyczących ochrony danych osobowych.
13. Wykonawca umożliwi Zamawiającemu lub podmiotom przez niego upoważnionym, w miejscach w których są przetwarzane powierzone dane osobowe, dokonanie kontroli, zgodności z Ustawą i Rozporządzeniem oraz niniejszą umową przetwarzania danych osobowych. Zawiadomienie o zamiarze przeprowadzenia kontroli powinno być przekazane Wykonawcy co najmniej 5 dni kalendarzowych przed rozpoczęciem kontroli.
14. W przypadku powzięcia przez Zamawiającego wiadomości o rażącym naruszeniu przez Wykonawcę zobowiązań wynikających z Ustawy, Rozporządzenia lub niniejszej umowy, Wykonawca umożliwi Zamawiającemu lub podmiotom przez niego upoważnionym dokonanie niezapowiedzianej kontroli w celu, o którym mowa w pkt. 13.
15. Kontrolerzy Zamawiającego lub podmiotów przez niego upoważnionych mają w szczególności prawo do:
    a) wstępu w godzinach pracy Wykonawcy, za okazaniem imiennego upoważnienia, do pomieszczeń, w których zlokalizowane są powierzone zbiory danych osobowych i przeprowadzenia niezbędnych

badań lub czynności kontrolnych w celu oceny zgodności przetwarzania danych z Ustawą, Rozporządzeniem oraz niniejszą umową.

b) żądać złożenia pisemnych lub ustnych wyjaśnień oraz wzywać i przesłuchiwać pracowników w zakresie niezbędnym do ustalenia stanu faktycznego;
c) wglądu do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli oraz sporządzenia ich kopii;
d) przeprowadzenia oględzin urządzeń, nośników oraz systemu informatycznego służącego do przetwarzania danych osobowych.

16. Wykonawca jest zobowiązany do zastosowania się do zaleceń dotyczących poprawy jakości zabezpieczenia danych osobowych oraz sposobu ich przetwarzania sporządzonych w wyniku kontroli przeprowadzonych przez Zamawiającego lub podmioty przez niego upoważnione albo przez inne instytucje upoważnione do kontroli na podstawie odrębnych przepisów.
17. W przypadku wygaśnięcia lub odstąpienia jednej ze stron od Umowy Wykonawca zobowiązany jest do:
    a) Niezwłocznego, ale nie później niż w terminie do 3 dni, usunięcia lub zwrotu wszelkich danych osobowych, których przetwarzanie zostało mu powierzone, wraz ze wszelkimi kopiami tych danych, w tym skutecznego ich usunięcia również z nośników elektronicznych pozostających w dyspozycji Wykonawcy,
    b) Podjęcia stosownych działań w celu wyeliminowania możliwości dalszego przetwarzania danych powierzonych na podstawie niniejszej Umowy.

Postanowienia dotyczące ochrony informacji

1. Za dane chronione Zamawiającego rozumie się wszelkie informacje lub materiały dotyczące Zamawiającego, które nie są znane lub nie powinny być znane publicznie, powzięte/otrzymane przez Wykonawcę, w związku z wykonywaniem lub przy okazji wykonywania Umowy, a w szczególności informacje stanowiące tajemnice prawem chronione.
2. Obowiązek zabezpieczenia danych chronionych spoczywa na Wykonawcy niezależnie od formy ich przekazania przez Zamawiającego (w tym w formie przekazu ustnego, dokumentu lub zapisu na komputerowym nośniku informacji).
3. Obowiązek zachowania poufności nie dotyczy informacji:
    a) których ujawnienie jest wymagane przez powszechnie obowiązujące przepisy prawa,
    b) które są powszechnie znane lub zostały podane do publicznej wiadomości przez Stronę uprawnioną lub za jej zezwoleniem,
    c) na żądanie uprawnionych organów.
4. Wykonawca nie będzie sporządzać kopii informacji chronionych Zamawiającego, z wyjątkiem kopii niezbędnych do realizacji przedmiotu Umowy. Wszelkie wykonane kopie będą określone jako należące do Zamawiającego.
5. Wykonawca nie będzie podejmował czynności mających na celu uzyskanie informacji chronionych Zamawiającego, innych niż udostępnione przez Zamawiającego w celu realizacji przedmiotu Umowy.
6. Wykonawca może ujawnić informacje chronione Zamawiającego osobie trzeciej wyłącznie po uzyskaniu uprzedniej pisemnej zgody Zamawiającego.
7. Obowiązek zachowania w tajemnicy informacji chronionych spoczywa na Wykonawcy także po wygaśnięciu Umowy lub jej rozwiązaniu przez Strony.
8. Realizacja zobowiązań wynikających z postanowień niniejszego paragrafu wymaga od Wykonawcy zachowania najwyższej staranności, uwzględniającej profesjonalny charakter działania Wykonawcy. Wykonawca jest w pełni odpowiedzialny za każdą, bezpośrednią lub pośrednią, szkodę poniesioną przez Zamawiającego w związku z naruszeniem przez Wykonawcę postanowień niniejszego paragrafu.