Zarządzenie Nr 114/2017
Wójta Gminy Michałowice
z dnia 9 czerwca 2017 r.

w spranie wprowadzenia dokumentu pn. „Polityka bezpieczeństwa informacji Urzędu Gminy Michałowice".

Na podstawie art. 31 i art. 33 ust. 3 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (Dz. U. z 2016 r. poz. 446 ze zm.) oraz art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U z 2016 r. poz. 922), a także Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2016 r. poz. 113 ze zm.) zarządzam, co następuje:

§ 1

Wprowadzam i wdrażam do stosowania Politykę bezpieczeństwa informacji Urzędu Gminy Michałowice w brzmieniu stanowiącym załącznik do niniejszego zarządzenia.

§ 2

Zobowiązuję wszystkich pracowników Urzędu Gminy Michałowice do zapoznania się z dokumentacją określoną w § 1.

§ 3

Pracownicy przetwarzający informacje w Urzędzie Gminy Michałowice (w tym również dane osobowe), są zobowiązani zachować w tajemnicy sposoby ich zabezpieczenia określone w polityce bezpieczeństwa informacji Urzędu Gminy Michałowice.

§4

Wykonanie zarządzenia powierza się Kierownikowi Referatu Informatyki.

§5

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT GMINY MICHAŁOWICE
mgr inż. Krzysztof Grabka

RADCA PRAWNY
Joanna Domańska
OI-C-851

KIEROWNIK
Referatu Informatyki
inż. Marcin Walichnowski

URZĄD GMINY MICHAŁOWICE

POLITYKA BEZPIECZEŃSTWA INFORMACJI URZĘDU GMINY MICHAŁOWICE

Zatwierdzam
Wójt Gminy Michałowice

WÓJT GMINY MICHAŁOWICE
mgr inż. Krzysztof Grabka

.....(podpis).....

Opracował:
Marcin Walichnowski

Oznaczenie dokumentu: **IT-SZBI-01**	Wersja dokumentu: 1.0	Dokument obowiązuje od: 09 czerwca 2017 r.

Rejestr zmian dokumentu:

Lp.	Imię i nazwisko wprowadzającego zmiany	Wersja	Data	Opis/Uwagi
1	Marcin Walichnowski	1.0	09.06.2017	Opracowanie dokumentu

Spis treści

I. SŁOWNIK STOSOWANYCH TERMINÓW

1) **System informatyczny** - system, w którym w trakcie zachodzących w nim procesów gromadzi się, przetwarza, przechowuje i udostępnia informacje, niezależnie od formy realizacji tych procesów przy czym którykolwiek z jego procesów odbywa się w formie elektronicznej;
2) **Urząd** - Urząd Gminy Michałowice;
3) **Informacja wrażliwa** - dane przetwarzane przez Urząd oraz informacje związane z ochroną takich danych, a w szczególności zawartości baz danych Urzędu i danych osobowych;
4) **ASI** – (Administrator Systemu Informatycznego) pracownik Referatu Informatyki zajmujący się zarządzaniem systemem informatycznym i odpowiadający za jego sprawne działanie oraz odpowiedzialny za stosowanie technicznych i organizacyjnych środków ochrony danych przetwarzanych w systemach informatycznych;
5) **Właściciel Zasobu** - kierownik komórki organizacyjnej lub osoba na samodzielnym stanowisku, który posiada odpowiedzialność kierowniczą za nadzór nad eksploatacją, rozwojem, utrzymaniem, korzystaniem, bezpieczeństwem i dostępem do zasobu dla właściwej komórki organizacyjnej;
6) **Kierownictwo** - osoby odpowiedzialne za zatwierdzanie, wdrażanie oraz nadzorowanie Systemu Zarządzania Bezpieczeństwem Informacji;
7) **Komórka organizacyjna** – Referat lub samodzielne stanowisko w Urzędzie Gminy Michałowice;
8) **Logowanie** - proces uwierzytelniania użytkownika w systemie teleinformatycznym;
9) **Kopia zapasowa (ang.: backup)** - kopia danych, które mają służyć do odtworzenia oryginalnych danych w przypadku ich utraty lub uszkodzenia;
10) **Nośnik informacji** - medium magnetyczne, optyczne, półprzewodnikowe lub papierowe, na którym zapisuje się i przechowuje informacje (forma utrwalenia dokumentu);
11) **Stacja robocza** - komputer, laptop bądź inne urządzenie informatyczne działające w ramach sieci Urzędu;
12) **Zasób (aktywa)** - wszystko to, co ma wartość dla Urzędu Gminy Michałowice, w szczególności bazy danych, katalogi sieciowe i aplikacje wspomagające pracę Urzędu (Dokument Systemu Zarządzania Bezpieczeństwem Informacji oznaczony IT-SZBI-07.01 oraz IT-SZBI-07.01a)
13) **Wiedza konieczna** - jest to wiedza niezbędna do wykonywaniu zadań na danym stanowisku;
14) **PBI** – niniejszy dokument tj. Polityka Bezpieczeństwa Informacji;
15) **SZBI (System Zarządzania Bezpieczeństwem Informacji)** - zbiór procedur, wykazów, polityk i instrukcji, gwarantujących poufności, dostępności i integralności informacji przetwarzanych w Urzędzie Gminy Michałowice opisanych w dokumentacji wymienionej w załączniku do zarządzenia 113/2012

II. INFORMACJA OGÓLNA

1. Niniejszy dokument jest zbiorem zasad określającym organizację i funkcjonowanie systemu zarządzania bezpieczeństwem informacji w Urzędzie Gminy Michałowice. Dokument został opracowany w związku z wymogami jakie stawia się podmiotom realizującym zadania publiczne w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2016 r. poz. 113 ze zm.).
2. Niniejszy dokument służy między innymi podniesieniu standardów ochrony informacji przetwarzanych w systemie teleinformatycznym Gminy Michałowice i udostępniany jest pracownikom Urzędu zgodnie z zakresem obowiązków.
3. Niniejszy dokument jest częścią Systemu Zarządzania Bezpieczeństwem Informacji, w wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w pozostałych procedurach i instrukcjach należących do SZBI lub innych procedurach obowiązujących w Jednostce, użytkownicy mają obowiązek stosowania unormowań dalej idących (bardziej restrykcyjnych), których stosowanie zapewni wyższy poziom ochrony danych.
4. Z dokumentem zapoznać należy w całości:
   1) Pracowników Referatu Informatyki realizujących zadania związane z ochroną informacji przetwarzanych w systemie teleinformatycznym Urzędu;
   2) Pracowników, którzy realizują zadania związane z nadzorem nad przestrzeganiem bezpieczeństwa informacji, w tym audytorów i kontrolerów wewnętrznych;
5. Kierownicy komórek organizacyjnych oraz pracownicy pracujących w systemach informatycznych powinni zostać zapoznani z niniejszym dokumentem, poza § 10 Mechanizmy bezpieczeństwa sieci, §11Bezpieczeństwo okablowania i §12 Bezpieczeństwo strefy wydzielonej oraz z dokumentami SZBI:
   1) IT-SZBI-07.03 - procedura tworzenia i przechowywania kopii zapasowych,
   2) IT-SZBI-07.07 - procedura nadawania, modyfikacji i odebrania uprawnień do zasobów informatycznych,
   3) IT-SZBI-07.08 - procedura rozpoczęcia, zawieszenia i zakończenia pracy,
   4) IT-SZBI-07.11 - procedura tworzenia i zarządzania hasłami;
6. Za zarządzanie, opracowanie, przegląd, aktualizację, ocenę PBI, kontrolę wdrażania bezpieczeństwa informacji odpowiada Kierownik Referatu Informatyki oraz pracownicy przez niego wyznaczeni.
7. Czynności dotyczące przeglądów PBI będą odnotowywane w Rejestrze zmian dokumentu.

III. EKSPLOATACJA SYSTEMÓW INFORMATYCZNYCH

§ 1.
Podstawowe obowiązki w eksploatacji, podział obowiązków.

1. Osobą odpowiedzialną za użytkowane systemu informatycznego w komórce organizacyjnej jest Właściciel Zasobu.
2. Właściciel Zasobu może przekazać administrowanie systemem (czynności wykonawcze) ASI co wymaga formy pisemnej. Właściciel Zasobu sprawuje kontrolę nad działaniami wykonawczymi realizowanymi przez ASI.
3. ASI ponosi odpowiedzialność za bezpieczeństwo funkcjonowania systemu informatycznego w ramach powierzonych mu obowiązków.
4. Role zarządcze (Właściciela Zasobu) i wykonawcze (ASI) w zakresie eksploatacji systemów teleinformatycznych mogą być wykonywane przez tą samą komórkę organizacyjną.
5. Oprogramowanie stacji roboczych podłączanych do systemu teleinformatycznego Urzędu konfigurowane jest zgodnie z dokumentacją Systemu Zarządzania Bezpieczeństwem Informacji – Konfiguracja Systemu Informatycznego oznaczenie IT-SZBI-07.10.
6. Osobą odpowiedzialną za prawidłową konfigurację stacji roboczej jest ASI.
7. ASI nadzoruje, poprzez dokonywanie okresowych przeglądów podczas których sprawdza skuteczność:
   1) zabezpieczeń systemów informatycznych, w których przetwarzane są dane osobowe przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do w/w systemów,
   2) przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych,
   3) nadawania uprawnień do systemów informatycznych, w których przetwarzane są dane osobowe i rejestrowania tych uprawnień w systemie informatycznym,
   4) stosowania procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania (sposób, miejsce i okres przechowywania, elektronicznych nośników informacji, kopii zapasowych),
   5) usuwania w możliwie trwały sposób danych osobowych z konta użytkownika oddającego stację roboczą przed udostępnieniem tej stacji kolejnemu użytkownikowi,
   6) monitorowania wdrożonych zabezpieczeń.

§ 2.
Role i zakresy odpowiedzialności pracowników.

1. Przed przystąpieniem do realizacji zadań i obowiązków nowo zatrudnieni pracownicy zostają przeszkoleni przez Kierownika komórki lub wskazaną przez niego osobę w zakresie odpowiednim do zajmowanego stanowiska oraz zapoznają się z dostępną dokumentacją i informacjami wynikającymi z funkcjonowania Urzędu. Pracownik jest zobowiązany do zapoznania się z zapisami PBI, fakt ten dokumentuje się w formie pisemnej.
2. Pracownicy przetwarzający dane osobowe podpisują stosowne oświadczenia zgodnie z zapisami Polityki Bezpieczeństwa Przetwarzania Danych Osobowych (oznaczenie dokumentu: IT-SZBI-02) wprowadzonej właściwym Zarządzeniem Wójta Gminy.

3. Pracownicy zaangażowani w proces przetwarzania informacji zobowiązani są przynajmniej raz na dwa lata uczestniczyć w szkoleniu uwzględnieniem takie zagadnienia, jak:
   1) zagrożenia bezpieczeństwa informacji,
   2) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
   3) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich,
   4) ochrona danych osobowych.

§ 3.
Monitorowanie zasobów i wydajności krytycznych systemów oraz zasilania.

1. ASI jest odpowiedzialny za prognozowanie wymagań dotyczących pojemności oraz wydajności kluczowych elementów systemów teleinformatycznych w celu ograniczenia ryzyka przeciążenia systemu.
2. Wymagania dotyczące pojemności nowych systemów, wynikające z rzeczywistych potrzeb Urzędu, są definiowane i zatwierdzane przed dokonaniem zakupu, zaakceptowaniem i wdrożeniem tych systemów.
3. Pracownicy Referatu Informatyki w miarę możliwości technicznych prowadzą monitorowanie eksploatowanych krytycznych systemów, przez gromadzenie informacji dotyczących następujących elementów i parametrów systemów:
   1) infrastruktury sieciowej, w zakresie przepustowości i obciążenia łączy (interfejsów) oraz procesorów urządzeń sieciowych,
   2) serwerów usług, aplikacji i baz danych Urzędu, w zakresie obciążenia procesora, pamięci RAM, zajętości pamięci dyskowej, obciążenia interfejsów sieciowych, przyrostu danych w okresie miesiąca,
   3) zasilania awaryjnego serwerowni.
4. Monitorowanie zasobów i wydajności krytycznych systemów jest prowadzone w sposób doraźny nie rzadziej niż raz na pół roku.
5. Testy zasilania awaryjnego serwerowni (UPS oraz agregatu prądotwórczego) przeprowadzane są pracowników Referatu Informatyki zgodnie z zaleceniami producenta. Wyniki testów odnotowywane są w rejestrze (wpis powinien zawierać datę testu, wynik testu oraz imię i nazwisko osoby wykonującej test)

§ 4.
Ochrona przed szkodliwym oprogramowaniem

1. Serwery i stacje robocze pracowników w Urzędzie objęte są ochroną przez działanie systemu antywirusowego w czasie rzeczywistym oraz zaporę systemową, które zapewniają integralność zasobów przechowywanych i przetwarzanych w systemie teleinformatycznym Urzędu.
2. W systemach Urzędu wdrożono centralnie zarządzany system antywirusowy.
3. Aktualizacja baz sygnatur wirusów oraz wymaganych aktualizacji systemów operacyjnych odbywa się automatycznie przez centralne ustawienia serwerów zarządzających.
4. Centralne ustawienia systemu antywirusowego wymuszają automatyczne skanowanie podłączanych nośników zewnętrznych.

5. Po każdej naprawie i konserwacji urządzenia, a przed ponownym włączeniem do systemu teleinformatycznego Urzędu, ASI dokonuje sprawdzenia czy jest zainstalowane aktualne oprogramowanie antywirusowe.
6. Urządzenia przenośne (laptopy) ze względu na okresową pracę poza systemem informatycznym Urzędu posiadają zainstalowane oprogramowanie antywirusowe aktualizujące się bezpośrednio od producenta systemu antywirusowego.
7. Za prawidłową aktualizację bazy sygnatur wirusów oraz wersji oprogramowania antywirusowego odpowiada ASI.

§ 5.
Kontrola licencjonowanego oprogramowania oraz własności intelektualnej.

1. Dla wszystkich systemów i aplikacji użytkowanych w Urzędzie ASI prowadzi spisy licencjonowanego oprogramowania.
2. Spis licencjonowanego oprogramowania jest kontrolowany przez Kierownika Referatu Informatyki pod kątem kompletności ewidencji.
3. Na komputerach służbowych oraz wszelkich służbowych nośnikach danych zabronione jest przechowywanie danych oraz plików objętych prawami własności intelektualnej, chyba że pracownik wykaże się posiadaniem stosownych praw autorskich.
4. Na komputerach służbowych oraz wszelkich służbowych nośnikach danych zabronione jest przechowanie prywatnych plików, danych niezwiązanych z realizacją zadań służbowych, w szczególności plików multimedialnych.
5. Okresowo, stacje robocze i udostępnione udziały sieciowe użytkowników są sprawdzane przez ASI pod kątem obecności nieautoryzowanego oprogramowania lub plików chronionych własnością intelektualną w ramach okresowego przeglądu eksploatacyjnego.
6. Do przeprowadzenia kontroli zgodności zainstalowanego oprogramowania z posiadanymi licencjami oraz plików chronionych własnością intelektualną ASI może stosować narzędzia programowe umożliwiające m.in.:
   1) automatyczne sprawdzanie stacji roboczych i serwerów,
   2) centralne zarządzanie spisem licencjonowanego oprogramowania.
7. Nieautoryzowane oprogramowanie jest niezwłocznie usuwane z systemu teleinformatycznego, a informacje o przypadkach używania nieautoryzowanego oprogramowania są przedstawiane niezwłocznie przez Kierownika Referatu Informatyki Kierownictwu oraz Kierownikowi Referatu w którym wystąpił incydent.

§ 6.
Kopie bezpieczeństwa

1. W celu zapewnienia optymalnego poziomu ochrony danych gromadzonych w systemach informatycznych Urzędu stosuje się architekturę klient-serwer do przetwarzania informacji zawartych w bazach danych. Jeśli aplikacje nie są zgodne z powyższymi rozwiązaniami, należy zapewnić możliwość przechowywania przetwarzanych danych w wyznaczonych zasobach serwerów plików. Osobą odpowiadającą za realizację powyższych wytycznych jest ASI.
2. Systemy operacyjne stacji roboczych konfiguruje się w taki sposób aby zawartość „Pulpitów" oraz domyślnych katalogów użytkowników „Dokumenty" znajdujących się w systemach Microsoft Windows przekierować na serwery domeny Windows.

3. Indywidualne stanowiska komputerowe, do których dostęp posiadają pracownicy Urzędu, stanowią jedynie końcówki systemu komputerowego. Wszystkie informacje (w tym dane osobowe) które nie są gromadzone przy pomocy uruchamianych na poszczególnych stanowiskach aplikacjach bazodanowych powinny być zapisywane w katalogach przechowywanych bezpośrednio na serwerach, np.:
   1) Pulpit,
   2) Dokumenty,
   3) Specjalnie wydzielone katalogi wspólne grup roboczych do których dostęp mają pracownicy poszczególnych komórek organizacyjnych.
4. Użytkownicy stanowisk mobilnych odłączanych od sieci i użytkowanych poza siecią urzędu nie posiadają domyślnych przekierowań zabezpieczających dane przetwarzane lokalnie. W celu zabezpieczenia danych przetwarzanych lokalnie stosuje się dedykowane oprogramowanie do wykonywania automatycznych kopii zapasowych.

§ 7.
Zarządzanie kopiami zapasowymi i archiwalnymi

1. Kopie zapasowe systemów, aplikacji, baz danych i dokumentów użytkowanych w Urzędzie służą do zapewnienia możliwości odtworzenia całości systemu w przypadku utraty aktualnie użytkowanych danych i/lub konfiguracji systemów i aplikacji.
2. Tworzenie kopii odbywa się zgodnie z procedurą „Tworzenia i przechowywania kopii zapasowych" opisaną w dokumencie Systemu Zarządzania Bezpieczeństwem Informacji oznaczonym IT-SZBI-07.03.

§ 8.
Przechowywanie nośników informacji

1. Elektroniczne nośniki informacji:
   1) szczegółowy opis postępowania z danymi osobowymi określa Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Michałowice (oznaczenie dokumentu: IT-SZBI-02) oraz Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Michałowice (oznaczenie dokumentu: IT-SZBI-03) w zakresie przetwarzania danych osobowych Urzędu Gminy Michałowice,
   2) wymienne elektroniczne nośniki informacji należy przechowywać w pokojach stanowiących obszar przetwarzania danych osobowych o którym mowa w załączniku nr 8 do Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Michałowice (oznaczenie dokumentu: IT-SZBI-02),
   3) po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji należy przechowywać w zamykanych szafach biurowych lub kasetkach,
   4) dane osobowe w postaci elektronicznej po ich wykorzystaniu należy usunąć niezwłocznie z nośnika informacji w sposób uniemożliwiający ich ponowne odtworzenie, chyba że z odrębnych przepisów wynika obowiązek ich przechowywania,
   5) w przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe należy fizycznie zniszczyć nośnik,
   6) dyski twarde z danymi osobowymi należy przed oddaniem do utylizacji zniszczyć w sposób uniemożliwiający odtworzenie danych.

2. Wydruki:
   1) wydruki, zawierające dane osobowe, należy przechowywać w pokojach stanowiących obszar przetwarzania danych osobowych o którym mowa w załączniku nr 8 do Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Michałowice (oznaczenie dokumentu: IT-SZBI-02),
   2) wydruki, zawierające dane osobowe, należy zniszczyć przez pocięcie w specjalnym urządzeniu niezwłocznie po ich wykorzystaniu, chyba że z odrębnych przepisów wynika obowiązek ich przechowywania.
3. Dane wejściowe do systemu, np. dane osobowe zapisane w postaci papierowej innej niż wydruki z systemu (pisma, ankiety itp.) należy przechowywać na podobnych zasadach, co wydruki, chyba że odrębne przepisy stanowią inaczej.

§ 9.
Zarządzanie poprawkami technicznymi

1. Zarządzanie poprawkami ma na celu eliminowanie lub ograniczanie zidentyfikowanych podatności systemów teleinformatycznych.
2. ASI jest zobowiązany do monitorowania i wprowadzania poprawek do kluczowych systemów oraz aplikacji Urzędu.
3. ASI jest zobowiązany do wprowadzania poprawek w oparciu o informacje uzyskane od producentów urządzeń sieciowych, systemów operacyjnych i aplikacji oraz od profesjonalnych organizacji zajmujących się tematyką bezpieczeństwa informacji i systemów teleinformatycznych.
4. Dla systemów operacyjnych na stanowiskach komputerowych w Urzędzie poprawki dostarczane są za pomocą automatycznych mechanizmów dostarczonych przez producenta systemu operacyjnego lub kontroler domeny.
5. Za zatwierdzanie, aktualizację i monitorowanie stanu wdrożonych aktualizacji odpowiada ASI.

IV. BEZPIECZEŃSTWO SIECI TELEINFORMATYCZNEJ

§ 10.
Mechanizmy bezpieczeństwa sieci

1. Urząd zapewnia bezpieczeństwo sieci za pomocą niżej wymienionych mechanizmów:
   1) aplikacji i urządzeń typu firewall na poziomie sieci,
   2) aplikacji i urządzeń antywirusowych stosowanych podczas wymiany danych pomiędzy siecią Urzędu, a sieciami należącymi do innych podmiotów lub sieciami publicznymi,
   3) rozdzielania sieci na mniejsze segmenty logiczne za pomocą technologii VLAN,
   4) monitorowanie ruchu sieciowego pod kątem ewentualnego wystąpienia zdarzeń wskazujących na możliwość niepożądanej działalności osób z zewnątrz (intruzów),
   5) aktualizowanie aplikacji, systemów operacyjnych oraz usług sieciowych do najnowszej oraz bezpiecznej i stabilnej wersji.
2. Reguły filtrowania zapór sieciowych ustalane są przez ASI i weryfikowane w zależności od pojawiających się zagrożeń.
3. Dostęp do sieci Urzędu z poza siedziby odbywa się za pomocą bezpiecznych kanałów VPN lub wydzielonych (dedykowanych) łączy teleinformatycznych.
4. Aktywność pracowników w sieci oraz dostęp do stron www jest monitorowany w sposób ciągły, a występujące zdarzenia rejestrowane w dziennikach zdarzeń przechowywanych na centralnych serwerach lub dedykowanych urządzeniach, które podlegają okresowym przeglądom przez ASI.
5. Dostęp zdalny do aktywów Urzędu przyznawany jest ASI oraz pracownikom wykonującym czynności poza siedzibą Urzędu, dla których jest on niezbędny do wykonywania czynności służbowych, wynikających z ich zakresów obowiązków.
6. Pracownik wykonujący czynności poza siedzibą Urzędu musi tak zorganizować miejsce pracy aby osoby trzecie nie miały dostępu do danych Urzędu.
7. Dostęp zdalny jest możliwy tylko i wyłącznie za pomocą bezpiecznych kanałów komunikacji.

§ 11.
Bezpieczeństwo okablowania

1. Okablowanie strukturalne składa się z traktów kablowych – listw PCV, przepustów kablowych, szaf dystrybucyjnych, szaf krosowych, tablic rozdzielczych.
2. Infrastruktura okablowania telekomunikacyjnego i elektrycznego jest ułożona w sposób zapewniający brak wzajemnego oddziaływania linii.
3. Okablowanie telekomunikacyjne i elektryczne prowadzone jest generalnie poza strefami ogólnie dostępnymi, w przypadku prowadzenia okablowania przez takie miejsca zastosowane są środki uniemożliwiające bądź ograniczające dostęp do okablowania przez osoby nieupoważnione.
4. Niewykorzystywane segmenty sieci strukturalnej są odłączone od sieci teleinformatycznej w sposób mechaniczny lub logiczny.

§ 12.
Bezpieczeństwo strefy wydzielonej

Dokumentację bezpieczeństwa strefy wydzielonej oraz zlokalizowanego w niej Bezpiecznego Stanowiska Komputerowego (BSK) prowadzi Pełnomocnik do spraw ochrony informacji niejawnych przy wsparciu Administratora systemu BSK.

V. BEZPIECZEŃSTWO SYSTEMÓW INFORMATYCZNYCH

§ 13.
Ogólne mechanizmy bezpieczeństwa

1. W Urzędzie stosuje się następujące mechanizmy bezpieczeństwa systemów informatycznych:
   1) uwierzytelnianie użytkowników,
   2) rejestrowanie udanych i nieudanych prób dostępu do systemu,
   3) rejestrowanie korzystania z przywilejów systemowych,
2. Systemy operacyjne pracujące w Urzędzie posiadają włączone mechanizmy bezpiecznego logowania zapewniające (w zależności od możliwości technicznych):
   1) ujawnianie minimum informacji o systemie,
   2) unikanie wyświetlania komunikatów pomocniczych, które mogłyby pomóc nieuprawnionemu użytkownikowi przy nieautoryzowanych próbach dostępu,
   3) unikanie wskazywania, która część danych jest poprawna lub niepoprawna w przypadku wystąpienia błędu podczas logowania,
   4) ograniczenie liczby nieudanych prób logowania się do systemu,
   5) wykonywanie zapisu nieudanego logowania w dziennikach (logach zdarzeń),
   6) blokowanie wyświetlania hasła w trakcie jego wprowadzania,
   7) szyfrowanie przesyłanych haseł.

§ 14.
Identyfikacja i uwierzytelnianie użytkowników

1. Generalną zasadą bezpieczeństwa systemów i sieci informatycznych jest ochrona informacji przed nieuprawnionym dostępem, ujawnieniem, losowym lub nieuprawnionym zniszczeniem lub modyfikacją, a także przed opóźnieniem lub nieuzasadnioną odmową ich udostępnienia.
2. Stosowanie zasad uwierzytelniania użytkowników systemów informatycznych ma bezpośredni wpływ na zachowanie poufności, rozliczalności oraz autentyczności danych.
3. Użytkownicy systemów posiadają unikalne identyfikatory użytkownika (login) do swojego osobistego i wyłącznego użytku.
4. Użytkownikowi przydziela się zasoby systemu teleinformatycznego i uprawnienia systemowe na poziomie minimalnym, niezbędnym dla wykonywania swoich czynności służbowych.
5. Stosowane identyfikatory użytkownika nie wskazują na poziom uprawnień danego użytkownika.
6. Niedopuszczalne jest wykorzystywanie jednego identyfikatora przez więcej niż jednego użytkownika.

§ 15.
Rozpoczęcie, zawieszenie i zakończenie pracy

Informacje na temat czynności jakie należy podjąć podczas rozpoczęcia, zawieszenia i zakończenia pracy na stanowisku komputerowym opisano w Procedurze rozpoczęcia,

zawieszenia i zakończenia pracy (oznaczenie dokumentu: IT-SZBI-07.08) będącej częścią Systemu Zarządzania Bezpieczeństwem Informacji.

§ 16.
System zarządzania hasłami

1. Każdy użytkownik posiada przypisane tylko jemu hasło, którym autoryzuje się w systemie informatycznym.
2. ASI poprzez ustawienia systemowe wymusza natychmiastową konieczność zmiany hasła początkowego, przydzielonego pracownikowi, na nowe przez niego wybrane. Hasła początkowe wydawane są zgodnie z procedurą „tworzenia i zarządzania hasłami" (oznaczenie dokumentu: IT-SZBI-07.11 będącej częścią Systemu Zarządzania Bezpieczeństwem Informacji).
3. Zabronione jest przekazywanie haseł osobom trzecim.
4. Przy konfigurowaniu ustawień logowania do systemu teleinformatycznego stosuje się następujące zasady:
   1) użytkownik musi podać swój login i hasło. Hasło jest prezentowane w postaci niejawnej,
   2) jeśli aplikacja lub inne oprogramowanie merytoryczne umożliwia integracje z domenowym systemem uwierzytelniania dopuszcza się stosowanie tego rozwiązania,
   3) logowanie odbywa się do domeny UGM.local
5. Procedurę tworzenia i zarządzania hasłami opisano w dokumencie: IT-SZBI-07.11 będącym częścią Systemu Zarządzania Bezpieczeństwem Informacji.
6. W przypadku kompromitacji hasła należy niezwłocznie zmienić hasło oraz powiadomić o tym fakcie ASI.
7. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym wglądu do danych wyświetlanych na monitorach komputerowych - tzw. „polityka czystego ekranu".
8. W przypadku zablokowania konta sieciowego należy powiadomić ASI. W szczególnych przypadkach nagminnego blokowania kont sieciowych logowanie zostaje ograniczone do konkretnej stacji roboczej.
9. Systemy, w których są przetwarzane dane osobowe muszą być zabezpieczone hasłami spełniającymi wymagania rozporządzenia wykonawczego do ustawy o ochronie danych osobowych.

§ 17.
Ograniczenia czasowe sesji połączeniowych

W celu wymuszenia ochrony urządzeń systemu teleinformatycznego stosuje się mechanizmy w postaci wygaszaczy ekranu, blokujące dostęp do stacji roboczej po upływie 15 min bezczynności. Odblokowanie stacji roboczej możliwe jest po ponownym uwierzytelnieniu użytkownika.

§ 18.
Zasady dostępu do plików i katalogów sieciowych

1. Uprawnienia dostępu do plików i katalogów sieciowych z poziomu systemu operacyjnego są nadawane przez ASI po zleceniu takiego przydziału przez Właściciela danego Zasobu.

2. Przydzielanie dostępu do plików i katalogów odbywa się na podstawie procedury „nadawania, modyfikacji, odebrania uprawnień do zasobów informatycznych" oznaczenie dokumentu: IT-SZBI-07.07 będącego częścią Systemu Zarządzania Bezpieczeństwem Informacji.

§ 19.
Eksploatacja aplikacji w systemach teleinformatycznych Urzędu

1. Za prawidłową eksploatację aplikacji i systemów informatycznych wspomagających funkcjonowanie i zarządzanie Urzędu odpowiada Właściciel Zasobu.
2. Właściciel Zasobu zobowiązany jest powiadomić ASI o wszelkich nieprawidłowościach związanych z funkcjonowaniem aplikacji i zasobów obsługiwanych w jego komórce.
3. Uprawnienia administracyjne do zasobów informatycznych nadawane są ograniczonej liczbie użytkowników.
4. Przydzielanie uprawnień do aplikacji i systemów informatycznych wspomagających pracę Urzędu odbywa się na podstawie procedury „nadawania, modyfikacji, odebrania uprawnień do zasobów informatycznych" oznaczenie dokumentu: IT-SZBI-07.07 będącego częścią Systemu Zarządzania Bezpieczeństwem Informacji.
5. W przypadku, gdy w systemie informatycznym przetwarzane są dane osobowe, zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922 ze zm.) przydzielanie lub odebranie uprawnień odbywa się na zasadach opisanych w Polityce bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Michałowice (oznaczenie dokumentu: IT-SZBI-02) oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Michałowice (oznaczenie dokumentu: IT-SZBI-03).
6. Nie rzadziej niż raz w roku ASI dokonuje przeglądu uprawnień użytkowników systemu informatycznego.
7. Modyfikacja uprawnień użytkownika systemu informatycznego może być dokonywana doraźnie na polecenie Właściciela Zasobu, czynności związane z modyfikacją uprawnień dokumentuje się w formie pisemnej.
8. Ustanawia się listę oprogramowania oraz innych zasobów użytkowanych w Urzędzie Gminy Michałowice stanowiącą część Systemu Zarządzania Bezpieczeństwem Informacji (oznaczenie dokumentu: IT-SZBI-07.01 i IT-SZBI-07.01a).
9. Wykaz o którym mowa w punkcie 8, jak i wszelkie zmiany w jego treści, zatwierdzany jest przez Kierownictwo Urzędu lub osoby upoważnione, doraźnie ale nie rzadziej niż raz w roku.

VI. ZARZĄDZANIE ZMIANAMI W SYSTEMACH TELEINFORMATYCZNYCH URZĘDU

§ 20.
Odbiór systemu teleinformatycznego

1. Kryteria odbioru obejmują dostarczenie:
   1) w przypadku oprogramowania - dokumentacji technicznej, instrukcji dla administratora i użytkownika,
   2) w przypadku infrastruktury - dokumentacji powykonawczej obejmującej w szczególności schemat połączeń fizycznych i logicznych elementów infrastruktury.
2. Odbiór oprogramowania obejmuje następujące główne elementy (jeżeli mają zastosowanie):
   1) wykonanie instalacji oprogramowania,
   2) wykonanie testowania systemu,
   3) odbiór oprogramowania potwierdzony stosownym dokumentem,
   4) odrzucenie oprogramowania potwierdzone stosownym dokumentem w przypadku negatywnych wyników testów,
3. Każdorazowo, wraz ze zmienioną wersją oprogramowania aplikacji Urzędu, wykonawca dostarcza:
   1) wykaz dokonanych zmian w systemie w stosunku do poprzedniej wersji wraz z ich opisem,
   2) uaktualnienie dokumentacji uwzględniające zmiany dokonane w oprogramowaniu.
4. Dopuszcza się odstępstwo od zasad wymienionych w ust.1-3 w przypadku rozwiązań trywialnych.
5. System, w którym przetwarzane są dane osobowe zapewnia (zgodnie z § 7 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych):
   1) datę pierwszego wprowadzenia danych do systemu
   2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do sytemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba,
   3) źródło danych, w przypadku zbierania danych, nie od osoby, której one dotyczą.

§ 21.
Kontrola zmian w eksploatacji systemów krytycznych

1. Kontrola zmian systemów i aplikacji ma na celu zapewnianie poprawnego i bezpiecznego działania systemów krytycznych pracujących w Urzędzie.
2. Zarządzanie zmianami polega na koordynacji, nadawaniu priorytetów, zatwierdzaniu, planowaniu zasobów i oceny ryzyka w związku ze zmianami dokonywanymi w krytycznych systemach teleinformatycznych Urzędu.

3. Zasady wskazane w niniejszym paragrafie odnoszą się do zmian aplikacyjnych będących poprawkami (w tym usuwanie błędów) albo modyfikacjami. Zmiany aplikacyjne są klasyfikowane jako:
   1) zmiany aplikacyjne regularne - oznaczają zmiany, które nie wymagają natychmiastowego wdrożenia,
   2) zmiany aplikacyjne awaryjne - wprowadzane w stanie pilnej konieczności z powodu zagrożenia działania aplikacji.
4. Za proces zarządzania zmianami w poszczególnych obszarach, odpowiedzialny jest Referat Informatyki.
5. Każda zmiana regularna jest poprzedzona:
   1) zapoznaniem się z opisem zmiany,
   2) zapoznaniem się opisem rodzaju wymaganych działań,
   3) wykonaniem kopii zapasowej z możliwością odtworzenia stanu poprzedniego na wypadek nieprzewidzianych zdarzeń (jeżeli ma zastosowanie),
   4) przetestowaniem zmian.
6. Zmiana mająca charakter awaryjny, którą trzeba wprowadzić bezzwłocznie w celu ograniczenia ryzyka poważnego zakłócenia działalności Urzędu wykonywana jest w porozumieniu z Właścicielem Zasobu

§ 22.
Bezpieczeństwo dokumentacji systemu

1. Dokumentacja powykonawcza infrastruktury oraz dokumentacja techniczna, administratora i użytkownika podlega ochronie.
2. Dokumentacja systemów teleinformatycznych prowadzona i utrzymywana jest w Referacie Informatyki.
3. Dokumentacja systemów jest udostępniana na zasadzie „wiedzy koniecznej".

VII. ZARZĄDZANIE WYMIENNYMI NOŚNIKAMI KOMPUTEROWYMI

§ 23.
Użytkowanie nośników

1. Nośniki komputerowe są przechowywane i eksploatowane zgodnie z zaleceniami producenta, z uwzględnieniem wymagań w zakresie ochrony informacji, w tym danych osobowych, które są umieszczone na nośnikach. Okres przechowywania nośników jest zgodny z wymaganiami Urzędu oraz ustawą.
2. Nośniki zawierające informacje w tym dane osobowe przechowywane są w zamykanych szafach zapewniających ochronę dostępem osób postronnych.

§ 24.
Wycofanie z eksploatacji nośników komputerowych

Zasady i tryb postępowania z nośnikami komputerowymi przeznaczonymi do wycofania opisano w procedurze „Wycofania z eksploatacji nośników komputerowych" będącej częścią Systemu Zarządzania Bezpieczeństwem Informacji (oznaczenie dokumentu: IT-SZBI-07.04).

VIII. BEZPIECZEŃSTWO WYMIANY DANYCH

§ 25.
Bezpieczeństwo wymiany poczty elektronicznej wewnętrznej i zewnętrznej

1. Wszyscy pracownicy Urzędu mają dostęp do służbowej poczty elektronicznej.
2. System poczty elektronicznej zapewnia w miarę możliwości technicznych:
   1) ochronę przed szkodliwym oprogramowaniem rozpowszechnianym za pomocą poczty elektronicznej,
   2) ochronę antywirusową załączników przesyłanych w poczcie elektronicznej,
   3) ochronę antyspamową,
   4) możliwość użycia dostępnych technik kryptograficznych do ochrony poufności i integralności wiadomości poczty elektronicznej,
3. Poczta elektroniczna w Urzędzie służy wyłącznie do celów służbowych.
4. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów teleinformatycznych Urzędu podlega rejestrowaniu i może być monitorowana. Kierownik Referatu Informatyki lub ASI posiada uprawnienia do monitorowania wiadomości w zakresie prawidłowego jej funkcjonowania lub w przypadku wystąpienia incydentu.
5. Informacje przesyłane za pośrednictwem sieci Urzędu (w tym do i z Internetu) nie stanowią własności prywatnej użytkownika.
6. Wiadomości elektroniczne niezwiązane z działalnością Urzędu, a zawierające słowa bądź temat uznane za niedozwolone, mogą być blokowane i następnie usuwane z systemu pocztowego.
7. Korzystanie z poczty elektronicznej Urzędu poza siecią wewnętrzną jest możliwe tylko za pomocą ustawienia połączenia szyfrowanego klienta poczty.
8. Możliwe jest korzystanie z poczty elektronicznej poza siecią Urzędu za pomocą przeglądarki internetowej pod adresem: https://poczta.home.pl/
9. Nie jest dopuszczalne:
   1) rozsyłanie z komputerów Urzędu oraz ze służbowych kont pocztowych wiadomości, których treść nie jest związana z wykonywaną pracą,
   2) wykorzystywania służbowych kont pocztowych do działań które mogą doprowadzić do narażenia Urzędu na szkody,
   3) odbieranie przesyłek z nieznanych źródeł,
   4) otwieranie załączników zawierających pliki samorozpakowujące się bądź wykonywalne typu bat, com, exe, itp., plików multimedialnych lub graficznych niezwiązanych z zakresem wykonywanych obowiązków służbowych,
   5) odpowiadanie na emaile określone jako spam (łańcuszki, wiadomości reklamowe),
   6) używanie adresów służbowych kont pocztowych do rejestracji na forach dyskusyjnych, chat'ach, stronach internetowych, niezwiązanych z zakresem wykonywanych obowiązków służbowych,
   7) wykorzystywanie służbowych kont pocztowych w celach prywatnych i innych niż wynikające z potrzeb Urzędu
10. Ustala się domyślne wartości i ograniczenia dla systemu poczty elektronicznej (w uzasadnionych przypadkach za zgodą Referatu Informatyki i w miarę dostępnych możliwości technicznych ustalone parametry mogą zostać przekroczone):
    1) wielkość skrzynki pocztowej przechowywanej na serwerze – 1GB,

2) wielkość skrzynki pocztowej przechowywanej na dysku lokalnym stacji roboczej – 30GB
3) wielkość jednorazowo przesyłanej wiadomości – 20 MB

11. Użytkownicy zobowiązani są do okresowego porządkowania i usuwania wiadomości zbędnych z folderów osobistych programu pocztowego tak, aby nie dopuścić do jej zablokowania z powodu przekroczenia dopuszczalnej pojemności skrzynki.

IX. GOSPODAROWANIE SPRZĘTEM KOMPUTEROWYM

§ 26.
Konserwacja i naprawa sprzętu

1. Sprzęt komputerowy w Urzędzie podlega okresowemu przeglądowi i konserwacji w celu zapewnienia nieprzerwanej i bezpiecznej pracy.
2. Konserwacje i przeglądy sprzętu komputerowego prowadzone są przez ASI.
3. Przegląd sprzętu komputerowego może odbywać się poprzez specjalistyczne oprogramowanie monitorujące pracę podzespołów komputera lub w trybie doraźnym na miejscu w momencie zgłoszenia takiego faktu do Referatu Informatyki.
4. Naprawy sprzętu komputerowego przeprowadzane przez autoryzowany serwis producenta w ramach gwarancji wykonywane są pod nadzorem ASI w siedzibie Urzędu.
5. W przypadku naprawy sprzętu komputerowego w serwisie producenta poza siedzibą Urzędu, dane poufne umieszczone na dysku twardym, w tym dane osobowe, który jest integralną częścią zestawu komputerowego, są skutecznie usuwane z nośnika przez ASI po uprzednim wykonaniu ich kopii bezpieczeństwa.
6. Dla uniknięcia utraty gwarancji zawierane jest stosowne porozumienie z dostawcą sprzętu odnośnie trwałego usunięcia informacji prawnie chronionych, w tym danych osobowych z nośnika informacji.
7. W przypadku likwidacji sprzętu komputerowego, zbywania lub przekazania go innemu pracownikowi do ponownego użycia ASI usuwa z niego informacje prawnie chronione, dane osobowe lub poufne przy pomocy specjalistycznego oprogramowania służącego do trwałego usuwania danych. Konto użytkownika oddającego sprzęt jest trwale usuwane z oddawanej stacji roboczej.

§ 27.
Zabezpieczenie sprzętu poza siedzibą

1. Wynoszenie sprzętu komputerowego, a w szczególności komputerów przenośnych poza siedzibę Urzędu jest możliwe tylko za zgodą Kierownictwa.
2. Pracownik użytkujący urządzenie przenośne, wykonujący zadania służbowe poza siedzibą Urzędu odpowiedzialny jest za jego ochronę. Zabronione jest pozostawianie urządzenia przenośnego bez opieki w miejscach szczególnie narażonych na kradzież takich jak: samochód, przedział kolejowy oraz w innych miejscach gdzie pracownik nie ma możliwości sprawowania nad nim skutecznego nadzoru.
3. Urządzenia przenośne pracujące poza siedzibą Urzędu posiadające dane poufne w tym dane osobowe należy wyposażyć w oprogramowanie szyfrujące.
4. W razie utraty komputera przenośnego pracownik niezwłocznie powiadamia o tym swojego przełożonego, a w razie kradzieży dodatkowo niezwłocznie zgłasza ten fakt właściwym służbom, określając rodzaj utraconych informacji.
5. W przypadku pozostawienia komputerów przenośnych w Urzędzie zaleca się umieszczenie ich po zakończeniu pracy w zamykanych szafach.

6. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, Użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.
7. Na komputerach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny znajdować się dane osobowe lub dane poufne.
8. Użytkownik komputera przenośnego jest zobowiązany do regularnego podłączania urządzenia do sieci urzędu w celu utworzenia kopii zapasowej przetwarzanych danych.

X. ZASADY MONITOROWANIA SYSTEMÓW I ICH UŻYCIA

§ 28.
Mechanizmy monitorowania systemów

1. Monitorowanie systemów i ich użycia ma na celu wykrywanie nieuprawnionych działań.
2. Rejestrowane i monitorowane są wszystkie zdarzenia polegające na użyciu urządzeń przetwarzania informacji oraz programów narzędziowych, diagnostycznych zapewniając weryfikację i rozliczalność użytkowników wykonujących zadania, do których zostali uprawnieni. W szczególności rejestrowaniu podlegają:
   1) identyfikatory użytkowników,
   2) daty i czasy zarejestrowania i wyrejestrowania w systemie,
   3) identyfikator stacji roboczej lub terminala (nazwę komputera w systemie),
   4) nieudane próby logowania do systemu,
   5) błędy systemu i procedury obsługi tych błędów,
   6) zawieszenie i ponowne uruchomienie systemu,
   7) zmiany w plikach konfiguracyjnych i krytycznych zmiennych systemowych.
3. Rejestry są utrzymywane i przechowywane dla wszystkich krytycznych dla Urzędu systemów i aplikacji.
4. Systemy rejestrów są objęte standardową procedurą tworzenia kopii archiwalnych.
5. W celu wykrywania incydentów związanych z bezpieczeństwem ASI regularnie monitoruje zapisy dokonywane automatycznie przez systemy w rejestrach zdarzeń pod kątem właściwego wykorzystania systemu teleinformatycznego i zarządzania nim.
6. Systemy zapisu zdarzeń są zabezpieczone przed manipulacją i nieuprawnionymi zmianami.
7. Zabronione jest usuwanie, manipulacja lub nieuprawnione zmiany w zdarzeniach, rejestrach, logach dla wszystkich krytycznych i wspomagających dla Urzędu systemów i aplikacji przez administratorów danego aktywu/w danym aktywie.

§ 29. Synchronizacja zegarów

1. Odpowiednia dokładność i możliwość korelacji rejestrów zdarzeń, których zapisy mogą służyć jako dowody w postępowaniu w przypadku wykrycia naruszenia bezpieczeństwa jest zapewniona przez właściwe ustawienie zegarów urządzeń teleinformatycznych.
2. Do synchronizacji czasu wykorzystuje się protokół NTP (ang.: Network Time Protocol) - internetowy protokół synchronizacji czasu.
3. Źródłem synchronizacji jest zewnętrzny wzorzec czasu.
4. Stacje robocze synchronizują czas z kontrolerów domeny.